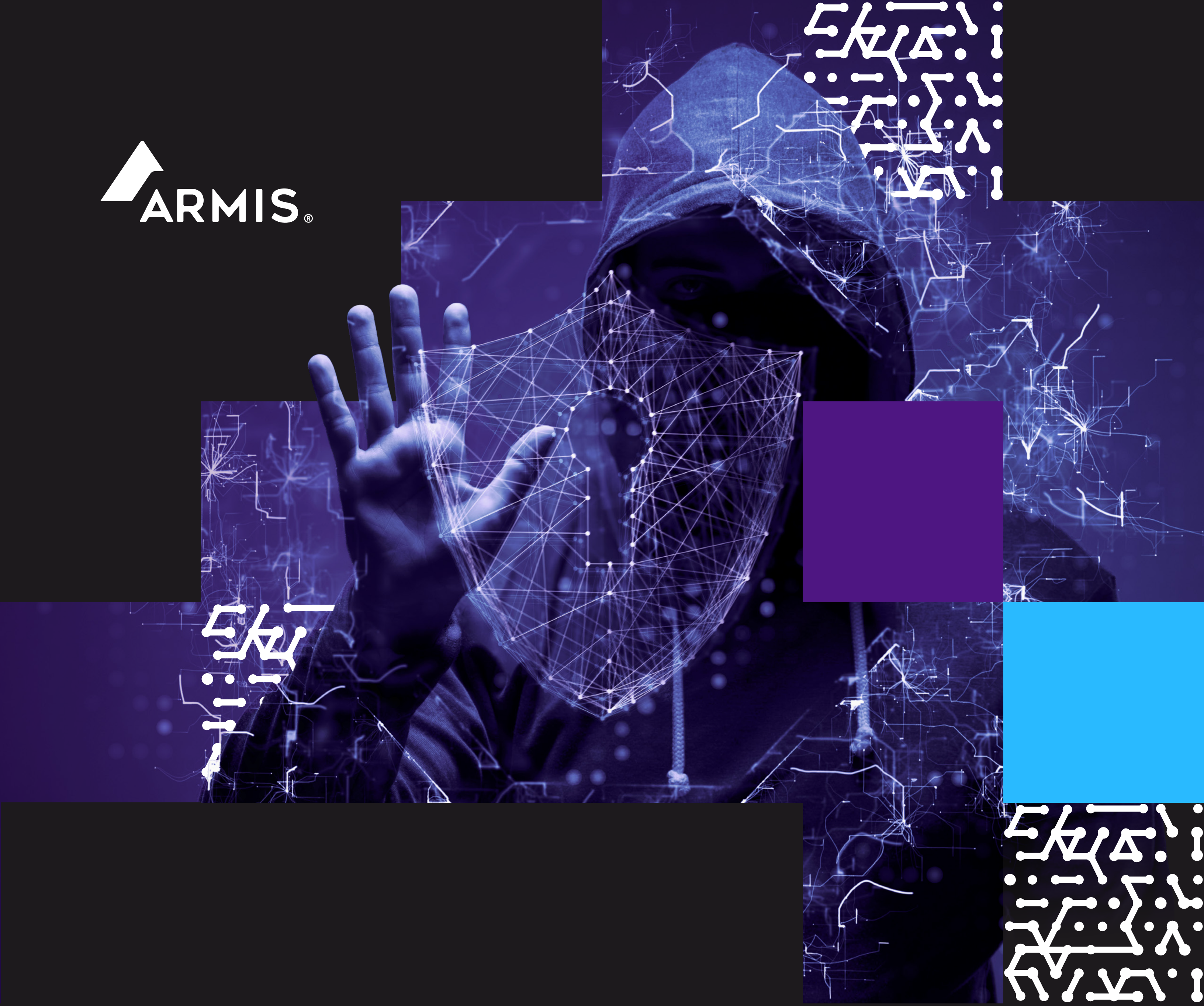


ARMIS RESEARCH REPORT

The Anatomy of Cybersecurity: A Dissection of 2023's Attack Landscape

By Armis Labs (Data and Research Team)

Armis' 12-month analysis of proprietary data finds cybersecurity equates to one never-ending game of chess, necessitating a strategic approach

Table of Contents

03 Introduction

04 Key highlights: by the numbers

05 SECTION 1
Rising threats

09 SECTION 2
The risks of the extended attack surface

13 SECTION 3
Vulnerability prioritization and remediation is a challenge

15 SECTION 4
Navigating the data deluge with Armis

15 SECTION 5
Securing the future

Introduction

Cybersecurity has become an endless game of chess. Players on opposite sides of the board. Each one, making calculated moves, anticipating the other's strategies and striving to stay ahead.

