



Armis Asset Management

Comprehensive Asset
Visibility and Security for
the Modern Enterprise

NAME
Title



It's 2022 and IT teams *still* face big problems.

“ I wish I knew what was really on my network. I've got dozens of tools, but my processes are still manual, my data is still old, and my IT inventory is still never right. ”

CIO

Fortune 500 Tech Company

Asset management is *still* a challenge.

49B

The estimated number of connected devices globally by 2023.

Source: IDC: Security and the Global DataSphere

84%

of IT professionals say they lack an effective ITAM program.

Source: Deloitte Global ITAM Survey, 2021

90%

say rapidly-changing environments make ITAM more difficult.

Source: Deloitte Global ITAM Survey, 2021

19+

The average number of comprehensive asset inventories per year.

Source: ESG survey, 2020



Servers



Desktops



Network



Mobile



Cloud



Bldg. Mgmt.



Unmanaged

As the number and diversity of assets grows, so does the number of products used to manage them.

Technical debt *still* gets missed.

- Do you know where all your legacy systems and assets are?
- Are you spending more than you need to support legacy assets?

70%

of chief experience officers say legacy modernization is a top business priority.

Source Tata Consultancy Services

Many studies suggest CIOs are spending

80%

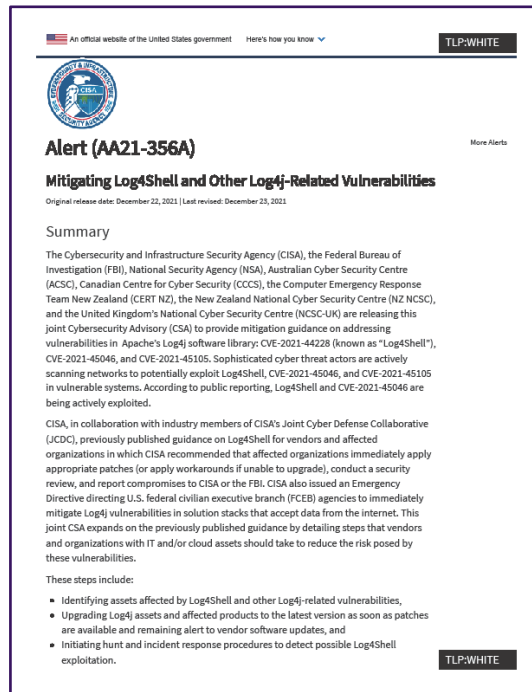
of their budgets to support and maintain legacy systems.

Source Nemertes Research 2021



Vulnerabilities *still* don't get addressed.

- Do you fully understand your organization's **security posture**?
- How are you finding and prioritizing **new vulnerabilities**?
- How do you identify **security gaps** across your business?



The screenshot shows a document header with the text 'An official website of the United States government' and 'Here's how you know'. A 'TLP:WHITE' label is in the top right. Below the header is the CISA logo and the alert title 'Alert (AA21-356A) Mitigating Log4Shell and Other Log4j-Related Vulnerabilities'. The document includes a 'Summary' section with the following text: 'The Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), National Security Agency (NSA), Australian Cyber Security Centre (ACSC), Canadian Centre for Cyber Security (CCCS), the Computer Emergency Response Team New Zealand (CERT NZ), the New Zealand National Cyber Security Centre (NZ NCSC), and the United Kingdom's National Cyber Security Centre (NCSC-UK) are releasing this joint Cybersecurity Advisory (CSA) to provide mitigation guidance on addressing vulnerabilities in Apache's Log4j software library: CVE-2021-44228 (known as "Log4Shell"), CVE-2021-45046, and CVE-2021-45105. Sophisticated cyber threat actors are actively scanning networks to potentially exploit Log4Shell, CVE-2021-45046, and CVE-2021-45105 in vulnerable systems. According to public reporting, Log4Shell and CVE-2021-45046 are being actively exploited.' It also mentions a joint CSA expands on previous guidance by detailing steps that vendors and organizations with IT and/or cloud assets should take to reduce the risk posed by these vulnerabilities. A list of steps includes: identifying assets affected by Log4Shell and other Log4j-related vulnerabilities; upgrading Log4j assets and affected products to the latest version as soon as patches are available and remaining alert to vendor software updates; and initiating hunt and incident response procedures to detect possible Log4Shell exploitation. A 'TLP:WHITE' label is in the bottom right of the document.

Cyberthreats *still* plague every business.

- Can you identify and impacted asset's owner and location?
- Are you sure a device is behaving as it should be?
- How can you stop or prevent attacks?



