Securing Democracy: Supporting Integrated and Effective Election Security with the Fortinet Security Fabric

Executive Summary

Election security is a top-of-mind concern for federal, state, and local governments, given increasing efforts by foreign players to target U.S. elections. Election systems in many jurisdictions face a significant risk of compromise because of inadequate funding for cybersecurity. Federal funding of $425 million in the 2020 budget from the Help America Vote Act (HAVA) will help address some of these needs, but state and local governments will need to be strategic in how they invest those dollars.

Given that many jurisdictions lack sufficient cybersecurity staff, the most effective solution is to move toward an integrated network security approach featuring automated capabilities, such as the Fortinet Security Fabric. Such a strategy integrates a next-generation firewall (NGFW) with identity management and access control, software-defined wide-area networking (SD-WAN) capabilities to support precinct and field users, sophisticated endpoint protection and response, user and entity behavior analytics (UEBA) to spot and mitigate insider risk as well as external threats, and advanced threat protection using artificial intelligence (AI) and machine learning (ML).

United States (U.S.) election security has historically been focused on preventing voter fraud or localized attempts to skew an outcome. U.S. election systems and practices are not as well-postured to resist meddling from nation-state adversaries, which bring more resources and greater capabilities. These capabilities include the ability to conduct reconnaissance over months to years, recruit insiders, and mount sophisticated cyber operations against state and local networks.

Exacerbating the problem, the bar of success may be lower for these more formidable adversaries, since their goal can be to create the appearance of having affected an outcome—and thereby call the integrity of the election into question even if no manipulation of votes has actually occurred. Even successfully placing malware on networks associated with election processes and claiming to have affected the outcome puts election officials on their back foot to “disprove a negative.” This difficult task can be made easier when officials can point to a robust and multilayered security posture that also supports incident management and investigation.

Election security has been in the news in the U.S. since the aftermath of the 2016 presidential election, when Russian meddling in particular filled the headlines and fueled controversy. Foreign efforts to breach U.S. election systems have accelerated, and numerous nations now have the capability or intent to attempt interference in U.S. elections. Since U.S. elections are decentralized by design, the responsibility for securing them falls on a patchwork of state and local governments. Most elections officials understand the challenge and are doing everything in their power to secure their systems, but insufficient funding has hampered their progress to date.
Targeting Election Spending to Maximize Its Impact on Security

Each state must match its share of the $425 million in federal HAVA funds with a further 20% of its own money, but many states and local jurisdictions are already planning to spend significant resources from their own coffers to update and better secure their elections infrastructure. Although HAVA funds and additional state and local resources will be welcomed by cash-strapped elections administrators, estimates of the overall resources needed to address critical problems in U.S. election security nationwide exceed $2 billion.2

Clearly, agencies will not be “spending their way out of the problem,” and jurisdictions need to ensure that they are making informed and strategic purchasing decisions in order to derive the maximum benefit from each dollar spent. A one-size-fits-all approach is not possible given the diversity of elections systems, legal frameworks, and current levels of readiness. Recognizing this, the federal Election Assistance Commission (EAC) has attached minimal strings to the funding, and how the grants are used will largely be determined by each state.

Critical Elements to Monitor and Secure in the Electoral Process Include:

Voter registration. Creation and maintenance of an authoritative, statewide database of potential registered voters. This is created from state and local data accessed via networks.

Creation/maintenance, transmission, and use of “poll books.” These precinct-by-precinct mappings of eligible voters are used to check them in at their correct polling place. These are created from voter registration data, and typically housed on locally networked tablets or notebook computers.

Voting. This includes both in-person on election day and absentee/early voting. While components in these systems are typically not connected to the internet, they are often accessible from networks or removable media and are susceptible to user error or attack.

Tallying and reporting. This involves tabulating the results within each precinct, followed by exporting the tally for aggregation with other jurisdictions. The process often uses magnetic media within precincts and networks thereafter.

Election management “back-end” systems. Software and networks support these and other election-related activities occurring before and after voting. Many of these systems share IT resources that are also used for non-election purposes, which heightens the challenge of adequately protecting them.

Integrating and Automating for Centralized Visibility and Control

As a general rule, HAVA grants and additional resources are best used to unify and integrate an organization’s security architecture rather than add more silos. Integration brings centralized visibility and control and enables true automation of security processes across all parts of the network. Given that local jurisdictions tend to have few if any cybersecurity personnel, choosing solutions that offer single-pane-of-glass visibility and integrated automated security capabilities are important. The Fortinet Security Fabric offers broad visibility and protection, integrated detection and response to advanced threats, and automated operations and analytics via a single console.