For security and IT decision-makers, 2023 has proven to be the toughest match yet. It was a year that witnessed a surge in cyber threats, a relentless onslaught that saw attack attempts double, leaving organizations grappling with a complex chessboard of challenges.

This included the growing adoption of AI by bad actors rivaling – and sometimes surpassing – that of organizations' technology teams. Meanwhile, there's the ongoing need to balance the security challenges of hybrid work.

In our ever-evolving digital world, where every device and network link becomes a potential gateway for intrusion, staying one step ahead in this game of chess has never been more vital. Particularly when each year gets harder than the last.

Yet, it's not just new threats and technological advancements that pose a risk. 2023 saw organizations and security teams, irrespective of size and stature, finding themselves engulfed in a deluge of data. It's not just information; it's a tidal wave of potential threats, risks, vulnerabilities and anomalies. This itself has become a colossal challenge, and one that's only expected to get worse without action.

29% of IT security and IT decision-makers are overwhelmed by the significant amount of threat intelligence data lacking actionable insights. There's simply too much and it's hard to know where to start.

Through the Armis Asset Intelligence Engine – the largest Artificial Intelligence driven engine in the world that monitors billions of assets worldwide, we can identify cyber risk patterns and behaviors and provide actionable plans for organizations so they do not get overwhelmed by the data.

This report highlights the most pivotal data from the previous year, offering a snapshot into the global cybersecurity landscape. Using this data we can accurately predict trends for next year as well as provide a proactive plan for all organizations as they prepare for what will be another year of cyber change. This report can serve as a blueprint for future cyber resilience, allowing decision-makers to adjust strategies in this ongoing game of chess. Every move matters.

KEY HIGHLIGHTS

By the numbers*

Attack attempts rose significantly in 2023, with an increase of

104%

Attack attempts on the Utility Industry rose by

200%

Older Windows server OS versions (2012 and earlier) are

77% more likely to experience attack attempts.

over **65,000**

unique CVEs discovered in 2023.

93%

wearable devices have the highest percentage of unpatched CVEs.

A third

of all devices are still not patched for Log4Shell.

41%

the Educational Services industry has a significantly higher percentage of servers with unpatched weaponized CVEs, compared to the general average of 10%.

45%

personal computers are most at risk in the Healthcare industry.

Legacy OS

industries still using EoL or EoS OSs: Educational Services (18%), Retail trade (14%), Healthcare (12%), Manufacturing (11%), Public Administration (10%).

Patch rates for critical CVEs are not prioritized:

Low CVEs	11% patch rate
Medium CVEs	58% patch rate
High CVEs	64% patch rate
Critical CVEs	55% patch rate

From the Armis State of Cyberwarfare and Trends Report: 2022-2023:

- **One-third (33%) of global organizations** are not taking the threat of cyberwarfare seriously, identifying as indifferent or unconcerned about the impact of cyberwarfare on their organization as a whole, leaving room for security gaps.
- **Nearly a quarter of global organizations (24%)** feel underprepared to handle cyberwarfare based threats. Even still, the lowest-ranking security element in the eyes of IT professionals is preventing nation-state attacks (22%).
- **Over half (55%) of IT professionals** surveyed agree with the statement, 'My organization has stalled or stopped digital transformation projects due to the threat of cyberwarfare.'

*All data presented throughout this report was gathered by the Armis Asset Intelligence Engine throughout 2023 and analyzed by our researchers.

SECTION 1

Rising threats

One data stat tells the story of 2023 best: attack attempts doubled. Armis researchers and data analysts analyzed these threats and events that were going on across the world and were able to extrapolate information and insights from our proprietary data.

