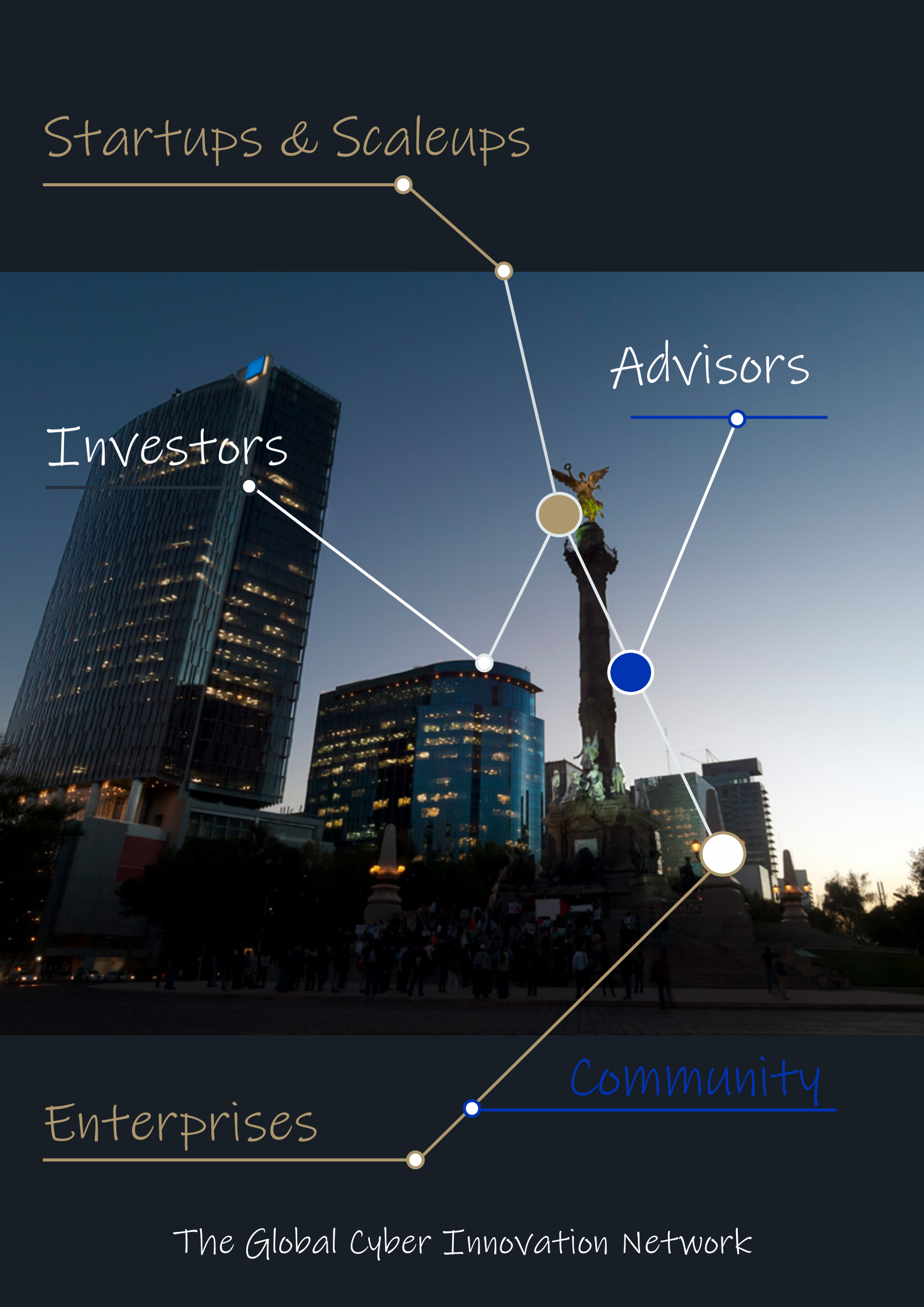
Cyber Startup Observatory®

LATAM

June 2022

The Global Cyber Innovation Network


Startups & Scaleups
Advisors
Investors
Community
Enterprises
The Global Cyber Innovation Network

Meet the Observatory Companies

...featured in this edition

Platinum

CYBER RANGES

AIRBUS CYBERSECURITY

senhasegura

STORMSHIELD

Gold

SEPIO

SafeBreach

ATEMPO preserving data ecosystems

Resecurity

STELLAR CYBER®

Fortanix®

Cyber Security Leaders

William Telles
CISO
Grupo Águia Branca

Avishai Avivi
CISO
SafeBreach

Alfredo Alva Lizárraga
Head of Information Security
Niubiz

The Global Cyber Innovation Network

Cyber Security Leaders

Dr. Almerindo Graziano
CEO
CYBER RANGES

Ygor Cezar
Head of IT
OEC

The Global Cyber Innovation Network

The purpose of the **Cyber Startup Observatory®** is to collaborate to build a safer society and to help solve important problems leveraging cyber security innovation. Find out more and tell us what matters to you by visiting us at:

cyberstartupobservatory.com

This publication has been prepared for general guidance on matters of interest only and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice.

No representation or warranty is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, Smartrev Analytics Consultants SLU, its members and employees do not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

In this document, **"Cyber Startup Observatory", "Cyber Security Observatory"** and **"Smartrev Cybersec"** refer to trademarks belonging to Smartrev Analytics Consultants SLU.

The information provided by the participating startups and companies belongs to them. They remain the sole and exclusive owner of any information provided to Smartev including without limitation, with respect to any intellectual property rights, copyrights and trademarks. Smartrev Analytics Consultants SLU have received explicit written permission to publish all the information included in this report.

Contents

12 Overview

14 In This Edition

17 The LATAM CyberSlide – Product

20 The Brazil CyberSlide – Product

22 The Mexico CyberSlide - Product

24 The LATAM CyberSlide Managed Security Services

26 Leadership: William Telles, CISO @ Grupo Águia Branca

30 Cyber Insurance – Why your company should consider it - senhasegura

33 Video Infographic - Key Actions to Limit an Adversary's Ability to Learn and Move Laterally

35 Leadership: Avishai Avivi, CISO @ SafeBreach

Contents

37 50 shades of ransomware: a retrospective on a year of cyberattacks - Stormshield

41 Video Infographic - The Incident Response Plan, Key Elements

43 Leadership: Alfredo Alva Lizárraga, Head of Information Security @ Niubiz

49 Cyber intelligence: how to anticipate the possible attack on behavioral analysis? – Stellar Cyber

52 Leadership: Dr. Almerindo Graziano, CEO @ CYBER RANGES

54 Seeing is Believing – But Can You Believe What You See? – Sepio

58 Leadership: Ygor Cezar, Head of IT @ OEC

63 Video Infographic - Zero Trust Architecture, Core Components

65 Key Observatory Components: The @CSOFinder

Contents

Pages 30 - 32

Cyber Insurance – Why your company should consider it - senhasegura

Pages 37 - 40

50 shades of ransomware: a retrospective on a year of cyberattacks - Stormshield

Contents

Pages 49 - 51

Cyber intelligence: how to anticipate the possible attack on behavioral analysis? – Stellar Cyber

Pages 54 - 57

Seeing is Believing – But Can You Believe What You See? – Sepio

Meet the Observatory Companies

...featured in this edition

Platinum

CYBER RANGES

AIRBUS CYBERSECURITY

senhasegura

STORMSHIELD

Gold

SEPIO

SafeBreach

ATEMPO preserving data ecosystems

Resecurity

STELLAR CYBER®

Fortanix®

Overview

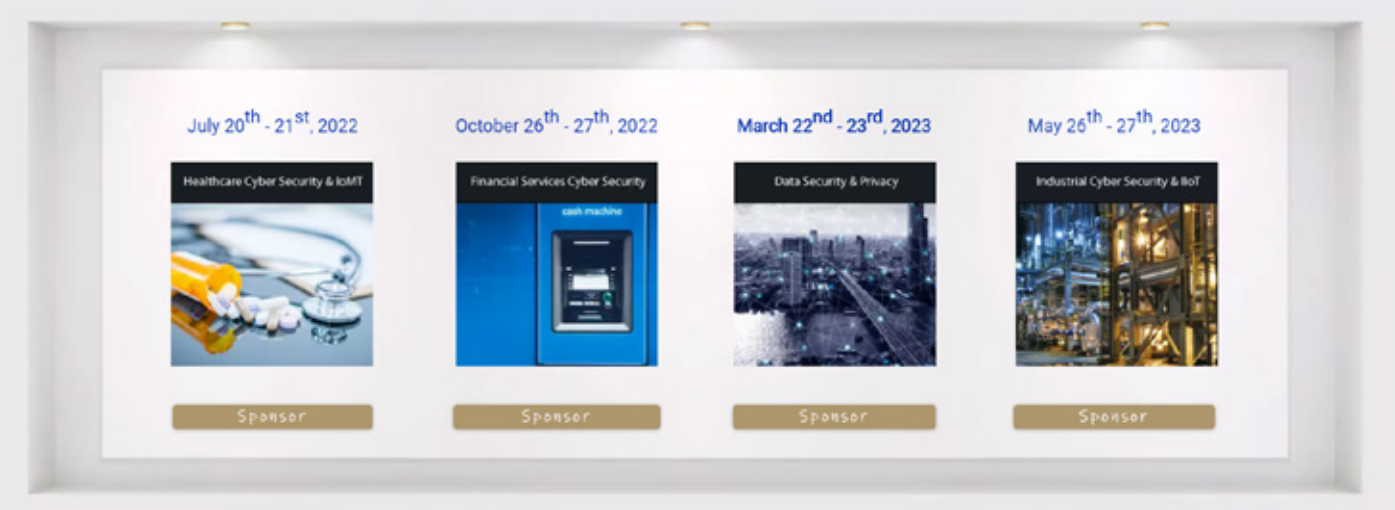
It is an honor to present the fourth edition of the **Cyber Startup Observatory LATAM.**

Since our first edition we have been able to see the high level of innovation in the region, particularly in markets such as **Mexico, Brazil, Colombia and Chile** - although there are also high-quality startups in the rest of the region.

The harsh years of the pandemic imposed significant barriers to innovation - in addition to the untold human cost. This severe event, however, accelerated digitization, generating great opportunities for innovative startups that saw the opportunities.

Ransomware attacks skyrocketed, even targeting critical infrastructure. Cyber security companies and entrepreneurs have played a key role in protecting our society.

On the front-line, defending businesses, public bodies and institutions and indeed, individual citizens, we find both established companies and burgeoning start up innovators, and we are proud and honored to be able to shine a light on some of the amazing work being put into practice by them in this Fourth Edition Observatory LATAM.



2022 will also see us build on the success of last year's Cyber Security Innovation Summits - our series of virtual events covering an extensive list of cyber security topics - and we are delighted to announce that this year we will offer two series of events:

- The Innovation Series (i-Series)
- The Bespoke Series

We are confident they will be of great interest and value to both CISOs and Cyber Security companies alike, and which will also support The Observatory in sharing and promoting its three key elements:

- Worldwide promotion of cybersecurity innovation
- Information sharing and collaboration across the industry
- Fostering leadership among cybersecurity practitioners

Putting together this Fourth Edition Observatory LATAM has provided us with an opportunity to connect with yet more companies in the industry and we are grateful to them all for sharing their vision and experience.

Together with our Regional Observatories covering North America, Europe, META and APAC, we now have in place a comprehensive program on a truly global scale.

In This Edition

One of the fundamental elements of the Observatory program is the way in which we have built up close relationships with some of the most highly-regarded Cyber Leaders in the industry. We believe this is crucial in order for us to present a trustworthy overview of the state of play within Cyber Security, regardless of the sector in which it is applied.

In this edition we are once again honored to share the views and insights of another fine selection of Cyber Leaders who have managed to spare us the time to share their thoughts on the crucial role they play within their organizations.

So we would like to extend our sincere thanks to:

Alfredo Alva Lizárraga, Head of Information Security @ Niubiz
Avishai Avivi, CISO @ SafeBreach
William Telles, CISO @ Grupo Águia Branca
Dr. Almerindo Graziano, CEO @ CYBER RANGES
Ygor Cezar, Head of IT @ OEC

The **Fourth Edition Cyber Startup Observatory LATAM** sees us publishing articles offering the insight, vision and solutions of top companies playing a major part in the cyber security landscape across the country.

We include an article looking at **Cyber Insurance – Why your company should consider it**. We also take a look at the **"50 shades of ransomware: a retrospective on a year of cyberattacks".** There is an article outlining covering **Cyber intelligence: how to anticipate the possible attack on behavioral analysis?**, and we also have a fascinating take on visibility **"Seeing is Believing – But Can You Believe What You See?".**

We hope that the material included in this **Fourth Edition Cyber Startup Observatory LATAM** will contribute to the goal of locking cyber security into our thinking, as we head into another year of challenges and opportunities.

It just remains for me to thank my team here at the Observatory Program - Co-editor, Maite Ortega, German Duarte, our CTO, Alvaro Vargas, our Research Manager, and Consulting Director, Alicia Peña for their infinite patience and support in the preparation of this publication.

Thanks, as ever, to Unsplash photo repository and its second to none photographers and creators (https://unsplash.com) for the inspirational pictures which have been used in this publication.

Jose Monteagudo
Editor-in-Chief

Jose Monteagudo
Editor-in-Chief
josem@smartrev-cybersec.com

Maite Ortega
Co-Editor
maiteo@smartrev-cybersec.com

Alvaro Vargas
Marketing Manager
alvaro.vargas@smartrev-cybersec.com

German Duarte
Platform Manager
german.duarte@smartrev-cybersec.com

Sections

This methodology is also applied to our web cyberstartupobservatory.com and will be consistent in future editions of the observatory.

The LATAM CyberSlide

Product

The CyberSlide - Product

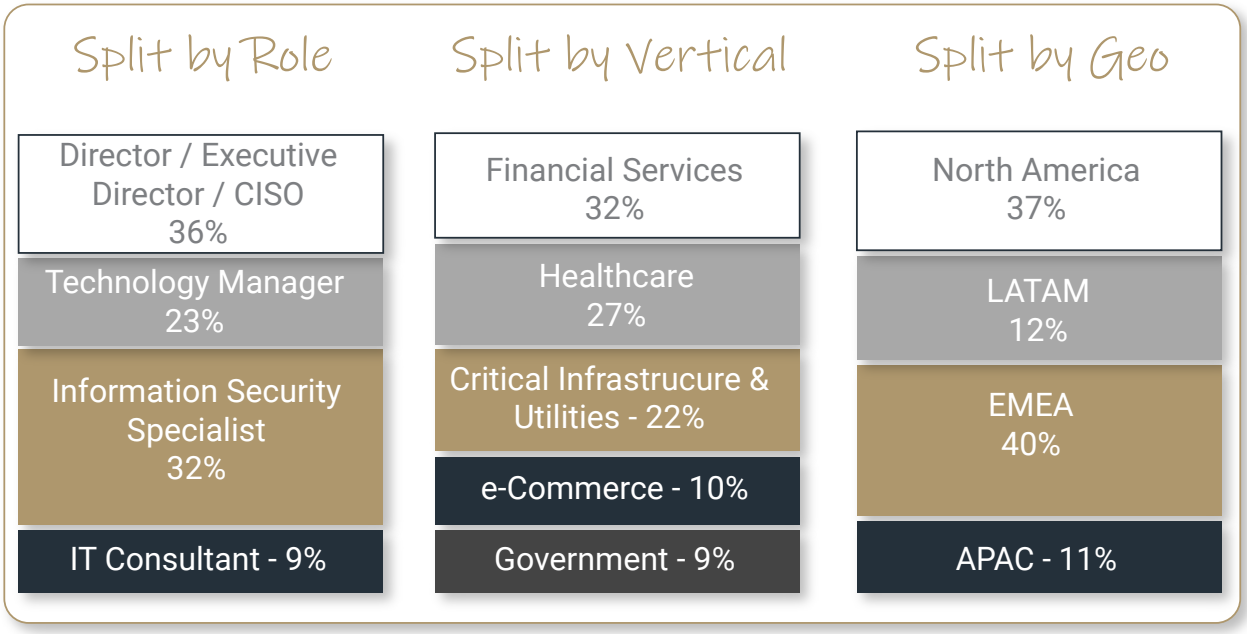
The CyberSlide is dedicated to supporting the extensive cybersecurity market active within the Cyberslide's country, but which has a truly global impact. Cybersecurity has a key part to play not only from the perspective of innovative startups looking to get a foothold in the industry, but also for those established companies who are already major players in the field. The solutions such companies provide form an integral part of our everyday security regime and highlight the fact that we cannot rest on our laurels in the fight against the bad guys.

The CyberSlide is part of a suite of solutions created by the Cybersecurity Observatory - most notably the @CSOFinder search engine - which aims to simplify the cybersecurity technology selection process and offer the best solution for any cybersecurity issue.

The @CSOFinder showcases the featured companies using a clear categorization that is standardized across the 100+ markets currently on our radar. As a result, a CISO from APAC, Europe, North America, LATAM - anywhere in the world, in fact - can identify companies more easily, helping them to navigate this ocean of complexity in which 1000s of new companies spring up every year.

Given the impossibility of including every single one of these companies on the CyberSlide, it's important to mention that all participating companies have been contacted individually in order to ensure the correct categorization process has been negotiated and agreed upon.

Furthermore, we are one hundred percent committed to keeping the CyberSlides updated, to promote them regularly, to educate the community and to provide the most effective support possible to these industry innovators and their mission.



