MeriTalk
Improving the Outcomes of Government IT

Underwritten by:
DELL Technologies
INTEGRITY GLOBAL SECURITY

Securing Federal Endpoints: Moving From Zero Trust to Zero Vulnerability

From ransomware to malware to hackers trying to break through barriers inside and outside of the network, no industry is immune to bad actors finding ways around traditional cybersecurity, including the Federal government.

Ransomware and malware attacks across all industries are up 350 percent since 2018[1]. To safeguard our nation's most important infrastructure and protect the American people, President Biden issued a cybersecurity Executive Order[2] in his first 100 days in office, noting that the Federal government "needs to make bold changes and significant investments in order to defend the vital institutions that underpin the American way of life."

Today's Security Is Built Around When, Not If

The current cybersecurity paradigm accepts that an organization must deal with a breach **when** it happens. Security teams find themselves in perpetual cybersecurity crisis mode, trying to catch a breach quickly, limit the spread within the network, and deal with remediation. Even zero trust architectures assume breach – limiting movement within the network once the bad actors are already there.

Software programs that initiate after the user logs in and connects to the network service are trusted to protect networks, servers, and endpoints. By then, as we have seen, it is often too late. And, with large numbers of Federal employees working from home, as well as in the office and in the field, risks are greater.

The reality is that breaches don't have to be inevitable. To create a truly secure environment, cybersecurity needs to start at the hardware level, when the user turns on their computer. This is the case in many safety-critical instances (consider airplane operating systems, medical devices, etc.), and this same approach can (and is) delivering fully secure, remote access – including to classified networks.

Zero Vulnerability Is Achievable

In the 1990s, INTEGRITY Global Security's experts created an operating system to provide the highest levels of security and reliability. In 2004, the United States Air Force had a requirement for the F35 Joint Strike Fighter to protect classified mission critical data while being exposed to potentially malicious network access. This prompted a rigorous four-year endeavor to test and confirm the INTEGRITY™ operating system was 100 percent secure.

This same system that securely controls the avionics, communications, and weapon systems on the most sophisticated aircraft in the world is now available to secure your employees' desktop computers, servers, thin clients, and laptops.

How Zero Vulnerability Works

No path is the same, but there are several logical steps to jumpstart the journey to zero trust adoption and a risk-based approach.

- Dell Technologies laptops, desktops, and tablets are delivered embedded with IGS INTEGRITY™ software
- When the user turns on their device, INTEGRITY runs a security check that validates the state of the system, and then verifies the user through multi factor authentication
- The user connects to a secure network server via an encryption stack that is embedded in the INTEGRITY software, providing a secure connection even through commercial Wi-Fi or hotspots
- All other software programs on the computer – including programs such as Windows – are housed in containers. If any software program on the endpoint experiences a security issue, that issue is contained without infecting the device or the network

One Solution Awarded Nation's Highest Level Security Designation

INTEGRITY Global Security has a 40-plus year record securing safety-critical endpoints.

Deployed on commercial and U.S. military aircraft since the 1990s, including Boeing and Airbus aircraft models and F-series fighter jets, INTEGRITY also secures safety-critical and purpose built systems in the medical, automotive, and industrial industries – where a breach can mean loss of life.

INTEGRITY meets the most stringent security requirements in the world and the National Information Assurance Partnership (NIAP) awarded INTEGRITY a Common Criteria Certificate twice – **the only security solution** to achieve this standard at the highest level of EAL6+. NIAP executed stringent testing for more than four years before award. The technology also meets the National Security Agency's Commercial Solutions for Classified (CSfC) requirements for Mobile Access Capability Package (MACP) and Data at Rest (DAR).

This means Dell Technologies endpoints embedded with INTEGRITY enables zero vulnerability remote access, including to classified networks.

INTEGRITY™ in Action

IP Protection

- Provides end-to-end encryption from client to server with private cloud overlay
- Prevents data leakage by enforcing the security policy in the hardware

Compliance

- Isolates regulated infrastructure from unregulated components
- Minimizes auditable infrastructure
- Provides seamless access to multiple security domains, isolating critical infrastructure

Remote Access

- Embeds VPN into hardware
- Enforces network traffic through controlled pathways

IT/OT Boundary

- Isolates managed IT infrastructure from IoT devices
- Prevents spread of ransomware and malware
- Reduces complexity by using common IP infrastructure

Prevent Threats from Breaching Your Network – Learn More

Dell Technologies endpoints for the enterprise, protected with the INTEGRITY solution are available through **DellTechnologies.com/Federal**.

Learn more:
integrityglobalsecurity.com/commercial.html
or contact us at (202) 844-2823.

[1] 12019/2020 Cybersecurity Almanac: 100 Facts, Figures, Predictions, and Statistics, Cybercrime Magazine

[2] Executive Order on Improving the Nation's Cybersecurity