WHITE PAPER

Achieving Cloud Benefits On-Premises Without Compromise: **Really?**

JUNE 2024

TEHTRIS

FACE THE UNPREDICTABLE

tehtris.com

FOREWORD

Enabling CISOs and cyber experts to reconciliate cyber risk management, market best practices, technical and data-centric realities through a single XDR platform.

Digital transformation drove heavy investments to host data in the cloud, enabling scalability, innovation and cost-effectiveness. However, this also expanded the attack surface, requiring an equal (if not higher) prioritization of cybersecurity. While cyberattacks grow in volume and sophistication, maintaining data confidentiality, integrity, and availability has become a daunting challenge. The evolution of market dynamics, industry practices, and evolving country-specific regulations influenced by geopolitical forces have made it even more complicated for CISOs to ensure effective protection.

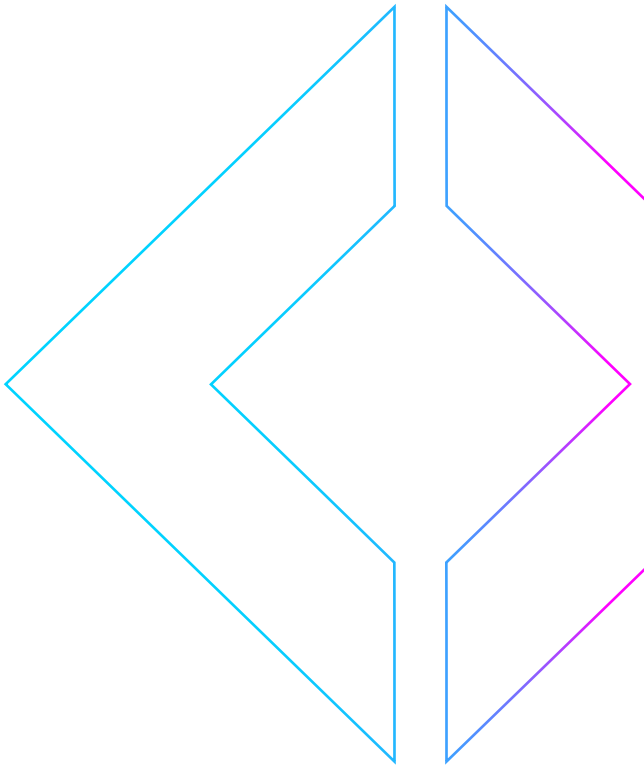
While the Cloud offers a lot of advantages, many organisations maintain an on premise environment to host their data. This choice hinges not only on IT legacy systems, internal resources, or the company's vision, but also on the unique requirements of each industry and its market.

Data sovereignty is also a critical point to take into consideration. As regions have distinct data protection standards influenced by national security priorities, ensuring data sovereignty means keeping sensitive information within national borders under stringent local regulations, vital for maintaining public trust and legal compliance.

The challenge for CISOs is to ensure strong cybersecurity, whether it is on cloud, on-prem, and/or through hybrid environments. This often means using multiple solutions from different providers, making it difficult to manage and integrate them. Having a single, unified console to gain a holistic view of their entire IT infrastructure is key for effective management and security. It also helps teams save time and better manage resources to ensure robust security. However, having a single and unified XDR platform that fully addresses any environment is not easy task.

Extending cybersecurity offer to organisations with On-Premises environments to address every scenario: TEHTRIS singular approach!

Recognizing these complex challenges, TEHTRIS has always offered cybersecurity solutions for either cloud, on-premises or hybrid environments. However, in order to address CISO's market-driven, technical and data-centric challenges, TEHTRIS has decided to go one step further: offering organisations cybersecurity for a full on-prem coverage. This strategic move ensures that organizations can tailor their cybersecurity strategies to their specific needs, leveraging the flexibility and strengths of both environments. Unlike many cybersecurity providers who either offer cloud solutions or on-prem solutions, often for limited products, TEHTRIS offers comprehensive on-premises support across all modules of its TEHTRIS XDR AI PLATFORM, interoperable with others security solutions that companies may have, and regardless of whether their environment is in the cloud, on-premises or hybrid. This unique capability allows TEHTRIS to deliver robust, adaptable, and compliant cybersecurity solutions to meet the diverse demands of each organisation.

