ARMIS

ARMIS BUYER'S GUIDE

Election Protection

Protecting Election Integrity and the Democratic Process

Armis Centrix™ provides full visibility into elections systems, documenting activity and automatically mitigating threats.

Secure, fair and transparent elections are a cornerstone of democracy. However, nation-states, ransomware gangs and other threat actors increasingly target elections systems to undermine trust in the democratic process, extort money and cripple devices.

Nearly 40% of IT professionals in the Armis 2024 Cyberwarfare Report believe cyberattacks could affect the integrity of an electoral process.[1]

Elections systems are particularly vulnerable. They are network connected, and they have many components — from voter registration databases and network servers to electronic polling machines and vote counters — that expand the attack surface. In addition, traditional security software used to monitor, detect and respond to attacks may not work on many election-related devices.

Elections officials need a comprehensive asset management and security strategy to protect elections and meet specialized security requirements. This Buyer's Guide covers key criteria and capabilities to safeguard elections systems.

[1] Armis. The State of Cyberwarfare, The Invisible Frontline: AI-Powered Cyber Threats Illuminate the Dark Side. April 2024. https://www.armis.com/cyberwarfare/

01

Elections systems are under attack

Elections systems face multiple risks and vulnerabilities.

02

Elections are complex

Multiple facilities, systems and devices create a large attack surface. All of it must be protected.

03

Elections devices can be hard to manage and secure

The devices used for polling, vote counting and other election functions are usually general-purpose computers that run proprietary software. Vendor lockdown makes it difficult to install, patch or update endpoint security agents on these devices.

04

Attacks are constant

The speed, sophistication and scale of attacks against elections infrastructure are escalating. Adversaries now use artificial intelligence (AI) to amplify ransomware, distributed denial of service (DDoS) and phishing attacks. They also use AI-generated synthetic media — like robocalls that impersonate officials or public figures — to spread disinformation.

Global nation-state attack attempts more than doubled in 2023.[2]

05

Siloed security tools present an incomplete picture

The average security organization has 76 security tools to manage. Each tool generates independent data points, leading to a fragmented view of security. Organizations also struggle to identify gaps and report on the hundreds of security controls defined in security frameworks such as those provided by the National Institute of Standards and Technology (NIST) and the Center for Internet Security (CIS).

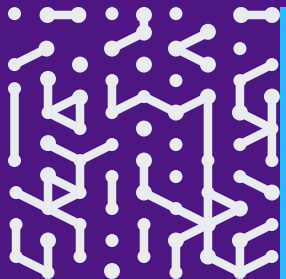
06

Lack of asset visibility and control increases risk

Organizations need to see, manage and protect their entire attack surface to safeguard elections assets and maintain the public's confidence in elections mechanisms. However, elections systems are closed and opaque.

"If you don't know what the risk is, how can you protect against it," says Michael Atkinson, principal public sector sales engineer for Armis.

[2] Armis. The State of Cyberwarfare, The Invisible Frontline: AI-Powered Cyber Threats Illuminate the Dark Side. April 2024. https://www.armis.com/cyberwarfare/



See, manage and protect your election system

When choosing a solution to see, manage and protect your elections system, consider these best practices and solution capabilities.

Maintain a complete asset inventory

Visibility is critical to obtain an accurate inventory of elections system assets and to control the attack surface. However, most organizations track these assets using spreadsheets or other error-prone manual methods.

“It’s very common for organizations to underestimate the number of devices they have on their network by a hundred percent or more,” says Atkinson.

Security teams often use device agents to capture information and help manage network devices. However, putting these agents on elections system devices often leads to malfunctions and degrades performance. In addition, agent software is difficult to apply due to vendor lockdown of elections solutions.

Bottom line

You need an agentless solution that passively and continuously tracks device type, manufacturer, OS version, reputation and connections.

Questions to ask

- How do you discover assets that connect to the network?
- Do you have a complete and up-to-date asset inventory across all asset types including managed and unmanaged assets?
- How much manual work is involved?
- Do you trust the data?
- Do you want to fix and enrich your configuration management database (CMDB)?

Promote IT hygiene and address technical debt

Visibility is essential to identify devices that need updates and patching, have reached end of life or end of support, or have been installed without network administrators' knowledge (e.g., employees' personal devices and unapproved "shadow" software).

Although traditional vulnerability scanning is an important tactic for identifying and remediating vulnerabilities, it can impair elections system devices.

