EVERFOX

Proactive Cybersecurity
Taking Center Stage

CYBER360

2025

Foreword

Government, defense and regulated industries are facing an onslaught of sophisticated cyberattacks.

Over the past 12 months, entities in these industries experienced, on average, a staggering 127 cyberattacks per week.

And these are the ones they know about, with polymorphic malware and zero-day attacks rendering it near impossible to detect some attempts. AI is also accelerating, automating attacks, making them faster and more scalable.

Our research of 1,000[1] senior security leaders and IT security professionals working in government, defense and regulated industries with Opinion Matters found that the high cost of this cyber threat landscape is untenable. Over the past 12 months, the regulated industries that we spoke to in the U.S. and U.K. that fell victim to a cyber incident paid, on average, over $531,000 in recovery costs. And this number does not account for the risk of reputational damage, compromised personally identifiable information, and potential legal consequences for security leaders.

While we should not be normalizing this threat environment, it has unfortunately become the new norm.

The detection-based security technologies that most companies rely on cannot keep up with the increase of sophisticated threats, particularly in a world where interconnectedness and data sharing underpin everything from service delivery within regulated industries to intelligence alliances.

IT security directors in government, defense and regulated industries recognize this fact, with 71% stating detection threat technology comes too late, as the damage is already done.

Instead, **78% believe security teams in these industries need to shift their mindset from detection to prevention**, with an increased awareness of how users interact with data, systems and each other.

Preventative cybersecurity technologies stop threats before they can reach your system or data, rather than just detecting and responding after they've caused damage.

Our CYBER360 report demonstrates the critical role these emerging technologies must play in the next generation of these organizations' cyber defenses.

Read on to learn how the cat-and-mouse game that detection-based cybersecurity solutions have created is falling short in this sophisticated cyber and digital landscape, why IT security leaders are turning to preventative security technologies to overcome this risk, and how to overcome the barriers – from legacy infrastructure to the necessary mindset shift – to making this change.

Sean Berg
Chief Executive Officer | Everfox

"It's like leaving your front door unlocked.

Would you prefer to **detect** someone coming into your house, or **prevent** them from getting in?"

Petko Stoyanov
Vice President of Product Strategy | Everfox

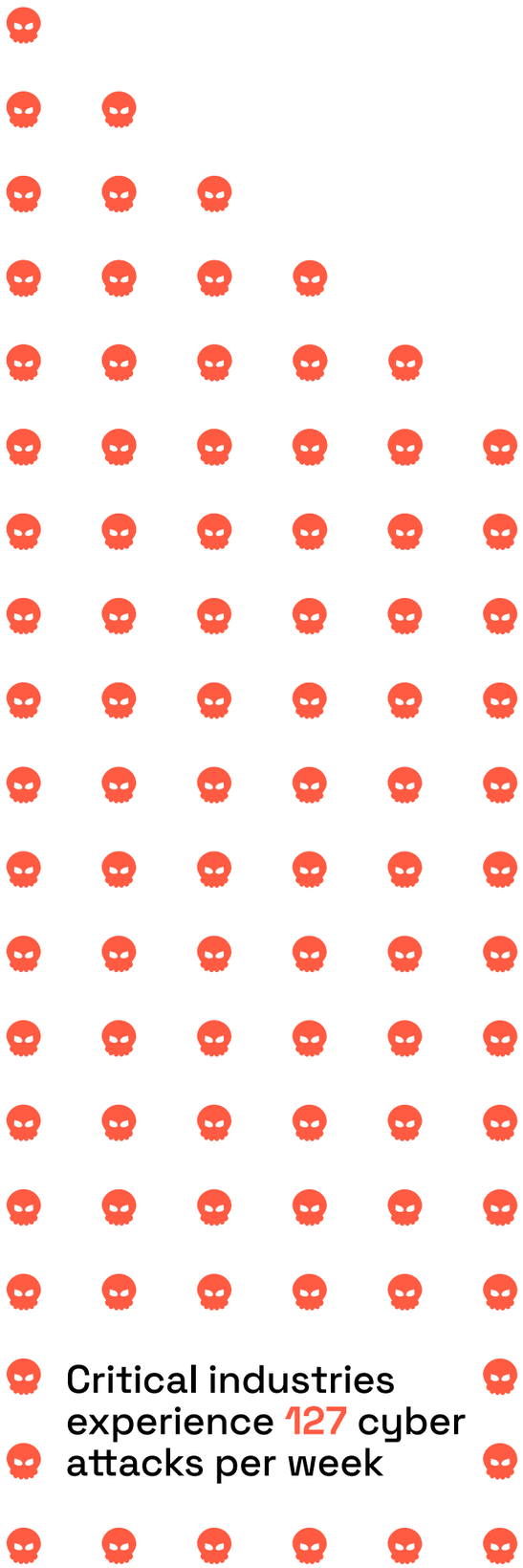
[1] All figures and percentages are based on Everfox Holdings LLC ("Everfox") research and may not be used for any other purposes or by any other entity without Everfox's express written permission.

