WHITE PAPER

From Chaos to Control: Simplifying Cybersecurity Asset Management

Introduction

As organizations continue to adopt and rely on digital technologies, the need for effective cybersecurity asset management becomes increasingly critical. However, with the proliferation of devices, applications, and cloud-based services, managing cybersecurity assets has become more complex than ever before. The combination of increasing complexity, fragmentation, and loss of control presents a significant challenge for security teams.

While organizations invest heavily in cybersecurity solutions, they often overlook the security of their own assets, leading to an enterprise security blindspot. Attackers can take advantage of this blindspot to gain unauthorized access to an organization's systems and data, resulting in serious consequences such as data breaches, financial losses, and reputational damage.

To address these challenges, organizations need a comprehensive framework for effective cybersecurity asset management that allows them to identify, prioritize, and protect their assets from various cyber threats. This white paper will explore the three main challenges in cybersecurity asset management - complexity, fragmentation, and loss of control - and present a framework for effective cybersecurity management that can help organizations overcome these challenges.

In the following sections, we will examine each of these challenges in detail and discuss how they impact cybersecurity asset management. We will also explore the enterprise security blindspot and its implications for organizations. Finally, we will present a framework for effective cybersecurity management that organizations can use to develop a proactive and comprehensive approach to cybersecurity asset management.

Table of Contents

From Complexity to Simplicity

In the context of cybersecurity asset management, the proliferation of digital assets across organizations has created a significant challenge for security teams. As the number of devices, applications, and cloud-based services continue to increase, the need for better visibility of those assets has become increasingly critical to properly manage the risk posture and threat landscape.

Unfortunately, managing these assets has become more difficult due to the "great silo-ization" of legacy tools. The management of assets is often spread across multiple IT and security solutions, resulting in a fragmented landscape with neither complete visibility nor a single source of trusted information. This means that IT and security teams struggle to understand what assets they truly have and to ensure that policies are properly enforced, risks are managed, and assets are protected.

Without proper cybersecurity asset management, organizations can face significant challenges when it comes to protecting their assets from various cyber threats. Attackers can exploit the lack of visibility and control over assets to gain unauthorized access to systems and data, leading to serious consequences such as data breaches, financial losses, and reputational damage.

To address these challenges, organizations need a comprehensive approach to cybersecurity asset management that includes identifying, classifying, and prioritizing assets based on their criticality to the organization. This approach should also provide a single source of truth for asset information, allowing IT and security teams to have a complete view of their assets and make informed decisions about risk management and asset protection.

By adopting a proactive and comprehensive approach to cybersecurity asset management, organizations can effectively manage their assets, reduce their attack surface, and mitigate the risk of cyber threats. It is essential that organizations prioritize cybersecurity asset management to ensure that their assets are properly protected in the constantly evolving cybersecurity landscape.

Can you see all the assets in your environment?

- How many assets do I have in my CMDB?
- How many managed vs. unmanaged assets do I have?
- What is the distribution of assets by site or department?
- Do I have any laptops missing an endpoint security agent?
- Do I have any end-of-life devices? If so, where are they and who is using them?
- How many users (by asset type) do I have and where are they located?
- How many unsanctioned applications are in my environment?
- Are there any devices reported missing that appear on my network?
- How many vulnerable assets do I have by CVE severity, business unit or location?
- How many devices run unpatched Operating Systems (OS) or applications?

Fragmentation and Loss of Control

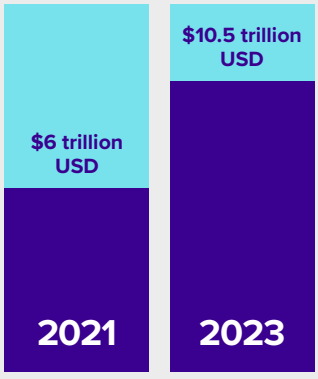
Recent studies have shown that the number of connected devices has exceeded earlier predictions. According to a report by Statista, the number of Internet of Things (IoT) devices worldwide is expected to reach 75.44 billion by 2025, up from 26.66 billion in 2019. Additionally, the pandemic years have accelerated the adoption of connected devices as organizations have had to rapidly increase the pace of digital transformation to support business continuity efforts.