A world-class

cyber security ecosystem

100+ Companies featured

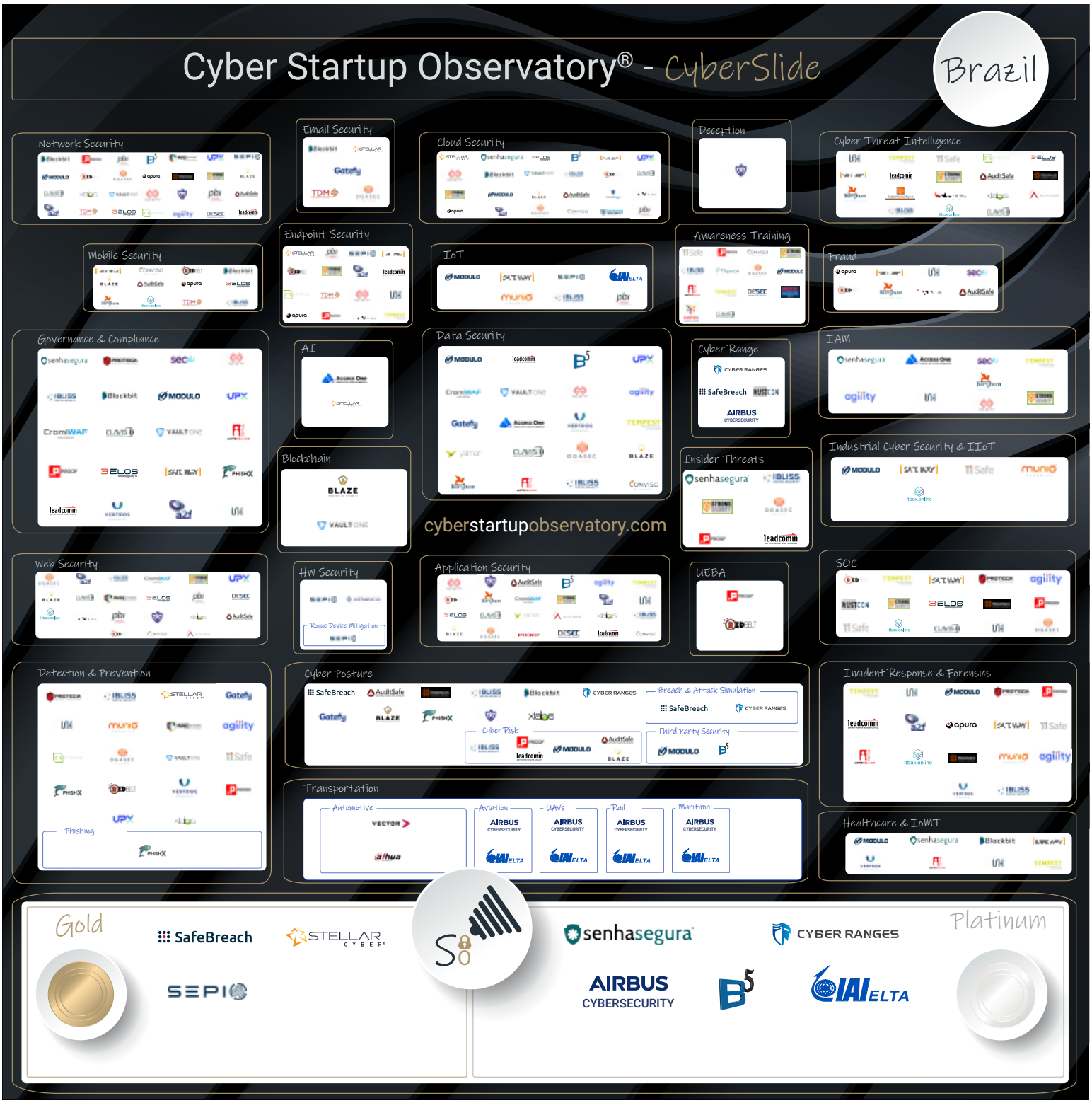
Resources

The Brazil CyberSlide

Product

A world-class

cyber security ecosystem



100+ Companies featured

Resources

The Mexico CyberSlide

Product

A world-class

cyber security ecosystem

100+ Companies featured

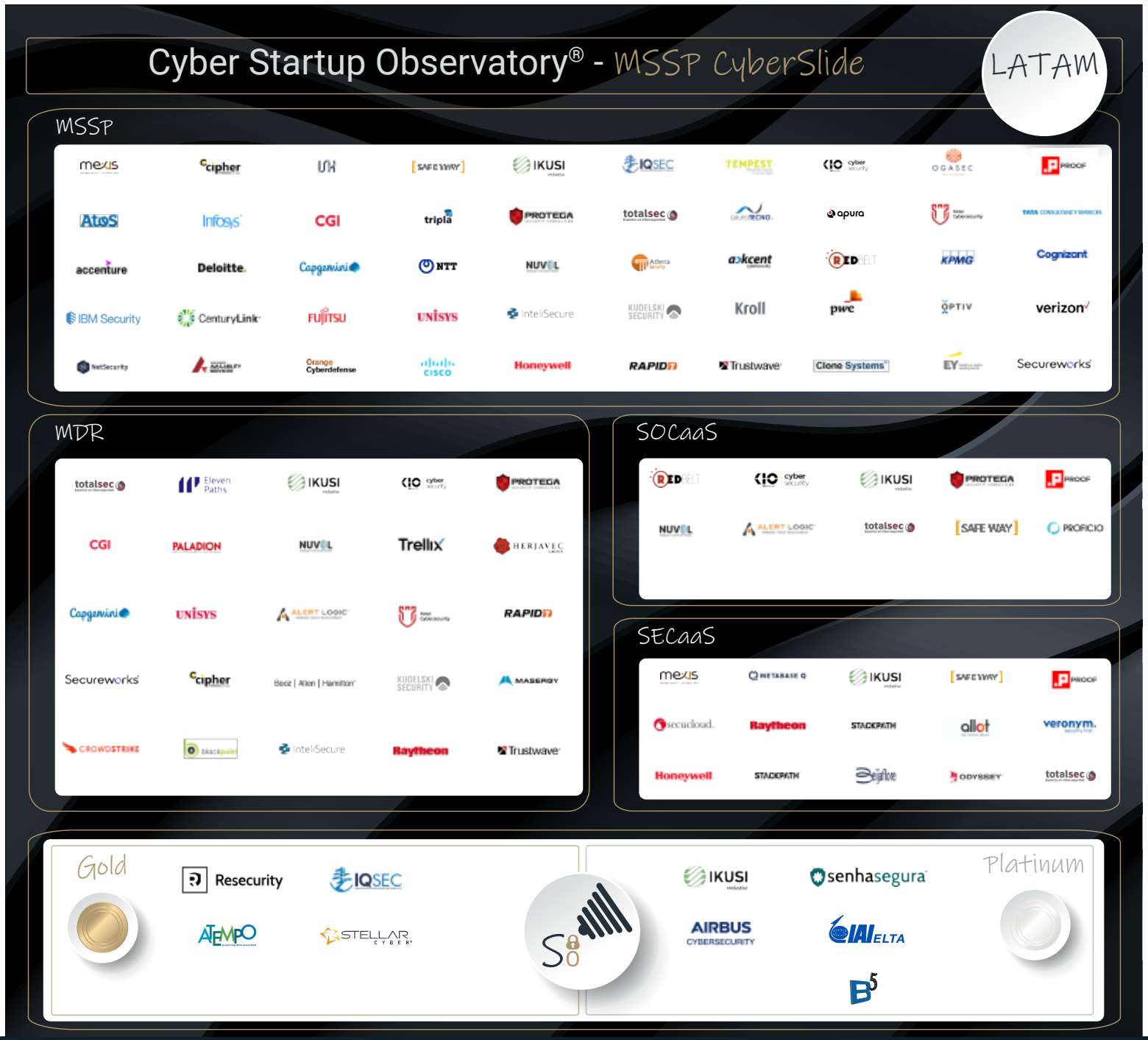
Resources

The LATAM CyberSlide

Managed Security Services (MSS)

A world-class

Cyber Security ecosystem



100+ Companies featured

MSSP, MDR, SOCaaS & SECaaS Providers

Leadership

William Telles

CISO @ Grupo Águia Branca

William Telles

CISO @ Grupo Águia Branca

It is a pleasure to have William Telles with us in this new edition of the LATAM Observatory.

Willia is currently the CISO of Águia Branca Group, one of the largest transportation and logistics conglomerates in Brazil.

In your opinion, what are the key considerations that organizations should factor while define their cyber strategy?

Without the slightest doubt, the first action should be the measurement and likely change in the culture of cybersecurity. If an employee is not aware of their role in the cyber resilience ecosystem, large investments in technologies and processes will be useless. What's more, culture change is a journey and not a one-off action. You don't change a culture with a course and certificate. To change culture, there needs to be regular and periodic actions that allow people to hear regularly about good cybersecurity practices, and put them into practice daily as well.

> "What's more, culture change is a journey and not a one-off action. You don't change a culture with a course and certificate."

How can a CISO ensure that staff get behind the idea of a cyber culture in teh company?

The CISO needs to be responsible for leading and managing actions to foster a cybernetic culture in the company. Other areas need to be involved, like the marketing area for example, but the responsibility for developing, implementing, monitoring and measuring the results of campaign effectiveness needs to be with the CISO.

A good practice to be adopted by the CISO is the creation of KPIs that allow measuring the level of commitment to cybersecurity of each department of the company, and thus develop complementary actions to raise the lower levels.

How can a company create a data privacy culture in the workplace?

A good starting point is understanding the risks that privacy laws bring in the face of non- compliance.

From there, it is important to understand what each department deals with personal data, and to put together a strategy to present the risks present in that department, and to implement a set of regular actions to mitigate these risks through the adoption of good cybersecurity habits.

How often do you think security drills and exercises should be employed in order to maintain the profile of cyber security within the company?

The frequency should be determined by the degree of risk the company is willing to take.

In a perfect world, this degree of risk should be close to zero and the frequency of training should be monthly, whether for training or basic exercises.

More elaborate exercises and training can have intervals between 3 and 6 months.

What are some of the barriers preventing organizations from implementing personal data and privacy protection initiatives?

Unfortunately, the short-sighted view of commercial speed at any price is the worst barrier to personal data and privacy protection initiatives. It is a fact that the commercial area needs to deliver faster and more solid results. But Commercial Directors need to be clear that unmitigated risks can paralyze the business, and when it comes to personal data privacy, this topic is also an excellent opportunity to show more value to the customer.

In a information technology environment where personnel are taking on increasingly complex responsabilities, what do you think is the role of the cyber security awareness program?

Priority, that's the watchword. Regardless of the responsibilities assumed by the information technology area, an effective cybersecurity awareness program should be at the top of the list of recurring actions.

Insight

senhasegura

Cyber Insurance – Why your company should consider it

senhasegura

Cyber Insurance – Why your company should consider it

Author: senhasegura

At a glance

- 2 minute read
- Cyber Insurance – Why your company should consider it
- Main factors that influence the growing demand of cyber insurance

Hiring insurance is nothing more than a risk management strategy. In this case, the organization transfers the responsibility in the event of an unexpected event to a third party (in this case, the insurance company). And with the increase in security incidents and data breaches, insurance companies have developed a new product to help organizations reduce the risk of cyberattacks: cyber insurance.

In this case, by hiring cyber-attack insurance, the organization transfers the obligations related to the costs they would have to pay in the event of a security incident to the insurance company. Typically, these costs are associated with recovering stolen data, paying ransomware ransoms, property damage, and even image recovery.

But what factors influence the growing demand of companies for cyber insurance?

The first of these is the increase in connected devices. With the development of technologies such as 5G, the Internet of Things, and Industry 4.0, the number of devices connected to the infrastructure has skyrocketed.

According to Zurich Insurance, the number of connected devices in 2020 has surpassed 50 billion, an increase of 19% compared to 2019. And this number is expected to grow even more in the next few years.

Moreover, the amount of data generated by these devices has increased exponentially. According to Ace Group, the volume of online data doubles every two years. And in times when data is the new oil, protecting an organization's data (in addition to the personal data of employees, partners, and suppliers) is not about just complying with security policies and personal data protection laws such as LGPD, GDPR, CCPA, and the Texas Privacy Act, it is about ensuring business continuity.

Another factor that influences the increase of cyber risks and contributes to an increase in the demand for cyber insurance is the migration to remote work, driven by the Covid-19 pandemic. Bring Your Own Device, shadow IT, and the use of insecure networks considerably increase the attack surface that can be exploited by malicious actors.

With this larger attack surface, the number of security incidents has also increased. A Checkpoint study has shown that the year 2021 broke records in terms of the number of cyberattacks. According to the study, there was a 50% increase in cyberattacks globally per week compared to 2020.

The costs of these cyber-attacks were also higher for organizations: according to the IBM Data Breach Investigation Report 2021, the cost of a data breach for organizations was $

4.24 million, a 10% increase compared to 2019. In addition, the costs associated with cybercrime are estimated to have reached $ 6 trillion in 2021.

By hiring cyber insurance, organizations can ensure the costs of a cyberattack are covered by the insurance company, including operational losses and incident recovery costs.

Moreover, insurance companies also offer full legal and security incident investigation support. In this way, the company can ensure that it is prepared if it falls victim to cyber attackers and that all efforts are made to recover its infrastructure affected by the security incident.

Resources

Video Infographic

Key Actions to Limit an Adversary's Ability to Learn and Move Laterally

Key Actions to Limit an Adversary's Ability to Learn and Move Laterally

Source: FBI, CISA, ACSC, NCSC - Joint CS Advisory

Available for download in Press Quality

Video Infographics

Cyber Startup Observatory - Community

Leadership

Avishai Avivi

CISO @ SafeBreach

VIDEO INTERVIEW

Why Are Continuous Security Controls Critical for CISOs Today?

Please Click on the Image below to watch the Interview...

Insight

STORMSHIELD

50 shades of ransomware: a retrospective on a year of cyberattacks

STORMSHIELD

50 shades of ransomware: a retrospective on a year of cyberattacks

Author: Sébastien Viou, cyberevangelist at Stormshield

At a glance

- 4 minute read
- 28 ransomware families
- Ransomware: an anatomy
- DDoS and data leakage, pressure tactics that go hand in hand with ransomware

STORMSHIELD

The ransomware business has (unfortunately) never been in better shape, and has diversified into a spectrum of shades that can be confusing to make sense of. At the FIC 2021 international cybersecurity forum, France's ANSSI agency reported that malware-related incidents were up by 255% in France. But just what are the realities and trends in the world of ransomware today? Are all companies under equal threat?

28 ransomware families

Also during the FIC 2021, the Judicial Division of the National Gendarmerie engaged in a small auditing exercise. It reported 28 active families of ransomware in France; meanwhile, the FBI identified over 100 in the United States.

Some families of ransomware have been notable for having reappeared over the last twelve months. For example, Babuk was used by the cybercriminal group of the same name in 2021 to infiltrate several large companies. Atom Silo and BlackMatter are other examples; and we recently discovered Blackbasta, which is actually a new name for an existing group. And last but not least, REvil (also known as Sodinokibi) and Ryuk made a big comeback in 2021. The former has been active since 2019, and has long been considered one of the most difficult to detect – as well as one of the most profitable for cybercriminals. Its source code is regularly updated in an attempt to defeat cyber-protection measures. Fortunately, it seems to have ground to a halt following the dismantling of the group by the Russian authorities.

Generally speaking, these malware programs continue to work in the same basic way. The two classic types of ransomware – Lockers, which block the operation of a computer; and Cryptos, which consist of encrypting data and selling a decryption key as a ransom payment – have not fundamentally changed. In other words, these are tools that we have already seen before. However, there has been innovation in methods of penetrating workstations and information systems. But how have these means of access – which are common to the different families of ransomware – evolved?

Ransomware: an anatomy

Unfortunately, there are many routes by which ransomware can enter. Not surprisingly, phishing is one of the main ones. By recovering credentials directly, cybercriminals can gain access to a VPN or email system. And it takes just one employee to fall into such a trap to put the entire company's information system at risk: and cybercriminals will have quickly made a point of moving laterally until they get their hands on the valuable administrator rights for the domain's directory. And beyond the obvious manager profiles, all employees of a company are in fact potential targets for cybercriminals.

But entry points can sometimes be more subtle (say, based on social engineering) – or more direct, via the exploitation of unpatched software vulnerabilities.

So the starting point for ransomware campaigns is often when a vulnerability in commonly-used software is discovered. The example of Microsoft PrintNightmare, or ProxyLogon – two vulnerabilities allowing remote code execution on Windows – are a perfect illustration of this. Given the rapid release of exploit kits on the darkweb, any organisation that has not applied the necessary patches will be an easy target.

This is an equation with two unknowns: there are X vulnerabilities, and Y ways to exploit them. On the one hand, according to the CESIN 2021 barometer, the "traditional" non-targeted "spray and pray" attacks are still the leading attack vector. But they are changing: although they are still delivered via major worldwide email campaigns that rely on a statistical approach, they are now much more sophisticated than was the case a few years ago.

We have moved on considerably from the standard phishing email that contained mistakes in almost every word. The quality is much better: for example, you can find realistic invoices in their appropriate context, addressed to accountants as if they were an email from a client. Since 2021, cybercriminals have even been reusing stolen email histories to re-initiate conversations, using the subjects and contents of old exchanges… naturally, with a contaminated file thrown in for good measure.

At the same time, small and medium-sized enterprises are coming in for twofold scrutiny from cybercriminals. Firstly, they are targets in their own right, as they are particularly sensitive to business interruptions. Secondly, they are still being used today as a staging point from which to attack their larger trading partners – the so-called "supply chain attack".

No one is safe from ransomware. And hackers whose aim is to convince an infected company to pay the ransom will resort to any means necessary...

DDoS and data leakage: pressure tactics that go hand in hand with ransomware

Although the official advice is not to pay ransoms, criminals obviously see things differently. And to tip the balance in their favour, they will devise and use additional pressure tactics. In 2018, patient data from around 20 Finnish psychotherapy centres was stolen. But when the company hit by the theft refused to pay the ransom to get the data back, the cybercriminals turned their attentions to... the patients themselves, threatening to make the data public. This is a new trend towards threats of data disclosure. It is a means of pressure that complements – or can sometimes now even replace – encryption as a way of forcing companies (and individuals) to pay ransoms. And the threat can also become a threat of encryption. In this innovative new process, cybercriminals demand a ransom... for not encrypting your data. Here, cybercriminals are seeking "gain without pain", relying solely on the fear they instil in their targets. There is no guarantee they will be able to carry out their threat… but would you take the risk?

In addition, cybercrime groups continued to become more professional in 2021, in ways that included their financial resources. In the case of some groups, this equates to several tens or even hundreds of millions of euros' worth of firepower. This is leading to another trend of conducting two types of attack simultaneously: a ransomware attack followed by a DDoS attack. By taking sites offline, cybercriminals increase the pressure on companies to pay. This principle of "double extortion" is estimated to have earned cybercriminal groups over $45 million in 2021, with Conti leading the way, followed by REvil and DarkSide.