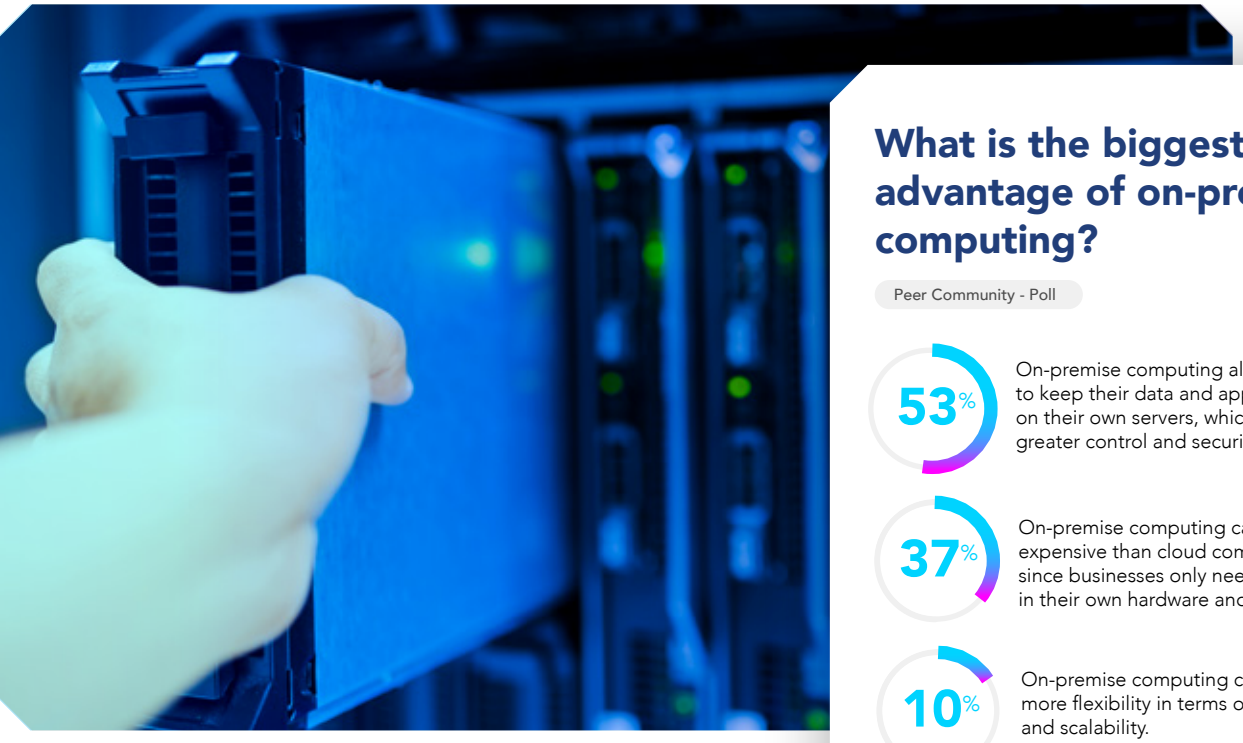


CHAPTERS

1

Cutting-edge security for on-prem perimeters

The business value and benefits from a single cloud-based **XDR AI PLATFORM** features delivered on-prem



What is the biggest advantage of on-premises computing?

Peer Community - Poll

On-premise computing allows businesses to keep their data and applications on their own servers, which can provide greater control and security.

On-premise computing can be less expensive than cloud computing since businesses only need to invest in their own hardware and software.

On-premise computing can offer businesses more flexibility in terms of customization and scalability.

4303 views - 540 participants

Source: Gartner (https://www.gartner.com/peer-community/poll/biggest-advantage-premises-computing)

Many factors, such as data protection, compliance, IT legacy systems, and managing multiple suppliers within budget constraints, make on-premises environments an attractive option for organizations seeking to enhance their security.

Cybersecurity providers offering a unified security solution on a single platform that can address all types of environments (cloud, on-premises, hybrid) are rare.

However, while many cybersecurity vendors offer on premise solutions, these are often limited to a single product. Cybersecurity providers offering a unified security solution on a single platform that can address all types of environments (cloud, on-premises, hybrid) are rare. For organizations with on-premises environments, it is even more difficult to find security solutions that provide a holistic overview of their systems and network, offering protection across all modules of an XDR platform.

Having a single XDR platform powered by AI provides numerous advantages and business value, especially when built with ethics by design and privacy by default models.

1.1 Protecting your data

When selecting a cybersecurity solution, decisions are often based on factors that may not fully address all needs for data protection. However, prioritizing data protection is becoming increasingly important for organizations. Regulations governing data are stricter than ever, making on-prem solutions more attractive. Additionally, on-prem options reduce cybersecurity risks associated with your data and your clients' data.

On-prem solutions offer the highest level of control over your data compared to other integration options for cybersecurity tools. By choosing on-prem, you gain full control over your organization's hardware and software, and therefore, your data.

A recent poll conducted by Gartner in its Peer Community confirmed this trend:

Shield your data: Encryption beyond the cloud

When choosing to go on-prem to protect your data, it is essential to ensure that your cybersecurity providers encrypt your data, even if you are not using the cloud. In our case, we have conceived the **TEHTRIS XDR AI PLATFORM** in a way that allows it to keep your data encrypted both in transmission and at rest. This is a choice to provide full traceability and ensures that sensitive information is always protected. Constant encryption guarantees that data remains secure against unauthorized access and breaches.