Today, almost every organization relies heavily on connected assets and devices to conduct all aspects of business. This is done through managed devices - such as laptops, desktops, and servers, smartphones and Bring Your Own Device (BYOD), virtual assets, cloud services, and IoT devices (the "great unmanaged"). The result is billions of devices connecting to critical data and infrastructure, with more continuously being brought online every day.

However, the growing number of devices and the lack of visibility and control have made it challenging for IT and security teams to manage and secure their assets effectively. The COVID-19 pandemic has also contributed to the rise of complexity issues as more and varying types of assets are being used to support remote work and distributed operational models. According to research from McKinsey, COVID-19 actually helped accelerate the adoption of connected devices because standard organizational barriers that typically limit innovation were removed to expedite productivity efforts.

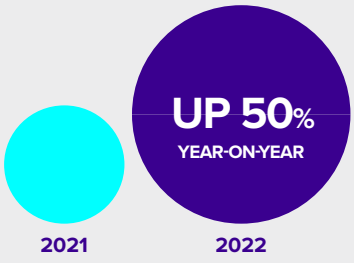
To effectively manage and secure their assets, organizations need to have visibility and control across disparate tools. This means identifying, classifying, and prioritizing assets based on their criticality to the organization and having a single source of truth for asset information. By adopting a proactive and comprehensive approach to cybersecurity asset management, organizations can effectively manage their assets, reduce their attack surface, and mitigate the risk of cyber threats.

Global Cost of Cybercrime



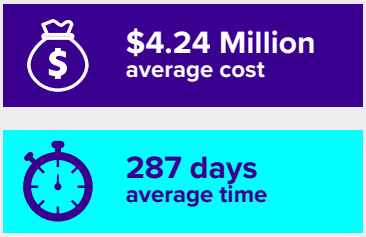
In 2023, the global cost of cybercrime is projected to reach **$10.5 trillion USD**, up from **$6 trillion USD in 2021**

Average Cost of a Cyber Attack



In 2022, the average cost of a single cyber attack on a business was **$2.7 million USD, up 50%** from the previous year.

Average Time to Identify and Contain a Data Breach



The average time to identify and contain a data breach is **287 days,** with an average cost of **$4.24 million USD** per breach.