Whether caused by geopolitical tensions or legacy technology and systems posing a risk, it's been an eventful year. In fact, there was a **104% increase in attack attempts**. Major players across various industries fell victim to threats and vulnerabilities in 2023, such as MGM Resorts, Sony and the NHS, while Critical National Infrastructure (CNI) from Ukraine and Denmark to the United States and Australia all dealt with unrelenting attacks. After all, malicious actors only need to identify one weak link in the attack surface to gain access to the network, move laterally and proliferate an attack between IT and OT environments.

And while almost all industries saw a significant increase in attack attempts, the two with the highest increase are Utilities (**over 200% increase**) and Manufacturing (**165% increase**). However, 2023 also saw Educational Services and Manufacturing as the most attacked industries, further signifying the escalating risks to CNI.

The first half of 2023 saw more high-profile cyber attacks occurring than the second half. This included the T-Mobile data breach and the PharMerica breach, the largest healthcare data breach to be reported by a single HIPAA-covered entity in 2023. The second half of the year saw a consistent month-over-month increase in attack attempts of around **13%**. This included attacks across an array of industries, including Healthcare, Finance and Insurance and Transportation.

But more than anything, 2023 was characterized by a deluge of data.

Armis research highlighted in November 2023 that 45% of IT security and IT decision-makers across the US, UK, Germany, France, Singapore, Australia and New Zealand rely on an extensive array of 10 or more sources for collecting threat intelligence data. This is a result of the variety of critical assets (IT, OT, building management systems, etc.) spanning today's various business environments (cloud, physical, remote/WFH). These multiple, disjointed data feeds are overwhelming IT and security teams causing a negative impact, limiting their ability to understand the full picture when it comes to seeing, protecting and managing their attack surface.

The last twelve months have also shown that prioritizing remediation of vulnerabilities is jeopardized by an absence of automation for threat intelligence, leaving once more, an open door for malicious actors. With minimal automation, much of the work needed to make use of the intelligence sources is manual, leading to 29% of cybersecurity teams feeling overwhelmed, hindering security and IT pros' ability to effectively remediate threats or prioritize threats in order of the potential impact to the business.

The Armis State of Cyberwarfare 2022-2023 report underscores this further, showing that many organizations face heightened cyber threats from an array of sources. As technology becomes more intertwined with our daily lives and the attack surface continues to grow, so does the threat of an attack.

The repercussions of an attack or a breach can disrupt industries and services, compromise reputation as well as sensitive information, and, in some cases, pose threats to national security; something that became a common theme in the headlines during 2023.

Geopolitical tensions amplified the cybersecurity landscape

As the year unfolded, a growing number of nation-state cyberattacks became apparent. Cyber war and regional tensions with China, Russia, Ukraine and Israel contributed to this. In the past year, cyberattacks have impacted more than 120 countries, where over 40% of attacks were aimed at government or private-sector entities involved in CNI.

In several prominent Western nations, fears that China is stealthily infiltrating critical infrastructure for future cyber disruption grew exponentially in 2023. This threat has seen the likes of the social media platform TikTok facing bans across the globe owing to national security concerns and its ownership by the Chinese company ByteDance. By June 2023, more than half of US states had banned or partially banned TikTok from state-issued government devices.

In the tail end of 2023, lawmakers in the United States, Europe and Canada further escalated efforts to restrict access to TikTok, while countries such as India and Nepal banned it completely, the latter facing more than 1,600 TikTok-related cybercrime cases over the last four years. And it all comes down to China.

> Armis data revealed that throughout 2023, the top industries exposed to attack from Chinese and Russian actors were those within Manufacturing, Educational Services and Public Administration.

These sectors continue to bear the brunt of diverse cyber threats, showcasing the multifaceted objectives of threat actors.

In Educational Services, intrusion attempts from .cn and .ru domains have risen to about 10% of total attacks. This trend signals a concerning uptick in cyber threats against teaching institutions, while Manufacturing experienced an intensified threat landscape, with .cn and .ru domains contributing to an average of **30%** of monthly attack attempts.

This heightened targeting suggests a focused effort by bad actors on a global scale, potentially driven by motives such as industrial espionage or disruption of critical manufacturing processes, as seen by events throughout the course of 2023.

Outdated devices contributed to the rising threats

Our very dependence on devices and BYOD has allowed them to become a vulnerability in our ever-evolving digital world. Data gathered over the course of 2023 illuminated some discernible trends.