Guarding Against Advanced Threats

A traditional perimeter-based approach to network security is no longer adequate given today’s distributed network architectures and the rapidly evolving nature of the threat landscape. The Fortinet Security Fabric is built on the foundation of FortiGate NGFWs, which provide security beyond the perimeter, incorporating web application firewalls and internal segmentation firewalls to drive security deep into the network.

FortiGate NGFWs also provide SD-WAN, allowing the efficient creation of secure networks in precincts on election day. These capabilities collectively ensure that applications are protected, and that sensitive voter information is isolated as it moves across the network. If a breach does occur, the FortiSIEM security information and event management solution provides the real-time visibility and analysis that is critical for rapid investigation and remediation. This visibility makes it easier for security teams to detect anomalous behavior that might indicate an attack or breach.
Keeping Up with Malicious Actors at Machine Speed

When it comes to threat detection, AI and ML are essential, especially since nation-state adversaries have used a “low and slow” approach. This enables them to exploit vulnerabilities and establish a persistent presence on state and local election networks that can be difficult to detect by traditional signature-based techniques.

FortiGuard AI is now a part of every solution in the Fortinet Security Fabric and autonomously collects, analyzes, and classifies threats at machine speed with an extremely high degree of accuracy. Fortinet Artificial Neural Networks (ANNs) are comprised of 20 billion nodes, which learn from unique global threat data collected over many years. Using ML to train the model, threat detection is continuously updated as threats evolve, and overall accuracy is improved.

Ensuring Zero-trust Network Access

One of the most critical components to election security is ensuring that only those verified as authorized users can view sensitive data. For instance, voter registration databases are built, curated, and used by a combination of state- and local-level users. This places a premium on strong access management, provided by the FortiNAC network access control solution, combined with secure network segmentation to prevent malicious actors from altering or compromising registration information.

The FortiAuthenticator user identity management service verifies the identity of those seeking access using two-factor identification, token management, single sign-on, and even biometrics. It also provides separate access channels to secure and isolate guests and bring-your-own-device (BYOD) devices accessing network resources through those same access points. These capabilities for real-time visibility and control of activity at the user, device, and even IT process level enable intent-based segmentation and zero trust architecture. These approaches are significantly more effective than perimeter-based defenses at providing defense-in-depth against both internal and external threats.
Bolstering Awareness Through Staff Training

Elections are administered by a very diverse group—often including full-time and temporary elections staff, other state and local government employees, contractors, and citizen volunteers who staff local precincts and vote-counting operations. Given the diversity of skills and experience represented, cybersecurity training is especially crucial.

Such training should explain cybersecurity best practices and how to maintain proper cyber hygiene. The Fortinet NSE program offers free training to enhance user awareness and cybersecurity practices. Fortinet Fabric components, such as FortiWeb web application firewalls (WAFs), provide a backstop to training with capabilities such as web application filtering to help avoid user errors that can compromise election-related networks.

Conclusion

Strong election security is crucial to the conduct of free and fair elections. Local election administrators have a difficult and important job in ensuring that local elections operate smoothly and that their results are reliable. Accomplishing this requires determining the part of the electoral process that is an organization’s responsibility, identifying the controls needed to secure it, setting a timeline for implementation, and putting an incident response plan in place to enable rapid response to potential attacks.

State and local governments obtain the most cost-effective and operationally effective outcome when they pursue an integrated security architecture that incorporates technology, awareness, and processes to protect their election environments in the face of potential malicious intrusions and breaches. The Fortinet Security Fabric provides a comprehensive approach to network security to cover a jurisdiction’s entire infrastructure—from voter registration through voting and the tallying and reporting of results.

Key Fortinet Advantages

- Just as paper ballots are viewed as the gold standard for the voting process because of their ability to support rigorous audit and assurance of the integrity of election outcomes, Fortinet security solutions bring this same commitment to transparency and integrity of outcome to election cybersecurity.
- For example, in the event of a potential intrusion into a Fortinet-protected network, the incident can be investigated with the assurance that FortiGate firewall activity logs cannot be overwritten by intruders seeking to cover their tracks—and these logs can be mirrored off-site for additional security and analysis.
- The ability to use Fortinet products in a “no-touch” operating mode is especially valuable to thinly resourced jurisdictions that need a security solution that is “plug and play.”
- Fortinet solutions offer a unique combination of industry-leading performance and low total cost of ownership (TCO).
- The AI-informed threat intelligence underpinning the Fortinet Security Fabric means that, when a potentially malicious activity is detected targeting one jurisdiction, others nationwide can be protected in an automated fashion before they are attacked.