1.2 Achieve seamless compliance

Using an on-premises option enables companies to meet all compliance requirements. Data processing and storage, especially in Europe, are subject to numerous compliance requirements that are difficult to achieve using an external cloud. With an on-prem cybersecurity solution, data remains in the organization's country and is not subjected to the data transfer laws that complicate daily operations.

Furthermore, country regulations and requirements add complexity. For example, in Europe, requirements are high when it comes to data processing and storage (GDPR, NIS 2, etc.). Using on-premises instead of the cloud ensures that the customer complies with these requirements. The choice of your cybersecurity provider must consider under which regulation it falls into.

The on premise TEHTRIS XDR AI PLATFORM, for example, is European-based where stringent regulations are upheld. This means it is not subject to the US Cloud Act, ensuring your data is fully protected.

TEHTRIS XDR AI

With the **TEHTRIS XDR AI PLATFORM On-Premises**, you will benefit from:

- Endpoint protection with our EDR
- Monitoring and correlation of logs with SIEM
- Tools to boost investigations: Threat Intelligence, Sandboxes
- Anticipating attacks with our Honeypots (Deceptive Response)
- Continuous network analysis with NTA
- Prioritizing alerts to support SOC teams with CYBERIA eGuardian

1.3 Minimize Suppliers, Maximize Savings

This advantage is unique to TEHTRIS. Unlike other on-prem cybersecurity solutions, TEHTRIS has invested in its technology to provide on-premises cybersecurity services not just for specific products, as many providers do, but for all TEHTRIS XDR AI PLATFORM modules on-premises.

What does this mean for you? Typically, choosing an on-premises solution means that most cybertech companies provide only a single cybersecurity tool on-premises. Consequently, to achieve comprehensive coverage of your infrastructure, you would need to source additional tools from multiple suppliers, creating a complex and costly cycle. TEHTRIS puts an end to this challenge by offering the complete TEHTRIS XDR AI PLATFORM on-prem. This means you gain access to all our modules, ensuring full protection for your organization without the hassle of multiple suppliers. Additionally, our product innovations and updates are consistently available on-premises, keeping your security measures cutting-edge.

To achieve comprehensive coverage of your infrastructure, you would need to source additional tools from multiple suppliers, creating a complex and costly cycle.

For example, in Europe, requirements are high when it comes to data processing and storage (GDPR, NIS2, etc.). Using on-prem instead of the cloud ensures that the customer complies with these requirements. The choice of your cybersecurity provider must consider under which regulation it falls into.

1.4 A fortified Defense: Reducing cyberattack risks

In the current digitalization of organizations, the risks of cyberattacks have been growing, especially with the increased use of IoT devices in companies, which made the attack surface larger and harder to cover. In the next chapter, we provide examples, pending your industry, that illustrate recent cases.

Using on-premises cybersecurity solutions gives organizations a unique opportunity to lower their risks of being victims of a cyberattack. With an on-premise option, you are not dependent on an internet connection or a functioning cloud. As an example, the TEHTRIS XDR AI PLATFORM is even designed to minimize internet network exposure to significantly reduce the attack surface. You will benefit from a secure environment with limited exposure to potential online threats, ensuring the resilience of your IT infrastructure.

1.5 Cost control: Secure your investment with transparent and predictable costs

The cybersecurity of your company comes at a cost. Choosing between all the different vendors for on-premises security can quickly become a complex decision.
The advantage of on-premises options lies in their predictability: once selected, you have a clear understanding of the long-term expenses for your organization. After purchasing your on-premise solution, you only have to care about maintenance, and not about the costs of ongoing fees. These recurring fees can often exceed the initial cost of an on-prem purchase. Additionally, on-premises solutions leverage your existing IT infrastructure, avoiding extra costs for third-party services such as compute resources and support.

1.6 Flexible integration: Tailored to your needs

On-premises solutions are easily integrated in your existing systems. With this option, you can truly leverage your existing IT infrastructure and avoid the costs of deploying an entirely new system. On-prem solutions are flexible and can easily be customized to fit your network infrastructure and specific policies.

With it, the unique needs of each customer are met, including the integration of third-party tools. TEHTRIS XDR AI PLATFORM excels in integrating IT and OT information systems on-prem, from legacy systems to the latest technologies. It supports both off-the-shelf and tailored implementation capabilities, ensuring seamless integration and modernization of existing infrastructures. This approach guarantees that organizations can maintain operational continuity while enhancing their security posture.

