Government Business Council

FEDERAL ISSUE BRIEF

ACCESS DENIED:

Threats to Endpoint Security in the Federal Government

Sponsored by: Quest Public Sector

The rapid growth of endpoints in the federal government creates significant security concerns.

THE BIG ISSUE

The number of device endpoints connecting federal employees to agency networks has grown at astonishing rates in recent years. Despite opening greater levels of mission mobility, the spike in endpoints has revealed gaps in conventional IT management and security practices.

WHY THAT MATTERS

Agencies face mounting pressure to update their IT to comply with federal mandates and resolve known vulnerabilities. Unless the federal government implements automated security endpoint management, it risks jeopardizing the personal data of 330 million Americans. The consequences are numerous and severe: sabotage of agency operations, theft of trade secrets and national security records, and disruption of critical infrastructure.

WHO NEEDS TO KNOW

Federal CISO, CIOs, system administrators, security personnel, and government software vendors

PLAYERS AND POLICIES TO KNOW

DoD Windows 10 Mandate: This 2015 Pentagon memorandum ordered US military services to transition IT to Microsoft Windows 10 by January 2017 to improve DoD's cybersecurity posture. However, compatibility issues with existing IT created delays for multiple agencies. The Army finally completed its transition in January 2018, while the Air Force and Navy anticipated finishing migration later in 2018.[1]

Internet of Things (IoT) Cybersecurity Improvement Act of 2017: With bipartisan sponsorship from Sen. Mark Warner (D-VA) and Sen. Cory Gardner (R-CO), this bill looks to ensure that devices sold to government are free of known vulnerabilities, receptive to software patches, and devoid of unchangeable password protocols. It also directs agencies to maintain and report to OMB an inventory of all IoT devices in use within 5 years.

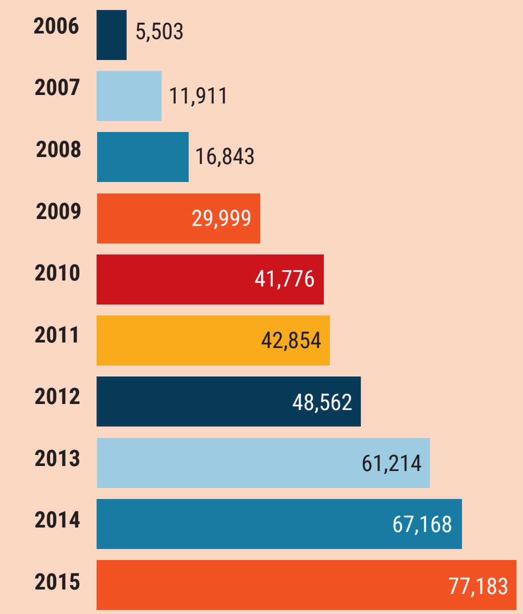
Wannacry & Spectre/Meltdown: The last few years saw a crippling barrage of cyberattacks. In May 2017, the virus known as Wannacry infected more than 200,000 computers across 150 countries.[2] The ransomware attack was successful because it preyed on devices using previous versions of Windows operating systems. In early 2018, researchers identified deep vulnerabilities in widely-used processor chips. The exploit known as Spectre/Meltdown highlighted continued gaps in unpatched systems of personal computers and cloud infrastructures.

THE STATUS QUO IS OBSOLETE

The federal government still spends roughly 80 percent of its annual $80 billion IT budget on operating and maintaining outdated systems.[3] This practice will continue so long as agencies deploy IT that fails to automatically identify and patch back-door vulnerabilities. Even when agencies are vigilant in deploying manual security updates, administrators can't account for employees who download software from unauthorized third party developers.

In light of this arrangement, it's no wonder that endpoint security tops the list of concerns cited by federal employees in a recent survey of IT officials.[4] According to a 2018 report, 57 percent of federal employees say their agency experienced a data breach in the last year, a 39-point increase from the 18 percent who reported attacks in 2016.[5] Agencies can no longer afford to manually track endpoints and software vulnerabilities through spreadsheets. Constant vigilance is required to ensure the workforce and its IT is resilient before, not after, vulnerabilities come to light.