SOURCE: ARMIS CYBERWARFARE REPORT, JANUARY 2023

More Devices, More Complexity

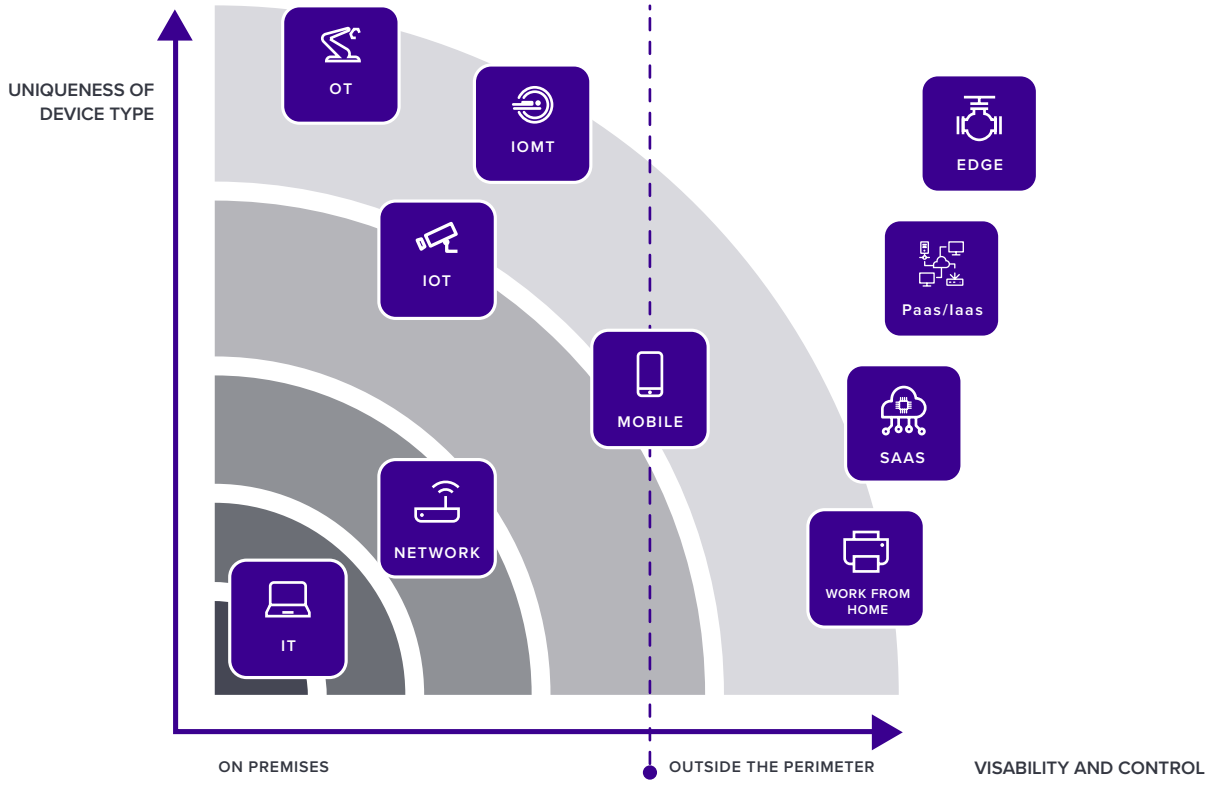
As the number of devices and tools used by organizations continues to increase, managing and securing assets becomes more complex than ever before.

Each device that connects to the network introduces a new set of considerations that IT teams need to account for. This includes the operating system, applications, user access, network connectivity, patches, and updates. These are just the basics, and the complexity only grows as new devices are added to the network.

The result is a highly complex and dynamic environment that creates blind spots, making it difficult for IT and security teams to have a comprehensive view of their assets. This complexity is preventing organizations from effectively managing and securing their critical data.

To make matters worse, the constantly evolving threat landscape adds another layer of complexity to cybersecurity asset management. Cybercriminals are constantly finding new ways to exploit vulnerabilities in devices and systems, making it even more important for IT and security teams to have complete visibility into their assets.

To overcome this complexity, organizations need a proactive approach to cybersecurity asset management. This involves implementing a framework that allows IT teams to identify, classify, and prioritize assets based on their criticality to the organization. By having a single source of truth for asset information, IT teams can effectively manage their assets and reduce the attack surface, mitigating the risk of cyber threats. Additionally, automating asset management tasks and leveraging artificial intelligence (AI) and machine learning (ML) can help IT teams manage the growing complexity of their environments.



Shining a Light on the Enterprise Security Blindspot

Mapping Out Your Network's Assets

The rapid growth and widespread adoption of new devices and technologies has outpaced the ability of security measures to keep pace, resulting in a proliferation of blind spots that create vulnerabilities in enterprise security. As companies embrace the convenience of easy connectivity and instant deployment of virtual machines, these devices and assets become targets for attackers seeking to exploit unprotected connections.

Despite the growing risks, many organizations are unable to detect these gaps in their security posture, providing cybercriminals with the opportunity to launch successful attacks. The emergence of these blind spots has created a pressing need for enhanced visibility and control over all devices and assets on enterprise networks, as well as more sophisticated threat detection and response capabilities.

Without adequate protection, cyber attackers can exploit these blind spots to gain access to sensitive data and compromise enterprise systems. It is imperative that organizations implement comprehensive security measures to address these blind spots and stay ahead of the evolving threat landscape. By taking proactive steps to secure their networks, companies can reduce the risk of cyberattacks and safeguard their critical assets and information.

