



Protecting election systems from cyberthreats

Trellix election security solutions detect and prevent malicious intrusions to assure election integrity



Preserving public confidence in election systems

Democracy depends on public confidence in the integrity of election systems. Today, 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.

In these times where nearly every election may be questioned, secretaries of state and county election officials must ensure their election systems are protected against advanced cyberthreats—so they can focus on election results with confidence.

The threat is real and growing

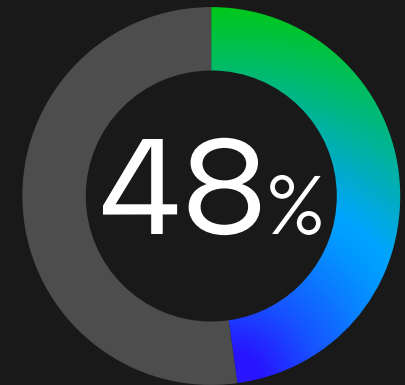
Cyberthreats are becoming more sophisticated and pervasive every day. According to reporting by CompTIA, the number of phishing attacks grew substantially during the first six months of 2022—up 48 percent—and ransomware incidents increased by 41 percent in the same period¹. Data for 2023 is likely to be on a similar track.

Phishing attacks can easily lure someone 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 shutting down operations—before anyone has a chance to react.

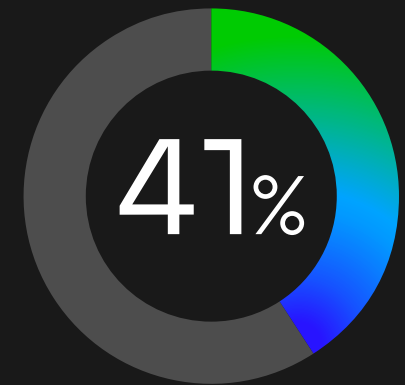
An advanced persistent threat could be surreptitiously moving through the network, harvesting data or capturing credentials, just waiting for the right moment to act. And even if systems and software are not altered or damaged, publicity about a threat actor infiltrating election systems could damage public confidence—and possibly ruin political careers.

Therefore, decisive steps should be taken today to bolster election system security and avoid damage—or embarrassment.

Cyberthreats in the first six months of 2022



more phishing attacks



more ransomware incidents

¹Source: CompTIA, <https://connect.comptia.org/blog/cyber-security-stats-facts>



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 means lack of centralized visibility is often an issue. Counties may not have 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—with great success.

Integrated, end-to-end cybersecurity solutions

Secretaries of state always strive to make elections as secure and trouble free as possible. Several states are now taking additional measures by investing in an integrated, end-to-end security solution—Trellix Secure Elections. This comprehensive solution brings together the 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 Secure Elections works in concert with existing legacy security solutions, adding agents to workstations and servers that

can instantly detect intrusions or anomalies. The solution also includes access to an incident response team that acts on alerts to proactively address any threat before it has a chance to do harm.

Leveraging funds made available through the Help America Vote Act (HAVA), states can implement Trellix Secure Elections 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 election system—and greater peace of mind for election officials.



How one state assures election system security

In one state, the Trellix Secure Elections solution provides the secretary of state with greater assurance by detecting malicious activity, preventing intrusions and exploits, and remediating incidents that may occur in any of its counties. Additionally, the solution includes forensic analysis of each incident, the results of which can be used to further improve cyber defenses across the state.

In this case, the solution includes Trellix Endpoint Security, Trellix Email Security, and Trellix Network Security. Additionally, the state deployed Trellix XDR, which centrally collects, correlates, and analyzes threat telemetry in real time, using artificial intelligence and machine learning to dramatically improve threat awareness, reduces investigation time and provides response orchestration.

This state made the Trellix solution 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. Therefore, this secretary of state is confident going into the next election cycle that the state's election systems are sound.

// "We entered into a contract with a company called FireEye (now part of 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, FireEye 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 another state outsmarts cyber threats

Another state employs the Trellix election security solution in a similar way, focusing on endpoint and network security using Trellix HX and NX products respectively. The solution also includes Trellix Helix to accelerate threat detection and response leveraging machine learning, AI, and integrated real-time cyber intelligence.

Security agents on servers and workstations across county election offices continuously look for suspicious activity attempting to compromise the endpoint or gain entry into the network. Similarly Trellix appliances on the network detect any anomalous or potentially malicious traffic coming from outside the network, and features such as Trellix SmartVision also detect suspicious lateral movements on the network.

In most instances, attempts by bad actors such as phishing—which is most common—are blocked by the Trellix solution before they ever have a chance of causing problems.



"FireEye (now part of Trellix) sold and protected the state's SoS central office and quickly expanded the opportunity to solving other vulnerabilities at the county level."