So the era of ransomware is far from over. And it spares no one. From very small businesses to large international groups, the entire global economic fabric is a potential target. According to specialist insurer Cybercover, almost 60% of the victims of cyberattacks are small and medium-sized enterprises. And the latest Hiscox cyber-risk management report states that the average cost of a cyberattack is around €9,000 for companies with 50-250 employees in 2020 – although there are wide variations, with some companies suffering losses in excess of €280,000. The result in many cases is bankruptcy, when the cost becomes too high.

Fortunately, there are ways of protecting yourself. Companies that are aware of the issue and make structured security efforts with a continuous improvement approach will discourage attackers, who will then move on to other targets...

Resources

Video Infographic

The Incident Response Plan,

Key Elements

The Incident Response Plan

Key Elements

Available for download in Press Quality

Cyber Security Observatory - Video Infographics

1st Global Cybersecurity Observatory - Insight

Leadership

Alfredo Alva Lizárraga

Head of Information Security
@ Niubiz

Alfredo Alva Lizárraga

Head of Information Security @ Niubiz

We are glad to have with us Alfredo Alva Lizárraga in the fourth Edition of the Cyber Startup Observatory LATAM.

Alfredo is the Head of Information Security at Niubiz, an organization that provides the best technological solutions and simplifies the shopping experiences in business. Niubiz is headquartered in Peru.

How can a CISO enable business, maintain competitiveness and still provide reasonable security?

COVID-19 has undoubtedly been a turning point between a reactive position and a more proactive position in terms of security for all businesses that have had to adapt to a new context and in a very accelerated manner. New technologies that were not planned, in many cases, to adopt so early, such as adoption of cloud technologies, growth in e-commerce, digital channels, teleworking and others, which have been more than significant challenges in recent years.

Organizations and businesses have entered a stage where the release times of new products and services mean their value growth in the market. The problem is that many organizations have not integrated cybersecurity into the decision-making process and have been exposed to incidents with great impact on the business.

The key, I believe, is to be able to implement flexible and adaptive models to be able to respond effectively to new business objectives and at the same time try to be efficient when defining strategies for new scenarios. Constant and objective communication to management groups is very important, clear language and real examples are key to understanding risks and making decisions.

"Constant and objective communication to management groups is very important, clear language and real examples are key to understanding risks and making decisions."

How can security executives strengthen their relationship with the board if they feel it needs improvement?

I think there is no perfect formula, but something that helps a lot is what is happening in the world, and landing a little more in the sector where organizations move, remember that executives are more attentive to keep the business and generate more value, but what they must be clear is that a product without security, can bring events of economic loss or even damage to reputation. Executives are not concerned about the ability of how the organization can respond to a cybersecurity incident, for them many times it is still a technical issue.

The truth is that in recent years, time has been too tight for cybersecurity teams to improve the definition of their controls, and this allows attackers to take advantage of situations of agility to exploit vulnerabilities.

In addition, security is often seen as an investment with no return, as controls and processes need to be rethought year after year in order to combat the new and increasingly complex strategies of cybercriminals.

We must incorporate cybersecurity into the DNA of organizations starting at the highest level.

In your opinion, what are the key considerations that organizations should take into account when defining their cyber strategy?

First and foremost, strengthening cybersecurity culture and processes by design. While organizations continue to advance and improve their business processes through digitization, security, considered by design, is still a big pending issue.

Another important point is that, just as organizations are going to face large investments to incorporate new technologies that make them competitive, security must be present and take a relevant position in the decision-making processes.

Finally, look for competent professionals who have a collaborative vision, a great power of investigation and who do it with passion. During the pandemic there have been numerous offers of courses and training, but in reality less than half have had the good fortune to implement what they have learned in a company, and many of those who have taught them are theoretical. Having the vision to hunt for talent is a vital part of building versatile and multidisciplinary teams to face new challenges and to confront cybercriminals. There is no perfect profile for cybersecurity.

How have you seen the attackers' techniques change over the years?

They have completely changed their strategies, they have learned not just to attack for the sake of attacking and thus demonstrate that they can bypass the layers of control, but now they focus on the process, understand it, analyze it and know its weak points. They have been trained, like many security professionals, and many of them try to apply what they learn in small companies in their countries through trial and error.

That's why the global cybersecurity compliance environment is becoming increasingly complex, with new regulations at the country level and in large numbers to combat ongoing data exposures, and the growing number of financial frauds. A big challenge to face.

All of this always falls on the CISO, who finds his day-to-day work more complicated, with a lack of adequate resources, high workloads and very tight timelines to implement new control measures.

Moving forward with digital transformation, many companies will migrate to the cloud, what are the main risks to consider when doing so?

In recent years, there has been a significant increase in cloud adoption. As more enterprises see its benefits, such as cost savings, easy scalability and improved performance, they are moving away from traditional physical data centers and network infrastructure. The reality is that cloud migrations fail when companies neglect at least a few issues crucial to the process.

First they feel the need to migrate everything at once, and the larger truth is that migrating all your data to a cloud at once is an organizational and technological challenge.

It is mistakenly thought to be the fastest way, but it is usually the other way around. If you do it in stages you can have the ability to make gradual adjustments to get all your systems working the way you need them to.

On the other hand, cloud migration is a complex process that is not necessarily part of a comprehensive business case because it does not take into account some basic issues such as a market analysis and research, planning, data adjustments, infrastructure configuration, migration itself, optimization, training and maintenance.

Each migration project is unique, therefore, the total cost to the company must be carefully estimated and compared to the expected gains. In addition, security issues are neglected during these changes.

On-premises infrastructure gives you full control over your digital assets. With cloud infrastructure, the situation is different. That's why you should check how your cloud provider defines security services (shared responsibility models).

Finally, the lack of experience is a common point, the absence of knowledge in security controls at the protection level by not having suitable personnel, where security teams, security architects and experienced cloud environment experts are mixed.

How important is the exchange of information within the industry to keep abreast of new threats and best practices in cybersecurity?

Very important to be able to take the necessary actions to contain any event that is happening in the environment. Intelligence sharing between trusts should be an essential feature, but today in reality it is one of their most important shared challenges.

No single stakeholder can sustainably identify and address all cyber threats in the rapidly changing digital landscape. We know that there are very small groups of professionals where proactive sharing of information on attacks and defensive mitigations is done very informally, it is more out of friendship than responsibility.

We need to try to have greater cybersecurity resilience among organizations and help drive collective action against cybercriminals through deeper partnerships between the private sector and government agencies. We all want the same thing, to prevent incidents that can affect not only a company but even a country.

Insight

STELLAR CYBER

Cyber Intelligence: how to anticipate the possible attack on Behavioral Analysis?

STELLAR CYBER®

Cyber Intelligence: how to anticipate the possible attack on Behavioral Analysis?

Author: José Ramírez, Sales Director at Stellar Cyber

At a glance

- 2 minute read
- Cyber intelligence and the possible attacks on behavioral analysis
- Cyber intelligence is a sophisticated tool that is applied to cyber security
- Solutions with User and Entity Behavior Analytics (UEBA)

We commonly hear about cyber security solutions and innovation for data protection in companies and users. This often has a strong focus on protecting information from external cybercriminals who may compromise the privacy of organizations with any of the existing threats, such as phishing, malware, blackmail programs or cyberbullying.

But what happens when the threat is internal and IT managers cannot detect this so easily?

Today, based on the growing threats in organizations across all industries, it is important to raise awareness of new, little-known approaches to cyber security and data privacy. This represents a substantial change in the way IT decision-makers think, because integrating efficient and intelligent cyber security models increases business opportunities, creates value in the marketplace and builds customer trust in the brand.

In a large number of industries, over the past few years we have experienced a hybrid world. Data and new technologies have become a vital ally for management areas, a trend in organizations should be the incorporation of innovative technologies to process the huge amount of information generated constantly, which with the use of Machine Learning (ML), makes them able to intelligently manage data and cope with changing scenarios and multiple risks.

The integration of Artificial Intelligence to these tools gives them the ability to deal with digital crimes by learning and automatically identifying behavioral patterns, which allows detecting possible anomalies in an agile, accurate and absolutely preventive way. This technology becomes more relevant when applied in systems that must process huge amounts of data per second, where vulnerability is higher, and analysis is not intuitive at all.

For this, it is important to see security from the data, analyzing all the resources that are generated from the different interaction channels that fall into the different security layers. All this type of information is vital to identify patterns of behavior that may represent risks for companies and collaborators through the creation of information cross-referencing.

The digital footprint generated by users who interact with the organization's resources on a constant basis must be monitored strategically to detect unusual or undesirable patterns of behavior, which can often be caused by employees, former employees or cybercriminals. The technology that employs this type of behavioral data analysis is often referred to as "Cyber Intelligence".

Cyber intelligence is a sophisticated tool that is applied to cyber security.

It is a discipline that anticipates and analyzes human behavior through data. It differs from cyber security, since cyber intelligence is a reactive activity, which takes action before any attack for the protection of data, systems, networks or more, without leaving aside that this security depends largely on the technology, as well as the training and commitment of the collaborator who uses it.

Solutions with User and Entity Behavior Analytics perform a historical analysis of data logs, as well as network and authentication logs that have been collected and stored in the management of records and computer systems, with the objective of identifying patterns in data traffic caused by external and internal user behaviors, which in many cases can be malicious.

Its Machine Learning (ML) algorithm enables systems with User and Entity Behavior Analytics to reduce false positives and provide more accurate actionable risk intelligence to cybersecurity teams. This technology has been created to use ML to detect all types of anomalies that pose a threat. Some organizations even implement these methodologies with business intelligence technologies, to analyze in detail the information collected as input for decision making for business strategy.

Leadership

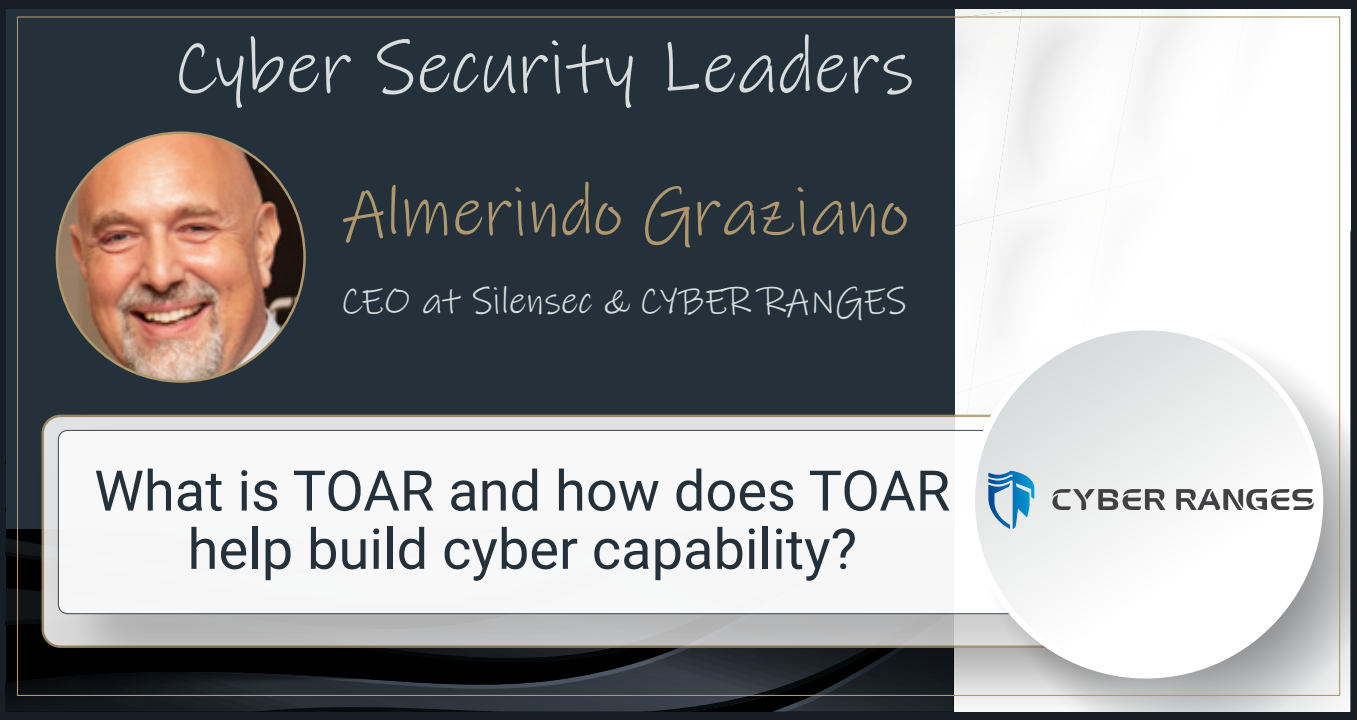
Dr. Almerindo Graziano

CEO @ CYBER RANGES

VIDEO INTERVIEW

What is TOAR and How Does TOAR Help Build Cyber Capability?

Please Click on the Image below to watch the Interview...



Insight

SEPIO

Seeing is Believing – But Can You Believe What You See?

Seeing is Believing – But Can You Believe What You See?

Author: Jessica Amado, Head of Cyber Research at Sepio

At a glance

- 3 minute read
- Seeing is Believing
- The root cause
- Unlimited access
- Taking advantage
- Seeing the unseen

Cybersecurity is a global topic, one that pertains to all countries and industries. While digital advancements differ among regions, the LATAM region is noticeably increasing its cybersecurity efforts – which comes at an appropriate time as attacks here are becoming more frequent.

However, effective cybersecurity relies on the complete understanding of one's environment: knowing what you have, the risks you face and, subsequently, which tools and policies to implement to stay protected. Yet, a lack of Layer 1 visibility limits an enterprise's understanding of its environment hardware information is missing. In turn, the efficacy of cybersecurity is limited, and the enterprise, unknowingly, remains exposed.

The root cause

Asset visibility and asset management are two well-covered topics that enterprises know serve as the foundation to cybersecurity. Cybersecurity strategies will always include investing in various asset visibility and management solutions. Through visibility enterprises create an asset inventory comprised of information about an asset's characteristics. It is such information that asset management tools rely on to enforce security policies. The process is similar to that of clubs and bouncers (bear with me on this analogy). Bouncers know the age restriction at the club and thus rely on ID cards to determine whether a person is allowed inside. But, sometimes, bouncers can gauge a person's age by appearance, giving way to the possibility that an underaged guest gets let in purely because they look above the age limit.

While the guest did not purposely mislead the security guard, forgoing an ID check meant information about the individual that would have influenced the security guard's decision did not get provided.

Going back to cybersecurity, misinformation about a device comes from a lack of complete asset visibility. Existing security tools, such as NAC, IDS, IoT Network Security and more, fail to cover Layer 1, resulting in a blind spot on the hardware level that leaves the asset inventory incomplete. Hence, with limited asset information, the efficacy of asset management tools - which rely on the asset inventory - is, too, limited. So, despite efforts to limit the enterprise's risk posture, the significant gap in visibility (and, thus, critical information) curbs the effectiveness of such efforts. Of course, however, the enterprise thinks its assets get adequately managed, unaware that it remains exposed – a risk in and of itself.

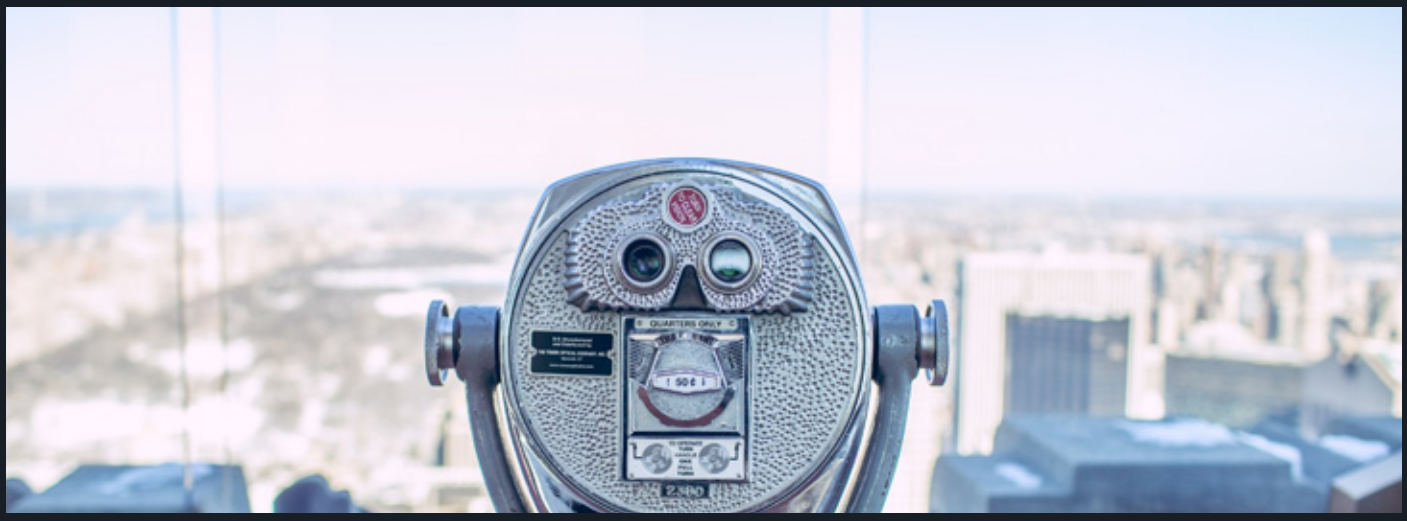
Unlimited access

In today's world, asset visibility and asset management are as critical as ever. The number of devices in use is growing rapidly, which means there is greater vendor diversity and, in turn, increased supply chain risks. Further, with the global boom in Work from Home and BYOD trends following the COVID pandemic, there are now a large number of unmanaged devices with access to company resources. In an employee's effort to be economical (not everyone can afford to kit out their home office with branded products), such devices may come from untrustworthy vendors who sacrifice security measures to lower production costs.

Thus, with the proliferation of network-connected assets (many of which operate remotely), ensuring a device's integrity is becoming an increasingly important task; but one that is not possible without complete asset visibility. The Layer 1 blind spot opens the door for unauthorized devices to bypass security policies simply because they have not been correctly identified.

Taking advantage

More worrisome are the threat of rogue devices – hardware attack tools designed to exploit the Layer 1 visibility gap. Malicious actors, in their quest to discover more sophisticated attack methods, have found that exploiting the Layer 1 blind spot provides nearly unlimited access to their target while raising no security alarms. Spoofed peripherals impersonate legitimate HIDs through Layer 1 manipulation, thereby getting authorized by security tools. Referring back to the security guard analogy, spoofed peripherals are the equivalent to (good) fake IDs. While the guest's ID does get checked, the bouncer gets fed false information about the individual's age; as IDs are the method of identification, the underaged attendee gets let inside.