2

Market industries' expectations for On-Premises approach

In the current cyber landscape, certain industries face unique challenges that make an on-premises cybersecurity a must-approach and in some cases mandatory. These sectors, including government and public organisations, financial services, healthcare, critical infrastructures, and manufacturing, encounter specific risks that necessitate robust, localized security measures. Depending your industry sector, this section explore unique cybersecurity requirements.

Governments and Public organisations

Sovereignty in cybersecurity:
A crucial consideration for governmental orga-nizations

For instance, the French government's decision to ban Microsoft 365 products for internal use underscores the importance of maintaining control over sensitive data.

The French authorities were particularly wary of the potential for data to be accessed by US government agencies under the Cloud Act. Similarly, the inability to host MS Teams on-premises, unlike its predecessor Skype for Business, prompted many privacy-conscious organizations to seek alternatives that offer greater control over their data.

2.1 Governments and public organisations

Governments and public sector entities are increasingly aware of the critical need to safeguard their data. In response to the global surge in cyber-attacks and heightened demands from citizens for data protection, many public sector organizations are more and more shifting away from cloud-based software towards on-premises solutions. This move is driven by the desire to enhance security and maintain better control over sensitive information.

In cybersecurity, sovereignty is paramount for governmental organizations. The 2018 US Cloud Act highlights the importance of this issue, as it allows US government agencies to request access to data held by US-based companies, regardless of where the data is stored.

Sovereignty in cybersecurity: A crucial consideration for governmental orga-nizations

Data sovereignty refers to the concept that information is subject to the laws and governance structures within the nation where it is collected. In cybersecurity, sovereignty is paramount for governmental organizations. The 2018 US Cloud Act highlights the importance of this issue, as it allows US government agencies to request access to data held by US-based companies, regardless of where the data is stored. This has led to significant concerns about data privacy and sovereignty, especially for non-US entities.

For instance, the French government's decision to ban Microsoft 365 products for internal use underscores the importance of maintaining control over sensitive data.

The French authorities were particularly wary of the potential for data to be accessed by US government agencies under the Cloud Act. Similarly, the inability to host MS Teams on-premises, unlike its predecessor Skype for Business, prompted many privacy-conscious organizations to seek alternatives that offer greater control over their data.

The Rising Threat of Cyber Attacks

For example, in March 2024, the Russian hacker group APT29 waged phishing attacks against German political parties by concealing ransomware in fake dinner invitations to install backdoors in the victims' computers. The effort was to build long-term access and exfiltrate data.

In the same month, after a cyber incident by an unidentified attacker, Canada had to take its financial intelligence system, the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), offline.

Increased data security and privacy compliance

Globally, companies aim to preserve their business reputation by adhering to region-specific and industry-specific privacy regulations. Public sector organizations, under intense scrutiny regarding privacy compliance, set the standard for these practices. As citizens demand improved services and increased transparency, these organizations seek to justify and enhance public trust. Consequently, privacy-conscious organizations, including those in the public sector, are increasingly opting for on-premises software solutions.

The Rising Threat of Cyber Attacks

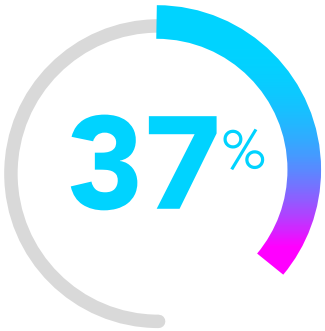
Governments and public organizations are top targets of cyber attackers. For example, in March 2024, the Russian hacker group APT29 waged phishing attacks against German political parties by concealing ransomware in fake dinner invitations to install backdoors in the victims' computers. The effort was to build long-term access and exfiltrate data.

In the same month, after a cyber incident by an unidentified attacker, Canada had to take its financial intelligence system, the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), offline.

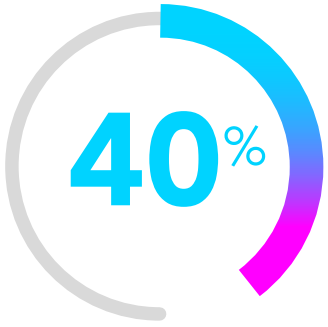
The imperative for data sovereignty cannot be overstated. National security threats demand that sensitive information remains within national borders, safeguarded under stringent governmental protocols which explains the choice for on-premises solutions enabling control and security to protect classified information and maintain public trust.

On-Premises: hosting trends

Research indicates that 37% of non-SaaS applications are run exclusively on-premises, with an additional 40% using a hybrid approach. This trend highlights the popularity of on-premises solutions in highly regulated sectors, including government and public sector organizations, due to their enhanced control over data privacy, security, and sovereignty. Governments worldwide are on the frontlines of national security, tasked with defending against a plethora of threats ranging from cyber espionage to outright cyber warfare.