The **Cyber Onslaught** on Highly Regulated Industries

To those working in the industry, it will come as little surprise that cyber incidents are at an all-time high. Government, defense, finance, and other regulated industries such as energy and healthcare, are facing an unrelenting barrage of threats.

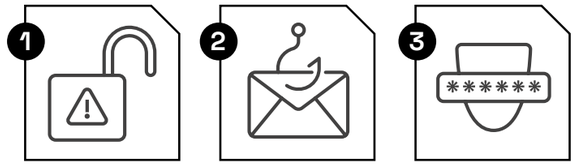
In the last year, 97% of organizations in the government, defense and regulated industries that we polled suffered a cyber-incident.

And they consistently face a huge number of attacks; on average, these industries experience 127 known cyberattacks per week, rising to 135 attacks on defense and 156 attacks on healthcare organizations. However, these are only the attacks that these organizations are aware of or informed us of - the actual figure is likely much higher.



Critical industries experience 127 cyber attacks per week

When looking at the types of attacks these organizations were most commonly subjected to, the top three vectors were consistent between 2023 and 2024:



1. **Exploited Vulnerabilities**
2. **Phishing Attacks**
3. **Compromised Credentials**

These longstanding security challenges continue to plague security teams. Not only has there been a 17% year-on-year increase in the volume of vulnerabilities, with a new vulnerability published every 17 minutes, but 75% of Common Vulnerabilities and Exposures (CVEs) are exploited within the first 19 days of being published.[i]

But these more common attack vectors are not the only ones consistently targeting regulated industries. Over the past year...

20% **suffered a compromise via the supply chain, rising to 27% for government organizations.**

The growing importance of interconnectedness and sharing access and data for service delivery, compliance and operations in hybrid working compounds the importance of secure data sharing with partners.

17% **of organizations in regulated industries suffered a zero-day attack.**

This attack exploits previously unknown vulnerabilities and is unstoppable by detection-based defenses, leaving systems defenseless until a patch is developed and implemented.

16% **of organizations suffered an insider incident.**

This demonstrates how cybersecurity must be implemented to also protect from within. In fact, our research found security leaders report increasing insider threats as their top challenge and primary security concern for securing data, systems, people and networks.

Financial services firms are also highly concerned about the risk of an employee, contractor, or other trusted individual exploiting their authorized access to harm their organization. 33% cite it as one of the main cybersecurity challenges they face compared with 27% in the regulated industries more broadly.

33%

of organizations within Financial Services cite their main concern is the risk of an employee, contractor, or other trusted individual exploiting their authorized access to harm their organization.

As cyberattacks continue to escalate, it leaves the question of whether our defenses are keeping up with the evolving threat landscape.

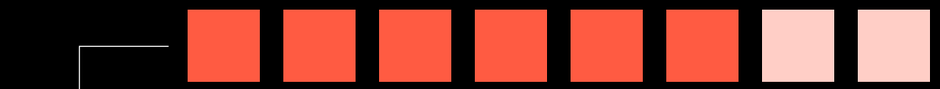
Weaponized Complexity

It's not only the volume but the growing sophistication of threats which is causing concern, with **62% of organizations in regulated industries recognizing that sophistication is increasing year-on-year.**

Half of IT Security Directors in these industries called out the increasing sophistication of threats as one of the main challenges they face in securing networks against cyber threats.

1/2 of IT Security Directors say increasing sophistication of threats is one of their main challenges

And they believe the primary reason for this is the continued reliance on failing detection-based technologies, such as detection-based Content Disarm and Reconstruction (CDR) , Sandboxing and Data Loss Prevention (DLP), with 74% stating these tools can't keep up with the increase and growing sophistication of attacks.



3/4 of IT Security Directors say detection technologies can't keep up with the increasing sophistication of attacks

But what's driving the growing complexity of cyberattacks?

It's impossible not to start with the significant impact that Artificial Intelligence (AI) is having on the security landscape.

Cybercriminals are now leveraging AI to automate attacks, making them faster and more scalable.

It's also adding to the challenge of mitigating the risk of vulnerabilities, as it enables cybercriminals to analyze vulnerabilities and develop exploits in near real-time.

The scale of the threat that AI poses to the wider cyber landscape remains to be seen. But OpenAI disrupted over 20 malicious cyber operations in 2024 abusing its AI-powered chatbot, ChatGPT, for debugging and developing malware, spreading misinformation, evading detection, and conducting spear-phishing attacks.[ii]

And this likely only scratches the surface.

AI is not only revolutionizing cybercrime, adding to the challenge, but also empowering defenses with faster and more efficient solutions - though it's just one piece of the evolving cybersecurity puzzle.

A few trends that have played a prominent role over the past 12 months include:

Polymorphic Malware

Polymorphic Malware changes its appearance or behavior to avoid detection by systems which only look at known threats.