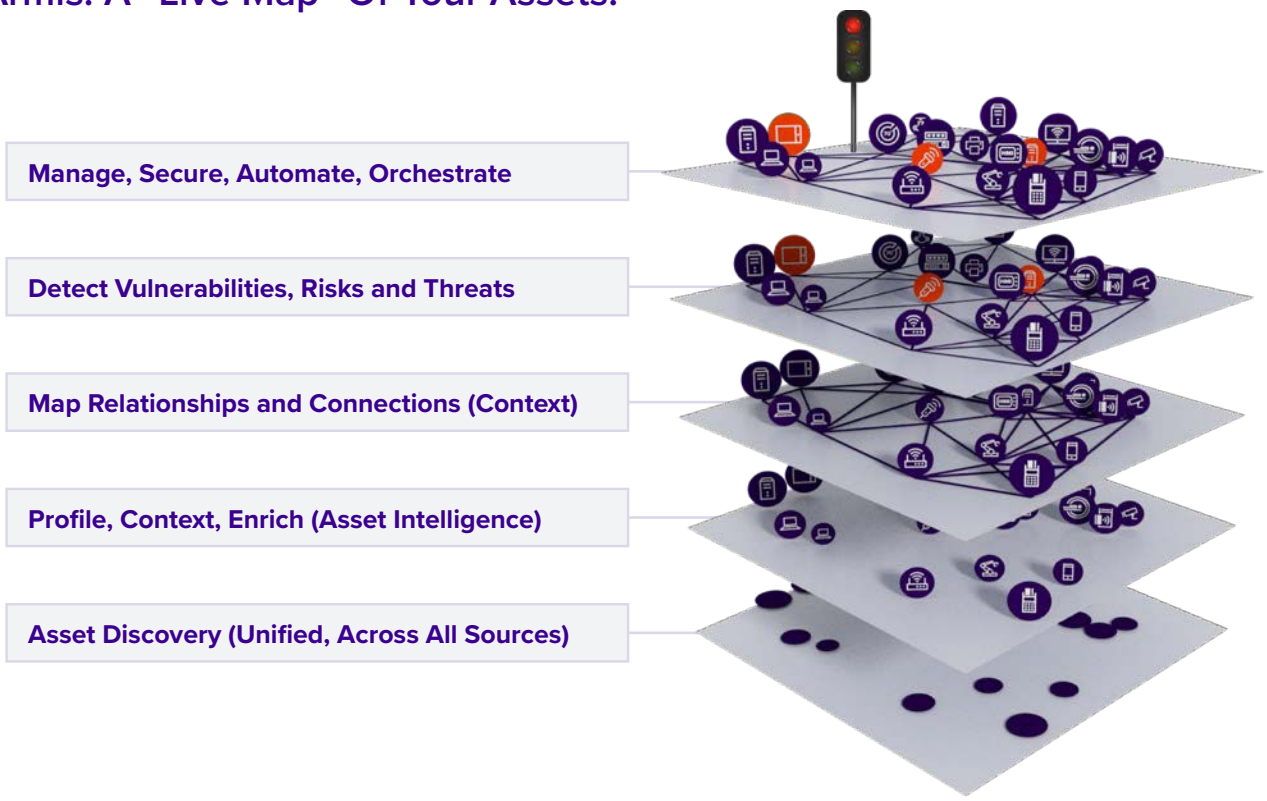
Seeing the Bigger Picture

The lack of a real-time, comprehensive view of assets is a common issue faced by many IT and security teams. Despite using various methods, including spreadsheets and manual counting, organizations often struggle to accurately identify the number and type of assets they have. This problem is compounded by the limited scope of single-purpose, siloed tools for device security, which fail to provide the necessary information to create a complete, unified, and real-time list of all assets. As a result, when IT or security leaders inquire about specific details such as the number of Windows hosts, they may receive conflicting answers from different teams or tools.

