Trellix

ELECTION SECURITY EBOOK

Protecting election systems from cyberthreats

Detect, prevent, and respond to malicious intrusions to assure election integrity

Preserving public confidence in election systems

Democracy depends on public confidence in the integrity of our election systems. Citizens must be able to trust that all votes will be counted accurately and securely.

Today, election integrity is continuously questioned. More than ever, state and local voting officials must ensure that voter registration databases, election management software, and associated IT infrastructure are safeguarded against malicious cyberattacks. Whether originating from nation-states or individual bad actors, any breach—or even the threat of a breach—could have deep, lasting impact on public trust.

Moreover, intrusions can occur any time—not just on election day. Bad actors are constantly working to breach networks, exploit vulnerabilities, exfiltrate or manipulate voter data, or otherwise cause disruption any way they can. And these days, they are more empowered than ever with AI.

When digital threats are increasingly sophisticated and relentless, secretaries of state and county election officials must ensure their election systems are protected against advanced cyberthreats. Cybersecurity plays a critical role in driving resiliency and creating a system that's designed to endure, recover quickly, and preserve trust among election offices and the public.

The threat is real and growing

Cyberthreats are becoming more sophisticated and pervasive every day. The Trellix Advanced Research Center (ARC) revealed that APT-backed (advanced persistent threats) detections increased 17% in the six months leading up to March 2024—on top of a 50% increase in detections in the preceding six months.

Leading up to elections, geopolitically motivated threats accelerate. ARC reported more than 11 million detections of malicious activities against US government organizations in a single day during the US Democratic National Party convention in 2024, exceeding daily average detections by 55 times.

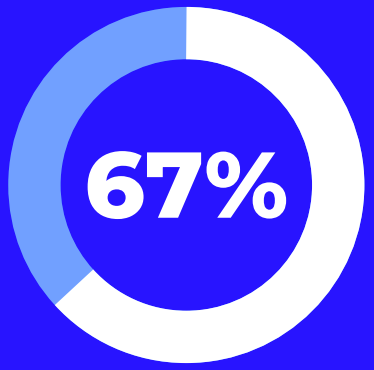
Cyberattacks can take many forms. An advanced persistent threat could surreptitiously move through the network, harvesting data or capturing credentials, just waiting for the right moment to act. And even if systems and software are not altered or damaged, publicity about a threat actor infiltrating election systems could damage public confidence.

Phishing attacks can easily lure someone via email into downloading malware that allows a command-and-control server to take over election systems. Clicking on an innocent-looking link might trigger ransomware that locks down the network—and shuts down operations—before anyone has a chance to react.

Using compromised credentials, threat actors might also impersonate an election official or staffer to gain higher-level permissions on a system or network, likely intending to explore a network or database of interest.

In addition, nation-state actors and cybercriminals are increasingly experimenting with AI. AI-generated videos, sophisticated deep fakes, and automated misinformation spread by bots pose significant threats to election security.

A staggering increase in threats



Jump in APT-backed detections in one year

55x

One-day spike in average daily detections of malicious activities against US government organizations

Sources:

- Trellix Advanced Research Center CyberThreat Report, June 2024
- Cyber Threats Targeting the US Government During the Democratic National Convention, Trellix, October 2024

Understanding the challenges

Naturally, secretaries of state and county election boards take every measure possible to protect election systems and voter data. But in many cases, weaknesses in existing cybersecurity solutions don't become apparent until after a breach has occurred.

Disparate security solutions among counties often mean lack of centralized visibility. Counties may lack sufficient resources to continuously monitor networks, servers, and workstations for incidents. And some legacy security solutions simply aren't able to use modern detection and response techniques or draw upon global threat intelligence to proactively defend against attacks.

Addressing these issues can be challenging. State and local election offices often have their own separate election systems and purpose-built solutions to secure those systems. But limited budgets preclude investing in comprehensive threat intelligence and analytics or centralized intrusion detection and response.

To resolve this dilemma, some states are making the investment in new technologies, offering counties more advanced cybersecurity capabilities and centralized monitoring—either as their complete security solution or to complement existing solutions.