Throughout the year, a noteworthy surge in attack attempts was also observed, peaking in July. During this period, specific device categories experienced intensified targeting. Communications devices, particularly VOIP systems, saw a substantial increase, emphasizing a targeted onslaught on communication infrastructure. IoT and IoMT devices such as Imaging devices, including printers and IP cameras, and manufacturing devices, such as SCADA servers and Programmable Logic Controllers (PLCs), encountered significant escalations in attack attempts too.

What does this mean? That these malicious actors have a very large attack surface to target, with many bad actors operating in different ways who are looking to get ahead in this game of chess.

In addition to the above concerning trends, were trends in vulnerabilities found in operating systems. Devices running older Windows Server OS versions (2012 and earlier) were **77% more likely** to experience attack attempts compared to newer Windows Server versions. This vulnerability is particularly evident in the server environment, with nearly a **quarter** of server versions facing end-of-support (EoS) scenarios.

In contrast, a mere **2%** of desktop versions found themselves in EoS situations. This disparity underscores the strategic targeting of aging server infrastructure, pointing to potential risks associated with legacy systems and vulnerable servers. This was uncovered in June 2023 within several UK government departments, such the HM Revenue and Customs (HMRC), the Department of Health and Social Care (DHSC) and the UK Atomic Energy Authority.

Turning to threat types, a triad of Tor access, and access to suspicious hosts took center stage throughout 2023. Once more, Educational Services also saw a rise in attack attempts, with suspicious host threats and Tor access dominating, highlighting the sector's vulnerability to these specific threat vectors.

Known also as The Onion Router, Tor takes online privacy to new extremes, helping users access the unindexed part of the internet known as the dark web, while also leaving users vulnerable to online threats found there. Tor access was also prominent in Utilities and Manufacturing, while suspicious hosts were prevalent in Educational Services, Manufacturing, Health Care and Social Assistance industries.

Put simply, these insights underscore the need for organizations to understand and navigate the rising threat landscape and attack vectors. As we move into the new year, organizations must prioritize solutions that offer visibility of the entire attack surface for early detection, rapid response and the mitigation of potential high-risk vulnerabilities. There is an increased risk of falling within the 61% of global organizations that suffered a breach at least once over the last 12 months if they do not.

SECTION 2

The risks of the extended attack surface

As the attack surface continues to grow, so does the opportunity for attackers to find a vulnerability and exploit it, underscoring the critical need for efficient vulnerability remediation. Unfortunately, the common theme of 2023 seems to be the lack of automation in processing, prioitizing and utilizing the sheer volume of threat intelligence.

Data from 2023 also suggests that all industries are vulnerable. All are at risk. And any asset is an attack vector and part of the attack surface. Various device types faced – and continue to face – a heightened cyber risk. In fact, IT devices such as VoIPs, virtual machines and personal computers were prime targets over the course of the year.

Moreover, the Healthcare industry, more specifically its devices, posed a significant risk to organizations' attack surface. In April 2023, Armis identified the riskiest medical and IoT devices in clinical environments. The research highlighted that nurse call systems are the riskiest connected medical device, with 39% having critical severity unpatched CVEs and almost **half (48%)** having unpatched CVEs.

Nurse Call Systems	39% have critical severity unpatched CVEs	48% have unpatched CVEs	
Infusion Pumps	27% have critical severity unpatched CVEs	30% have unpatched CVEs	
Medication Dispensing Systems	4% have critical severity unpatched CVEs	86% have unpatched CVEs	32% run on unsupported Windows versions

As the year continued, other Internet of Medical Things (IoMT) devices witnessed increased risks for imaging workstations, workstations and media writers. While advances in technology are essential, connected care brings a bigger attack surface. Without full visibility, healthcare organizations are opening themselves up to the rising threats.

Outside of healthcare, in June 2023 Armis identified the riskiest operational technology (OT) and industrial control systems (ICS) devices across critical infrastructure industries. The analysis revealed that OT and ICS devices, including engineering workstations, SCADA servers and PLCs, pose heightened risks. Combined with the Armis data, engineering workstations emerged as the year's most targeted OT device, emphasizing the pressing need for prioritized vulnerability management.