To effectively manage cybersecurity assets, organizations must start by addressing the issue of visibility. Security teams must be aware of all assets, including volume, type, and applications, to properly manage them. While business teams prioritize speed and innovation, these factors can create risks for security organizations. The constantly evolving nature of technology means that there will always be more assets and new versions, creating variation and fragmentation. Therefore, IT and security teams require a single source of truth that provides complete visibility into their entire landscape of compliance and security for all devices and assets.

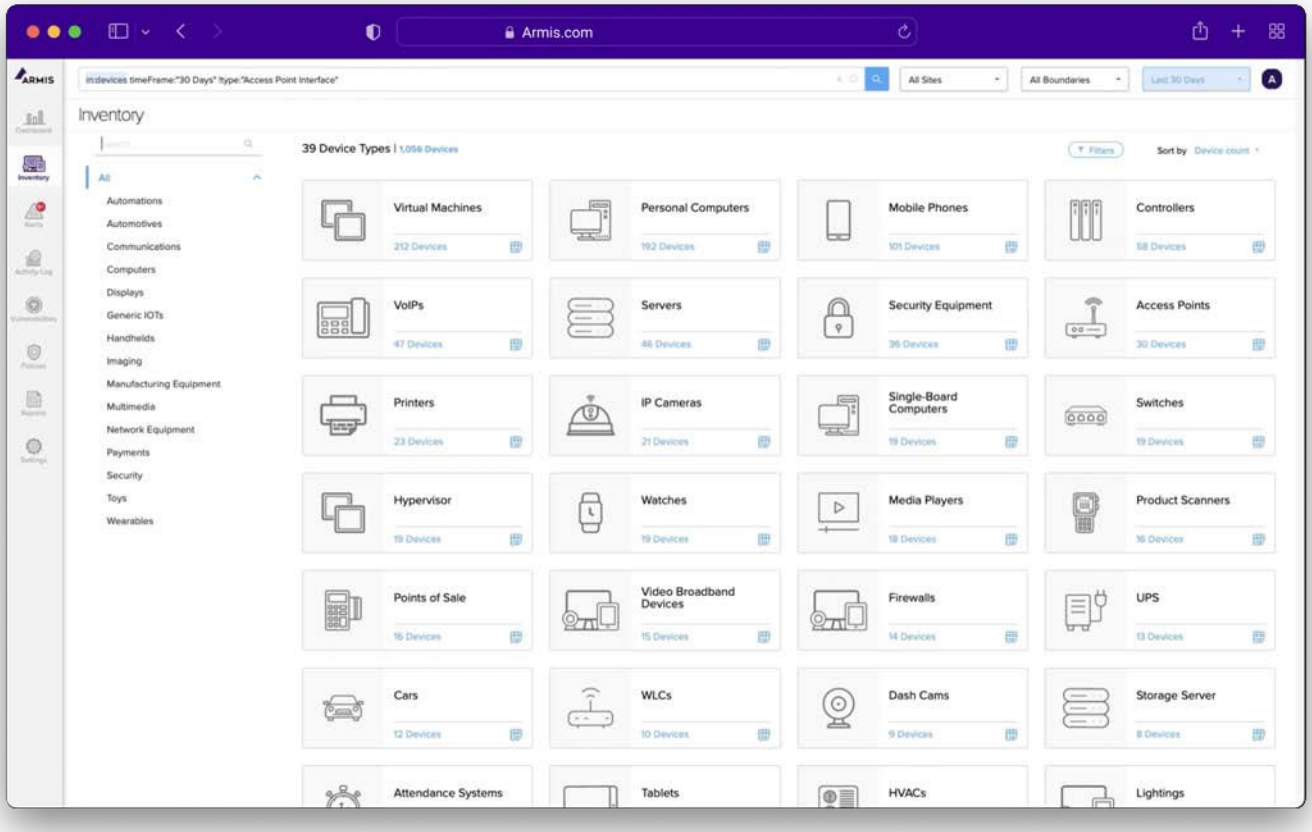
The Armis platform provides enterprise IT and security teams with the necessary visibility into all assets, both managed and unmanaged, to eliminate the asset security blind spots that pose a persistent and increasingly aggressive threat. By identifying all devices, including those off the corporate network, and providing continuous information about their posture, users of the Armis platform can isolate threats and remediate security issues quickly and effectively.