Designed to bypass anti-virus and fool sandboxing solutions, this is just one of many attack vectors that **demonstrates the limitations of relying on threat intelligence** and **where detection falls short as a defense**.

Particularly when compared to solutions that take a proactive approach focused on preventing exploitation and infection in the first place, like Preventative Content Disarm and Reconstruction (CDR), which assumes all incoming files and content are potentially weaponized, and extracts and verifies the business information to build a new, safe and fully functioning file.

Hacking-as-a-Service

Hacking-as-a-Service and open source resources increase access to malicious actors and attack vectors. The extreme end of this scale is the rise in state-sponsored cyberattacks, with governments sponsoring **Advanced Persistent Threats (APT)** for espionage, sabotage or economic advantage, with regulated industries and defense systems acting as primary targets.

Expanding Attack Services

Expanding Attack Services continue to present challenges with Internet of Things (IoT), smart devices, edge devices, and even those devices used for hybrid working.

As many as 71% of IT Risk Analysts highlighted how the increasing volume and complexity of managing endpoint security makes it difficult to meet the stringent requirements of high-assurance security environments.

71% said rising volume and complexity make it difficult to meet high-assurance security requirements

Supply Chain Attacks

Supply chain attacks continue to target the weaker links that contribute to government, defense and regulated industries service delivery or those with whom they share information.

For example, the ransomware attack on Synnovis, a pathology laboratory which processes blood tests on behalf of a number of the U.K's National Health Service (NHS) organizations, resulted in the NHS not being able to use some of its systems for running blood tests in South East London.[iii]

In the week that followed, this led to more than 800 planned procedures and more than 700 hospital outpatient appointments being postponed.[iv]

Supply Chain Attacks also focus on embedding malware into products at the source, ahead of them being used by regulated industries.

This was the case in 2020, when hackers installed malicious code into a new batch of Orion software distributed by SolarWinds, knowing it was used by many multinational companies and government agencies.[v]

The New Security Headache

It's not only external threats compounding the security challenge.

Digital transformation is creating major integration hurdles for regulated industries, with 44% of large organizations struggling to modernize legacy systems.

44% **of large organizations struggle to modernize legacy systems.**

At the same time, greater interconnectedness and data sharing are piling on additional pressure for cybersecurity professionals.

With key drivers including:

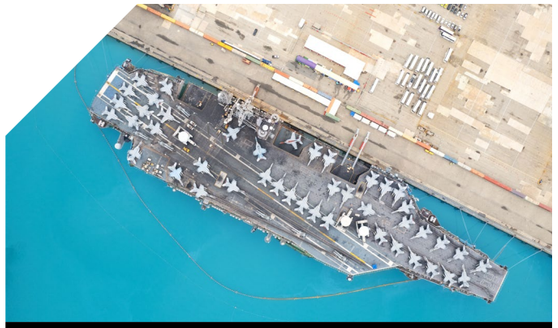
Increased Collaboration

Information and intelligence sharing both between international agencies and domestic bodies plays a critical role in national security, with 81% of IT Security Directors highlighting an increased need to share and transfer sensitive data with external parties.

81% **of IT Security Directors report a growing need to share sensitive data externally.**

This includes secure data exchanges between allied nations to identify threats from other nation-state threat actors such as NATO and The Five Eyes.[2]

Information sharing within domestic government and defense in high-risk sectors and environments is also playing an increased role. Organizations like the US's Defense Information Systems Agency (DISA), which is charged with providing connectivity for a globally deployed fighting force and its multinational coalition partners, promote a more centralized data-sharing architecture to improve data accessibility, interoperability and compliance with governance standards.



"The ability to share all forms of information rapidly and securely across US government agencies and with allies and partners with little set-up time and advance notice is more critical today than ever before.

The US must **effectively collaborate** to successfully conduct operations ranging from the potential for multinational combat operations to frequent non-combatant military operations, and Humanitarian Assistance and Disaster Relief, to routine national efforts. Successful partnership is how we have won in the past and **how we will win in the future**."

Nancy Norton
Vice Admiral, US Navy | Retired

[2] NATO is the political and military alliance of countries from Europe and North America, and The Five Eyes (FVEYs) is an intelligence alliance comprising Australia, Canada, New Zealand, the United States of America, and the United Kingdom

76%

Advanced Capabilities

The potential of new IT technologies to offer improved insights into OT data is leading to increased data sharing and access between IT and OT systems.

Take, for example, production data from OT systems which can be combined with market data from IT systems to optimize production schedules and inventory levels. However, while offering undeniable benefits, it also presents new security challenges;

Over three quarters of IT Security Directors highlighted how the increased need to access and share sensitive data between IT and OT environments significantly expands the threat landscape.

Heightened Compliance

From anti-money laundering and **Know Your Customer (KYC)** to the **Health Insurance Portability and Accountability Act (HIPAA)**, there are a growing number of compliance frameworks that require organizations to share and receive data from multiple untrusted sources, which is driving an increase in cyberattacks.

