

Absolute Secure Endpoint for Federal Government

Fortify Data, Secure Devices and Stay Audit Ready



Enabling The Federal Digital Transformation

Government agencies are diverse; but the struggle to adequately address cybersecurity gaps, with limited resources, is universal. Ensuring the safety and integrity of the information in your care is vital to maintaining the trust of the people your organization serves.

Protecting Sensitive Data and Complying with Federal Regulations


Federal agencies often face a collection of complex challenges when it comes to cybersecurity, ranging from legacy IT infrastructure to insufficient staffing. To provide optimal public service, highly sensitive information needs to be accessible to the distributed workforce.

The emergence of remote and hybrid work policies, however, has made sensitive public data on mobile endpoints more susceptible than ever to being accessed illegally, held for ransom or leaked by cybercriminals. Due to these challenges and the increasingly complex threat landscape from local and state actors, Federal agencies are now under more pressure than ever to strengthen their security processes and comply with a variety of strict cybersecurity guidelines and regulations.

Current Challenges Faced by IT and Security Teams

 **IT Challenges:**

- Maintaining visibility across endpoints, on or off the network
- Devices going dark, being lost or stolen
- Hardware and software waste, overlaps, and inefficiencies
- Securely offboarding remote employees
- Identifying suspicious device usage

 **Security and Compliance Challenges:**

- Limited resources to keep up with cyberthreats or enforce security controls
- Limiting data risk exposure
- Difficulty assessing risk and avoiding compliance violations
- Lack of confidence to adopt cybersecurity frameworks such as NIST 800-53, NIST CSF, NIST 800-171, CMMC and FISMA
- Inability to track progress against compliance regulations or to automate audits

The Solution: Absolute Cyber Resilience to Maintain Continuous Compliance

Cyber Resilience through Absolute Secure Endpoint empowers Federal agencies to obtain continuous endpoint visibility and control across their distributed endpoint fleet to comply with regulations and respond to security risks in a swift and efficient manner. Absolute helps improve your IT and security efficiency, accuracy and confidence through **granular endpoint visibility**, **resilient security controls** and **continuous compliance**. This arms your team to view, monitor, and control your entire endpoint population from a single pane of glass — including off-network devices.

Granular endpoint visibility through technology already in the firmware of your devices, ready to be activated. Device manufacturers such as Dell, HP, Lenovo, and Microsoft, among many others, ship their machines with Absolute's patented Persistence™ technology. This unbreakable connection to every device keeps your inventory automatically up to date. Additionally, a variety of collected data points enables you to be alerted to device performance issues impacting end user productivity as well as potential security risks. These include hardware and software inventory, geolocation, device usage, anti-malware and encryption health, the presence of sensitive data across devices, among others.

Resilient security controls are the result of Absolute's self-healing capabilities. Through Application Resilience, your IT and Security teams get peace of mind in knowing that the security products your organization has invested in are installed, healthy and functioning across your entire endpoint population. Application Resilience monitors the structural health of applications and self-heals them through repair and reinstall policies to boost their uptime and thus maintain your organization's security posture. Application Resilience is supported **across 80+ of the most used security products** in the market today including Endpoint Protection (EPP), Endpoint Detection and Response (EDR), Data Loss Prevention (DLP) and Unified Endpoint Management (UEM) products, among others.

Continuous compliance becomes your new normal with ongoing, flexible checks that adapt to any cybersecurity framework like the NIST CSF, or other internal or regulatory standard. Absolute identifies where compliance has failed and restores controls that cause compliance drift when disabled or outdated. Absolute validates your compliance posture with regulations like NIST 800-53, NIST CSF, NIST 800-171, CMMC and FISMA to ensure you are always audit-ready.

When compliance violations do occur, administrators can execute a set of device actions through the Absolute Secure Endpoint Console to respond swiftly, efficiently and remotely. These include freezing devices to block access whenever devices are compromised or when suspicious activity is detected, deleting specific files or folders containing sensitive public or personal information and running pre-built or custom scripts catering to variety of IT and security use cases. You can also wipe devices to purge data as part of your employee off-boarding process to reduce the risk of sensitive information being exposed.

Key Capabilities and Benefits

1 Tamper-Proof Security
Already embedded in the firmware of your devices, Absolute cannot be removed; once activated, you instantly have a self-healing, digital tether to all of your endpoints

2 Automated Single Pane of Glass
With no required infrastructure, your Absolute console is automatically fed information sent by your endpoints on and off your network; your inventory is always up to date and audits become quick and efficient

3 Device Hardening
Enforce your ideal of endpoint hygiene and configuration, transforming your gold image to a diamond

4 Encryption and Anti-Malware Monitoring
Identify any broken or disabled safeguards and restore each one with zero human touch

5 Endpoint Data Discovery
Put a finger on devices holding sensitive data and mitigate exposure by automating controls or deleting data remotely on demand

6 Application Continuity
Stop disruptions to user and business continuity by self-healing your critical applications

7 Rapid and Confident Risk Remediation
Automated alerts to focus on what needs attention; powerful remediation capabilities to fix any issues, and isolate, freeze or wipe devices remotely as required, on or off network

8 Cybersecurity Experts at Your Fingertips
Our team of cybersecurity experts will help you assess your endpoint risk and the maturity of your security controls, so you can prioritize corrective actions and strategies

Spotlight on Zero Trust

Defining 'Zero Trust' is relatively simple. The concept revolves around the notion of 'never trust, always verify'. Any device or user attempting to gain access to a network or application must always be authenticated and their identity validated before 'trust' or access is given. Absolute Cyber Resilience helps federal agencies implement Zero Trust principles to fortify their security posture and block critical resources from being accessed by unauthorized users.



Securing the Future: Building a Resilient Zero Trust Strategy

With the world economy now fully digital, and cyberthreats only getting more sophisticated, adopting a Zero Trust security framework is the goal for most organizations. Today's escalated threat landscape has made it imperative to ensure both productivity and security for employees to get their jobs done. To be effective when establishing Zero Trust principles across an organization, two essential ingredients are needed - the creation of capabilities that are resilient, allowing for self-healing based on data intelligence to recover from any incident, and it must be part of an integrated approach.

absolute.com

Securing the Future: Building a Resilient Zero Trust Strategy

How secure are your endpoints? Discover how Absolute Security strengthens every pillar of Zero Trust Architecture for Federal Agencies.

Download Now