Asset management and security made simple.

**Effortless, accurate,
comprehensive.**

See it all, all in one place.
Unified visibility across all the
assets and tools in your environment.

Manage hygiene and technical debt.
Accurately track and get alerts
about legacy assets and systems.

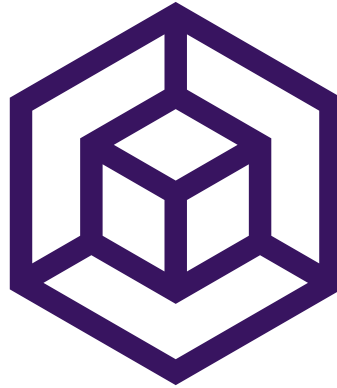
Mitigate vulnerabilities.
Easily identify vulnerable assets
and security gaps so you can reduce
your risk with confidence.



The Armis Platform: A new way forward.



**Consolidated
View of Assets**



**Multi-dimensional
Visibility**



**Real-time, Up-to-date
Asset Information**

Why Armis?

Asset Management

Get a unified, trusted source of information.

- Single view of every asset, everywhere
- Un/managed, mobile, cloud, and more
- Device identification and classification
- CMDB enrichment

IT Hygiene & Technical Debt

Identify legacy systems and assets.

- Reporting on aging hardware and software assets
- Alerts for certificates near expiration
- License and service contract cost control

Vulnerability Management

Identify and prioritize vulnerabilities.

- Better understanding your security posture
- Security gaps like missing agents
- Access to previously unavailable asset data, contextualized

Threat Detection

Identify threats and the assets impacted.

- Real-time threat intelligence
- Behavior analysis
- Asset owner and location information
- Mitigation using SOC tool integrations

DocuSign

Mondelēz
International

MATTRESS
FIRM



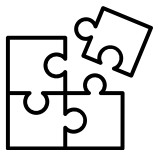
Sysco

Booking.com

JOHN MUIR
HEALTH

Democratize asset data across your business.

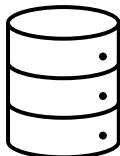
Architects



Operations



CMDB



EAM



Service Desk



Configuration – Software – Connections – Vulnerabilities – Risk – Reconciliation

REAL-TIME ASSET INTELLIGENCE



Servers



Desktops



Network



Mobile



Cloud



Bldg. Mgmt.



Unmanaged

Hundreds of meaningful integrations.



Some of our featured, prebuilt integrations.

The Armis Platform

- Unified asset inventory and security
- Analytics, reporting, and insights
- Knowledgebase of 2B+ devices
- Contextual insights
- Risk scoring



