Trellix

CASE STUDY

How a Midwestern US State Ensures Safe and Secure Election Systems

Industry

Government

Trellix® and Partner Solutions and Services

- Trellix Security Platform
- Trellix Network Security
- Trellix Endpoint Security
- Trellix Email Security
- Trellix Data Loss Prevention
- Trellix Helix Connect
- Trellix Security Information and Event Management
- Trellix Threat Intelligence Exchange
- Trellix Professional Services
- Skyhigh Security Secure Web Gateway
- Google Mandiant Incident Detection and Response

The Results

- Faster threat detection
- Reduced incidents
- Tighter data protection
- Cost savings from avoided breaches
- Peace of mind regarding election integrity
- Public trust

An Unprecedented Threat Landscape for Elections

Elections should make news, but not for what goes wrong. As cyberthreats become more sophisticated and pervasive each day, now aided by AI, the risk of an attack escalates—with potentially serious impacts on elections and public trust.

State and county election entities have never faced more geopolitically motivated cyberthreats, on election day or any time. On just one day during a US political convention, more than 11 million malicious activities were detected against US government organizations—exceeding daily average detections by 55 times.[1]

In one midwestern US state, the pursuit of election system integrity led the Secretary of State to seek a comprehensive security solution for stronger protection from the state capital to all county election offices.

Secretary of State officials were concerned about potential internal or external interference with any technology, systems, or hardware that touched critical election information. Adding to their risk, disparate, potentially outdated security solutions among counties meant low visibility and high vulnerability.

Many counties also lacked sufficient resources to continuously monitor networks, servers, and workstations for incidents or to keep up with the latest threats. The state sought a technology partner to help county election boards bridge the gaps in existing solutions and stay on top of emerging threats.

AI-Powered Extended Detection and Response

The Secretary of State has continuously chosen Trellix as part of its well-rounded effort to protect election system integrity. To drive standardization and security statewide, they make Trellix available to each of their counties free of charge.

In counties with legacy security solutions, Trellix enhances those measures. The AI-powered extended detection and response platform brings together diverse technologies to protect endpoints, email systems, and networks, and the resources and expertise to implement, run, monitor, and improve the security posture across the election landscape.

"We partner with Trellix, for detection of activity, prevention of hackers, and remediation. If something would happen in one of the counties, Trellix is 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

The counties that adopt Trellix gain a world-class security solution, threat intelligence to match daily changes, and professionals to help them deploy and manage their election security regardless of their level of IT resources.

Defense Against Cyber Threats in All Their Forms

With remote help from Trellix Professional Services, counties roll out the solution within weeks—getting protection in place rapidly. Counties that choose to roll out the most complete coverage are protected against today's leading threats in all their forms:

- **Advanced persistent threats (APTs) –** Counties guard against sophisticated, often state-sponsored campaigns that aim to breach critical infrastructures and harvest data. Trellix XDR employs machine learning and AI to detect, correlate signals across threat vectors, and respond to threats across endpoints, networks, email, and cloud systems before they can cause damage.
- **Phishing attacks –** An innocent-looking link might trigger ransomware that locks down the network—and shuts down operations. Trellix Email Security scans incoming emails for common and sophisticated phishing attempts, malicious links, and suspicious attachments using advanced threat intelligence and machine learning.
- **Ransomware and malware –** Ransomware and malware could mean data breaches and bring down the network. Counties turn to Trellix Endpoint Security to continuously monitor endpoints like election workers' computers for suspicious behavior. The system can block malicious activity, isolate the endpoint, and perform forensic analysis to understand how the attack occurred and what was affected

  Trellix's sister company Skyhigh Security further protects internet traffic against malware attacks with its Secure Web Gateway, ensuring access to business-critical, web-based systems.
- **Network attacks –** As threats to critical election networks grow more complex, Trellix Network Security spots and stops evasive attacks. The Network Security solution uses behavioral techniques to establish baseline network behavior patterns and help contain intrusions with speed and intelligence.
- **Data loss –** Internal and external threats put election data at risk. Trellix Data Loss Prevention delivers unprecedented protection for sensitive and proprietary information from workstations to the cloud. Counties gain visibility so they can find critical data, classify only the data that requires added protection, set policies, and detect inappropriate activity for remediation.
- **Rapid alerting and response –** Trellix partner Mandiant (now part of Google Cloud) handles alerts and then analyzes and mitigates threats.

Across it all, Trellix Helix Connect integrates security controls from the Trellix security platform and 500+ third parties to create deep multi-vector threat detections and prioritized, AI-guided responses to threat events.

One Large County: Trellix and Legacy Solutions

Many counties deploy Trellix in addition to their legacy security. With an endpoint detection solution already in place, one large county fortifies its posture with Trellix Endpoint Security. Trellix works in the background to detect indicators of compromise without interfering with workstation performance or requiring significant input from county staff.

Meanwhile, 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.

A Responsible Partner

No county is the same in terms of systems, resources, and knowledge. Adding to the challenge, the state cannot assist them because they lack visibility into county-level election data. That's why a trusted advisor like Trellix becomes crucial to help the state and counties.

Trellix Helix and Mandiant watch for threats while counties maintain their sovereignty. Regardless of their setup, from implementation and throughout the relationship, Trellix serves as their primary cybersecurity partner, providing guidance across the Trellix platform and the entire security landscape.

In light of recent high-profile outages related to security updates, Trellix acts as a responsible partner giving users a view into the solutions, choice in how they roll out updates, and protection against people and process errors.

Preserving Election Integrity—and Public Trust

With a track record of protecting election system security, the midwestern state has repeatedly chosen Trellix and made it available to every county. Threat actors and threats continuously evolve, but the state trusts Trellix to help keep it abreast of emerging risks.

For the midwestern state and its counties, the Trellix partnership has meant faster threat detection, reduced incidents, tighter data protection, and cost savings from avoided breaches. Most importantly, the Secretary of State and counties have peace of mind that they are doing everything possible to maintain election system integrity—and preserve public trust.

Sources

1. https://www.trellix.com/blogs/research/cyber-threats-targeting-the-us-government-during-the-democratic-national-convention/