Research indicates that 37% of non-SaaS applications are run exclusively on-premises



an additional 40% using an hybrid approach

Source: Source: Red Hat 2022 Global Tech Outlook

Financial Services

2.2 Financial Services

The financial services industry - operating under a complex web of compliance regulations including GDPR, DORA, and various national banking standards like PCI DSS - is one of the industries most subjected to contractual or regulatory constraints, yet it is also the sector with the most maturity regarding security. These institutions are frequent targets of sophisticated cyber-attacks due to the high value of financial data they handle. In this section, we will explore why some financial organizations opt for on-premises.

Maintaining reputation and credibility:

Financial institutions are also held accountable to higher standards of consumer trust by safeguarding customers' money and data. Failing to do so can severely dent a financial services organization's reputation and credibility. Moreover, cyberattacks can lead to expensive penalties for financial institutions. For example, Equifax paid over $1 billion in penalties after a data breach in 2017.

According to the International Monetary Fund, the **financial sector has survived over 20,000 cyberattacks** over the last two decades, and consequently suffered $12 billion in losses. These establishments are a lucrative target for cyber attackers.

Financial sector has survived over 20,000 cyberattacks

According to the International Monetary Fund, the financial sector has survived over 20,000 cyberattacks over the last two decades, and consequently suffered $12 billion in losses. These establishments are a lucrative target for cyber attackers.

Data Residency and Sovereignty

Certain jurisdictions mandate that sensitive financial data be stored within the country's borders, such as FINRA for the US or DORA for Europe. This requirement can pose significant challenges for cloud providers with global data centers, making it difficult to comply with local data residency laws. As mentioned earlier in the context of public organizations, data sovereignty is critical. The US Cloud Act, which permits US government agencies to access data from US-based companies regardless of where it is stored, heightens concerns about data privacy for financial institutions. Consequently, many banks prefer on-premises solutions to ensure their data remains within national borders and safeguarded from external access.

Adherence to Industry Standards

The financial services industry is governed by stringent regulatory requirements, including unique data encryption standards and transaction handling procedures. Cloud providers do not universally support these specialized standards, which can complicate compliance for banks.

Customized Security Protocols

Banks need to implement specific security protocols tailored to their compliance and operational requirements. Adapting these protocols to a cloud environment can be complex and often requires close collaboration with cloud providers. In-house solutions enable banks to apply tailored security measures and maintain full control over their data, thereby reducing exposure to external vulnerabilities.

Integration with Legacy Systems

Many banks operate with legacy systems that are deeply embedded in their infrastructure. Transitioning these systems to the cloud is a complex task that can disrupt operations. On-Premises solutions allow banks to integrate legacy systems seamlessly, ensuring business continuity without the complications of cloud migration.

Healthcare

2.3 Healthcare

There are numerous reasons why the healthcare industry prefers on-premises solutions. This section will explore the motivations behind this preference, which also influenced TEHTRIS to expand its cybersecurity offerings for organizations like the healthcare sector seeking to adopt on-premises solutions.

Safeguarding Patient Data and Compliance

Cyberattacks like the one on Change Healthcare, the largest US billing and payments system, disrupt the processing of millions of prescriptions and services, delaying critical access to medication and care. Even two months later, an AHA survey revealed that many medical practices would be compelled to close because of lost revenue from unpaid claims. The attack is expected to cost up to $1.6 billion.

These deeply consequential and dire cyberattacks on healthcare systems are growing because of vulnerabilities in healthcare systems. The European Repository of Cyber Incidents recorded an increase in such attacks from 32 events in 2022 to 121 in 2023.

Safeguarding Patient Data and Compliance

Healthcare organizations are custodians of highly sensitive patient data, subject to strict regulations such as HIPAA in the United States and GDPR in Europe. Protecting this data is paramount not only for compliance but for maintaining patient trust.

Cyberattacks like the one on **Change Healthcare**, the largest US billing and payments system, disrupt the processing of millions of prescriptions and services, delaying critical access to medication and care. Even two months later, an AHA survey revealed that many medical practices would be compelled to close because of lost revenue from unpaid claims. The attack is expected to cost up to $1.6 billion.

These deeply consequential and dire cyberattacks on healthcare systems are growing because of vulnerabilities in healthcare systems. The European

Cyberattacks like the one on Change Healthcare

Repository of Cyber Incidents recorded an increase in such attacks from 32 events in 2022 to 121 in 2023.

On-premises cybersecurity solutions allow healthcare providers to implement customized security protocols tailored to their unique needs, ensuring robust protection of sensitive health information and compliance with regulatory requirements. Data sovereignty in healthcare is particularly crucial, as different regions may have specific legal mandates regarding patient data storage and access.