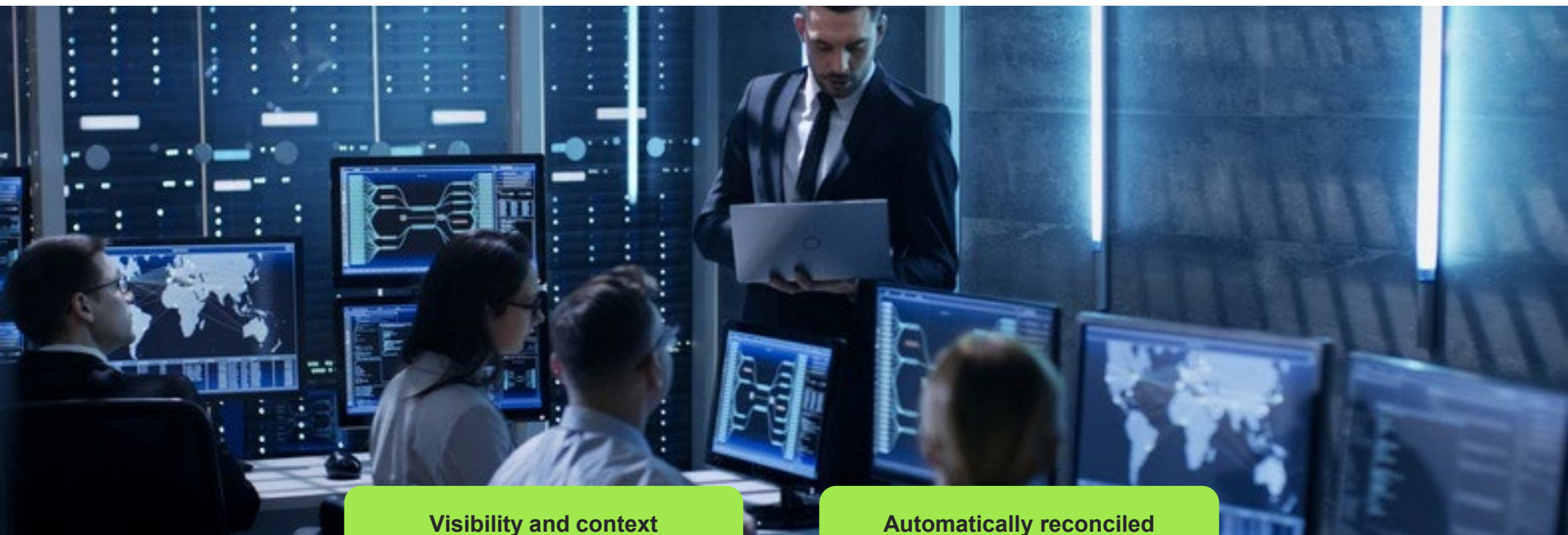
BYOD DEVICES

MANAGED DEVICES

CLOUD & VIRTUAL

UNMANAGED AND IOT DEVICES

Case Study: Fortune 50 Tech company

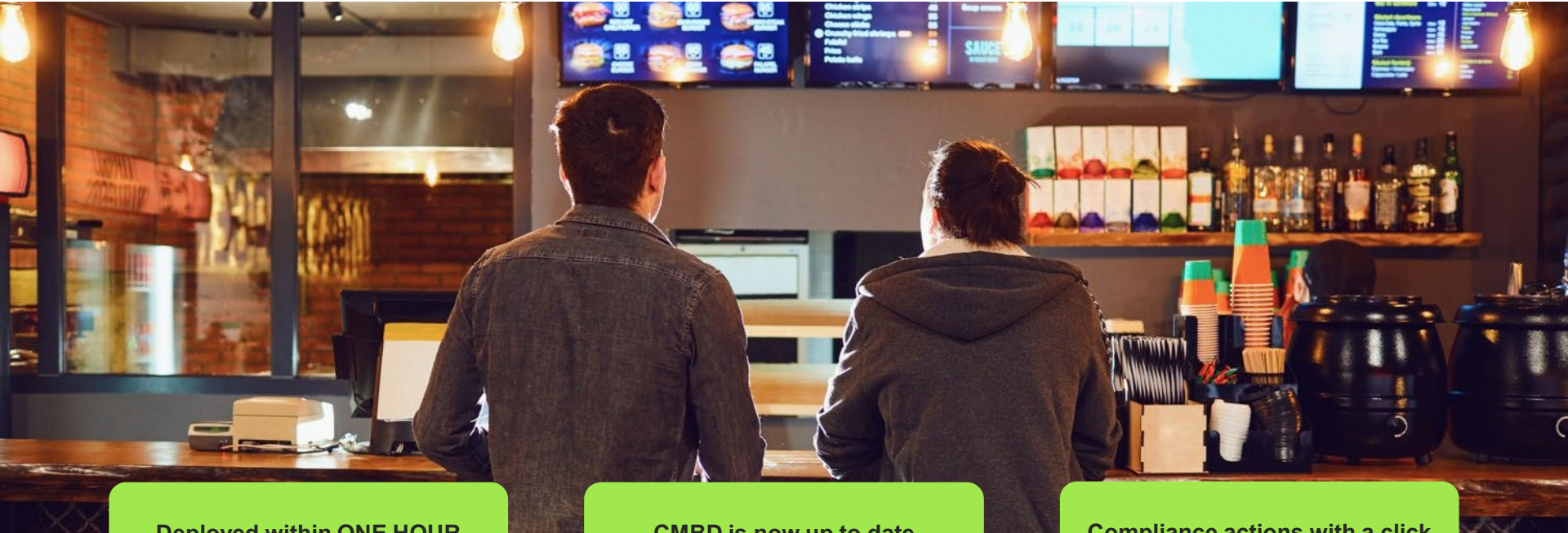


Visibility and context
in seconds

Automatically reconciled
with CMDB

“It used to take SOC days to weeks to track down asset information on an IP address somewhere in Bangalore.”

Case Study: US Food retailer, 10,000+ locations



Deployed within ONE HOUR

CMBD is now up to date

Compliance actions with a click

"Other solutions required appliances, agents, or a costly years long deployment—a mission impossible across 10,000+ sites"

Questions?



Let Us Prove It!

Take the Armis Quick Asset Visibility Assessment

- Get started in 30 minutes or less!
- Identifies devices, risks, exposures
- Provides an executive findings report to share with your colleagues and staff.

Learn more: armis.com/visibility



Thank you.