Armis: A “Live Map” Of Your Assets.



Closing the Gap

Existing security tools in the IT and security stack provide only a fragmented and incomplete view of the threat landscape, leaving organizations vulnerable to cyberattacks. While these tools are used to protect individual services and devices, they fail to provide a comprehensive picture of where threats exist. Managing security and compliance policies and configurations for each asset and corresponding service requires identification of the operating systems and applications running on those assets, all while keeping an eye on the ever-changing internal and external threat landscape.



However, this approach creates isolated views of the number of assets and their security posture, resulting in gaps in visibility and enforcement. These blind spots become easy targets for cyberattackers, who seek out weaknesses in the security infrastructure. To address this issue, IT and security teams require a single source of truth for device security coverage that encompasses all assets and related information from all systems.

Ironically, the deployment of “more” security tools for unique purposes can actually complicate security efforts, resulting in blind spots that leave organizations at risk. Therefore, there is a pressing need for a comprehensive approach to device security that provides complete visibility and protection for all assets, and ensures that organizations stay ahead of the constantly evolving threat landscape.

Breaking Down the Silos to Get Actionable Insights

In order to obtain meaningful and effective insights in today’s complex security landscape, it is necessary for organizations to break down the silos that have traditionally compartmentalized risk and mitigated security threats through generic approaches.

While legacy security tools have been effective in mitigating certain risks, they have also created silos that hinder visibility and control, resulting in a lack of actionable insights. The modern security landscape demands a more dynamic and asset-specific approach that can adapt to the ever-changing environment in which devices and assets operate.

Without an asset-specific approach, devices and assets can easily be brought online without proper policy

controls and enforcement, leading to an exponential increase in security and governance issues. To overcome this challenge, organizations must embrace a more proactive and holistic approach to security that breaks down silos and enables better visibility and control. This approach must be centered around asset-specific policies that are designed to adapt to the unique characteristics of each device and asset, ensuring that security and governance remain a top priority in today's fast-paced digital landscape.

Cybersecurity Asset Management Made Simple: A Practical Framework

In today's interconnected digital world, effective cybersecurity asset management is essential to protect organizations against cyber threats. A critical aspect of this is having a complete and unified view of assets, which enables organizations to understand and manage the true risk landscape of their environment.

While network access control (NAC) products are often considered a starting point for asset management, they are not enough. Many devices remain undetectable to those responsible for their security. To address this challenge, organizations need to leverage IT and security management tools that can identify issues across multiple locations, such as the network perimeter, cloud environments, and specific devices and applications.

Moreover, organizations need to move beyond point-in-time assessments and adopt continuous monitoring. This approach provides a more comprehensive view of an environment's security state and enables teams to detect and respond to threats in real-time.

Unfortunately, many existing tools are designed to address specific issues, resulting in isolated consoles with narrow views that create visibility gaps and false precision. To overcome these limitations, organizations should adopt a holistic approach that integrates various security and IT management tools into a centralized platform. This platform should provide a unified view of assets and their associated risks, allowing teams to make informed decisions and take proactive steps to mitigate threats.

Effective cybersecurity asset management requires a comprehensive, continuous, and holistic approach that enables organizations to gain a unified view of assets and their associated risks. By adopting such an approach, organizations can better protect themselves against cyber threats and ensure the resilience of their digital infrastructure.