Industry leading threat detection and response

About half of US states and numerous counties have invested in an integrated, end-to-end security solution from Trellix. This comprehensive AI-powered security platform brings together diverse technologies to protect endpoints, email systems, and networks, combined with the resources and expertise to implement, run, monitor, and improve the security posture across the election landscape.

Trellix works in concert with existing legacy security solutions, adding agents to workstations and servers that can instantly detect intrusions or anomalies. Behind the scenes, an incident response team acts on alerts to proactively address any threat before it has a chance to do harm.

Drawing on the industry's best threat intelligence, Trellix meets AI threats with Trellix Wise GenAI insights and responses. And in light of high-profile outages related to security updates, Trellix takes a responsible security approach by giving users visibility into the solutions, choice in how they roll out updates, and protection against people and process errors.

Leveraging funds made available through the Help America Vote Act (HAVA), states can implement Trellix solutions today to ensure consistent cybersecurity that extends from the secretary of state's office across county election organizations. The result is greater oversight and control of the election system—and greater peace of mind for election officials.

How a Midwestern state assures election system security

When one midwestern US state wanted to fortify its cybersecurity, it made Trellix solutions available to all counties. Counties have the option to deploy Trellix to monitor and secure the network against threats, watch for anomalies on staff workstations, protect email systems from phishing attacks, and gather forensic analysis if necessary.

Counties with the most comprehensive coverage deploy Trellix Network Security, Trellix Endpoint Security, Trellix Email Security, and Trellix Data Loss Prevention, with Trellix Helix Connect for centralized visibility across it all. Trellix partner Google Mandiant provides incident detection and response while Skyhigh Security protects internet traffic with Secure Web Gateway.

Because IT resources vary widely across counties, the Trellix team serves as a trusted advisor to guide a quick rollout—typically within weeks—and provide ongoing cybersecurity best practices.

This US state made Trellix available to each of its counties free of charge because, as the secretary of state points out, when the county election systems are secure, the entire state system is secure. Going into the next election cycle, the secretary of state is confident in the security of its election systems.

> “We entered into a contract with Trellix. That company is world-renowned. It’s a detection of activity, a prevention of hackers, and remediation. If something would happen in one of the counties, Trellix would be right there—they can gather the forensic evidence and notify all the other counties of here’s what you need to watch for.
>
> - Secretary of State (former), Midwestern State

How a county extends election system protection

A large US county relies on Trellix to complement its existing security solutions. With an endpoint detection solution already in place, the county bridges gaps with Trellix Endpoint Security to detect and respond to cyberthreats on workstations. Trellix Data Loss Prevention prevents unauthorized data transfers while Trellix Security Information and Event Management (SIEM) provides centralized analysis of security events. Skyhigh Secure Web Gateway then monitors and filters potentially harmful internet traffic.

Given the county's hybrid security infrastructure, Trellix Threat Intelligence Exchange brings insights from real-time, global sources to identify emerging threats, recognize patterns, and block threats. With support from the Trellix team, the county ensures best practices across its security solutions.

> "Trellix sold and protected the state's SoS central office and quickly expanded the opportunity to solve other vulnerabilities at the county level.
>
> - Account Representative, Global Technology Services Provider

Delivering peace of mind

For secretaries of state, Trellix solutions and security experts bring peace of mind. Both digital and human “eyes” are continuously watching for any attempts to infiltrate election systems. In fact, by leveraging the most current threat intelligence gathered from around the world, Trellix security solutions can detect the very latest threats and exploits that could be missed by legacy signature-based security approaches.

In the digital age, cyberthreats are a reality every state and county election office must face. But with strong defenses in place, those threats can be prevented from causing trouble. This is the key to keeping election systems secure every day and, most importantly, on election day—so election officials and the voting public can maintain confidence in the democratic process.

Build greater trust and confidence in the integrity of your election systems.

Get the strongest defense possible against cyberthreats with Trellix.

For more information, visit www.trellix.com/elections.