Network implants are another type of rogue device, yet these tools go entirely undetected as they operate on Layer 1. Instead of a fake ID, think of network implants as a backdoor without the barrier of a security guard. A person underaged need not even go through the hassle of falsifying their age as the bouncer is unaware of their presence.

Whether manipulating or hiding their identity, rogue devices evade security measures as asset management tools get fed inaccurate information. As such, the covert nature of these devices allows attackers to move laterally across the network and execute harmful attacks (from espionage and data theft to DDoS and ransomware) without raising security concerns.

Seeing the unseen

Sepio's Hardware Access Control (HAC-1) solution deals with the root cause of the problem – asset visibility. HAC-1 provides complete visibility and continuous monitoring of all IT/OT/IoT/IoMT hardware assets, managed or unmanaged, through Layer 1 visibility. In doing so, HAC-1 completes the asset inventory, ensuring it is accurate and maintained in real-time. Such information enhances policy enforcement and hardware access control by verifying that only authorized devices are granted access, thus offering a Zero Trust Hardware Access approach.

HAC-1 also provides a Rogue Device Mitigation (RDM) feature that handles unwanted, hidden and spoofed devices. By instantly detecting the presence of such devices through its Layer 1 visibility, HAC-1 triggers a mitigation process that blocks the device through third-party integrations, preventing potentially disastrous attacks.

Leadership

Ygor Cezar

Head of IT@ OEC

Ygor Cezar

Head of IT @ OEC

I'm the Head of IT at OEC, the largest engineering and construction company in Brazil. I have nearly 30 years of experience in IT, first as a developer and later in leadership roles in the areas of development, integration, infrastructure, and operations. My experience spans IT departments of Utilities, E&C, Sugar & Ethanol and Real Estate companies. I have a bachelor's degree in Computer Science from UFBa and an MBA in Management from FGV.

Should we be focusing on technological innovation or shift to a more people-centered approach for cyber risk mitigation?

I believe the key is to achieve a balanced approach. As the threat landscape is always evolving, it's impossible to keep up with all the technological tools needed to mitigate all risks without a proper security awareness program, the user is the last barrier.

If you have a user base properly trained to identify and report suspicious behavior and attack vectors, you can make up for the lack of state-of-the-art tools. At the same time, it's not possible to survive without leading technologies, such as zero trust, to ward off attackers, especially in the current working from home / BYOD scenario brought on by COVID.

How do you convey the importance of cyber resilience to the board as a way of mitigating risk, while reducing expectations of a 'silver bullet' solution?

The board is much more aware of the importance of information security these days than ever before, particularly after the latest ransomware attacks.

> "The board is much more aware of the importance of information security these days than ever before."

So, they already have this awareness that there is not only one solution. In fact, the challenge is that there are too many solutions and not enough budget to cover them all... Our dialogue is how to proper measure current risk and balance investments and initiatives to mitigate it.

In an information technology environment where personnel are taking on increasingly complex responsibilities, what do you think is the role of the cyber security awareness program?

The security awareness program is critical to ensuring as much as possible that the last barrier (the user) is prepared to identify and report attacks, and the key is how to balance an up-to-date training program on the most common attack vectors, and also that raise awareness of computer habits outside the company, as most of the time, the user will be out of the office these days, at home, and safe behavior will help not only the company but as well at the personal life.

Your business is only strong as your weakest partner. Can you trust that your partners are keeping your data safe from attackers and how ca we manage third-party risk?

A combined approach of information security due diligence at the bidding/ contracting stage, followed by specific contractual clauses and ongoing monitoring throughout the contract proved to be a successful recipe for us.

Current data privacy regulations have helped all companies strengthen their security information programs and controls, and in my opinion, one of the areas that benefited most was third-party management.

In fact, our own customers also require us to maintain and ensure the same controls, so the entire industry is evolving.

How do you prioritize what risk is acceptable or not in a highly innovative business environment?

We have this dilemma every time we must evaluate a new startup found by end users. As a 'new' company, startups often do not cover all corporate information security requirements. First, we map out what kind of data will be shared, asking questions like if it is PII or if it will be integrated and how it will integrate with a legacy system and what is the coverage of the solution (whole company or just one branch/department).

We then conduct a security assessment of the solution and share our recommendation with the business users. We tend to be more flexible when we're only in the proof-of-concept stage because it's important to validate the solution. It doesn't matter that a solution is bulletproof regarding information security, but the UI/UX does not meet the expectations of business users...

If the solution is validated, we work together with the startup to have a vision of their roadmap regarding the problems we may have found and we reflect this in the final contract. The CIO/CISO's ultimate role is how to properly balance enterprise security without killing innovation and business needs.

In the doomsday scenario of a data breach, how can this be effectively communicated to external customers, shareholders and other interested parties?

First, being transparent to all stakeholders, the truth is always the best policy. So, have a clear and tested communication procedure within your incident response policy, with all stakeholders mapped and updated, a well-defined channel with federal authorities and cybercrime sites, and with a constant flow of information to all parts.

We've seen this as one of the key points in most cyber insurance offerings so far. And it's always a good lesson to talk to fellow CISOs/CIOs at companies that have successfully resolved a data breach.

Closing Statement

As the entire industry is discovering, it is no longer a question of IF you will be violated, but WHEN you will be violated. As important as rapid detection is the ability and speed of breach recovery.

And, at the same time, balancing risk, innovation, budget, tools, users' needs and awareness in this dynamic scenario we live in today.

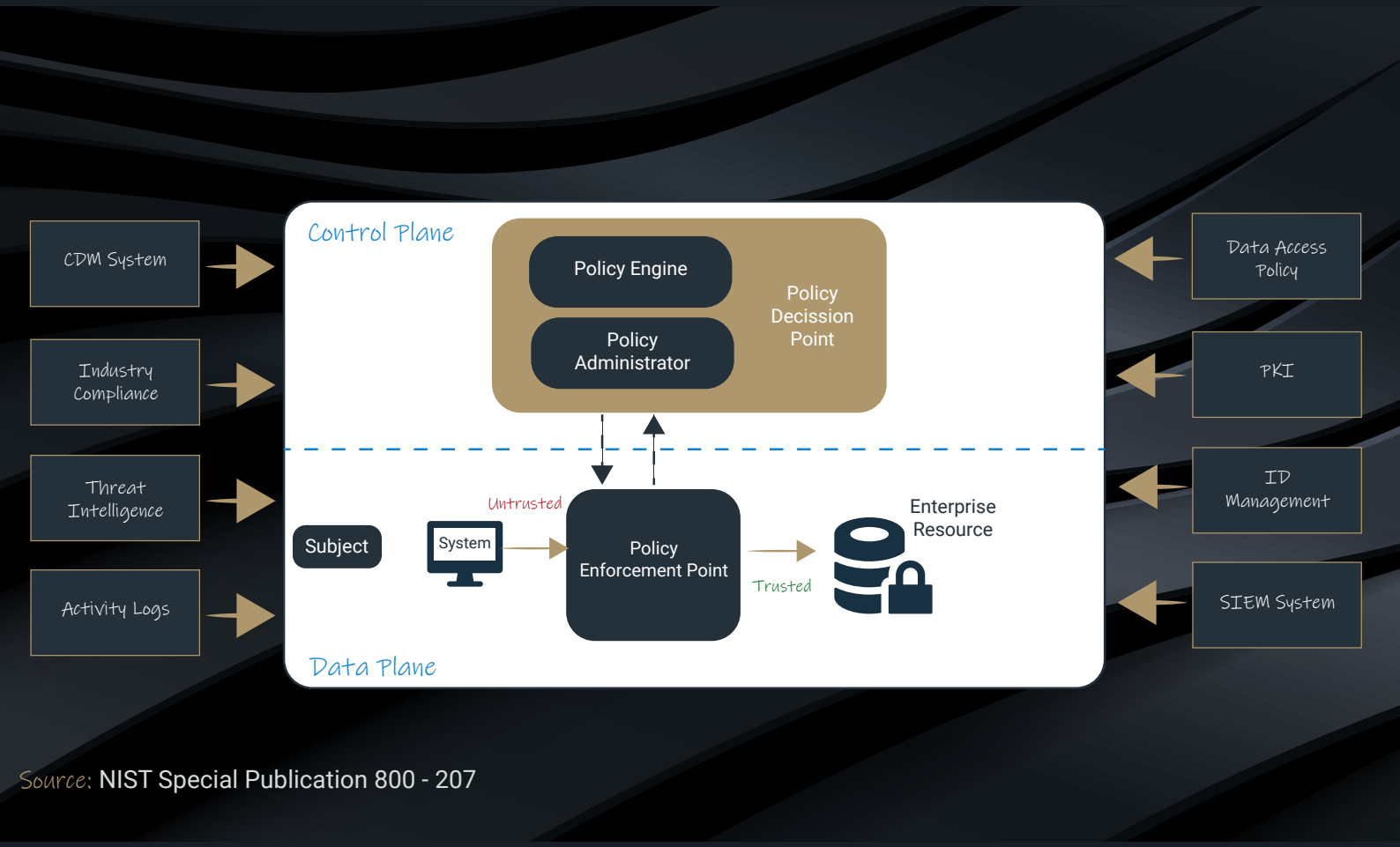
Resources

Video Infographic

Zero Trust Architecture, Core Components

Zero Trust Architecture

Core Components



Source: NIST Special Publication 800 - 207

Available for download in Press Quality

Video Infographics

Cyber Startup Observatory - Community

@CSOfinder

Our Global Search Engine for Cyber Security Companies

How It Works

Visit... @CSOFinder

Airbus Cybersecurity

European specialist in cyber security

AIRBUS
CYBERSECURITY

01

AIRBUS CYBERSECURITY

Company Description

Airbus CyberSecurity is a European specialist in cyber security. Our mission is to protect governments, militaries, critical national infrastructure (CNI) and enterprise from cyber threats, in full compliance with the cyber protection measures required by national institutions.

We are a fully owned subsidiary of Airbus Defence and Space, with over 900 cyber professionals based across offices in Europe, including Security Operations Centres (SOCs) in France, Germany, the UK and Spain. Our main offices are located in Paris, Munich and Newport; however we also have several other offices in our home countries. Additionally, our organisation includes Stormshield, a France-based subsidiary which offers security products to enterprise and government clients.

With over 30 years of experience providing reliable cyber security products and services, we have become one of the most advanced sovereign cyber security players in Europe. Having protected Airbus Defence and Space's complex systems and networks with our SOCs for years, we have leveraged our Airbus DNA to develop products and services for customers facing similar challenges as us, based on state-of-the-art trusted technologies.

We provide a global cyber defence approach that dynamically protects, detects and responds to cyber threats with a portfolio that includes managed security services, design and integration solutions, industrial control system offerings, encryption, key management and consultancy services.

02

Company Information

Company Name: Airbus
Founded: 2011-1
Employees: 500 up to 1000
Web: airbus-cyber-security.com
Headquarters: France
Other Offices: Germany, UK, Spain

Key Target Verticals:

- CNI (in France, Opérateurs d'Importance Vitale)
- Transport
- Manufacturing
- Defence
- Public institutions

03

AIRBUS CYBERSECURITY

The Product

Product Category: Cyber Range, Detection & Prevention; SOC

Product Stage: Released

Product Names and Brief Description:

- Cyber Range: Training and simulation platform

Services Provided:

- Cyber threat intelligence
- Network security
- Cyber resillience

04

Product in detail: CyberRange

The Airbus CyberSecurity CyberRange is an advanced simulation solution that allows customers to easily model IT/OT systems composed of tens or hundreds of machines and to simulate realistic scenarios including real cyber attacks.

It is used by administrators, integrators, testers, trainers and more to design virtualised or hybrid networks, emulate unit activities such as communications between two machines or to launch complex scenarios reproducing a realistic activity (file exchange, email, web traffic and potentially real cyber attacks).

The main functionalities of our CyberRange are:

- Modelling of real or representative systems
- Simplified construction from the graphical interface (drag-and-drop of machines)
- Management of multiple and isolated workspaces
- Collaborative modelling and integration work
- Integration of equipment or real systems
- Live traffic generator
- Scenario engine
- Import and/or export capacity of machines or topologies
- Access to the screen offset or command line at each machine
- Management of the virtual machine park

The CyberRange is available in a mobile box, in a bay or accessible from our cloud.

AIRBUS CYBERSECURITY

How does it work?

The CyberRange is a unified technical platform on which teams can work together or share elements–such as machine models or scenarios. In order to meet the constraints of a complex environment, the platform is open to interface with external equipment such as a physical industrial control system, a hardware traffic generator or a real physical or virtual system.

There are endless use cases for the highly realistic environment recreated on our CyberRange:

Pre-production tests:

- Easy access to an integration platform
- Collaborative work in isolated or shared environments
- Testing new safety equipment and procedures in a realistic environment

Operational qualification:

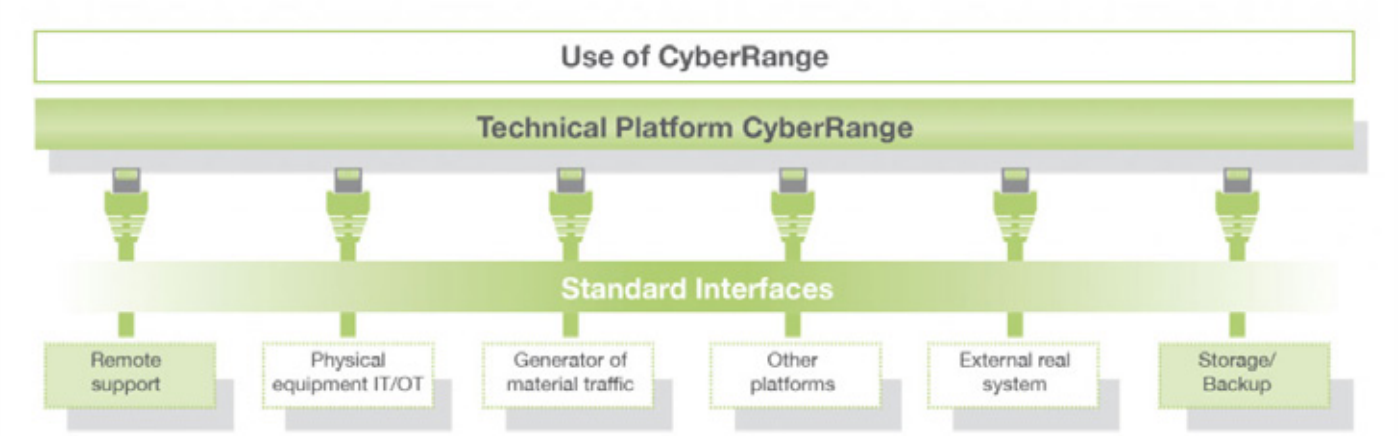
- Assessment of the impact of new equipment on a system
- Study of rule integration or the implementation of new procedures
- Analysis of cyber attack behaviour on its infrastructure without taking any risks

Training

- Awareness training for all staff and training on cyber security best practices
- Development of skills of cyber teams or knowledge retention to face new threats

Exercices

- Training of teams as part of operational exercises close to their daily environment
- Evaluation of the effectiveness of its security system as part of a cyber crisis management



Key Benefits

06

AIRBUS CYBERSECURITY

- **Realistic Simulations:** Immersion in complete IT/OT systems and animation with a complex scenario framework
- **Capacity:** Possibility to create complex systems composed of tens or hundreds of VMs or containers
- **Productivity:** Save time on configuration and integration to focus your business objectives
- **Agility:** Work alone or in a team in the same workspace or in parallel in different spaces
- **Safety:** Perform operations in an environment isolated from production systems
- **Scalability:** Possibility to complete the hardware configuration to increase the capacity

Unique Differentiators

- Easy environment to simulate highly complex networks with up to hundreds of virtual machines and thousands of dockers
- Perfect tool to train professionals at any level and improve skills of cyber experts
- Range of pre-defined cyber attacks
- Available both as a mobile box or through an online access
- Reliable customer service from an established cyber supplier

Future Functionality

- New scenarios integrated by default
- Various training packages available

AIRBUS
CYBERSECURITY

Infographic

Cyber Range

Main Functionalities

Stormshield

A European Leader in Digital Infrastructure Security

STORMSHIELD

01

Company Description

STORMSHIELD

A European leader in digital infrastructure security, Stormshield offers smart, connected solutions in order to anticipate attacks and protect digital infrastructures. Stormshield offers innovative end-to-end security solutions to protect networks, workstations and data.

02

Company Information

Company Name: Stormshield

Founded: 01/16

Employees: 300+

Web: www.stormshield.com

Headquarters: Issy les Moulineaux

Other Offices: Lyon, Villeneuve d'Ascq, Toulouse, Munich, Madrid, Milan, Dubai, Warsaw

Key Target Verticals: Industry, Energy, Transportation, Manufactoring, Healthcare, Education, Administration, Defence, CNI

03

The Product

Product Category: Network security, (Cloud Security), Endpoint Security, ICS/SCADA, Information Privacy (Compliance and Data Leakage Prevention)

Product Stage: Released

Product Names and Brief Description:

- Stormshield Network Security (Network protection/Firewall/ UTM/Industrial cybersecurity)
- Stormshield Endpoint Security (workstations protection)
- Stormshield Data Security (data confidentiality and privacy)

Services Provided:

- Threat Intelligence, Training, Support

Customer Footprint

Markets with Customers:

- EMEA Market (France, Germany, Italy, Spain, Benelux, Poland, Hungaria, UK, Switzerlands, Nordics, Saudi Arabia, UAE, Jordania, ...),
- APAC Market (Thailand, Vietnam, Malaysia, Singapour, Taiwan,...)