"It's a very common problem for devices outside of traditional enterprise IT," says Atkinson. "Take a poorly made device that lives on the network. If you scan it for vulnerabilities, the network component of it can't respond to the requests in time and it crashes. It can knock out the device and cause physical damage."

Bottom line

If you don't have a continuous, passive and agentless asset management and security solution, you won't be able to maintain good IT and security hygiene on elections devices that can't tolerate a software agent or vulnerability scanning.

Questions to ask

- How do you keep track of assets that need to be upgraded or patched?
- Do you have systems that should have been retired? Are you sure they have been disconnected?
- Are you paying for too many/not enough software licenses?
- How do you track expired licenses and certificates?

Control and reduce the asset attack surface

The fewer assets connected to the elections system, the smaller the attack surface and the easier it is to defend it. However, controlling and reducing the asset attack surface is extremely challenging.

Atkinson recalls an attack on a statewide elections management system during the November 2020 general election where a state sponsored threat actor compromised the state's network through an unprotected department of transportation traffic camera.

Organizations may have assets on their network — or even whole network segments — that they don't see. In addition, many elections authorities run their elections system on the general-purpose network rather than a dedicated segment.

You can shrink the attack surface by segmenting your elections system from other parts of your network, implementing firewalls and patching vulnerabilities. Where patches don't exist, find a compensating control that helps protect the elections system.

Bottom line

Because understanding, controlling and reducing the attack surface is so complex, it's important to work with a vendor with deep expertise in attack surface management.

Questions to ask

- How do you ensure that elections networks are properly segmented from the voting system components?
- Which elections system assets are most vulnerable in the event of a cyberwarfare attack on your organization?

Manage asset vulnerabilities and prioritize by risk

Nearly 60 percent of data breaches are due to exploitation of a known vulnerability that has not been patched.[3]

It's vital to patch devices quickly. However, the sheer volume of vulnerabilities can easily overwhelm even well-staffed IT organizations.

More than 26,000 vulnerabilities were disclosed in 2023 alone. The total volume of accumulated vulnerabilities that organizations need to address today is in the millions. In addition, threat actors increasingly use a combination of known vulnerabilities in a single attack.

Known software vulnerabilities aren't the only risk to elections systems. You must also identify and address improper network segmentation, wireless security and other configuration issues.

[3] Higgins, Dark Reading. Unpatched Vulnerabilities the Source of Most Data Breaches. April 2018. https://www.darkreading.com/vulnerabilities-threats/unpatched-vulnerabilities-the-source-of-most-data-breaches

Bottom line

The key to prioritizing vulnerabilities and issues appropriately is to understand them in context. Not all vulnerabilities present an imminent risk. Not all risks have the same potential impact. Choose AI-driven solutions that prioritize risk-based alerts and offer contextual insights based on comprehensive, in-depth intelligence from billions of devices.

Questions to ask

- When assessing vulnerabilities, do you have the data you need, such as: What type of asset? Where is it located? How critical is it? Who owns it?
- Would this data help improve your mitigation efforts?
- Do you have a process for prioritizing and remediating vulnerabilities?
- How do you ensure that all your endpoints are properly protected by endpoint security solutions (i.e., they have agents installed and agents are the correct version)?

Detect and mitigate assets impacted by threats early

The volume, veracity and variety of vulnerabilities that a threat actor can choose in targeting an organization is endless.

Armis Centrix™ for Actionable Threat Intelligence will empower revolutionary prioritization - leveraging early warning detection and threat intelligence to address the vulnerabilities that are actually being exploited by threat actors.

Early warning intelligence is essential to anticipate and mitigate cyber threats effectively. It is a key solution differentiator and includes:

Human Intelligence Integration: Targeting the humans behind the keyboard, HUMINT captures threat activity.

Smart Honeypots: Dynamically deploys purpose-configured honeypots into potential "hotspots" and allows for the observation of malicious behaviors and techniques.

Dark Web Intelligence: Leverages proprietary AI to gain valuable intelligence into threats still in the formulation stage.

Bottom line

An agentless solution is an important differentiator because it understands every type of device — not just those that have a software agent attached. Use a passive, agentless solution that draws on extensive intelligence to interpret behavior in real time.