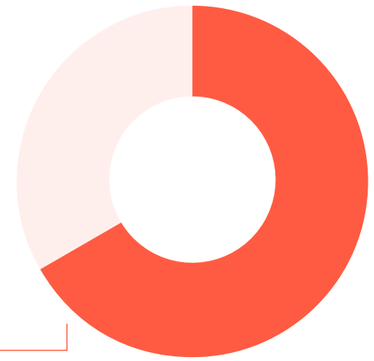
Take KYC regulations as an example, which require businesses to verify the identities of their customers.

This often involves collecting sensitive data from various sources, including credit bureaus, government databases, and utility companies.

This presents a data security challenge.

Two Thirds

of financial services organizations struggle to strike the right balance between information protection and information sharing.



These key drivers are essential to enabling the modern exchange of data and information that drives progress and collaboration across governments, regulated industries and society as a whole.

However, this interconnectedness also introduces significant cybersecurity challenges that cannot be ignored.

Balancing the need to share and receive data with the need to protect it requires a paradigm shift.

Unfortunately, many current **detection-based cybersecurity approaches are failing to meet these challenges**, leaving critical systems vulnerable to increasingly sophisticated threats.

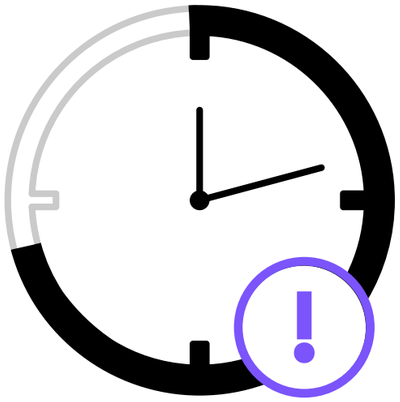
Detection is Not a Strategy

With the rise in advanced threats and sophisticated threat actors, detection is increasingly becoming outdated.

IT Security Directors can see what has worked previously is no longer the answer for modern-day and future threats.

74%

of IT Security Directors feel detection technologies are **unable to keep up** with the increasing sophistication of threats and fall short

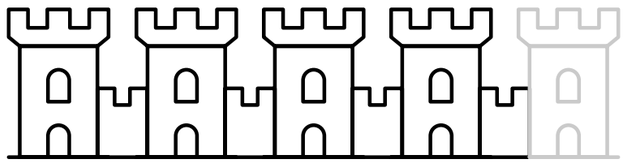


71%

believe detection threat technology comes too late - the damage is already done

4/5

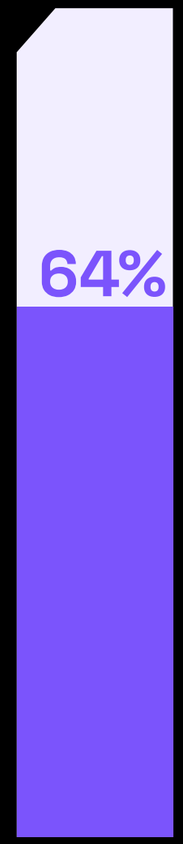
believe security teams need to **shift their mindset** from detection to prevention and focus on procuring more preventative solutions



What do IT Security Directors mean by preventative cybersecurity?

Preventative cybersecurity technology refers to systems and technologies designed to defend cyber threats before they can cause harm. Unlike detection-based approaches that identify and respond to threats after they have infiltrated a network.

64% of organizations agree that leveraging threat prevention solutions will ultimately reduce the likelihood of costly data breaches and operational disruptions



To understand what this looks like in practice, let's explore the preventative security approaches for the **most prominent threats** facing government, defense and regulated industries:

Securing Networks

The ability to securely access and transfer sensitive information between different security domains is critical for governments, defense and regulated industries and requires high assurance cybersecurity.

Cross Domain Solutions (CDS) offer a secure route for data transfer and access for high-security environments, including air-gapped networks, Multi-Level Security (MLS) systems, and Sensitive Compartmented Information Facilities (SCIFs).

These systems can support both bi-directional and unidirectional data transfers, while also integrating with other preventative software, like prevention-based CDR, to help sanitize data and files before entering your network.

Hardsec Solutions are also growing in popularity for providing enhanced protection against advanced threats, with a third of regulated industry organizations planning on implementing it into their defense plans.

What is Hardsec?

Hardsec focuses on using hardware logic and electronics to implement defenses, offering stronger security and resilience against external and insider threats compared to software alone.

Built to secure the access or transfer of data without compromise, Hardsec fortifies solutions with Field Programmable Gate Arrays (FPGA) technology to enable mission critical activities across multiple network levels.

Instead of Central Processing Units, Hardsec uses non-Turing-machine digital logic to implement physical security, bolstering the foundation of your software stack.

64%

of organizations have already adopted or are planning to implement network air gapping

One in Three

organizations are gearing up to adopt Hardsec technology to fortify their defenses

"Today's cyber adversaries are increasingly sophisticated and often cause irreparable damage leading to loss of critical Intellectual Property, personal data or malfunction of operations. Implementing robust preventive measures to protect your network, your data and your people are critical to ensure secure business operations.