Relevant Public Success Stories per Key Target Vertical:

- Université de Cergy Pontoise
- Rossman
- Port Boulogne Calais
- More References Available Upon Request

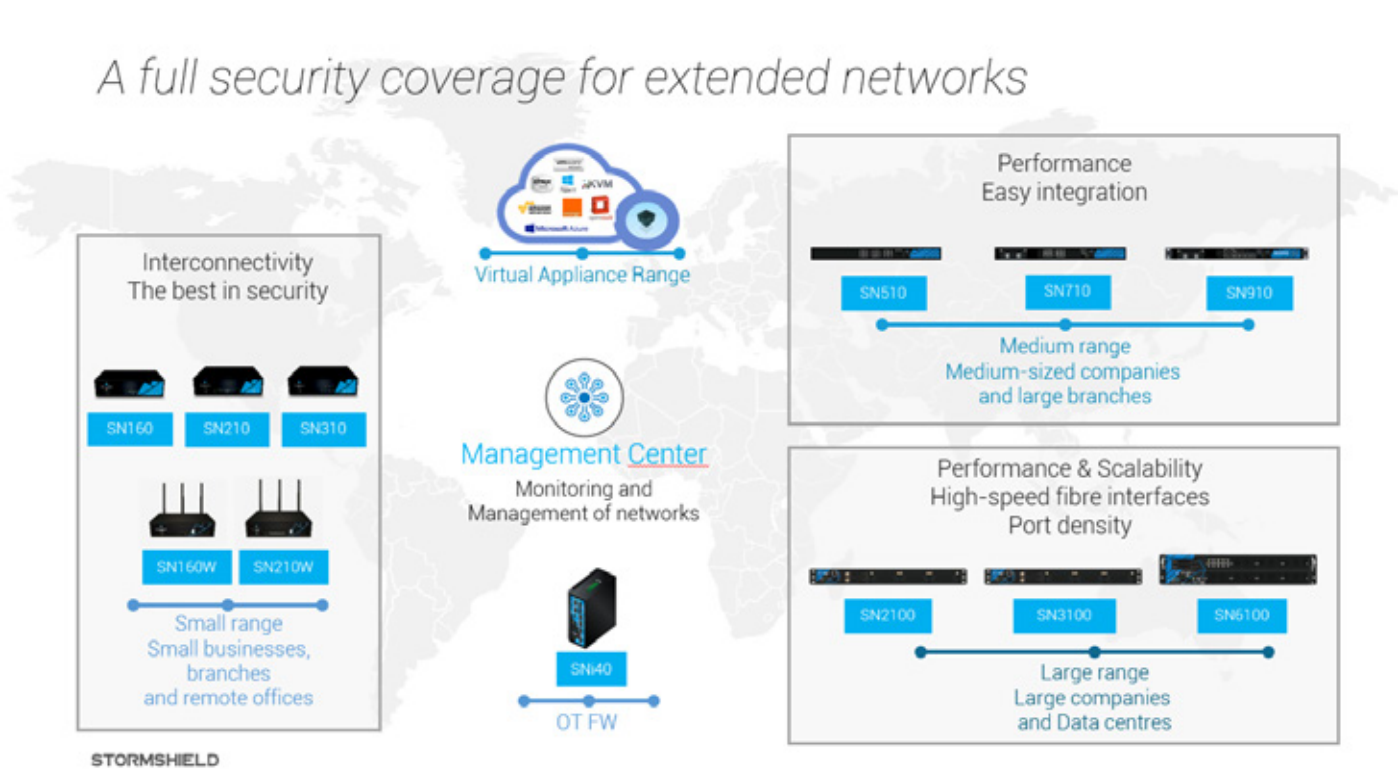
STORMSHIELD

Product in detail

The Stormshield Network Security (SNS) range is designed to protect IT & OT infrastructure against all types of threats transparently for users and administrators. These Unified Threat Management Solutions and Next Generation Firewalls combine all network security functions in a single hardware device or virtual appliance.

How does it work?

- **SNS appliances are available in different form-factors** (physical, ruggedized, virtual) in order to provide extended protection of hybrid environments (IT/OT/Cloud).
- **SNS appliances offer multi-layer traffic analysis and control based on Security Policy Management and Filtering up to layer 7**, Host and IP Reputation, IPSec/SSL VPN, Intrusion Prevention, Malware Prevention, Web and Email Control, Sandboxing, Security Reporting,...
- **SNS appliances can be managed in different ways:** embedded web interface, centralized management console, CLI, or orchestrated using an open API.



05

Key Benefits

STORMSHIELD

Ensure that business activities will remain uninterrupted

Our solutions include all of the protection technology needed to hold out against even the most sophisticated attacks.

Protect the internet use

Monitor internet usage, manage threats from the wild and control the impact on your business applications.

Connect employees and remote offices

Employees have secure access to the company's resources, no matter where they are and what device they're using.

Meet compliance requirements

Ensure your compliance with access control standards, regulations, and norms (PCI-DSS, ISO 27001, NIS, GDPR, LPM, etc.).

Unique Differentiators

Unrivaled Trust

The highest-level of European certifications to ensure integrity and transparency

Global Protection for Converged IT/OT Networks

A unique platform to inspect and control IT and Industrial-related traffic

Performance

An optimized system to ensure maximum performance when security engines are activated.

STORMSHIELD

Product in detail

The Stormshield Data Security (SDS) ensures the confidentiality of sensitive data and integrates transparently into usual communication tools so that business teams can create secure collaborative environments, whatever the media (email, USB keys, etc.), terminals (workstation, mobile) or applications (collaborative, intranet, collaborative cloud platforms, etc.).

How does it work?

- **Encryption everywhere:** Encryption is performed end-to-end and is exclusively controlled by the company. The file comes with its own security and can be shared with total peace of mind on various Cloud platforms or within the company as it is an agnostic solution. This means that the encrypted file remains accessible regardless of where it is stored.
- **User-oriented:** The user is central to data security. They can decide who has permission to access their information and can create workspaces in which we collaborate securely.
- **The keys belong to the company:** Data protection management is completely independent of its storage. Thus, the system administrator manages solutions and storage while sensitive data can only be accessed by authorised users. Furthermore, where outsourced storage such as the Cloud is concerned, the company is still the owner of the protection keys.

Key Benefits

- **Comprehensive protection suite:** Stormshield Data Enterprise ensures the confidentiality of all data, from local file to email protection and including a company's internal collaborative spaces. This solution is easily integrated whether or not it has an Active Directory or a PKI.
- **Easy management of zones of confidence:** Easily integrated into collaborative or communication tools, this encryption solution is scalable and especially suited to global deployment, commercially or by projects (BU or transverse services) or to safeguard exchanges with subcontractors.
- **Compliance:** In accordance with the GDPR* and the ANSSI requirements, a geolocation feature enables blocking of the application depending on the risk associated with the country where the user might be: confidential documents do not have unencrypted access.

07

STORMSHIELD

Unique Differentiators

Unrivaled Trust

The highest-level of European certifications to ensure integrity and transparency

Global Protection for Converged IT/OT Networks

A unique platform to inspect and control IT and Industrial-related traffic

Performance

An optimized system to ensure maximum performance when security engines are activated.

Future functionality

Agentless Encryption for external collaboration: A protected file can be shared with an external recipient without the need to install a local agent.

Certifications

- ANSSI Qualification (Standard Level)
- VISA ANSSI
- UE Restricted Classification
- NATO Restricted Classification
- EAL3+/EAL4+ Common Criteria

Innovation

CYBER RANGES

A Next-generation Cyber Range as a Service

CYBER RANGES

01

CYBER RANGES

Company Description

Silensec is an international Information Security Management, Training and Technology Company with offices in **Cyprus (HQ), England, Kenya and Canada** and worldwide clients and partners. Silensec specializes in the delivery of services in IT Governance, Security Audits and Assessments, Value-Added Systems Integration, Managed Security with a 24x7 SOC, Security Training.

Established in England in 2006, Silensec is ISO 27001-certified by the **British Standards Institute (BSI). CYBER RANGES** is a wholly owned subsidiary of Silensec for the development and operation of **ISO 27001-certified** cyber range platforms and services.

CYBER RANGES, a.k.a. Silensec Cyber Range, is a next-generation military-grade full-content-lifecycle cyber range for the individual and team development of cyber capabilities, competencies assessment of competencies, organizational cyber resilience. CYBER RANGES is available as a public subscription-based/private managed service and as On-Premise and Portable deployment options.

02

Company Information

Company Name: CYBER RANGES
Founded: 2006-2
Employees: 50 up to 100
Web: cyberranges.com
Headquarters: Limassol, Cyprus
Other Offices:
Sheffield, UK
Nairobi, Kenya
Calgary, Canada

Key Target Verticals:
CYBER RANGES by SIlensec is used by:

- government agencies
- military entities
- higher education institutions
- training providers
- financial institutions, incl. central banks
- telcos and utilities
- consulting firms

03

CYBER RANGES

The Product

Product Category: Cyber Range, Detection & Prevention; SOC

Product Stage: Released & Deployed

Product Names and Brief Description:

- Next-generation Cyber Range as a Service on public/private cloud or as On-Premise and Portable

Services Provided:

- Immersive simulation training, cyber capability building and assessment, cyber resilience testing

04

Product in detail: CYBER RANGES

CYBER RANGES is the world-renowned platform by Silensec for immersive simulation training, cyber capability building and assessment, cyber resilience testing. Government and military entities, large companies, telcos and utilities, central banks and universities successfully use CYBER RANGES.

Since 2017 the UN's International Telecommunications Union (ITU) has used CYBER RANGES to run cyber drills around the world, such as the ITU 2020 Global Cyber Drill with over 210 participants, organised in teams from both technical and management roles, from 57 national CERTs/CSIRTs. This exercise ran over 2 weeks with 6 complex scenarios designed/developed together with industry partners using the CYBER RANGES content suite for scenarios authoring, infrastructure virtualization, traffic & attack injections, external technologies integration.

CYBER RANGES offers you:

- an environment for on-tap individual training practice with an ever-growing library of simulation scenarios.
- a service for blue/red team exercise platform for SOC/IR teams.
- your own platform, hosted/on-premise according to your organisation's mission, to model even true replicas of your live or target infrastructures (technologies - OT/SCADA/ICS etc. - tools, processes, etc.) and to run your capability and product testing exercises in secure conditions, even with safe online access.
- comprehensive data capture to measure the performance of individuals, teams, processes, tools and products towards ultimate capability evaluation.

How does it work?

- CYBER RANGES has led on the innovative use of cloud technology for cyber-ranging.
- CYBER RANGES can scale up to 1,000s of concurrent users and VMs.
- With a user interface designed according to gamification principles, CYBER RANGES provides user and administration support for individual and red/blue/white/... team-based exercises.
- CYBER RANGES offers the ability to design, develop, host and run custom virtual environments and a variety of multi-format simulation scenarios to meet specific objectives and according to many performance criteria.
- CYBER RANGES offers the ability to integrate third-party technologies and tools in the virtual environment besides its library of pre-built infrastructure assets.
- CYBER RANGES contains advanced technology for user traffic and attack simulations according to the latest exploits and vulnerabilities (e.g. MITRE ATT&CK).
- CYBER RANGES provides support of standard (e.g. NIST NICE) and custom competency frameworks for scoring and assessment, with start-to-finish performance metrics.
- CYBER RANGES is available in all deployment options for clear cyber-ranging economics: public cloud or hosted, on-premise and even portable.
- CYBER RANGES offers real-life situational practice in on-the-job like conditions.
- Many cyber ranges are designed to deploy at a physical location. CYBER RANGES PORTABLE supports cyber-range-in- a-room. it takes your cyber range to users rather than users to it, incl. remote places or in-theatre, for several even complex use cases.

CYBER RANGES

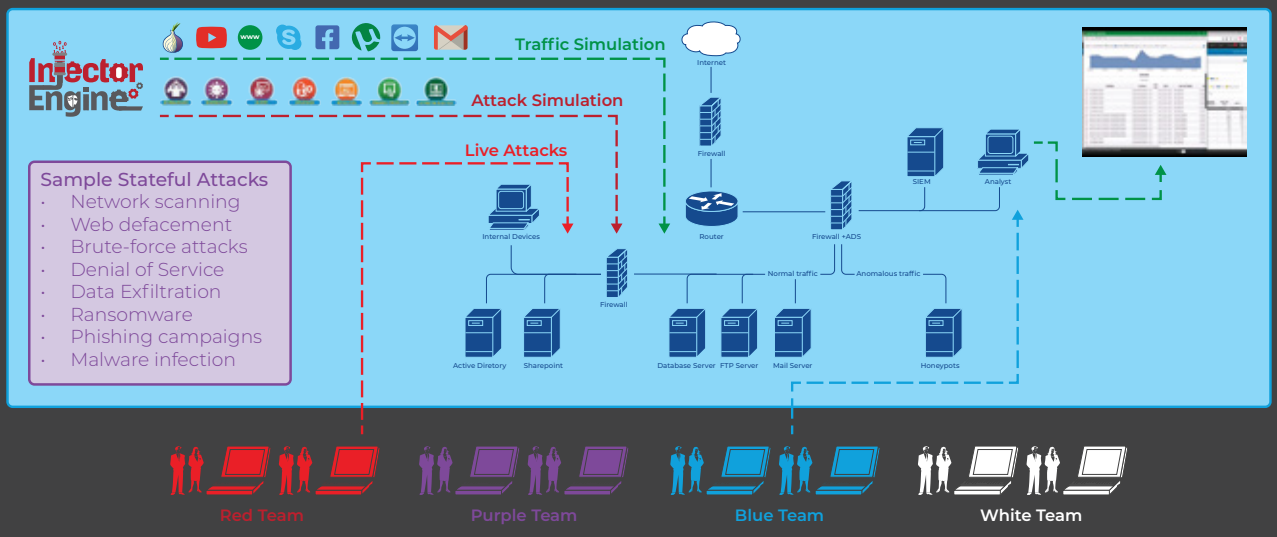
How does it work?

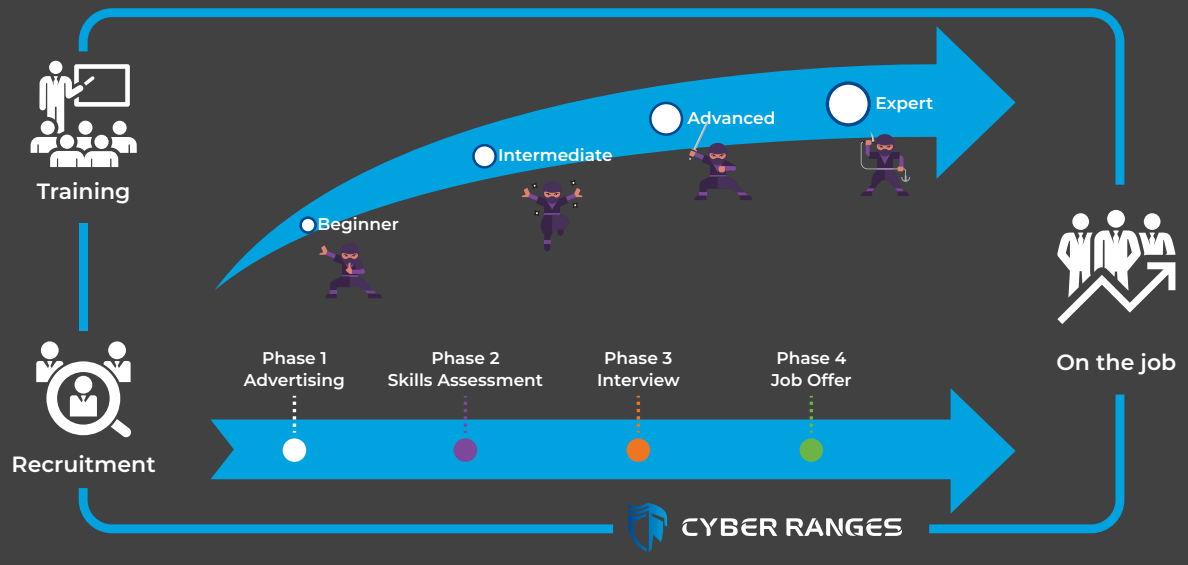
CREATE Design and build custom scenarios, including complex virtual environments, storylines with clear mission/task objectives and cyber challenges.

PUBLISH Make your scenarios available on CYBER RANGES for continuous, easy and on-demand access by users, anytime anywhere, even on pay-as-you-go terms.

USE Set up and run cyber exercises from the extensive library within minutes, using nothing but a few clicks.

ASSESS Assess the competencies of individuals or teams using standard or custom competency frameworks against the latest attacks, threats and vulnerabilities.





06

CYBER RANGES

Key Benefits

CYBER RANGES delivers the following benefits according to the chosen deployment option:

- Continuous security competencies development for your team at a fixed cost
- On-demand deep-dive hands-on security labs anywhere anytime
- Several security tracks, expert-defined, objective-based and mapped to different security roles and career paths to cover all your competence needs in your SOC/CSIRT/CERT/business ecosystem/etc.
- Visibility of individual and team capabilities to know about the areas of strength, weakness and improvement of your personnel's hard and soft cyber security skills
- Advanced traffic and red-team simulation engine for realistic blue-team training scenarios
- Competence-based assessment to support your staff hiring and on-boarding
- Validation of cyber security training and certification programmes against actual real performance
- Training/testing securely on live/planned infrastructure replicas
- Testing the cyber resilience of your organization against current and future threats.

07

Unique Differentiators

Key differentiators of CYBER RANGES are:

- **Orchestration**, i.e. managing great numbers of users and scenarios, even large/complex ones
- **Collaborative authoring tools** for scenario design, development and re-purposing
- **Agent-based user traffic and attack simulations**, also based on MITRE ATT&CK
- **Support of Competency Frameworks** and other performance criteria (custom or industry-specific)
- **Scoring and reporting**
- **All the benefits on a portable system too!**

08

CYBER RANGES

Future Functionality

The CYBER RANGES innovation is backed by a highly focused Research & Development team, whose architects are regularly engaged in large-scale research projects with academic, industry and government partners.

Silensec operates an ecosystem of partners, leaders in their own industries and subject matter experts. This ecosystem already provides those organisations choosing CYBER RANGES, with additional access to:

- specialist knowledge
- engaging simulation scenarios
- focused consultancy services for CYBER RANGES powered cross-team exercises
- integration of CYBER RANGES with domain-specific systems and technologies, such as LMS, HCM and OT/SCADA/ICS and more.

Direct research, partner ecosystem, and active participation in such international industry associations as the European Cyber Security Organization (ECSO) and the Global Cyber Alliance (GCA) help position CYBER RANGES as one of the few most robust long-term committed vendors in the cyber range and cyber exercise market.