Comprehensive and Complete Asset Discovery

In today's ever-evolving technology landscape, the concept of a traditional perimeter has become obsolete. Assets and devices are no longer confined to a single location, and they can operate both wirelessly and physically. Therefore, any comprehensive and complete asset discovery solution must be able to identify all types of assets regardless of their location, whether they are connected to the network or not, and whether they are on-premises or virtual.

To ensure a thorough understanding of an organization's security landscape, an asset management tool must be inclusive of all devices, applications, operating systems, and other systems and services - both on-premises and in the cloud. This requires the ability to leverage existing infrastructure, APIs, network connections, and other protocols to connect to all data sources.

To achieve comprehensive and complete asset discovery, it is crucial to have an asset management solution

that can identify all types of assets, regardless of their location or connection status, and can connect to all data sources via existing infrastructure, APIs, network connections, and other protocols.

Armis' approach to effective cybersecurity asset management begins with establishing a centralized and up-to-date inventory of all assets and devices present in an environment. This inventory includes all virtual instances, cloud services, and the rapidly expanding number of unmanaged assets and IoT devices that are currently connected to the environment.

The Armis platform constantly discovers and identifies new devices and assets as they connect to the network, ensuring comprehensive and continuous coverage of the entire asset landscape. By providing a complete and accurate view of all assets, the Armis platform enables organizations to gain insights into the potential risks associated with each device, prioritize security efforts, and proactively manage threats across the entire network.

Benefit from the intelligence of over 3 billion assets from around the globe.

Actionable Intelligence: From Asset Identification to Gap Analysis

With a comprehensive understanding of all assets in an environment, IT and security teams can start identifying and assessing asset details to proactively manage risk, such as which applications are installed on devices. It's not just about knowing whether policies are being enforced or not; it's equally important to understand the complete context associated with each asset, including its user, configuration, and posture, in order to identify any compliance gaps or potential risks. Achieving this level of insight requires the ingestion and analysis of contextual data for each asset.

While many security tools have basic capabilities for this type of analysis, they often focus on a single area of security, such as perimeter access or cloud storage, without considering the broader context of a device or asset. As a result, these tools are often unable to identify issues in aggregate when they are unique to specific devices or assets.

To deliver truly actionable insights, an asset management solution must have the ability to identify gaps and potential risks across all areas of security, including access control, cloud storage, and other disciplines. It must also be capable of analyzing data in aggregate to identify issues that are unique to specific devices or assets, providing IT and security teams with a complete and contextual understanding of the organization's security landscape.

The Armis platform simplifies cybersecurity risk reduction by identifying all devices, apps, and operating systems, evaluating CVEs and assigning risk scores to each asset. The Armis platform leverages the Armis Collective Asset Intelligence Engine, the largest device knowledgebase in the world, which tracks over 3 billion devices. A unique component of the Armis' platform, it continuously analyzes device behavior and identifies potential security threats to provide a comprehensive view of asset behavior and identify any anomalies or suspicious activity that may indicate a potential security breach.

Dynamic Security Policies for Agile Threat Response

Prompt identification and resolution of vulnerabilities, risks, and security gaps is essential for maintaining a secure IT environment. However, manually addressing these issues consistently can be a challenge, even for small organizations with simple IT setups. To overcome this challenge, organizations require real-time policy enforcement and automated security measures that can orchestrate necessary actions, such as isolating devices, initiating software updates, triggering alerts, and scanning for vulnerabilities across all the assets that a device may touch.

Automated security measures can streamline the process of addressing security gaps, reducing response times and minimizing the risk of human error. These measures can include automatic isolation of affected devices, policy-based software updates, and real-time vulnerability scanning. By orchestrating these actions through automation, organizations can quickly and effectively mitigate security risks and ensure their IT environments remain secure.

To achieve this level of automation and real-time response, organizations require a comprehensive asset management tool that can integrate with existing security solutions and manage all devices across the organization, both on-premises and in the cloud. By leveraging automation and real-time security measures, organizations can achieve a more proactive and effective approach to security management.