The inability to regularly take down OT environments for regular maintenance windows poses a challenge since vulnerabilities can stay open for an extended period of time between said scheduled outages.

The concerning trend of OT devices accessing the internet highlights further potential vulnerabilities, with around **80%** of engineering workstations and **60%** of SCADA servers having internet access over the past year. The vulnerabilities in these devices, along with them having internet access, pose a significant risk to the attack surface, becoming potential entry points for infiltrating an organization.

When analyzing the susceptibility to weaponized CVEs by category from 2023, the devices causing most risk to the attack surface include:

IT	16%	Personal Computers	15%	Switches	13%	Routers
IoMT	71%	Media Writers	47%	Workstations	27%	Central Stations
IoPT	15%	Media Players	9%	Watches	1%	Tablets
OT	34%	Engineering Workstations	24%	SCADA Server	20%	Industrial PCs
IoT	50%	AV Transmitter	28%	IP Cameras	5.5%	TVs

End-of-Support systems threaten the attack surface

Research from 2023 further highlighted the number of devices susceptible owing to EoS operating systems and applications. Across an array of devices, from OT and IT to IoPT and IoMT, it was one of the most common risk factors. It has become a huge threat to the attack surface and global businesses.

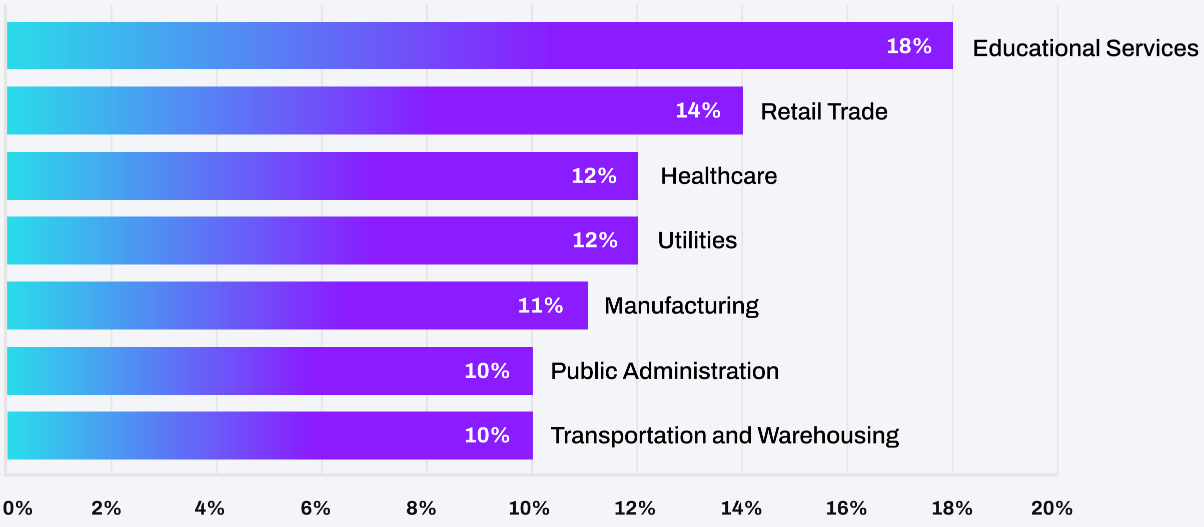
EoS assets are no longer actively supported or patched for vulnerabilities and security issues by the manufacturer. Malicious actors are intentionally targeting these assets because they're externally accessible, have an expansive and intricate attack surface and are easier to target.

Further examination shows that personal computers particularly in IT are susceptible, owing to EoS operating systems and applications, while IoMT devices like media writers face risks related to EoS applications and SMBv1 (Server Message Block version 1) usage.

For context, SMBv1 is a legacy, unencrypted and complicated protocol with vulnerabilities that have been targeted in the infamous Wannacry and NotPetya attacks. The original SMBv1 protocol is over 30 years old, and like much of the software made in the 80s, it was designed for a world that no longer exists. Previous Armis research found that 74% of organizations today still have at least one asset in their network vulnerable to EternalBlue – an SMBv1 vulnerability.

Devices from engineering workstations and SCADA servers to product scanners, tablets and Point of Sale systems were all susceptible to SMBv1 and outdated firmware as well as exhibiting vulnerabilities tied to EoS operating systems.