09

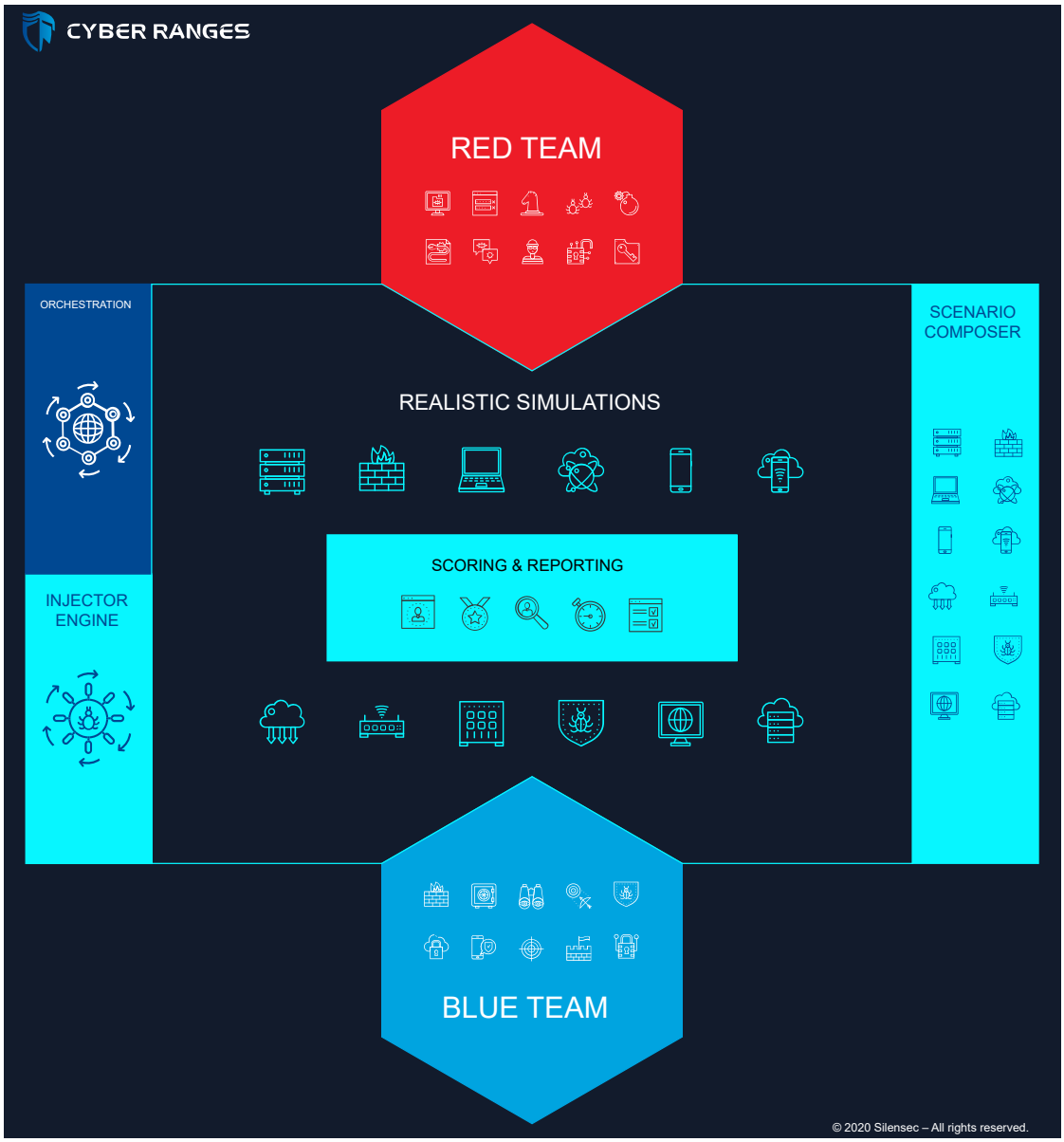
Services provided

CYBER RANGES comes with a comprehensive set of Value-Added Services, provided by Silensec and its Industry Partners, to deliver you and your organization a unique high-return use experience based on the CYBER RANGES capabilities.

Such value-added services can be accessed no matter whether you have opted for a cyber range on pay-as-you-go/subscription terms, hosted/MSSP terms, on-premise or portable:

- Advanced scenarios including APT and cyber threat simulation
- Custom simulation replicating the target organization's environment
- Delivery of cyber drills and hybrid table-top hands-on simulation exercises
- Large-scale security personnel selection and recruitment based on hands-on competence assessmentScoring and reporting
- All the benefits on a portable system too!

Infographic: Red vs Blue Team realistic simulations



Certifications

silensec™ iso27001 Certified

senhasegura

Global Privileged Access Management (PAM) Vendor

senhasegura®

01

Company Description

senhasegura is a global Privileged Access Management (PAM) vendor.

Our mission is to eliminate privilege abuse in organizations around the globe and build digital sovereignty. To accomplish this, senhasegura works against data theft through the traceability of privileged actions of both human and machine identities on assets such as network devices, servers, databases, Industry 4.0 and DevOps environments.

In 2020 and 2021, senhasegura has been recognized as a Challenger in the Gartner Magic Quadrant (MQ) report. In the same year Gartner also placed us among the three best PAM Technologies in the world in their Critical Capabilities PAM report. In January 2021, we were one of the only two companies in the world that received the Customers' Choice stamp in the 2021 Voice of the Customer report by Gartner Peer Insights. In the same portal our customers' reviews offered a 97% recommendation rate*, the highest one among all PAM vendors.

02

Company Information

Company Name: senhasegura
Founded: 2010-3
Employees: 50 up to 100
Web: senhasegura.com

Headquarters: São Paulo, Brazil
Key Target Verticals:
Energy & Utilities; Finance; Telco; Healthcare; Legal & Government; Retail

03

The Product

Product Category: Cloud Security, Gov. & Compliance, IAM, Healthcare

Product Stage: Released & Deployed

Product Names and Brief Description: senhasegura Privileged Access Management platform - PAM 360º, an advisory process developed by senhasegura that identifies an organization's maturity level in terms of privileged credential management.

Services Provided:

- Assessment 360º to evaluate the privileged access management process;
- Top down approach starting from a broad view of business

Product in detail

senhasegura is a Privileged Access Management platform composed by the following product families:

For PASM:

- senhasegura PAM Core: https://senhasegura.com/en/products/access-management-pam/
- senhasegura DevOps Secrets Management (DSM): https://senhasegura.com/en/security-and-risk-management/devops/
- senhasegura Domum - Remote Access: https://senhasegura.com/en/products/domum/
- senhasegura PAM Express SMB

PS: All PASM components run on Linux Virtual Machine but this is totally transparent to the customer

For PEDM:

- senhasegura Privileged Escalation Delegation Management for Windows, also referred as senhasegura.go for Windows: https://senhasegura.com/en/products/endpoint-privilege-management/endpoint-privileges-windows/
- senhasegura Privileged Escalation Delegation Management for Linux, also referred as senhasegura.go for Linux: https://senhasegura.com/en/products/endpoint-privilege-manageme
- senhasegura Certificate Management: https://senhasegura.com/en/products/certificate-management/
- senhasegura PAM Multi-Tenant: https://senhasegura.com/en/security-and-risk-management/cloud-security/
- senhasegura PAM Load Balancer: https://senhasegura.com/en/products/pam-infrastructure/pam-load-balancer/

PS: All Others run on Linux Virtual Machine but this is totally transparent to the customer

- senhasegura PAM Crypto Appliance: https://senhasegura.com/pam-crypto-appliance/

05

How does it work?

senhasegura is a privileged access management software solution that stores, manages and monitors all credentials, such as passwords, SSH keys and digital certificates, in a secure digital vault. Using encryption mechanisms, the password vault offers users the ability to use only one password to access a series of credentials registered in the solution.

Additionally, senhasegura can be used to access all network resources through SSH and RDP protocols, storing all records of their use for audit and compliance analysis purposes. Its intelligence allows for real-time analysis of actions taken by users and alert generation to identify fraud or inappropriate action.

06

Key Benefits

- Operational gain in the password change process.
- Guaranteed password delivery in a secure and controlled manner.
- Transparent authentication on the target system or network device without displaying the password to network administrators or third parties.
- Greater security maturity in DevOps environments (DevSecOps).
- Reduced security risks and better governance.
- Reduction of security risks and improper access to sensitive data.

senhasegura allows segregation for access to sensitive information, isolating critical environments and correlating environments with and without correlation. Taking this into account, it is important to avoid data breaches, the biggest challenge in the management of privileged users.

Overcome the challenges of implementing regulations such as PCI, ISO, SOX, GDPR, and NIST, with automation of privileged access controls to achieve maturity in the audited processes.

07

Unique Differentiators

Features that differentiate senhasegura against our competitors:

- SaaS-based solution of intelligently distanced Privileged Access that is agentless and VPN-less
- Exclusive native feature of creating and executing Ansible playbooks as a tool for building new privileged tasks
- AI & ML Powered User Security Posture Rating
- DevOps - Secret Automation
- Certificate Management
- Change Audit
- AWS OpsWorks Integration

Other differentials:

Governance and Administration
- built-in SCIM connector for IGA integration
- built-in MFA App

Privileged information
- Personal vault
- Privileged data

PEDM Windows
- offline credential take-out
- file integrity monitoring
- application sandboxing

Secret Management
- Cloud IAM provisioning

Ease of Deployment
- All-in-One virtual machine with no need of 3rd licenses

Future functionality

08

Our main innovation drivers are:

1. Use of AI to predict frauds instead of reporting them
- AI DevSecOps Analysis
- AI PEDM Threat Analysis
- AI Cloud Entitlements Analysis

2. PAM as a SaaS
- Open billing Process: It gives more transparency to legal sponsors of product
- Flexibility to increase or reduce license: which results in greater customer flexibility
- Easier support, community and documentation access: to improve customer experience to solve issues faster

3. DevOps Integrations In 2021 our innovation team will continue to close gaps in market demands, working to accelerate the development of unique and differentiated functions or improving our functions in relation to the competition. We will drive the market even more than we have in the coming years.

Video

Innovation

Resecurity, Inc.

Data Driven Cyber Security Solutions

01

Resecurity

Company Description

Founded in 2016, Resecurity, Inc. has been globally recognized as one of the world's most innovative cybersecurity companies with the sole mission of protecting enterprises globally from evolving cyber threats through intelligence. Resecurity, Inc. has developed a global reputation for providing best of breed data-driven intelligence solutions.

02

Company Information

Company Name: Resecurity, inc.
Founded: 2016-10
Employees: 30 up to 50
Web: www.resecurity.com
Headquarters: Los Angeles, USA

Key Target Verticals:

All

03

The Product

Product Category: Cyber Posture; Third-party Security

Product Stage: Released & Deployed

Product Names and Brief Description:

- Context™ - Cyber Threat Intelligence Platform
- Risk™ - Digital Risk Monitoring Platform

Services Provided:

- APT Emulation
- Red Teaming
- Digital Forensics & Incident Response
- Investigations
- vCISO

04

Resecurity

Product in detail

Context™

Resecurity Context™ – Cyber Threat Intelligence Platform: Platform for cyber threat intelligence acquisition, monitoring, analysis and further distribution across internal parties. Commonly used as threat workbench for intelligence and operators.

05

How does it work?

Resecurity Context™ is a Cyber Threat Intelligence Platform enabling enterprises and government agencies to collect actionable intelligence from multiple sources by different criteria and to accelerate analysis, prevention and investigation workflow required for strategic and timely decision-making.

Resecurity Context™ is provided in form of dedicated secure portal with capability to produce automated intelligence feeds through API, STIX&TAXII protocol and/or other exportable formats (JSON, XML, TXT, etc.) for integration with third-party systems.

The production of finished intelligence including but not limited to IOCs, TTPs, threat artifacts is organized through TAXII server located at taxii.resecurity.com. Resecurity developers, engineers and technical support team will provide documentation and assistance in configuration of secure data exchange based on Client specifications.

Resecurity Context™ supports flexible set of search filters in order to increase targeting, accuracy and relevancy of the search results. Search filters can be configured by operator through UI or API interface. The operator may define complex search filters and rules in specific module or across the whole platform.

06

Resecurity

Key Benefits

Key benefits and business problems we solve:

1. Threat Intelligence
2. Business Email Compromise
3. Account Take Overs
4. Vulnerability Management
5. Zero Day Intelligence
6. Botnet Intelligence
7. Automation/Orchestration
8. Case Management System

07

Unique Differentiators

- Powerful workbench, which requires no learning time for operators to perform intelligence collection from day 1.
- Data, all source intelligence, which is tailored to each of our clients against global threats.

08

Future functionality

GEO-IP, Netflows, data science analytics platform utilizing our data lake.

Resecurity

Product in detail

Risk™

Resecurity Risk™ – Digital Risk Monitoring Solution: Powered by Context™, this is the management or platform dashboard. Provides immediate context to real time threats and heads up dashboard to provide immediate situational awareness.

How does it work?

Resecurity Risk™ is Artificial Intelligence driven Digital Risk Monitoring solution acting as a defensive component in scope of Cyber Threat Intelligence Platform.

It enables operator to evaluate, quantify, forecast and mitigate the identified cyber threats and security challenges using comprehensive risk-scoring metrics to guide timely and strategic defensive actions.

Resecurity Risk™ allows to track security posture changes depending on the identified security events, Dark/Web/Surface Web and other malicious activity.

Resecurity Risk™ identifies and eliminates potential blind spots and security gaps throughout your network infrastructure and exposed digital footprint.

Key Benefits

- **Accurate:** Artificial Intelligence driven engine will provide accurate insights that enterprise can act on and focus on.
- **Scalable:** Monitor any size digital presence – from a single domain to a globe-spanning network of applications, users, services, and clouds.
- **Effective:** Track evolving security risks in near real-time and respond proactively to mitigate vulnerabilities.

Unique Differentiators

Powered by Context™, key is in collection of all-source intelligence, not just commodity data like open source, but tailored to each of our clients.

Stellar Cyber

High-speed high-fidelity detection and automated response across the entire attack surface

STELLAR CYBER®

01

Company Description

Stellar Cyber was founded in 2015 by Aimei Wei (Senior VP of Engineering) on a mission **to transform security operations,** changing the conversation from analyzing data to correlating incidents, covering the entire attack surface and bringing the right intelligence, while retaining investments.

Today, Stellar Cyber is the **leading Open XDR** (Everything Detection and Response) platform for enterprises and MSSPs, unifying all currently disjointed security tools and data sources to fully visualize and automatically detect, investigate and respond to all attack activities.

We continue our relentless drive to enhance the platform through ongoing research and development.

02

Company Information

Company Name: Stellar Cyber
Founded: 2015
Employees: 70 up to 100
Web: stellarcyber.ai

Headquarters: Santa Clara, CA
Key Target Verticals: Enterprise : Manufacturing, Finance, Education, Government, Healthcare

03

The Product

Product Category: XDR, Cloud Security, Detection & Prevention, Email Security, AI, Endpoint Security, Network Security, Orchestration & Automation, UEBA

Product Stage: Released & Deployed

Product Names and Brief Description: Stellar Cyber's Open XDR platform delivers **Everything Detection and Response** by unifying all currently disjointed security tools and data sources to fully visualize and automatically detect, investigate and respond to all attack activities. organization's maturity level in terms of privileged credential management.

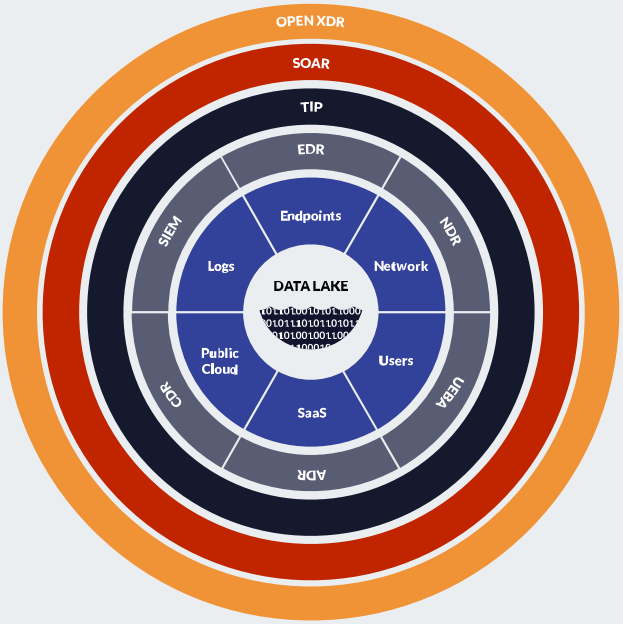
Product in detail

Open XDR is a unified, AI-powered approach to detection and response, that collects and correlates all existing security tools, to protect the entire enterprise attack surface effectively and efficiently. **Open XDR is Everything Detection and Response,** more than eXtended Detection and Response, because it must defend against all threats across the entire attack surface. The only way to do this is by integrating with existing security tools.

How does it work?

Architecturally, Open XDR is about **unifying and simplifying the entire Security Stack** for the purpose of radically improving detection and response. At any given enterprise, a Security Stack will consist of numerous capabilities like SIEM, EDR, NDR, SOAR and more. These capabilities were never designed to work with each other, and teams spend too much time managing multiple tools, which is what leads to the problems of today – too many tools, not enough people, not right data. That's where Open XDR comes in – unify all capabilities together, correlate alerts from individual tools into a holistic incident, simplify by reducing administrative overhead. AI and automation comes in as the only technically feasible way of protecting the entire attack surface effectively and efficiently, which is why it is a key architectural attribute of Open XDR.