Questions to ask

- How do you detect asset behavior anomalies that can indicate a threat?
- What early warning, evidence-based sources do you use to track threat actors and their activity?
- How do you integrate your various early-warning intelligences sources (e.g., honeypots, dark web, human intelligence) to get a unified view?
- When a threat is detected, how quickly can you pinpoint impacted assets?
- How do you locate impacted devices and their owners? Do you know what type of devices they are?
- How easily can you block problematic devices from accessing the network?
- If you had all the data you need in a single view, would it improve your mean time to respond (MTTR)?

Achieve compliance with internal policies and industry standards

Achieving compliance ensures elections systems meet minimum criteria for security, functionality and accessibility. Demonstrating compliance is also critical for addressing challenges to the outcome of an election and for defending against lawsuits.

"When somebody says their elections management system malfunctioned and changed the outcome of an election, the elections authority must be able to show evidence that they were exercising due diligence and that devices were working as designed," says Atkinson.

Bottom line

To achieve compliance and prove it, be sure your solution tracks and logs hundreds of different kinds of activity for devices that are very unusual on most networks, such as elections machines and elections management systems.

Questions to ask

- How do you ensure all your endpoints have required agents installed on them? How do you confirm the correct version?
- How do you validate that asset configurations meet internal policies?
- How do you demonstrate compliance across different assets?
- How do you track your overall security posture?
- In the event you face a lawsuit or must defend an election outcome, do you have the data you need to prove your elections management system operated as required?

Leading the way in asset intelligence, context and management

Armis excels at delivering comprehensive asset management and security solutions that safeguard elections systems. More than 50 executive branch agencies rely on Armis solutions to manage and secure their most valuable assets.

The Armis Centrix™ cyber exposure management platform and products are powered by the Armis AI-driven Collective Asset Intelligence Engine, which sees, secures and manages billions of assets around the world in real time. By protecting the entire attack surface and managing cyber risk exposure as it occurs, Armis solutions help ensure elections are secure, fair and transparent.

Armis differentiates its offerings with a depth of intelligence and technology that other vendors cannot match:

- Passive, agentless and continuous asset management. Armis Centrix™ understands every kind of device. It discovers, monitors and documents every single asset on the network and provides contextual intelligence about it.

> *"We've had issues in the past where somebody would bring in a device from home that they shouldn't connect. Now with Armis, as soon as something like that happens, it gives us immediate notification,"*
>
> **Jamie Pownall**
> Chief innovation office
> Henry County, Georgia.[4]

- Extensive, multi-faceted intelligence. The Armis Collective Asset Intelligence Engine logs and analyzes more than 100 different types of activities across more than 4 billion devices. It's 10 times the size of all Armis competitors combined. In addition, it analyzes asset intelligence as a whole to provide greater context about asset behavior and relationships.
- Rapid deployment. A single console provides a complete view and easy management of all assets — with zero configuration.

[4] Armis Case Study. Fast-Growing Georgia County Finds a Better Way to Discover Devices and Secure the Network. 2024. https://www.armis.com/case-studies/fast-growing-georgia-county-finds-a-better-way-to-discover-devices-and-secure-the-network/

Armis Centrix™ for Asset Management and Security

Streamlines asset management while fortifying security posture. An intuitive interface and advanced analytics provide deep situational awareness and track and manage assets across diverse environments, ensuring optimal utilization and cost-effectiveness. Real-time threat detection and response safeguards assets from potential cyber risks and vulnerabilities.

Armis Centrix™ for OT/IoT Security

Is tailored to protect operational technology (OT) and Internet of Things (IoT) devices in industrial, critical infrastructure and enterprise environments. It enables organizations to monitor and manage their OT/IoT ecosystems precisely and efficiently. Sophisticated policy, anomaly and behavior analysis capabilities ensure early threat detection and proactive mitigation, minimizing the risk of cyberattacks and operational disruptions.

Armis Centrix™ for Vulnerability Prioritization and Remediation

Lets organizations see all vulnerabilities and prioritize their response based on vulnerability criticality and business risk.

Armis Centrix™ for Actionable Threat Intelligence

Proactive cybersecurity solution designed to empower organizations with early warning intelligence to anticipate and mitigate cyber threats effectively. By leveraging AI-driven actionable threat intelligence, Armis Centrix™ provides insights into potential threats, allowing organizations to understand their impact and take preemptive action.

Time is of the essence

With the U.S. presidential election just months away, elections authorities must move swiftly and decisively to procure and implement the capabilities needed to protect elections system assets.

The Armis team can help you fully deploy and integrate an Armis solution across your county or state elections systems within days, if not hours. Get started now.

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