> ***“Endpoints are a critical piece of the security puzzle. The successful attacks against government typically start with a phishing message aimed at an end user and grow from there.”[6]***
>
> *-- Larry Reed, Acting Chief Information Security Officer, Department of Justice*



Incidents Reported by Federal Agencies

WHAT’S WORKING

Fortunately, some agencies are waking to the danger and taking steps to guard their endpoints. More money is being devoted to endpoint security and mobile device management in 2018 than other IT security priorities, with 56 percent citing an increase in spending for endpoint security upgrades.[7]

Given their focus on national security, defense agencies are largely outpacing their civilian peers when it comes to these efforts. Aside from DoD’s imminent completion of the Windows 10 migration, its branches have taken measures to implement biometrics, multiple user personas, location-based security, and added protection for devices used in the field.[8] Likewise, the recent update of the NIST Cybersecurity Framework (V1.1), which features additional guidelines for endpoint protection and IoT security, saw 129,000 downloads by federal customers in just four months, whereas its predecessor took four years to reach 262,000 downloads.[9] Awareness is rising, and that’s a positive.

WHAT ISN’T

Many agencies are still asleep, leaving their attack surface wide open for exploit. While more than 90 percent of federal respondents indicated their agencies have secured mobile access for work-issued devices, only a quarter support secure access via employees’ personal devices.[10] That’s problematic for agencies like NASA, who recently discovered 28 unsanctioned cloud services operating in its IT environment.[11]

Another problem agencies face is privileged user access. The default approach deployed by many IT departments is to assign privileged accounts to a wide swathe of officials. As NIST points out in its Risk Management Framework, this raises significant risk by opening the door to malware and phishing schemes designed to exploit such credentials.[12]

Lastly, while more agencies would like to secure their endpoints, they may find themselves integrating fixes from multiple vendors, each with their own requirements and user interfaces. This “point-tool sprawl” can overwhelm administrators looking to cover all their endpoint bases, creating a headache for the end user.[13]

▶▶ THE BOTTOM LINE

For endpoint security to succeed, agencies need solutions that detect emerging vulnerabilities, automate patches, and reduce administrative burden.

ACTION ITEMS

- **Ditch the spreadsheet:** Agencies are spending more on endpoint security in 2018 than ever before. That's a positive step forward, but such investments should focus on solutions that reduce manual oversight and outdated IT inventory practices. Adversaries are counting on the fact that agencies will continue to patch and manage systems when it's convenient, not necessarily when it's critical. Wannacry and Meltdown/Spectre are evidence of the damage that can ensue when security takes a backseat to expediency.

- **Raise awareness:** Agency CIOs have a responsibility to raise workforce awareness and enforce sound cyber hygiene. The Department of Homeland Security (DHS) is a great example, having authored a 2017 study on mobile device security that brought attention and awareness to endpoint security.[14] More agencies can follow suit by training employees to recognize classic symptoms of phishing, malware, and other exploits, as well as by running red-team exercises that test resilience of agency networks.

RISK OF INACTION

Unless federal agencies shore up their rapidly-growing network of endpoints, the data breach nightmare will only get worse. With so much at stake — the data of millions of Americans, the maintenance of critical infrastructure, and the security of our armed forces — agencies can't afford to gamble on security any longer.

WORKING WITH QUEST

Every IT organization faces a dual-challenge of technological growth: first, the proliferation of endpoints, and second, the proliferation of security threats to those endpoints. What's more, manual, ad-hoc management of these growing endpoints is time-consuming and reactive, putting organizations at risk of updating and patching after threats are identified. This can lead to unchecked vulnerabilities, system downtime, and, at worst, network breaches.

Quest Unified Endpoint Management solutions enable federal agencies to address these challenges by proactively provisioning, managing, securing and servicing their growing endpoint environments.

- **Security:** Allows for the separation of individual user and corporation data for BYOD situations and for corporate devices. IT users can lock, erase or wipe a device, manage password settings, and restrict mobile device features.

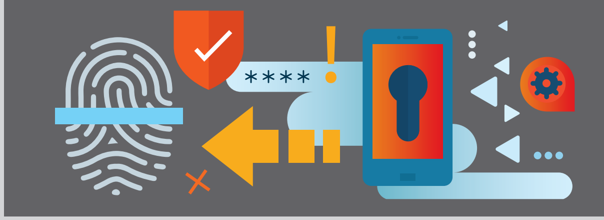
- **Control:** Adds management for Android and iOS devices and the ability to inventory, track and easily distribute corporate account settings.