Crucial Gap Analysis

- Identify endpoint agent deployment gaps
- Address agent "drift" from functional versions
- Ensure proper module installation (e.g., Uninstall Protection, Remote Response)
- Simplify assessment and reporting on gaps without direct tool administration

Ensure a Secure & Compliant Environment

- Identify unscanned assets and network segments
- Report on assets unscanned within the last 7 days (or other timeframes)
- Correlate scan data with information from other security tools
- Gain context on scanned devices (e.g., distinguishing between computers and IoT devices)

Agile Security Management with an Agentless Approach

Many security tools rely on deploying agents into IT environments to gather and analyze activity trends. However, IT and security professionals are hesitant to add another agent to the already crowded asset list. An agentless approach offers a passive but effective solution for building a comprehensive device inventory in real-time, including transient assets.

Providing context to device and asset usage requires analysis of configurations, activities, and other anomalies. It should focus on the following:

Complete visibility: Achieve powerful discovery and unified asset inventory with Armis, providing comprehensive visibility into your organization's devices and networks. This robust solution discovers 3x more assets, ensuring prospects can effectively manage and secure their entire infrastructure.

Contextual Intelligence: Obtain multidimensional views and comprehensive analytics for enhanced contextual intelligence. Armis' advanced approach reduces SOC investigation time by 50%, improving efficiency and effectiveness in addressing security incidents.

Understand Risk and Threats: Identify vulnerability management and prioritization gaps in security controls with Armis' assistance. By improving agent coverage by 15%, organizations can better understand and address risks and threats, strengthening their overall security posture.

Why Customers Around the World Choose Armis

Complete Visibility

Powerful Discovery
Unified Asset Inventory.

3x **More assets** discovered

Contextual Intelligence

Multidimensional views
Comprehensive Analytics & Intelligence.

50% **Reduction in SOC** investigation time

Understand Risks & Threats

Vulnerability Management & Prioritization
Gaps in security controls.

15% Improvement in **agent coverage**

Rapid Time to Value

Modern Cloud Architecture
Industry Leader, Trusted Partner.

10% Improve **Mean Time to Response**

Armis sets itself apart from other security tools by offering a completely agentless approach to asset management. This unique approach simplifies and accelerates deployment across a variety of environments, from single offices to sprawling global networks, without disrupting device operations.v

Real-time monitoring allows for continuous asset discovery and automated enforcement to ensure that every device is properly inventoried. The Armis platform analyzes device data and calculates risk scores based on multiple factors, including device information, manufacturer, reputation, and known vulnerabilities. Additionally, activity and behavior are evaluated and compared to known good profiles of devices to identify any issues or threats.

The agentless and passive nature of the Armis platform means that organizations can quickly and easily gain complete visibility into their assets without interrupting device operations. This is especially important as the number of connected devices and remote work continue to increase, making it more challenging to manage security risks across a distributed workforce.

Conclusion

As technology innovation and IT change continue to bring important efficiencies, they also bring added complexity to protecting organizational assets. With the ever-growing number of assets, it becomes increasingly difficult to maintain visibility into what's touching important organizational data.

To overcome these visibility challenges, IT and security teams can rely on the Armis platform to provide a solution that can identify assets and devices while overcoming siloed fragmentation. The Armis platform starts with asset discovery, enabling IT and security teams to identify critical security gaps and apply automated enforcement of security policies to address risks immediately.

With the Armis platform, modern organizations are well-equipped to keep up with IT change and innovation. The Armis platform provides visibility across all assets and devices on the network, creating the base framework for cybersecurity asset management.

About Armis

Armis is the leading unified asset visibility and security platform designed to address the new threat landscape that connected devices create. Fortune 1000 companies trust our real-time and continuous protection to see with full context all managed, unmanaged, and IoT devices, including medical devices (IoMT), operational technology (OT) and industrial control systems (ICS). Armis provides passive and unparalleled cybersecurity asset management, risk management, and automated enforcement. Armis is a privately held company and headquartered in Palo Alto, California.

armis.com

info@armis.com

20231102-1