FORESCOUT

Solution Brief

Ensuring Secure Elections

ForeScout secures the vote by protecting "unsecurable" and outdated voting machines

Highlights

- Complete visibility of election system devices
- Automated asset compliance and management
- Behavioral monitoring and management of election networks

Benefits

- Improve security of entire election system, not just a component
- Secure voting machines, voter databases and vote tabulation systems
- Secure previously vulnerable systems or unsecurable voting machines

Elections in the United States are the fundamental tools for citizens to have a voice in our democracy. Oftentimes, federal, state and local elections are decided by razor-thin margins, making every vote a critical factor in electoral decisions. ForeScout offers and agentless visibility and control platform to help secure voting machines and critical election systems.

After the deadlocked 2000 presidential election focused national attention on obscure details of election administration, Congress passed the Help America Vote Act (HAVA). HAVA provides states with funding for modern voting equipment, requirements on election administration, and a new independent agency to administer grant programs and assist state and local agencies by issuing guidelines and guidance. Despite this progress, today nearly every voting machine in the United States may be susceptible to some form of compromise, and even election systems that have a paper trail may not be completely secure.[1] In fact, the Department of Homeland Security recently notified 21 states that Russia attempted to hack their election systems before the 2016 election.[2] In March 2018, the Federal Government provided funding to upgrade election systems in an attempt to improve election systems security.

ForeScout Technologies recognizes that the first step to address the challenge of voting system security is to improve basic cyber hygiene of those systems and then, where time or resources prevent replacing old, unsecured voting machines, implementing innovative technologies that can secure previously unsecurable devices.

The Challenge

Election systems are unique, purpose-built information technology (IT) networks designed to maintain a list of eligible voters and collect and tabulate votes. However, no matter how unique election systems may be, at their core they share the same basic characteristics and vulnerabilities of all IT systems. Each component of an election system—the voter registration database, the vote tabulation system, and the voting machines—must be secure to keep voting records confidential and maintain system integrity and availability. Upgrading to new voting machines alone will not be enough to secure election systems without following common design standards and widely recognized security practices. Expecting new voting machines to be secure would be the same as purchasing a new laptop and expecting it to be secure without antivirus or security software.

Today, even organizations with the best monitoring, vulnerability and cybersecurity tools do not have visibility of, or are not managing, a high percentage of devices on their networks. In fact, according to analyst firm IDC, customers discover 24 percent more previously unknown devices on their networks upon installing the ForeScout platform. A leading firewall vendor recently found that 90 percent of organizations they protect have experienced cyberattacks where intruders tried to exploit vulnerabilities that were three years old or older.[3] These asset inventory blind spots and device compliance failures can be fixed with basic cyber hygiene practices.

Due to a combination of physical and logical vulnerabilities, nearly all voting machines are unsecured. In many cases, even a paper record is not enough to ensure the security and privacy of voting data.[4] As more features are added to new voting technologies, new risks can often be introduced. Older voting machines are often unsecurable because their operating systems and source code cannot be updated or patched, or are simply too expensive to replace. Unsecurable assets may also include existing technologies that are no longer (or may never have been) maintained by a vendor with physical and logical controls to prevent vote tampering. Securing the seemingly unsecurable devices on a network is a challenge, but it is not impossible.

The recent commitment of federal funds to secure election systems is important, but it will take time to replace outdated voting machines and secure election systems. In the meantime, as we continue to hold elections, we will need to improve the cyber hygiene of America's election systems with complete visibility, simple task automation and a cooperative sharing of data across systems to automate simple processes and take steps to secure vulnerable voting machines.

The ForeScout Solution

Start with Cyber Hygiene

Nearly all election security experts recommend improving the cyber hygiene of election systems. From the voting machine to the voter registration databases, election authorities should follow industry best practices to secure their networks. Replacing outdated and vulnerable voting machines alone can be a waste of time and money if the networks where voter registration databases reside can be hacked and vote tallies altered.

ForeScout helps over 2,800 customers in over 80 countries improve their network security and compliance posture.* We help these customers harden their systems and implement security best practices in three important ways:

See Delivers comprehensive asset intelligence to organizations looking to secure and manage their connected assets. Detects devices the instant they connect to the network without requiring agents. Profiles and classifies devices, users, applications and operating systems. Continuously monitors managed devices, Bring Your Own Devices (BYOD) and Internet of Things (IoT) devices.

Control Provides the ability to automate simple, repeatable tasks. Allows, denies or limits network access based on device posture and security policies. Assesses and remediates malicious or high-risk endpoints. Assists with improving compliance with industry mandates and regulations, including NIST standards and beyond.

Orchestrate Acts as the connective tissue across existing IT investments, improving their asset intelligence and task/process workflow automation. Shares contextual insight and data with IT security and management systems. Automates common workflows, IT tasks and security processes across systems. Accelerates system-wide response to quickly mitigate risks and data breaches.

The ForeScout platform discovers the unmanaged and hidden assets connected to the network and shares that information with other security tools to improve the scope and function of patch, vulnerability, configuration and endpoint security solutions. By discovering hidden and unmanaged assets, ForeScout can dramatically reduce the attack surface that hackers use to land and expand their control over our networks, and do so in near-real time.

Secure the Unsecurable

It can often be cost-prohibitive to replace outdated IT systems and infrastructure that still perform basic functions and are critical to an organization's mission while remaining unsecurable due to their age or lack of support. In circumstances where resources are constrained and timelines are tight, the ForeScout platform can help to build a secure perimeter around unsecured systems and continuously monitor device activity across connected networks.

ForeScout can help mitigate risks associated with unsecurable devices by identifying devices as they connect to the network and protecting those connections throughout their lifecycle. This includes, but is not limited to, the traditional election system assets (for example, voting machines, web and database servers, and laptops) and non-traditional devices such as cameras, IP phones and printers. One way ForeScout protects devices during and after they connect to the network is by building a device profile based on expected behavior. ForeScout can help define and enforce a specific range of acceptable behaviors for each device type in an election system to limit how a device can behave and prevent it from performing unauthorized actions. For example, if a vote tabulation system attempts to communicate with a web server or call outside the election system IT network, the ForeScout platform can automatically block that behavior, quarantine the device and automatically initiate a process to remediate the situation.

Experience the before-and-after difference of the ForeScout platform with a hands-on test drive that takes you through five powerful cybersecurity use cases.

Visit www.forescout.com/testdrive to learn more and register for a Test Drive in your area.

Learn more at
www.ForeScout.com

*As of December 31, 2017

[1] https://freedom-to-tinker.com/2016/09/20/which-voting-machines-can-be-hacked-through-the-internet/ Professor Michael Shamos: *"Every manipulation of elections that's been proven has involved the manipulation of paper."*

[2] Mulvihill, Geoff and Pearson, Jake (2017, September 23). Federal Government Notifies 21 States of Election Hacking. Associated Press, https://www.apnews.com/cb8a753a9b0948589cc372a3c037a567

[3] Fortinet Q2 2017 Global Threat Landscape Report (https://www.fortinet.com/fortiguard/threat-intelligence/threat-landscape.html)

[4] https://freedom-to-tinker.com/2016/09/20/which-voting-machines-can-be-hacked-through-the-internet/

ForeScout Technologies, Inc.
190 West Tasman Drive
San Jose, CA 95134, USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support 1-708-237-6591