Examining the data from 2023 further and there's an array of industries still using legacy operating systems:



ARMIS

CENTRIX™

The Cyber Exposure Management Platform

Armis Centrix™ for Asset Management and Security

FIND OUT MORE

Armis Centrix™ for OT/IoT Security

FIND OUT MORE

Armis Centrix™ for Medical Device Security

FIND OUT MORE

Armis Centrix™ for Vulnerability Prioritization and Remediation

FIND OUT MORE

armis.com

SECTION 3

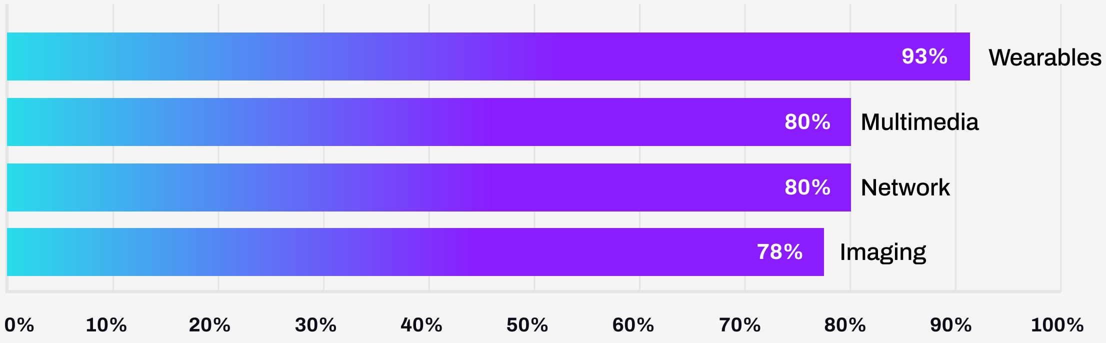
Vulnerability prioritization and remediation is a challenge

Security professionals found themselves grappling with an overwhelming number of vulnerabilities in 2023, making prioritization and remediation an increasingly complex challenge. Over the past year, the cybersecurity community identified and dealt with an astonishing **65,000 unique CVEs**, underscoring the sheer breadth of potential threats. This proliferation of vulnerabilities is further exacerbated by the staggering figure of over **3.6 billion CVEs associated with active assets**, as found by Armis, emphasizing the interconnected nature of the digital ecosystem.

With so much to contend with, it's not a question of if, but when, a cyberattack will occur. Unseen, unscanned or unaccounted assets can introduce critical security exposures, especially if configured non-securely, security updates aren't installed or patches are not applied. Put simply, organizations often don't have the complete visibility of their network as they may think.

When categorizing vulnerabilities by device type from 2023, it becomes evident that computers, medical devices and manufacturing equipment bear the highest burden, showcasing the wide array of targets for potential exploitation.

Unpatched vulnerabilities also pose a significant concern, with certain device categories exhibiting alarming rates:



These devices stand out as those with the highest percentage of unpatched CVEs, exposing a substantial portion of the attack surface.

More worryingly, high-profile vulnerabilities, such as **Log4Shell**, continue to pose a threat, with a **third** of devices still lacking the necessary patches. This underscores the challenges faced by organizations in swiftly addressing and neutralizing known vulnerabilities, leaving potential avenues for exploitation.

Other vulnerabilities found by Armis in July 2023, such as the Crit.IX vulnerabilities, further echo the urgent need to consider cybersecurity not merely as a reactive shield, but as an integral part of any business strategy. Other instances such as the exploitation of MOVEit exposures, amplify the real-world consequences of cybersecurity lapses and the abundance of threats lurking on the other side of the checkered chess board, urging businesses to proactively address vulnerabilities.

Patching has become an issue

Throughout 2023, organizations struggled to manage physical and virtual assets connected to their networks.

Organizations continue to face a formidable challenge in prioritizing and remedying critical vulnerabilities within their cybersecurity landscape. Despite maintaining similar patch rates across severity levels, the actual number of critical CVEs being patched remains notably low.

Patch rate of CVEs:

Low CVEs	**11%** patch rate
Medium CVEs	**58%** patch rate
High CVEs	**64%** patch rate
Critical CVEs	**55%** patch rate

This trend persists, irrespective of the weaponization status of a CVE, as organizations consistently grapple with patch rates at 62% for non-weaponized and **61% for weaponized vulnerabilities**. It underscores the intricate challenges organizations face in addressing and mitigating the most critical cybersecurity risks effectively.