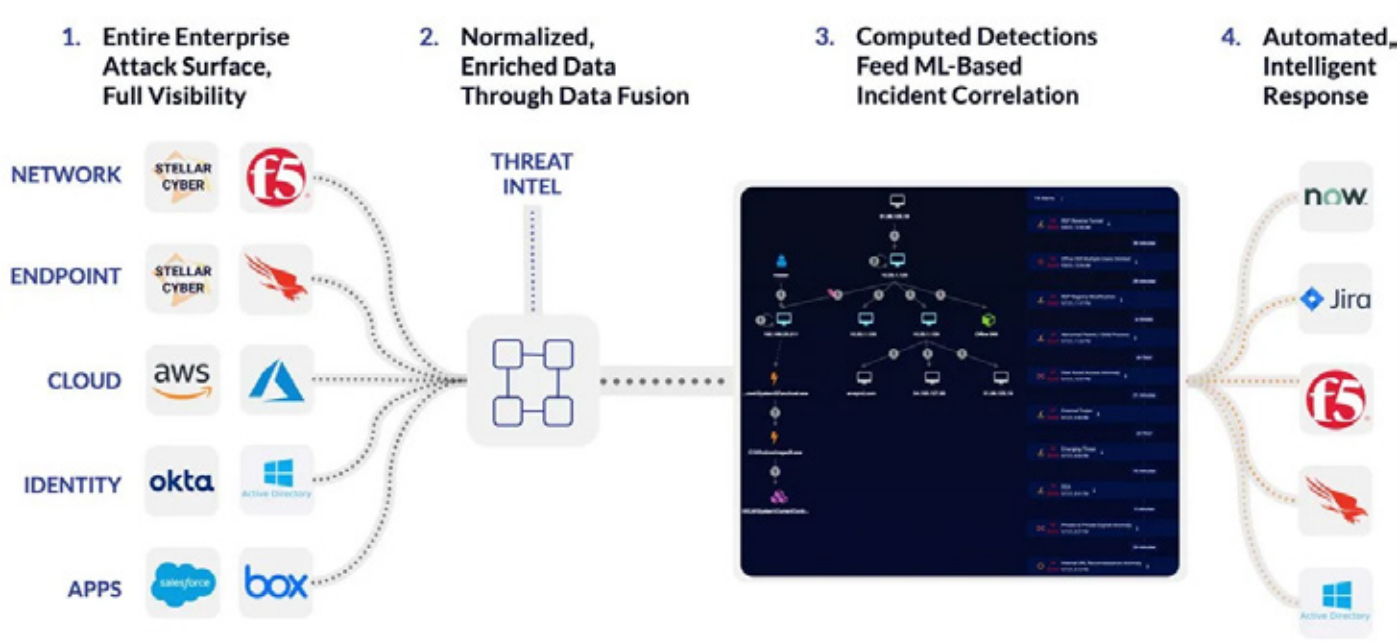
The outcome of Open XDR is protecting your enterprise from threats from a single platform versus multiple tools that have weak or non-existent connections band-aiding it all together. And the ultimate outcome of Open XDR is radically improved detection and response at a price enterprise's can afford.



Stellar Cyber's Approach To Open XDR

While integrating with your existing security tools as part of our open platform, Stellar Cyber's Open XDR Platform also packages together multiple capabilities, all built on core technology that enables the outcome of Open XDR – radically improved detection and response at a price enterprise's can afford. In our view, it's not enough for Open XDR to be "eXtended", that is a marginal improvement over status quo, and today's security environment demands something dramatically different, which is why we believe Open XDR is Everything Detection and Response.

From a technology standpoint, we believe the right approach to XDR is Open-first, partially-Native. If an Open XDR platform is only a "correlation layer" on top of existing tools including a SIEM, that does not deliver a unified experience and does not simplify the Security Stack. Conversely, a Native-only XDR platform requires an enterprise to move their entire infrastructure to one vendor. The Open-first, partially-Native approach to XDR is core to our Open XDR platform. The Stellar Cyber Open XDR Platform works with whatever you have already, gives you better visibility where you don't yet have it, and helps you consolidate multiple capabilities under one platform if you choose to do so.



06

Key Benefits

The value of Open XDR:

- Radical Performance
  Unification of the Security Stack, with AI powered detection and response, translates a faster, better approach to security opeartions.

- No Vendor Lock-in
  Open XDR leverages existing security tools, not forcing you to migrate your Security Stack to a single vendor's firewalls, SOAR, EDR, etc.

- Economics
  Simplification and consolidation of security products reduce the number of licenses, tool training and overall capital required to run a security operations program.

07

Unique Differentiators

Our unique differentiators are:

1. Automated Incident Correlation:
   - Automatically groups related alerts into incidents that show the progression of an attack – reducing the investigation effort from the number of alerts to the number of incidents, orders of magnitude reduction.
   - Automatically combines related alerts into incidents with high fidelity – reducing the noise from the false positive of individual alerts – an order of magnitude improvement in accuracy.
   - Automatically prioritizes incidents to clearly identify the most serious attacks – shows analysts exactly where and how to respond.
   - Leverages telemetry from existing security tools as well as its own sensors – preserves existing security investment and provides 360-degree visibility by filling in the gaps.
   - Feeds the AI engine with normalized and enriched quality data to initiate instant and effective responses – AI works better when it has the right data to work from.

07

Unique Differentiators (Cont'd)

2. XDR Kill Chain™:

- First new kill chain invented in years – designed specifically for XDR detections, where threats can attack any point in theinfrastructure.
- Loop interface prioritizes detections into five phases: initial attempts, persistent foothold, exploration, propagation, and exfiltration / impact – analysts can easily see attacks as they happen and respond to the most emergent needs first.
- Captures the progression of complex attacks – alerts appear in the context of the five-phase kill chain so analysts can easily prioritize them without getting lost in details.
- Incorporates commonly used MITRE ATT&CK framework for detailed analysis and adds new tactics and techniques beyond the MITRE ATT&CK framework.

08

Videos

Stellar Cyber Incident Correlation

Stellar Cyber XDR Kill Chain

Innovation

Fortanix

Data Security and Confidential Computing Solutions

Fortanix®

01

Company Description

Fortanix®

Fortanix® is a data-first multi-cloud security company solving the challenges of cloud security and privacy. Data is the most precious digital asset of businesses, but this data is spread across clouds, SaaS, applications, storage systems and data centers. Security teams struggle to track, much less secure it.

Fortanix empowers customers to secure all this data with a centralized solution. Its pioneering Confidential Computing technology means data remains protected at-rest, in-motion and in-use, keeping it secure from even the most sophisticated attacks.

02

Company Information

Company Name: Fortanix
Founded: 2016-3
Employees: 100 up to 500
Web: www.fortanix.com
Headquarters: Mountain View, CA, USA

Key Target Verticals:

- Healthcare/Life Sciences
- Financial Services
- Retail
- Professional Services
- Government

03

The Product

Product Category: Cloud Security, Data Security, Cryptography

Product Stage: Released & Deployed

Product Names and Brief Description: Fortanix Data Security Manager SaaS

- Full power of Fortanix delivered as a service

Services Provided:

- Key Management Service
- Tokenisation
- Cloud Data Control
- HSM Gateway
- Secure Business Logic

04

Product in detail

Fortanix

With increased use of SaaS apps and cloud, IT infrastructure today is more nimble, more scalable, and cost-effective than ever before. But is it also more secure? At a time when cyber risks are higher than ever organizations are grappling with a severe talent drought to handle their data security infrastructure and are stuck with legacy security solutions that were never designed to integrate with the modern, dynamic environment of cloud and DevOps. Even the most robust data security tools and processes available today were never designed keeping a cloud-first world in mind. With more and more data migrating to the cloud while being subjected to regulatory controls — data security is an innate issue. Organizations can no longer afford to get tied by the on-prem and other architectural limitations. Data security must be infinitely scalable and offer elasticity that matches the agility of your new modern cloudbound IT infrastructure.

Fortanix Data Security Manager (DSM) SaaS combines the full proven capabilities of the Fortanix on-premises solution and flexibility of the cloud. It is the first and only multicloud data security service certified to the rigorous FIPS 140-2 Level 3 security standard. DSM SaaS lets organizations opt for a new service-based model that makes data security simpler to deploy, easy to manage and above all, more cost-effective SaaS-based data security for a cloud-first world.

05

How does it work?

Ease of Integration - The SaaS based model is built from the ground up for easier integration with apps, IT infrastructure and services.

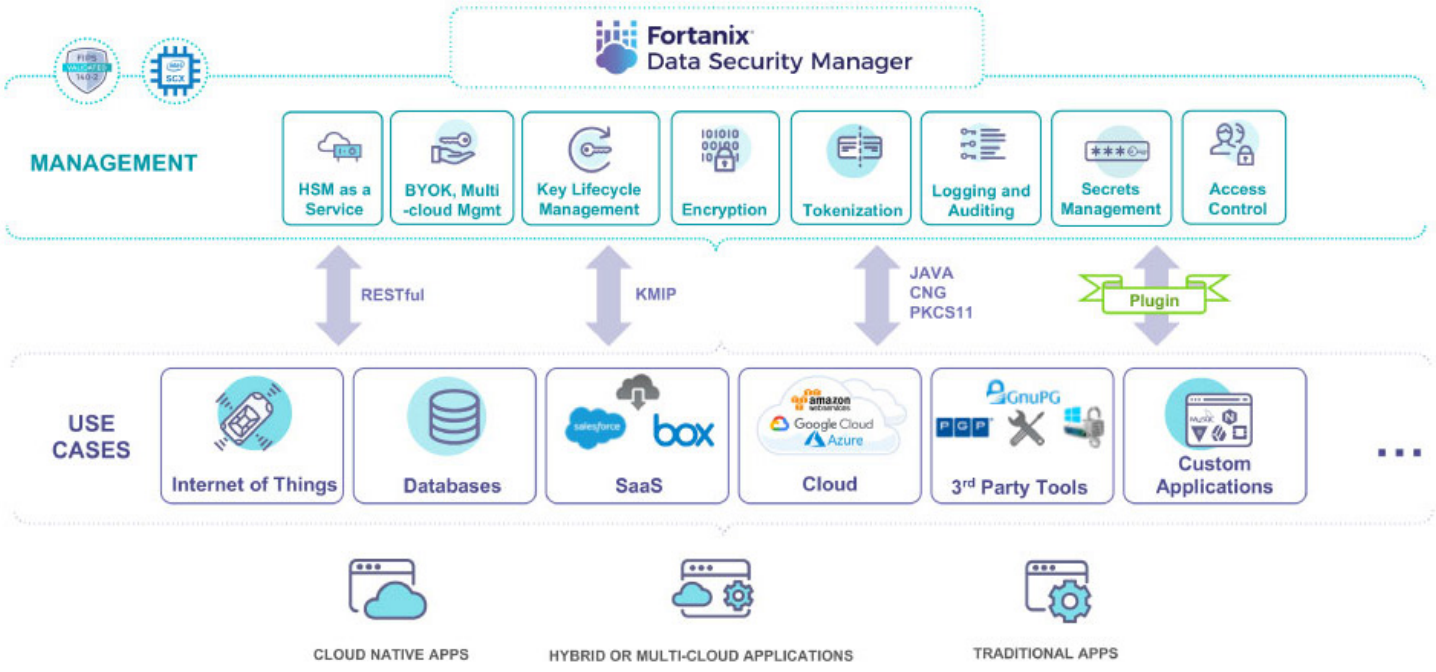
No Specialized Expertise/Skills Required - Keeping the cybersecurity skill shortage in mind, our SaaS based data security is designed for easy usage and faster adoption. No additional/ special skillset required. Simplified operations with zero management overhead/ hardware.

Start Small and Start Immediately - Quick to set up, quicker to start. Data Security at your fingertips that can scale as you grow with increasing operational volumes.

06

Key Benefits

- Uniform Security Across Clouds
- Easy to Use, Developer Friendly Service
- Highly Resilient, Distributed Architecture with Maximum Flexibility
- Simplify Operations and Ensure Ease of Management
- Pay As You Grow



07

Unique Differentiators

Data-centric security demands a new approach. Fortanix created a new technology, Runtime Encryption, that makes it possible to decouple security from the infrastructure. With Runtime Encryption, compromised credentials, unmitigated vulnerabilities, and network intruders no longer threaten critical data. Today, this technology has evolved into a revolution of sorts – Confidential Computing – that is recognized by Gartner, Forrester, and the largest cloud and technology companies.

08

Future functionality

Can be provided under NDA

Fortanix

Video

Innovation

SafeBreach

Automated & Continuous
Breach & Attack Simulation

SafeBreach

01

SafeBreach

Company Description

SafeBreach simulates thousands of attack methods to provide a hacker's view of an organization's security posture, paint a picture of the security exposures to an enterprise and prioritize remediation, securing against TTPs.

SafeBreach Labs is dedicated to threat research from real-world investigation with the most extensive breach and attack methods in the industry with **over 15,000 attack methods and growing.**

02

Company Information

Company Name: SafeBreach
Founded: 2014-6
Employees: 50-100
Web: safebreach.com

Headquarters: Sunnyvale, CA
Key Target Verticals: Financial Services, Healthcare, Pharmaceuticals, Biotech, Insurance, Manufacturing, Energy, Utilities, Oil & Gas, Food & Beverage, Hospitality, Technology, Banking, Transportation

03

The Product

Product Category:
- Breach & Attack Simulation, Cyber Posture, Cyber Range

Product Stage: Released & Deployed

Product Names and Brief Description:
SafeBreach Platform
SafeBreach safely executes breach simulations across the entire cyber kill chain.

04

SafeBreach

Product in detail: SafeBreach Platform

The **SafeBreach platform** carries out continuous, automated testing of an organization's security architecture using advanced, patented simulation technology.

SafeBreach attack simulations are exact reproductions of an attacker's tactics and techniques, but pose no risk to the organization's operations or assets. Attacks are executed between simulator instances deployed both within and outside the organization's network.

This approach provides broad coverage and fully tests the entire security ecosystem deployed by your organization.

05

How does it work?

SafeBreach simulates thousands of attack methods to provide a hacker's view of an organization's security posture, paint a picture of the security exposures to an enterprise and prioritize remediation, securing against TTPs.

SafeBreach Labs is dedicated to threat research from real-world investigation with the most extensive breach and attack methods in the industry with over 15,000 attack methods and growing.

SafeBreach

Key Benefits

SafeBreach enables security teams to provide data-driven proof of security, eliminate security blind spots and weaknesses, and validate that controls are working as expected.

SafeBreach delivers the following key capabilities:

- Automated, continuous and network-wide attack simulation
- Paint the picture of how an attack would play out in your environment with SafeBreach Explorer view and mapping TTPs to the MITRE ATT&CK framework
- Real-time prioritization of business risks and actionable intelligence on the effectiveness of operational security posture

Unique Differentiators

- Largest playbook consisting of over 15,000 attack methods
- Dedicated threat research team that continues to add new attack methods to playbook
- Largest coverage of the MITRE ATT&CK Framework
- Safe to run tests against your controls in production
- Methods used in headline attacks and US CERT Alerts added to playbook for clients to test controls within 48 hours

Future Functionality

SafeBreach is committed to the increase of coverage by continuously increasing the size of our breach and attack method library consisting of over **15,000 methods today and continued expansion of integrations.**

Sepio

Software Only Solution - Mitigating Rogue Devices

01

Company Description

Sepio is disrupting the cyber-security industry by uncovering hidden hardware attacks. Sepio Prime provides security teams with full visibility into their hardware assets and their behavior in real time. A comprehensive policy enforcement module allows administrators to easily define granular device usage rules and continuously monitor and protect their infrastructure.

Leveraging a combination of physical fingerprinting technology together with device behavior analytics, Sepio's software-only solution offers instant detection and response to any threat or breach attempt coming from a manipulated or infected element.

02

Company Information

Company Name: Sepio Systems
Founded: 2016-2
Employees: 53
Web: sepiocyber.com
Headquarters: Rockville MD, USA

Other offices:
Tel-aviv, Israel Lisbon, Portugal
Key Target Verticals:
Finance, Critical Infrastructure, Telcos/ISP, Data centers, Healthcare

03

The Product

Product Category:

- HW-based attacks
- Rogue Device Mitigation
- IoT – IIoT
- Endpoint Security
- Network Security

Product Stage: released & deployed

Product Names and Brief Description:

- Sepio Prime: A software only solution mitigating Rogue Devices by providing visibility from Physical layer.

Services Provided:

- Deployed as on-premise or SaaS based
- Visibility to both IT & OT devices

Product in detail 04

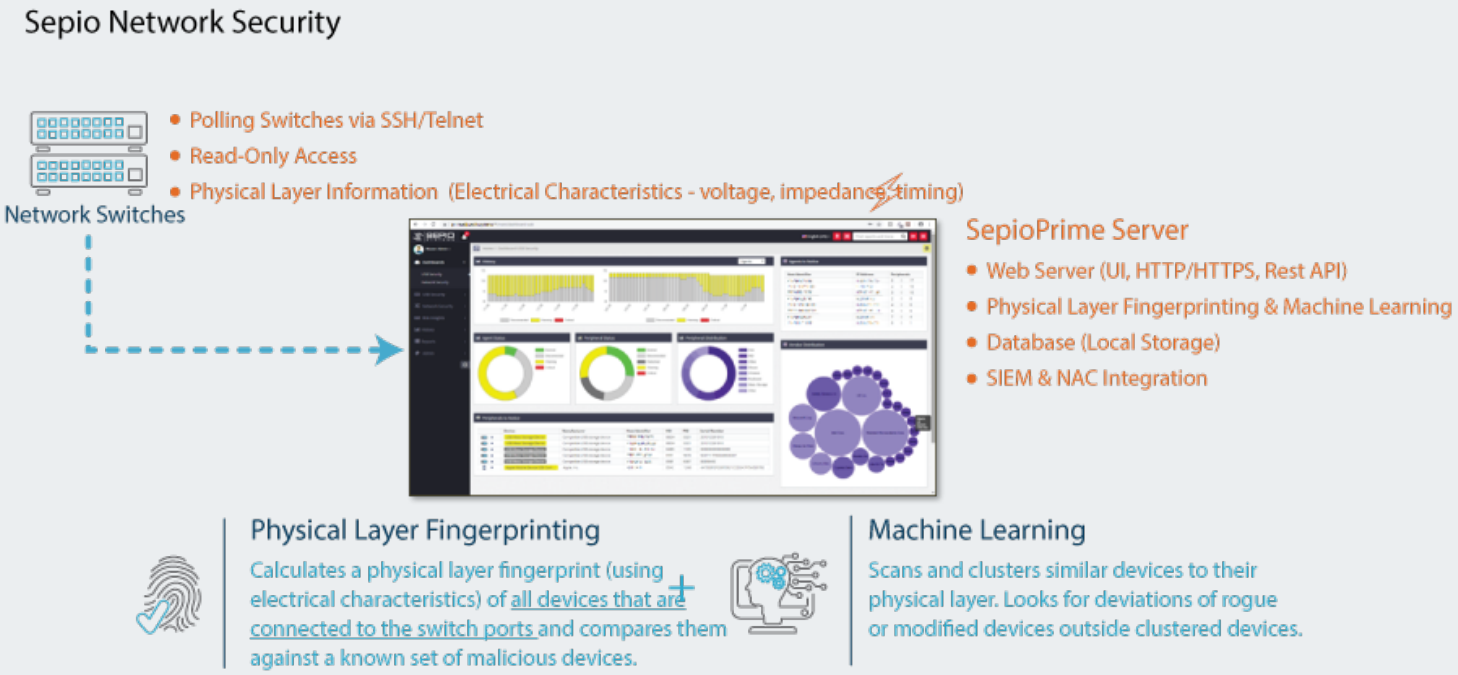
A software only solution that may be deployed as an on-premise or SaaS based.