- **Ease of Use:** Provides a single pane of glass to discover and manage devices within a customer's environment.

- **Reporting:** Users can create .pdf formatted reports, in addition to those in .csv and .html formats.

The Quest UEM solution including KACE Systems Management Appliance (SMA), KACE Systems Deployment Appliance (SDA) and KACE Mobile Device Management (MDM) — enables you to easily deploy and manage all your endpoints across multiple platforms, including mobile devices, from a single solution.

For more information, please visit https://www.quest.com/kace/



END NOTES

1. Stars and Stripes: "Military approaches Windows 10 upgrade deadline." March 20, 2018. https://www.stripes.com/news/military-approaches-windows-10-upgrade-deadline-1.517766
2. USA Today: "Remember WannaCry? It's not too late to update your Windows systems." December 19, 2017. https://www.usatoday.com/story/tech/news/2017/12/19/remember-wannacry-its-not-too-late-update-your-windows-systems/964131001/
3. Nextgov: "Some agencies spend more than 90% of IT budgets on legacy systems, report finds." October 25, 2016. https://www.nextgov.com/cio-briefing/2016/10/idc-report-legacy-it-in-agencies/132618/
4. FedScoop: "Closing the gaps in federal endpoint security." February 26, 2018. https://www.fedscoop.com/closing-gaps-federal-endpoint-security/
5. Dark Reading: "Federal agency data under siege." April 13, 2018. https://www.darkreading.com/attacks-breaches/federal-agency-data-under-siege/a/d-id/1331467
6. FedTech: NSA, NOAA and Other Agencies Rethink How They Tackle Endpoint Security." February 15, 2016. https://fedtechmagazine.com/article/2016/02/nsa-noaa-and-other-agencies-rethink-how-they-tackle-endpoint-security
7. Thales: "2018 Thales Data Threat: Trends in Encryption." http://go.thalesesecurity.com/rs/480-LWA-970/images/2018-Thales-Data-Threat-Report-Federal-Edition-ar.pdf
8. See [4]
9. NIST: Cybersecurity Framework. https://www.nist.gov/cyberframework
10. CyberScoop: "Closing the Gaps in Federal Endpoint Security." https://www.fedscoop.com/accelerating-innovation-in-government/assets/images/ClosingtheGapsinFedEndpointSecSamsung.pdf
11. Network World: "NASA has a shadow IT problem." February 8, 2017. https://www.networkworld.com/article/3167609/security/nasa-has-a-shadow-it-problem.html
12. NIST: "Best Practices for Privileged User PIV Authentication." April 21, 2016. https://csrc.nist.gov/csrc/media/publications/white-paper/2016/04/21/best-practices-for-privileged-user-piv-authentication/final/documents/best-practices-privileged-user-piv-authentication.pdf
13. InfoSecurity: "Is Your InfoSec Tech Stack Causing Dangerous Blind Spots?" September 11, 2018. https://www.infosecurity-magazine.com/opinions/tech-stack-blind-spots/
14. DHS: "Study on Mobile Device Security." April 2017. https://www.dhs.gov/sites/default/files/publications/DHS%20Study%20on%20Mobile%20Device%20Security%20-%20April%202017-FINAL.pdf

Government Business Council

ABOUT GOVERNMENT BUSINESS COUNCIL

As Government Executive Media Group's research division, Government Business Council (GBC) is dedicated to advancing the business of government through analysis, insight, and analytical independence. An extension of Government Executive's 40 years of exemplary editorial standards and a commitment to the highest ethical values, GBC studies influential decision makers from across government to produce intelligence-based research and analysis. Learn more at www.govexec.com/insights

Report Author: Daniel Thomas

Quest®
Public Sector

ABOUT QUEST

Quest helps solve the complex technology and security problems that stand in the way of organizations' ability to always be ready for what's next. With Quest solutions, companies of all sizes can reduce the time and money spent on IT administration and security, so they have more time to focus on and invest in business innovation. Quest has more than 100,000 customers worldwide across its portfolio of software solutions spanning information management, data protection, endpoint systems management, identity and access management, and Microsoft platform management. For more information, visit www.quest.com.

Government Business Council

Sponsored by:

Quest® Public Sector