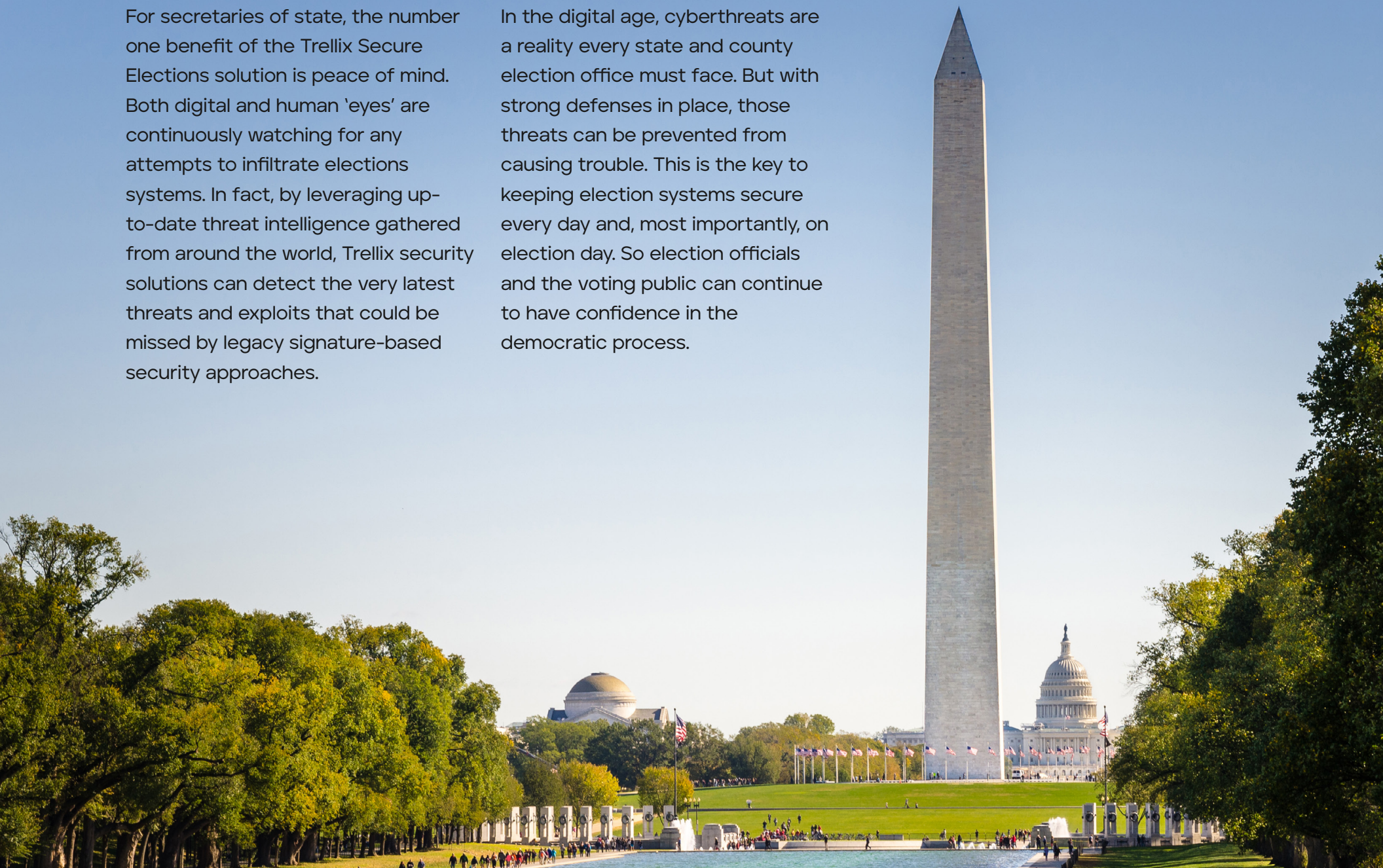
— Account Representative, Global Technology Services Provider




Delivering peace of mind

For secretaries of state, the number one benefit of the Trellix Secure Elections solution is peace of mind. Both digital and human 'eyes' are continuously watching for any attempts to infiltrate elections systems. In fact, by leveraging up-to-date 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 continue to have confidence in the democratic process.





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

Get the strongest
defense possible against
cyberthreats with Trellix
election security solutions.

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



About Trellix

Trellix is a global company redefining the future of cybersecurity and soulful work. The company's open and native extended detection and response (XDR) platform helps organizations confronted by today's most advanced threats gain confidence in the protection and resilience of their operations. Trellix, along with an extensive partner ecosystem, accelerates technology innovation through machine learning and automation to empower over 40,000 business and government customers with living security.

Copyright © 2023 Musarubra US LLC 072023-21

Trellix

6220 American Center Drive
San Jose, CA 95002

www.trellix.com