On-premises cybersecurity solutions allow healthcare providers to implement customized security protocols tailored to their unique needs, ensuring robust protection of sensitive health information and compliance with regulatory requirements.
Data sovereignty in healthcare is particularly crucial, as different regions may have specific legal mandates regarding patient data storage and access.

Performance and cost management

On-premises solutions can offer better performance and lower latency compared to cloud-based solutions, which is crucial for real-time medical applications, imaging, and telemedicine services. This ensures that healthcare providers can deliver timely and efficient care. While cloud solutions offer scalability, they often come with unpredictable costs based on usage. On-premises solutions provide more predictable cost management, allowing healthcare organizations to plan their budgets more effectively without unexpected expenses from cloud service providers.

Customization, flexibility, and regulatory adaptability

Healthcare organizations often require highly specific configurations for their IT systems to meet unique operational needs. On-premises solutions provide the flexibility to customize systems extensively, which can be more challenging in a cloud environment where configurations are often standardized. Maintaining patient trust is critical for healthcare organizations, and high-profile data breaches can severely damage a healthcare institution's reputation. On-premises solutions, by offering enhanced security and control, help in safeguarding this trust and maintaining the organization's reputation. Additionally, healthcare regulations are subject to change, and keeping up with these changes can be easier with on-premises solutions. These solutions offer the flexibility to quickly adapt to new regulatory requirements without relying on third-party cloud providers to update their compliance measures.

The unique challenges of integrating legacy systems, ensuring high availability and performance, managing costs projection, and adapting to regulatory changes drive healthcare organizations to favor on-premises solutions. However, these solutions require robust cybersecurity measures that offer a holistic view of the various events across their IT infrastructure. The TEHTRIS XDR AI PLATFORM enables healthcare providers to achieve this comprehensive protection, ensuring their data remains secure and compliant with regulatory standards should they decide to opt for an On-Prem solution.

Critical infrastructures

2.4 Critical infrastructures

Critical infrastructure sectors, including energy, utilities, and transportation, are essential to national security and economic stability. These sectors are increasingly targeted by state-sponsored and sophisticated cyber-attacks with the potential to disrupt vital services.
Vital systems include all assets, systems and networks - both physical and virtual - that are essential to the proper functioning of a society's economy, public health, safety, and security. This includes food and agriculture sectors, transportation systems (e.g., roads, railways, highways, airports), water supply (e.g., drinking water, wastewater/sewage), internet and mobile networks, public health (e.g., hospitals, ambulances), energy (oil and gas), electric utilities, financial services, telecommunications, defense, and more.

Increasing cyber threats

US Environmental Protection Agency (EPA) recently revealed that cyberattacks are on the rise without providing further data, their recent report from September, 2023 also revealed that water systems surveyed failed to meet security standards. When onsite, EPA discovered some facilities having critical vulnerabilities such as unchanged default passwords, prompting the agency to urge water system operators to enhance their cybersecurity measures.

Attacks are on the rise

Hacktivist attacks against European infrastructure that aim to cause disruption have doubled from Q4 2023 to Q1 2024. The increased digitalization of energy systems makes them more beneficial for consumers but also leads to increased exposure to cyberattacks. **The European Commission**, recognizing this persistent threat to critical infrastructures, published the first-ever network node on cybersecurity for the electricity sector in May 2024.

Additionally, critical infrastructure often encompasses industrial control systems (ICS), including supervisory control and data acquisition (SCADA) systems, which automate industrial processes. Attacks against SCADA and other ICS pose significant risks, potentially causing wide-scale compromise in vital systems, such as transportation, energy, and water distribution.

Challenges and the role of on-premises solutions

On-premises cybersecurity solutions offer these industries enhanced security and control needed to protect their systems against these high-level threats. By keeping security operations in-house, these sectors can better defend against attacks that could have catastrophic consequences.

Data sovereignty in critical infrastructures is crucial, as different states may have distinct protocols for managing and protecting infrastructure-related data.

Challenges to securing control systems in critical infrastructure include gaining granular visibility over network traffic, segmenting networks to limit attack vectors, protecting unpatched systems, preventing advanced cyberattacks, managing disjointed security products, securing IoT devices, and complying with regulations like NERC CIP and NIST CSF.

Governments and agencies responsible for critical infrastructure are evolving to meet cyber risks and the diverse needs for more data for more users in more places than ever. Initiatives such as «Smart Government» are driving innovative approaches to data use and real-time data integration from various sources, necessitating new cybersecurity considerations.

To effectively protect today's SCADA and ICS networks in critical infrastructure, a modernized security approach is necessary.

Manufacturing

2.5 Manufacturing

The manufacturing sector, particularly those involved in critical infrastructure, is a growing target for cyber espionage and ransomware attacks. The implications of such breaches extend beyond economic loss to potential national security risks.