Providing the ultimate visibility to every device present in the Enterprises infrastructure - whether its an IT or IoT device, whether its fully visible or trying to hide its presence.

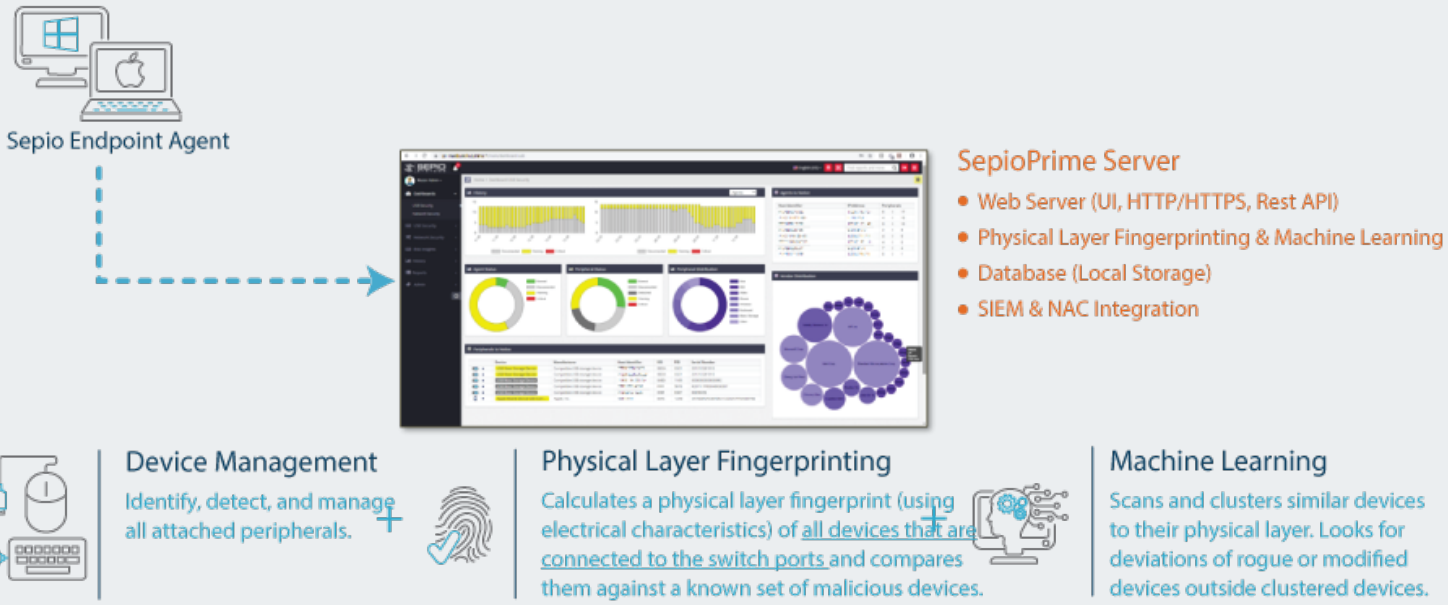
With a powerful, unique detection algorithm couple with an actionable, usable data for the non-expert user.

How does it work? 05

A novel algorithm based on Physical Layer fingerprinting and assisted by Machine Learning.



Sepio Endpoint Security



Key benefits

06

Endpoint protection benefits -

- Detects and identifies all attached USB peripherals
- Real-time behavioral analysis on all peripherals
- Alerts on known to be risky or badly-behaving devices
- Recommended best practice security policies
- Continuous small footprint or Dissolvable mode

Network Security benefits -

- Polls switches to analyze physical layer information
- Detects ghost devices that are invisible to other tools
- Real-time fingerprinting on retrieved data
- Vulnerability management for switch firmware
- Integrated with NAC, SIEM and other tools.

Future functionality 07

Additional interfaces support.
Additional 3rd. party vendors integration.

Unique differentiators 08

The ONLY solution capable of detecting Physical Layer network implants.

The ONLY solution capable of differentiating a legitimate HID device from an impersonating attack tool (i.e., RubberDucky, BashBunny) even when they share the same parameters.

Awards 09

Gartner - 2020 - Cool Vendor Cyber Physical Security
Frost & Sullivan - 2019 - Technology Leadership Award
Frost & Sullivan - 2019 - Best Practice Award - RDM

Atempo

Data Protection Solutions

preserving data ecosystems

Company Description

01

Atempo is a leading independent European-based software vendor with an established global presence providing solutions to **protect, store, move and recover all mission-critical data sets** for thousands of companies worldwide. With this feature set and an **extensive range of supported storage technologies and applications**, Atempo is suitable for all centralized or multi-site organizations including those having extreme scale data volumes, petabyte and above.

Company Information

02

Company Name: ATEMPO

Founded: 1992

Employees: 160

Web: www.atempo.com

Headquarters: Massy, South of Paris, France

Other French offices: La Ciotat, Lyon, Toulouse, Vannes.

Worldwide offices: UK, Germany, USA, Singapore, Korea.

The Product

03

Miria: A unique solution to back up and migrate or synchronize billions of unstructured data files between heterogeneous storage.

Tina: Enterprise backup and restore solution for physical and virtual machines, supporting a wide range of operating systems and applications.

Lina: Continuous data protection for desktops, laptops and file servers, offering self-service restore capabilities.

Customer Footprint

Relevant Public Success Stories:

- Public Administration
- Healthcare
- Research & Higher Education
- Industry & Manufacturing
- Media & Entertainment
- Other

Product in detail: Miria

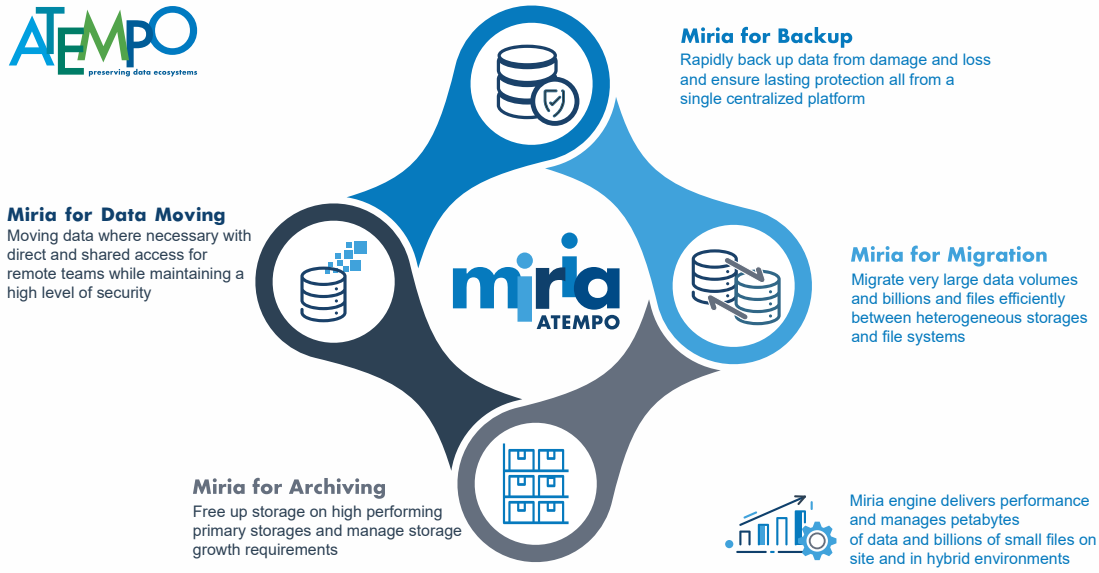
Miria is a powerful and scalable backup, archive, copy/move, migration and synchronization solution for petabyte scale unstructured file-based storages.

How does it work?

Miria for Archiving allows organizations to cost effectively manage the growth of their file-based data, particularly for data-intensive industries.

Miria for Archiving is a high-performance file management software for large file-based data sets that delivers:

- Cross-platforms backup and restore capability for large scale-out NAS, parallel file systems and file servers
- Express post-disaster restart for protected NAS by offering direct use of the backup target for read/write use
- File and folders on-going synchronization between heterogeneous storages with ACLs and remote sites support
- Automated permanent storage migration between heterogeneous platforms with ACLs preservation
- End-User driven or automatic Archiving via simple drag-and-drop interface allowing end-users operations without IT staff assistance And much more...



Key Benefits: Miria

- Efficient backup and restore for petabyte-scale volumes and billions of files:
  - Fast-scanning large storages for new, modified or deleted files
  - Complying with backup windows constraints
  - Preserving users rights/groups (ACLs)
- Making migration or synchronization of very large data set of files between heterogeneous storage simple and efficient

Unique Differentiators

- Heterogeneous platform integration that preserves ACLs across storages, operating systems and platforms
- User driven or automated workflows
- Fast data movement due to heavy parallelization and leveraging scalable groups of data movers

Future Functionality

- **SnapStor –** New capability to leverage a GPFS storage as a backup target that enables direct and immediate restart of production directly from the backup in case of disaster – as well as empowering the rebuilding of the storage platform once ready to restart

Product Video

Product in detail: Tina (Time Navigator)

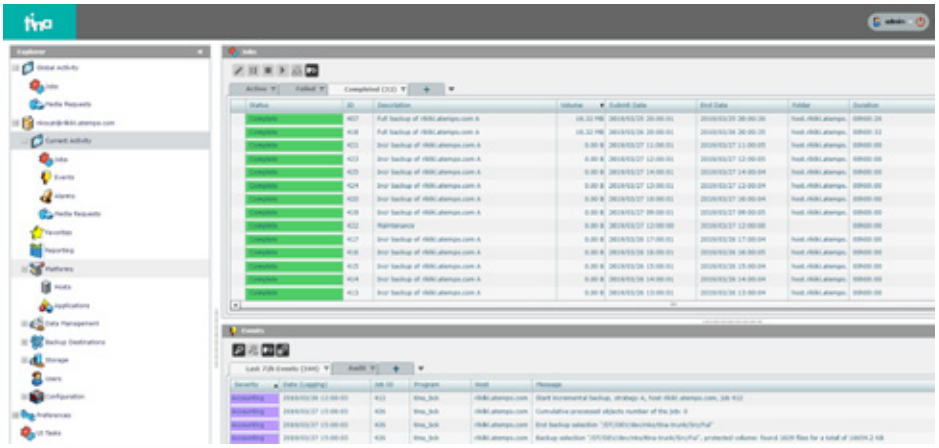
Built for **complex, heterogeneous enterprise environments, Tina** offers complete data protection, whether you manage a single work group or multiple data centers. Time Navigator makes it easy to **meet backup windows, to ensure digital security and to manage tiers of backup storage**, regardless of the platform, application or media.

How does it work?

Tina transforms backup by focusing on what matters in your business: recovery of data. Whatever the platform, restore is always based on three simple concepts:

1-Select data.
2-Choose date & time.
3-Restore.

Restore-centric solution that provides visual access to the file system in real-time showing not only files and directories but also deleted files. The user never needs to worry about where the data has been saved. Data is tracked throughout its lifecycle and can be restored with just 3-clicks regardless of the complexity of its backup history. Tina provides a common interface that displays the files in the same way regardless of platform.



Key Benefits: Tina

- **Security and compliance:** encryption, digital certificates, key management and activity trails can be applied to specific sets of protected data.
- **Unique restore:** no need to know where the data resides, only the date/time to restore back in time. File restore operations are made easier by providing a unique restore interface across a wide support of platforms and infrastructure.

Unique Differentiators

- **Tina** - A unique approach to data restoration locates and restores individual files from any point in time and from any tier of storage, enabling both IT staff and end users to quickly restore lost files.
- **Tina** is the ONLY solution able to visualize all files, including deleted ones (from physical and virtual machines) and restore them with the same 3-click approach through a simple interface.

Future Functionality

- Support of VMware vSphere
- Enhanced security for data encryption
- Fine granular restore of Active Directory
- Deduplication for all applications and Operating Systems
- Oracle RMAN script configuration wizard

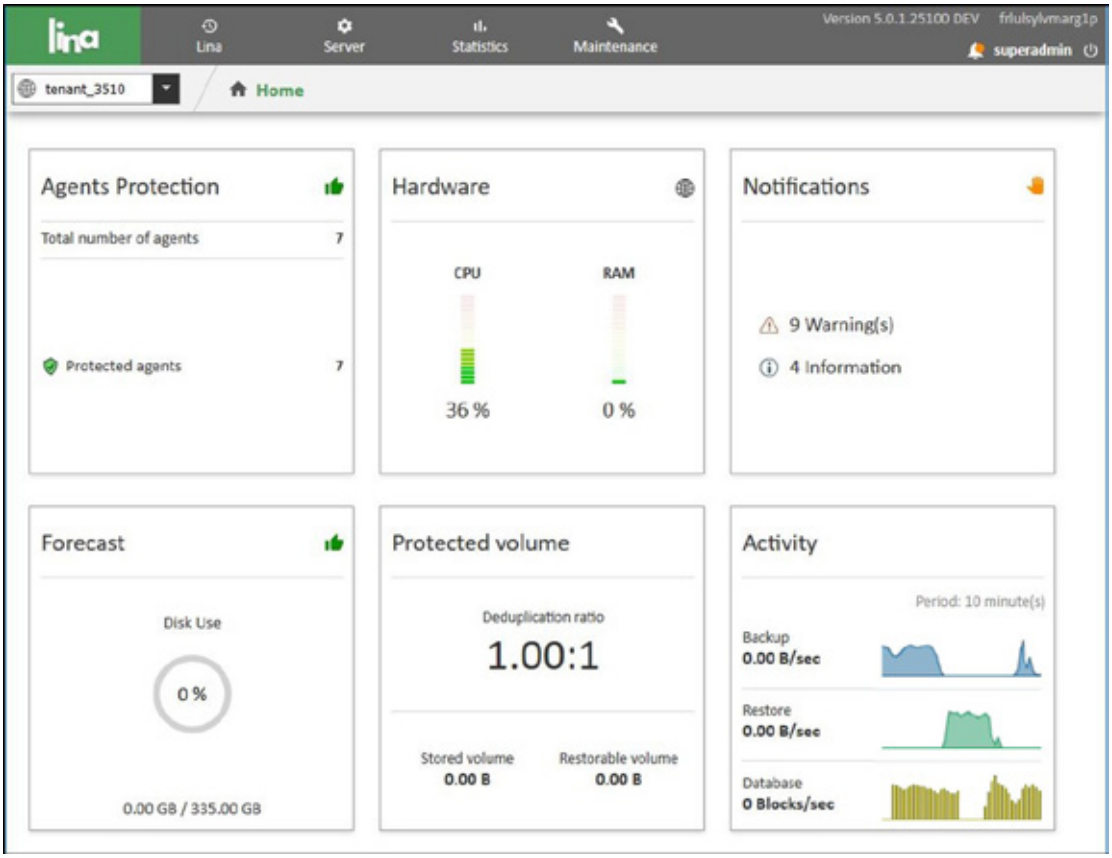
Product in detail: Lina

Lina provides a standalone, continuous data protection solution with advanced data de-duplication for remote offices, workstations, file servers and laptops.

How does it work?

With more and more critical data being stored on laptops, data protection is essential to protect the business. **Lina** provides continuous data protection for files residing on desktops, laptops and file servers, offering self-service restore capabilities.

With **Lina**, administrators just need to roll-out data protection policies across the enterprise and end users are empowered to restore data, through a wizard or a web browser.



Key Benefits: Lina

- End-users benefit from seamless protection of their data. There is no need to ask the administrator for the restore
- Administrators save time by not having to deal with numerous end-user restore requests
- Infrastructure managers benefit from reduced storage costs and optimized network performances
- Continuous data protection, no need to schedule backups, no risk of exceeding backup windows

Unique Differentiators

- **Lina** offers wizards to restore, but also advanced restore features (Time Navigation, cross restore).
- **Lina** can protect laptops and file servers with millions of files.
- De-duplication mechanism reduces storage space and network use.

Future Functionality

- Multi-servers Architecture
- Encryption
- Fail over Replication
- Restore Audit Trail

Certifications & Awards

Label France CyberSecurity identifying French Cybersecurity quality solutions which respects the highest level of computer security requirements.

Atempo is also participating actively to the French Government Program, to bring assistance to cyberattack victims, through the **Cybermalveillance.gouv.fr platform**.

Based on our ability to back up, protect, manage, and recover data, the most valuable asset of all business, to ensure data security and business continuity, Atempo has been named by the Insight Success Magazine one of the 10 Most Reliable Cybersecurity Solution Providers - 2020.

AI Global Media Ltd has put the Cyber Security Awards in place to honour companies that have gone above and beyond in this highly competitive sector. Atempo has been named: “Best for Data Protection & Restore Software - Europe”, as recognition of our outstanding performances within the sector.

MyTechMag, a pioneering tech magazine has acknowledged Atempo—a leading independent European-based software vendor with a global presence, offering Disaster Recovery solutions to protect, store, move and recover all your data—one among the **“Top 10 Promising Disaster Recovery Solution Providers 2020**" who are transforming companies with their unique solutions.

The Atempo.Wooxo Group has been selected to join the Alumni **French Tech 120** program, designed to nurture 25 unicorns by 2025.

Luc d'Urso has been named "**Best Cyber Security CEO**" in Europe in the 2020 European competition, in recognition of his active role in the fight against cybercrime.

Institutional Partners

Feedback and suggestions

Your feedback is extremely important to us and we value and appreciate receiving your suggestions or comments to help us improve our content, services and the way we communicate.

We appreciate receiving compliments

If you are satisfied with the Cyber Startup Observatory, please let us know. It helps us to know that we are delivering our services effectively and provides us with an opportunity to recognize our team's valuable effort.

Suggestions on cyber security topics, news, solutions and innovations are a valuable input

We strive to cover relevant topics, provide valuable resources and to shed some light on important issues. The team welcomes your contribution as a way to widen our vision, the quality of the content and the depth of our knowledge.

You can contact us at:

info@cyberstartupobservatory.com

The Global Cyber Innovation Network

The Cyber Startup Observatory®

The Cyber Startup Observatory®

LATAM - 4th Edition