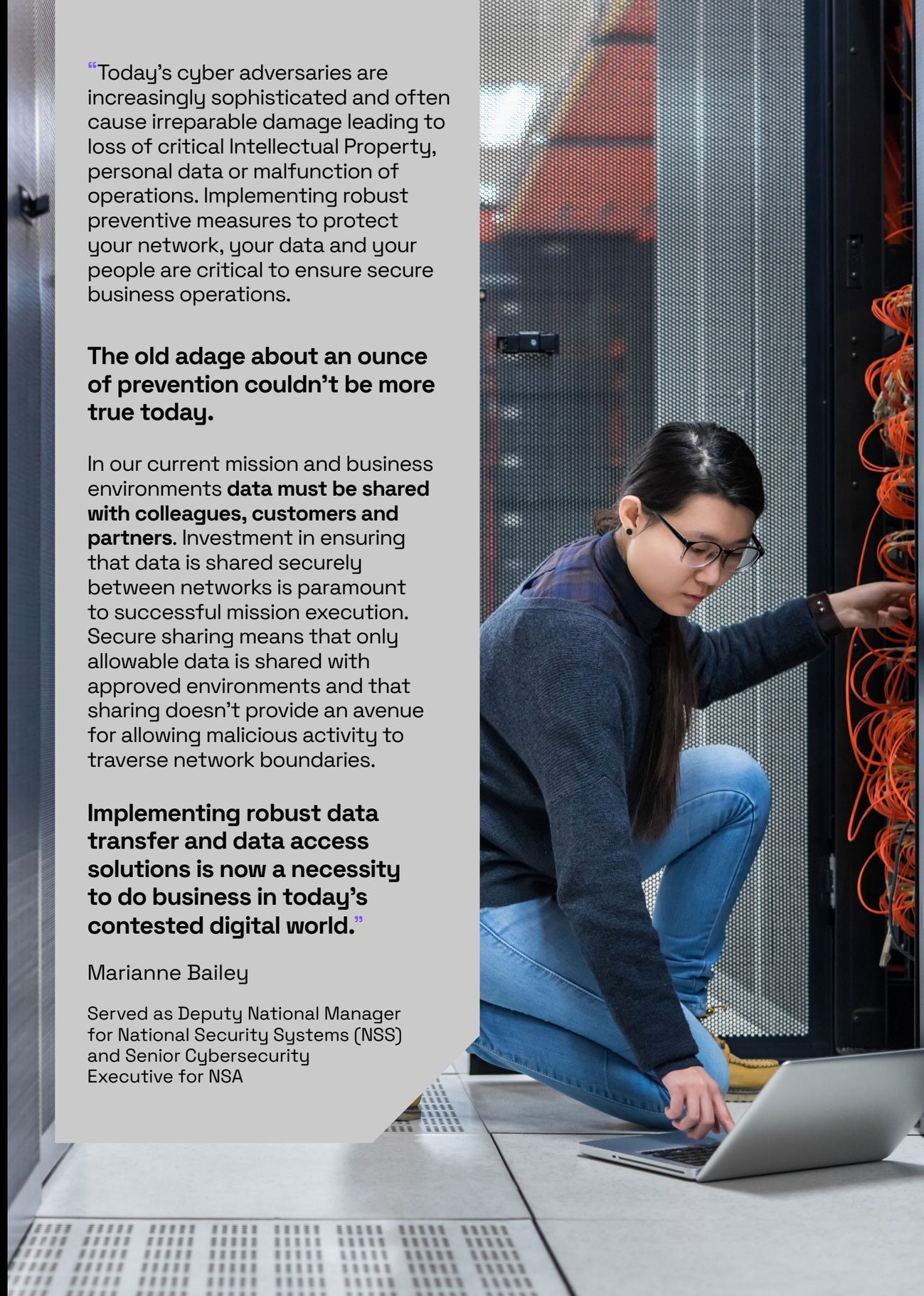
The old adage about an ounce of prevention couldn't be more true today.

In our current mission and business environments **data must be shared with colleagues, customers and partners**. Investment in ensuring that data is shared securely between networks is paramount to successful mission execution. Secure sharing means that only allowable data is shared with approved environments and that sharing doesn't provide an avenue for allowing malicious activity to traverse network boundaries.

Implementing robust data transfer and data access solutions is now a necessity to do business in today's contested digital world."

Marianne Bailey

Served as Deputy National Manager for National Security Systems (NSS) and Senior Cybersecurity Executive for NSA



Securing People

Instead of identifying instances after data has been exfiltrated, for example, a preventative security approach to the insider threat is to monitor for potential behaviors that could lead to a threat, identifying, mitigating and protecting.

This is how implementing User Activity Monitoring (UAM) and Behavior Analytics is helping to prevent an insider risk event from happening.