Preventing cyberattacks:

Manufacturing facilities can't run SaaS security services as sometimes there's no operating system to install such services. The lack of proper cybersecurity in manufacturing infrastructure can lead to horrendous incidents, such as when Simpson Manufacturing Company faced a cyber attack in October 2023, leading to prolonged system outages. Another example is from Applied Materials, which suffered a supply-chain ransomware attack in February 2023, resulting in significant shipment disruptions and a $250 million loss in sales.

On-premises cybersecurity solutions enable manufacturers to deploy stringent security measures, closely monitor their systems, and respond rapidly to threats. This proactive approach is essential for minimizing disruption and protecting valuable intellectual property and production processes. Additionally, data sovereignty is vital in manufacturing, as different countries may impose specific requirements on how data generated by manufacturing processes is stored and managed.

42% of organizations surveyed in the US are either considering or already have moved at least half of their cloud workloads to on-premises infrastructures, a phenomenon called cloud repatriation. Such change would require companies to get holistic and unified cybersecurity for their on-premises infrastructure.

42%

of organizations surveyed in the US are considering or moved cloud data to On-Premises

Source: Helpnetsecurity 2024 Cloud repatriation projects-reasons

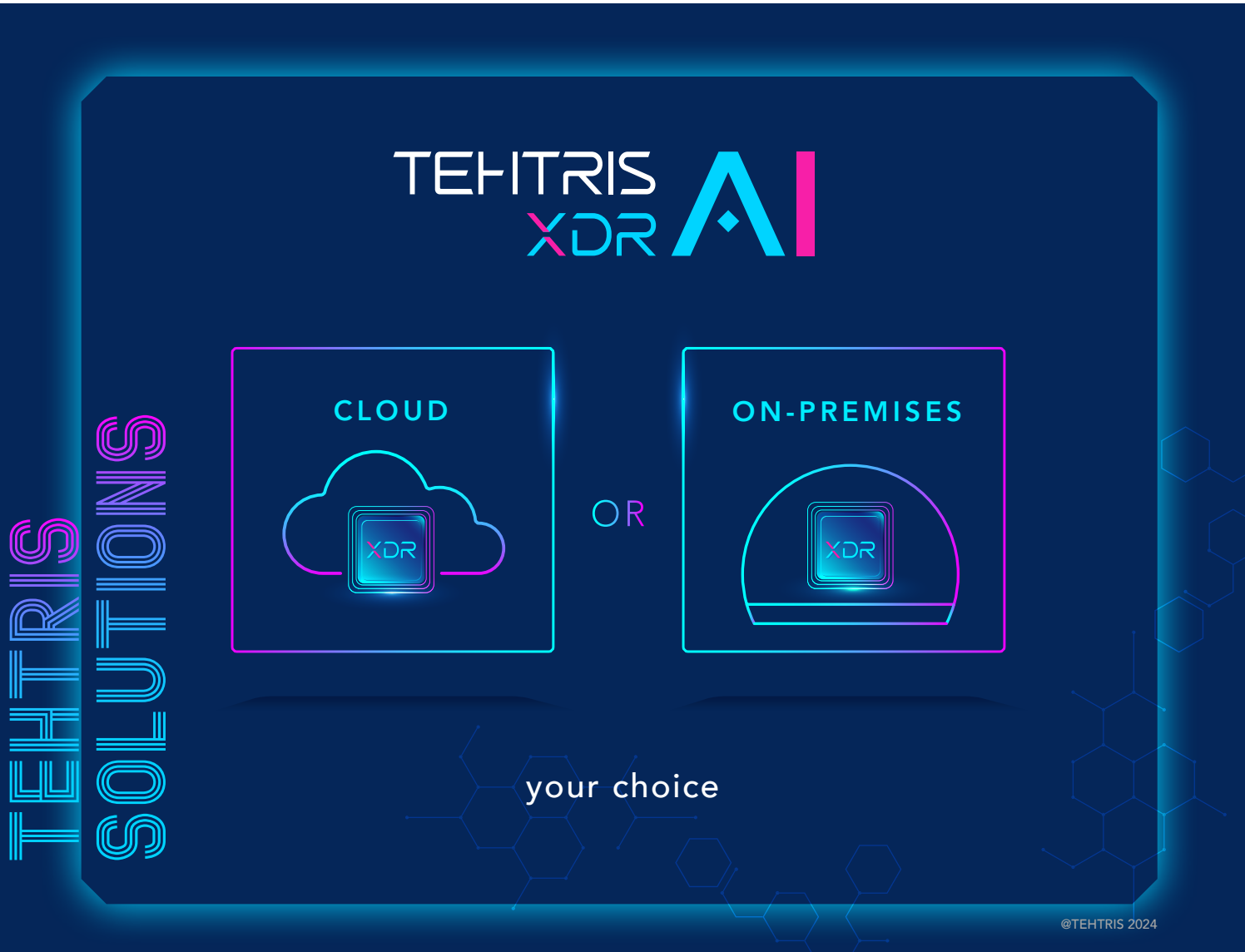
3

TEHTRIS XDR AI PLATFORM and solutions

A single console for global orchestration and security

Unify your cybersecurity by bringing together all your solutions in a single console for high-speed detections and responses. Within the TEHTRIS XDR AI PLATFORM, you will find an **EDR**, **MTD**, **SIEM**, **Honeypots**, **NTA**, **CYBERIA**, **Threat Intel**, **Zéro Trust Response**, **Email Protection** and **Identity Access Management**.

Orchestrate all your cybersecurity tools simultaneously, including your existing solutions such as Zscaler and Proofpoint, with the TEHTRIS XDR AI PLATFORM. Our platform is available in our secured cloud or on-prem. Easily deploy it in your ecosystem with in & out APIs. With its customizable playbooks and its hyperautomation capabilities you will get immediate response to cyberattacks.



@TEHTRIS 2024

TEHTRIS SOAR

Orchestrate all your solutions and enable Hyperautomation at the service of your teams

Saving time is essential when remediating attacks. In order to achieve this objective, TEHTRIS has designed its own SOAR. Perfectly integrated into the XDR Platform, our SOAR orchestrates the actions of your cybersecurity tools and automates them. Combined with CYBERIA (artificial intelligence), the detection, contextualization and response to incidents are hyperautomated.
Supported in its decision making and freed from repetitive tasks, your SOC gains decisive seconds during cyberattacks.
Interoperate your cybersecurity for augmented and hyperautomated remediation.

TEHTRIS SOLUTIONS

CYBERIA

