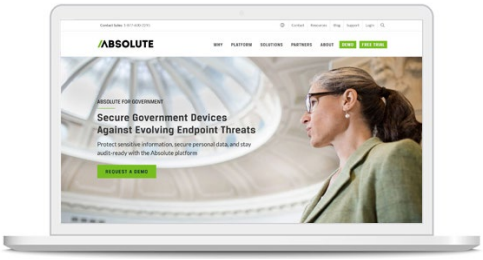
Absolute for Government

Fortify data, secure devices, and stay audit-ready

Before Absolute, it was a guessing game. We have a lot of mobile devices, but Absolute has provided incredible transparency and it is our single source of truth. We also have the ability to clear the data if a device is lost, stolen or misplaced. If I didn't have Absolute, I would be in the dark.

KEITH MORRISON
DIRECTOR OF INFORMATION SECURITY
COOK COUNTY SHERIFF'S OFFICE



Learn more about Absolute for Government:
absolute.com/government

PROTECT THE GOVERNMENT 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.

SENSITIVE, DISTRIBUTED DATA

From Capitol Hill to the county sheriff, data abounds — and is increasingly mobile. To provide optimal public service, highly sensitive information needs to be accessible to this distributed workforce.

IT and security teams in government organizations face the challenge of keeping devices under control and secure at all times. Ensuring compliance with data regulations — even when devices are off the government network — and adopting a cybersecurity framework such as the NIST CSF are top priorities.

Government's IT and Security Challenges:

- Controlling off-network devices and remote employees' data
- Hardware and software waste, overlaps, and inefficiencies
- Limited resources to keep up with threats or enforce security controls
- Difficulty assessing risk and avoiding compliance violations
- Lack of confidence to adopt the NIST CSF or other cybersecurity frameworks
- Inability to track progress with reliable metrics, or automate audits

THE SOLUTION: CONTINUOUS VISIBILITY AND CONTROL OF EVERY ENDPOINT

Enable a secure, digital government, and increase your IT and security efficiency, accuracy and confidence, with deep **asset intelligence, automated endpoint hygiene**, and **continuous compliance**, on all of your endpoints and at all times. Absolute arms your team to see, understand, and control your entire endpoint population from a single pane of glass — including off-network machines.

Asset Intelligence through technology already in the firmware of your devices — you just have to activate it. Laptop and desktop manufacturers, including 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, collects hardware, software and geolocation data points, reveals waste and inefficiency, and pinpoints security risks and compliance failures.

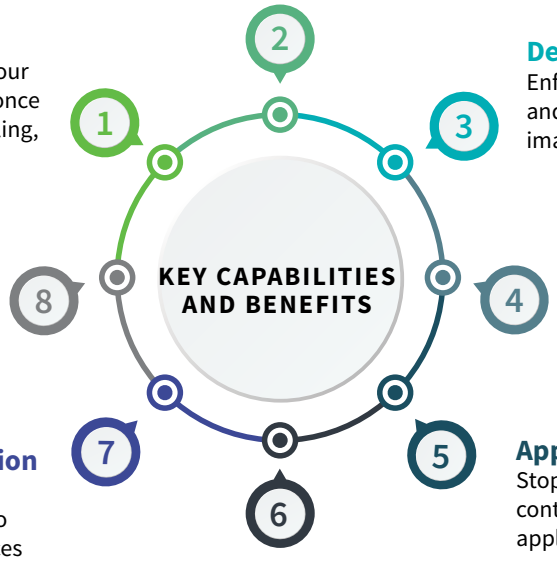
Automated Endpoint Hygiene is the result of Absolute's self-healing capabilities. Absolute examines endpoint hygiene and compliance drift, and regenerates your security controls — such as encryption, anti-malware, VPN, EDR, DLP — whenever necessary. Your endpoints become self-healing machines, capable of safeguarding your distributed device population and the data they contain. You keep control of every endpoint; freeze or wipe it remotely at any time.

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 CJIS, HIPAA, CCPA, GDPR, PCI, etc. You are always audit-ready.

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

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

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



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

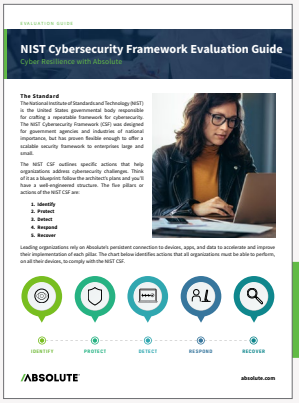
Encryption and Anti-Malware Monitoring
Identify any broken or disabled safeguards and restore each one with zero human touch

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

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

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

Spotlight on CJIS
For law enforcement and justice departments, uninterrupted access to criminal justice information (CJI) is critical in order to do their jobs safely and efficiently. CJIS regulates the minimum endpoint security controls required to grant access, such as encryption, anti-malware, access control, data drift detection, and remote device wipe on or off the government network.



NIST CYBERSECURITY FRAMEWORK EVALUATION GUIDE

This guide outlines the comprehensive suite of capabilities delivered by the Absolute platform that are crucial for success with the NIST CSF.

GET IT NOW

ABOUT ABSOLUTE
Absolute is the leader in Endpoint Resilience™ solutions and the industry's only undeletable defense platform, embedded in over a half-billion devices. Enabling a permanent digital tether between the endpoint and the enterprise who distributed it, Absolute provides IT and Security organizations with complete connectivity, visibility, and control, whether a device is on or off the corporate network, and empowers them with Self-Healing Endpoint® security to ensure mission-critical apps remain healthy and deliver intended value. For the latest information, visit **absolute.com** and follow us on **LinkedIn** or **Twitter**.

CONTACT FEDERAL SALES TEAM:
federalsales@absolute.com

REQUEST A DEMO:
absolute.com/request-a-demo

PHONE:
North America: 1-877-660-2289
EMEA: +44-118-902-2000

WEBSITE:
absolute.com