The benefit of this approach is that it also helps to differentiate between genuine mistakes and malicious actions among the workforce, such as Intellectual Property (IP) theft and espionage. Accidental data loss, for example, is as big a threat as malicious behavior, so implementing preventative solutions, such as access controls or triggers, is important and supports employee safety. Take a good employee trying to complete work on their holiday by sending data to their personal email address, who might not think about the significant data risk it presents.

"The insider threat incident continues to be one of the **most devastating events** to an enterprise.

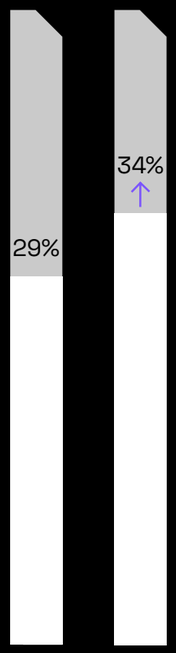
In addition to the potential financial and data loss, it can result in **significant reputational damage**, culture impairment, and **erosion of customer trust**."

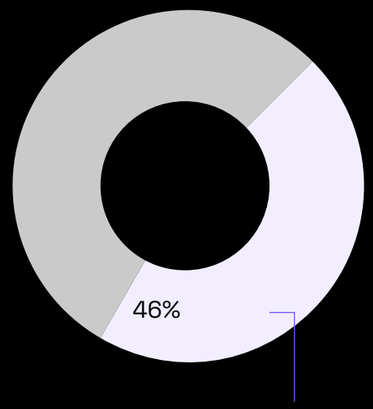
William Evanina,
Chief Executive Officer
The Evanina Group, LLC

Previously the Director of the US National Counter Intelligence and Security Center

Implementing UAM:

29% of organizations are looking to adopt User Activity Monitoring (UAM) to identify and prevent insider threats, rising to 34% in Government Services.

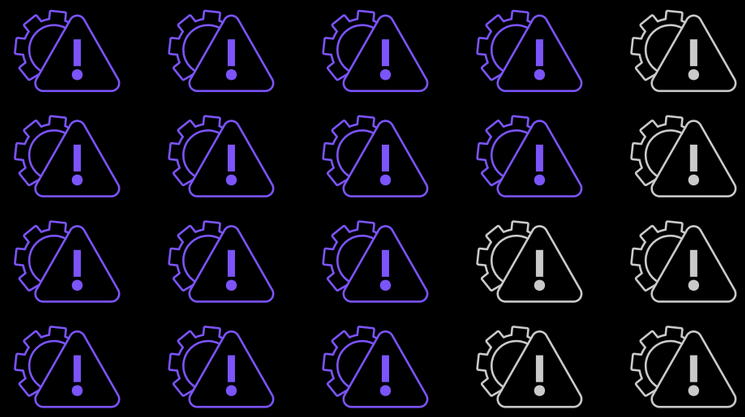




46% of Financial Institutions have already integrated UAM technology to secure their data against people related concerns.

70%

of IT Risk Analysts think that detection technologies are flawed as they can't prevent attacks exploiting zero-day flaws



Securing Data

Cybercriminals are increasingly embedding **zero-day, evasive and undetectable threats** in file transfers to breach organizations' perimeters, taking advantage of increases in volumes of data caused by increased uptake of AI, cross-department collaboration and remote working.

Given as we've outlined, data and information sharing are fundamental to the modern delivery of critical services, **the preventative approach must focus on eliminating threats rather than changing business processes.**

Adding prevention-based **Content Disarm and Reconstruction (CDR)** into the data flow sanitizes potentially harmful content before it reaches your network, extracts the useful information from the file and transforms the verified information into an entirely new useable file, leaving the original data – along with any potential malware – outside the network perimeter.

Remote Browser Isolation (RBI) also helps protect data from web-based threats, such as phishing and ransomware, stopping malware and other malicious activities by isolating web browsing activity.

Two Thirds

of organizations are turning to CDR to stay ahead of threats

Why Prevention Can't Wait Any Longer

60%+ **of industry professionals agree that detection technologies are falling short on preventing cyberattacks**

Over the past 12 months, the U.S. and U.K. organizations we spoke to in regulated industries that fell victim to a cyber incident paid, on average, over

$531,000 **IN RECOVERY COSTS**

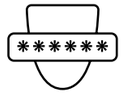
rising to over

$603,000 **IN HEALTHCARE ORGANIZATIONS**

But the cost of a data breach goes far beyond monetary value and can lead to severe consequences and even jail.

The three consequences of a cyberattack that security professionals are most concerned about are:

Internal security leaders facing legal consequences of a breach



The compromise of personally identifiable information

The cost and time requirements to repair/recover systems

In their executive roles, CISOs take a slightly different outlook. While the risk of internal security leaders facing legal consequences of a breach is similarly their top concern, they then fear reputational damage or a fine or penalty from a regulator.

The heightened risk in the complex regulatory environment has been demonstrated time and time again, with organizations receiving significant fines for regulatory non-compliance.