Enhance your cybersecurity with our artificial intelligence. With CYBERIA, you are protected from threats undetectable by humans.

Addressing the pressing challenges faced by cybersecurity experts, TEHTRIS has invested and developed its proprietary Artificial Intelligence: TEHTRIS CYBERIA, a multi-modular AI and a cornerstone component of TEHTRIS XDR AI Platform.

Overcoming cyber security workforce shortage and fatigue, TEHTRIS CYBERIA is embedded through TEHTRIS XDR AI Platform, offering hyperautomation of real-time detection, triage of every single alert, without compromise, remediation, without human intervention VS traditional approaches based on use-cases and filters creating blind spots: a safer alternative to cyber solutions currently offered on the market.

ABOUT TEHTRIS

Founded in 2010, TEHTRIS is the publisher of the TEHTRIS XDR AI PLATFORM, global leader in the automatic detection and neutralization of cyber espionage and cyber sabotage, in real-time and without human action.

With its «Zero Trust» approach and a unique «Security & Ethics by design» concept, TEHTRIS supports organizations of all sizes and sectors, guiding them to anticipate and confront the unpredictable and become exemplary guardians of their cyber space.

Deployed all over the world, the TEHTRIS XDR AI PLATFORM provides cybersecurity specialists with a holistic view of their infrastructure while ensuring the confidentiality of their data. By ensuring real-time detection and neutralization of cyber attacks, ransomware, and malicious behaviours without requiring human intervention, it also guarantees interoperability with market security solutions via its APIs.

The company continues to enrich its Threat Intel database through globally deployed sensors, ensuring high-level contextual detection and security alert prediction, thanks to behavioral analysis and its TEHTRIS CYBERIA Artificial Intelligence. Compliant with all relevant regulations, including GDPR and NIS2, TEHTRIS provides organizations with the confidence needed to tackle cybersecurity challenges, thereby enhancing their defensive posture against active and emerging threats.

With its 8 subsidiaries and the global deployment of the TEHTRIS XDR AI PLATFORM, TEHTRIS realizes its concept of a 'follow the sun' service, enabling real-time monitoring of its clients' infrastructures and 24/7 support through its CyberSphere offer.

Alongside its international partners, the TEHTRIS XDR AI PLATFORM monitors, analyzes, detects, and neutralizes threats worldwide for key players in industry, transport, engineering, services, and public administrations. In November 2020, TEHTRIS achieved a record fundraising in cybersecurity by securing €20 million in Series A and a second fundraising of €44 million in Series B from sectoral investors. TEHTRIS is actively recruiting to accelerate its development and pursue its technological research strategy.

Constantly vigilant on cybercrime trends and attentive to its clients, TEHTRIS helps minimize risks and progress towards its vision of reinventing cybersecurity to secure freedom for all and everywhere.

Follow us on:

LinkedIn Twitter Youtube

tehtris.com

Newsletter

@TEHTRIS 2024