Put simply, organizations are not prioritizing the right CVEs. Why?

The Armis Global Attack Surface Management (ASM) research presented in November 2023 revealed that organizations have been using 11 different tools to manage assets connected to their network, while 44% admit to still using manual spreadsheets. There's just too much data and no way of knowing what the priorities are.

Without complete control, management and/or visibility of the potential security gaps introduced by these assets, organizations are putting themselves at even more risk. Therefore, organizations must grapple with the imperative to fortify their cyber defenses, all under the assumption that compromise is not a possibility but a certainty.

SECTION 4

Navigating the data deluge with Armis

2023 posed a number of challenges around cyber resilience. The key is now learning from them. Finding a way to make the right moves. And deploying the right solutions to help manage and cope with the deluge of data.

Therefore, the first step is to gain complete visibility into your attack surface. This involves identifying all devices, including known and unknown physical and virtual assets, that are connected to your network. Indeed, on an average business day, there are over 57,000 physical and virtual assets connected to the organizational networks of Australian and New Zealand businesses. For those based in Singapore, it's 56,000 assets. In the UK and other European nations, its approximately 45,000 connected assets. Each comes with a significant risk, no matter where in the world organizations may be.

SECTION 5

Securing the future

The data from the Armis 2023 report revealed critical insights into the multifaceted challenges organizations face in safeguarding assets and the attack surface. As these complex adversaries continue to make strategic moves in this game of chess, the call for a proactive and comprehensive cybersecurity strategy has never been more apparent.

Preparing for 2024 and beyond requires not only a reactive stance but a proactive one. Organizations must go beyond reacting to opponents' moves; they must anticipate and counteract with strategic foresight. And Armis provides organizations with the tools needed to do so, gaining complete visibility into the attack surface before identifying and mitigating threats proactively, while continuously monitoring and optimizing the security postures of organizations.

After all, in this cyber chess game, every move matters. Armis stands as an indispensable piece on the board, offering organizations the capability to not only defend against the current threat landscape but also position themselves strategically for the dynamic challenges of the future.

As the pieces align, embracing these advanced tools becomes a checkmate move toward a secure and resilient digital future.

The Armis way

Armis Centrix™, the cyber exposure management platform that's powered by the Armis AI-driven Asset Intelligence Engine, sees, secures, protects and manages billions of assets around the world in real time. Armis Centrix™ collects, aggregates and analyzes data from every connected source, using machine learning and artificial intelligence to identify and prioritize potential threats.

The seamless, frictionless, cloud-based platform proactively mitigates all cyber asset risks, remediates vulnerabilities, blocks threats and protects an organization's entire attack surface. Armis Centrix™ is designed to support organizations in managing the deluge of data and gaining visibility to the entire attack surface and the assets connected to it.

In fact, organizations across the globe have recognized the importance of intelligence into every kind of asset, Armis customers such as multinational consumer products company, Colgate-Palmolive, United Airlines, Mondelēz International and the City of Las Vegas, all implemented and trust Armis Centrix™. These organizations, among hundreds of others, use Armis to benefit from a powerful and streamlined approach to cyber exposure management, enabling security teams with broader visibility, insights into gaps and the ability to stay ahead and stay protected against current threats and risks.

More importantly, Armis Centrix™ solves the data deluge problem by providing organizations with a single solution to see, protect and manage their entire attack surface, while the platform's vulnerability intelligence allows you to focus your efforts where they're needed most.

For more information please visit: www.armis.com

Armis, the asset intelligence cybersecurity company, protects the entire attack surface and manages the organization’s cyber risk exposure in real time.

In a rapidly evolving, perimeter-less world Armis ensures that organizations continuously see, secure, protect and manage all critical assets.

Armis secures Fortune 100, 200 and 500 companies as well as national governments, state and local entities to help keep critical infrastructure, economies and society safe and secure 24/7.

Armis is a privately held company headquartered in California.

1.888.452.4011

Website

Platform

Industries

Solutions

Resources

Blog

Try Armis

Demo

Free Trial