Take, as an example, how the Office for Nuclear Regulation (ONR) fined nuclear waste processing facility, Sellafield, £332,500 ($440k) for failing to adhere to cybersecurity standards and putting sensitive nuclear information at risk from 2019 to 2023.[iv]

While Marriott International and its subsidiary Starwood Hotels will pay $52 million and create a comprehensive information security program as part of settlements for data breaches that impacted over 344 million customers.[vii]

$52M **IN FINES**

344M **CUSTOMERS AFFECTED**

These two cases do not even stand out in this regulatory landscape. A massive number of fines are being handed out for data breaches and the frequency is only set to increase with the rise in attacks that circumvent detection-based defenses.

83%+

of Information Security Analysts believe that leveraging threat prevention solutions will ultimately reduce the likelihood of costly data breaches and operational disruptions

Detection is too little too late

It is clear that the need to make the shift from detection to prevention is now.

Detection is too little too late and organizations are suffering the consequences.

If organizations continue to pursue detection, they risk being on the back foot against the ever-growing sophistication of cybercriminals and open themselves up to significant consequences.

79%

of IT Security Directors believe their organization should be procuring more preventative cybersecurity solutions

Overcoming the Barriers to Change

With advances in preventative cybersecurity solutions, more and more agencies and organizations are making these investments and reducing their reliance on detection-based solutions. Yet, as with all new technologies, perceived challenges are holding organizations back.

These concerns ultimately come back to the detect and respond cycle that cybersecurity teams are trapped in.

This is breeding reactivity and making it more challenging for proactive strategy changes to be implemented.

"The detect and respond cycle may feel like the norm, but **norms are only habits we have yet to challenge**. True security comes when prevention becomes the standard. By challenging these norms, we empower ourselves to **create a more secure future.**"

Shaun Bierweiler
Chief Revenue Officer | Everfox

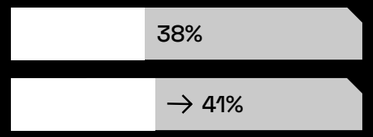
Why is this the case?

Firstly, the environment in which security teams are operating makes it difficult for some teams to make the leap.

The greatest challenge in promoting a preventative security approach, as reported by cybersecurity professionals in regulated industries, is the difficulty they face in **keeping up with the rapidly evolving threat landscape and adapting preventative measures accordingly.**

Given the threat levels discussed earlier in this report, it comes as no surprise this was **cited as a challenge by 39% of respondents**.

This concern is exacerbated by the myth that integrating preventative security solutions into existing IT infrastructure is complex (38%).



This rose to 41% among financial services organizations, a sector which in many instances still relies on older mainframe systems, databases, and applications that can struggle to integrate with some modern, and particularly cloud-based, solutions.

The false perception of complexity can be enough for stretched security teams to conclude that they don't have the time or resources to change their current setup.

Stretched security budgets also play their role.

36% of security professionals reported that stretched security budgets make it difficult to invest in new technologies.

Stretched security budgets particularly resonated with **government organizations**, who cited it as their greatest obstacle in **promoting a preventative security approach internally**.

Given the huge risk and costs of cyberattacks to organizations in these industries, a more holistic outlook is clear.

Continued investments in detection-based solutions that falls short, not to mention the cost of a breach which can go into the millions, far outweigh the cost of integrating more effective solutions.

Finally, the mindset shift also presents a particular challenge in certain sectors.

Not only is the detect and respond cycle perceived to be the norm, leading to a focus on improving detection or response times, but in regulated industries change can feel like a risk.

35% of cybersecurity professionals in defense organizations, for example, identified resistance to change and a preference for traditional, reactive security approaches as a significant obstacle in promoting a preventative security approach internally.

To help organizations begin to make the shift toward prevention-based technologies. Here are four recommendations from Everfox on overcoming these common concerns:

1. Stretched Budgets

Take a holistic view of the cost to the organization when it is clear that detection-based technologies alone are not preventing cyberattacks, as typically the upfront costs are outweighed by just one breach. Preventative technologies can create a stronger cyber defense and, in turn, reduce the risk of the costly impacts of a successful attack, such as recovery and repair costs, regulatory fines, and the loss of income due to reputational impacts or downtime in services.

Security leaders should also consider the reduction in real attacks requiring remediation and administrative overhead from false positives and negatives associated with prevention technologies, such as Preventative CDR. Adopting such technologies means security teams are not consistently following up, reviewing and responding to over 50 attacks weekly.

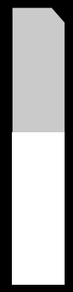
Two thirds of security teams face over 50 cyberattacks every week*, highlighting the relentless nature of today's threat landscape

Finally, while preventative security can be added to existing investments, it also presents an opportunity to re-evaluate existing technologies to determine if they meet existing and emerging requirements. Often organizations acquire technologies thinking they will satisfy the mission needs but once implemented it does not make a tangible impact on making the company more secure. This is where pride must be left at the door and a better solution should be found. An internal culture which accepts not all solutions will deliver on their pre-implementation promises is better than accepting the risk of substandard security.

2. Integrating Preventative Security Solutions

Prioritize tools that integrate with your existing systems. Security solutions need to have the ability to adapt to existing technologies through flexible Application Programming Interfaces and integration techniques. Meeting customers where their data resides, whether that's on-premise or in a public or private cloud.

Partnering with a trusted and proven provider for comprehensive protection and guidance for this integration is also important. An experienced cybersecurity company understands what it takes to secure your networks, people and data. Resulting in a consistent approach that eliminates gaps caused by managing multiple vendors.



55% of Information Security Analysts cite complexity of integrating preventative solutions into existing architecture as their most significant hurdle in switching to a preventative security approach

When choosing that partner, it is important that the day-to-day IT lead is involved, offering a steer on the requirements and constraints.

Their understanding of the company's operational needs and the realities of the technical environment will allow them to help implement preventative cybersecurity that meets the organizational needs.

*attempted or successful

3. Keeping Up With the Rapidly Evolving Threat Landscape

Embracing preventative solutions is crucial. Rather than simply identifying known malware and relying on regular updates, solutions such as prevention-based CDR, are run on a zero-trust basis.

Prevention-based CDR extracts key information and creates a new digital copy in near real time. This new file is then verified using advanced threat protection processes and delivered to the user, while the original is discarded along with any potential malware – known or unknown.

Nearly half of IT Security Directors are planning to adopt CDR solutions to protect their organizations from external threats

By including Hardsec in preventative solutions, the threat surface of the security mechanism can be greatly reduced and is not dependent on a commercial operating system.

Therefore, the lifetime of Hardsec can be much longer, with less need for security updates.

4. Resistance to Change

The perception of leadership being the blocker to cybersecurity investments has largely changed. They are now keenly aware of the cyber threat landscape and fully understand that the need to increase visibility across data, systems and users will enable organizations to better understand what prevention solutions can be used to protect their IT infrastructure. However, change can be overwhelming to stretched security professionals tasked with making the changes without negatively impacting their organizations' defenses.

It's clear that the role of strong leadership to drive collaboration, align security goals with business objectives, and champion the shift to proactive prevention-first methodologies is key. This is starting to happen as technology leaders move from government and defense into regulated industries, bringing their experience of preventative technology with them.

34% of security staff say leaders fail to promote a shift to preventative security

Another critical way to overcome the resistance to change is to shift the focus to mission success over vanity metrics. Detection-based technologies often provide easily digestible metrics, such as the number of attacks stopped. That number looks impressive when reported to leadership, but ultimately it reveals how many threats reached your systems to be detected, creating a reactive security posture.

A reassessment of what success looks like is needed for both leadership and security teams.

Instead of tallying threats, governments, defense agencies and regulated industries should be asking themselves:

- → Are our **networks** safe from intrusion?
- → Are our **people** protected against internal and external threats?
- → Is our **data** secure and accessible only to those authorized?

Those who take a **preventative approach** will be far more confident answering those questions than those relying on vanity metrics and technologies that are failing to keep pace with modern threats.

Just ‘detecting bad’ is **no longer enough.**

Sources

[i] **Skybox Security. “Vulnerability and Threat Trends Report 2024 | Skybox Security”**
n.d.

[ii] **Toulas, Bill. “OpenAI Confirms Threat Actors Use ChatGPT to Write Malware.” BleepingComputer**
October 11, 2024.

[iii] **Everfox. “From Serious Breach to Ransomware Resilience”**
July 9, 2024.

[iv] **NHS England - London, “NHS England — London » Update on Cyber Incident: Clinical Impact in South East London – Friday 14 June 2024”**
June 14, 2024

[v] **Oladimeji, Saheed & Kerner, Sean. “SolarWinds hack explained: Everything you need to know.” Tech Target**
November 3, 2023

[vi] **Tickell, Pamela. “Sellafield Nuclear Site in Cumbria Fined for IT Security Breaches.” BBC News**
October 2, 2024

[vii] **Federal Trade Commission. “FTC Takes Action Against Marriott and Starwood Over Multiple Data Breaches”**
October 9, 2024

EVERFOX

About Everfox

Everfox, formerly Forcepoint Federal, has been a trailblazer in defense-grade cybersecurity for over two decades, delivering high-assurance solutions designed to secure the world's most high-threat environments. With expertise spanning **Cross Domain Security, Insider Risk Management,** and **Advanced Threat Protection**, we build solutions that protect sensitive systems and critical data with unmatched reliability.

Trusted by Global Governments, Defense Organizations and Regulated Industries, safeguarding critical operations against today's most advanced cyber threats. At Everfox, we're not just leading the way in cybersecurity innovation. We're redefining what it means to secure the world's critical environments.

And we're just getting started.

2025
CYBER360

Learn More

www.everfox.com