

BENCHMARK YOUR SECURITY POSTURE WITH CYBERSECURITY FRAMEWORKS

CONTINUOUSLY MEASURE AND IMPROVE AGAINST SECURITY BEST PRACTICES



HOW TO SECURE WHAT YOU CANNOT SEE

Embedded Endpoint Visibility and Control with an unbreakable connection, deep in your device's firmware, that cannot be removed by negligent users or malicious attackers.

Centralized Command to all your endpoints – on and off the network – with precision controls tailored to your cybersecurity framework.

Endpoint Data Discovery to monitor your endpoints, probing for sensitive and at-risk data to prevent overly permissive data controls and protection.

Risk Scoring benchmarks your endpoint security posture, aligning your security controls with risk-based analysis to reduce exposure.

Automated Response to mitigate threats, remove exposures, and restore security to any device, anywhere – on and off the network.

CHALLENGE: ADOPT A CYBERSECURITY FRAMEWORK, APPLY IT EVERYWHERE

Changing your company's mindset toward security is hard. Cybersecurity frameworks invite companies to question assumptions, shift from the status quo, and conform security controls to universal standards. However, to begin the journey toward compliance, organizations discover that it is impossible to secure what cannot be seen.

Endpoints hide. Data stays out of sight, hidden away in files and folders, leaving IT and security teams blind to violations that could lead to non-compliance. Users change configurations, disable encryption, and send sensitive data to the cloud. Attackers dismantle security controls and navigate around anti-malware and detection tripwires without anyone noticing it.

The result: security projects stall, compliance fails, and data protection is broken.

Specific challenges include:

- Inability to see security controls on all endpoints – on and off the network
- Limited data and device awareness hindering the ability to maintain a robust security posture
- Increased risk of non-compliance and inability to validate controls in real time
- Time-consuming manual audit and compliance reporting
- Remediation and recovery practices that lack automation

SOLUTION: PERSISTENT ENDPOINT VISIBILITY AND CONTROL FOR CONTINUOUS COMPLIANCE

Absolute levels the playing field and gives you the endpoint visibility and control to adopt your chosen cybersecurity framework. From a single, centralized platform, you see every endpoint, configuration, control, and all at-risk data to baseline your current security posture, with clear direction to pull your organization back into compliance.

Absolute's Data Discovery capabilities probe deep into your devices to uncover sensitive data to help assess risk. With flexible search and triggers, you have the full picture of what is happening and where to take action, and you have automated workflows to restore compliance.

SOLUTION OVERVIEW

With Absolute, you have complete visibility and control to anchor your cybersecurity framework in an ever-changing world. By leveraging centralized endpoint control, you are in command of every device, every configuration, and every action to ensure airtight compliance.

Absolute brings your cybersecurity framework to life with instant analysis, industry benchmarks, sensitive data discovery, and automated response to mitigate threats and exposures.

Nothing is hidden, nothing is unprotected.



NIST CYBERSECURITY FRAMEWORK

Persistent endpoint security to identify, protect, detect, respond, and recover in minutes – precision control over all data and all devices.



HIPAA AND HITRUST

Total endpoint visibility and control that uncovers hidden data and protects PHI (Protected Health Information) from misuse and leakage, with instant detection and response.



CIS CONTROLS

Continuous compliance with industry standards and best practices marked by controls that you can apply across your globally distributed endpoints.



PCI COMPLIANCE

Data protection that conforms to the world's leading compliance protocols and standards, to ensure resilience against financial data leaks.

ABOUT ABSOLUTE

Absolute empowers more than 12,000 customers worldwide to protect devices, data, applications, and users against theft or attack – both on and off the corporate network. With the industry's only tamper-proof endpoint visibility and control solution, Absolute allows IT organizations to enforce asset management, endpoint security, and data compliance for today's remote digital workforces. Absolute's patented Persistence® technology is embedded in the firmware of Dell, HP, Lenovo, and other leading manufacturers' devices for vendor-agnostic coverage, tamper-proof resilience, and ease of deployment. See how it works at absolute.com and follow us at [@absolutecorp](https://twitter.com/absolutecorp).



EMAIL:
sales@absolute.com



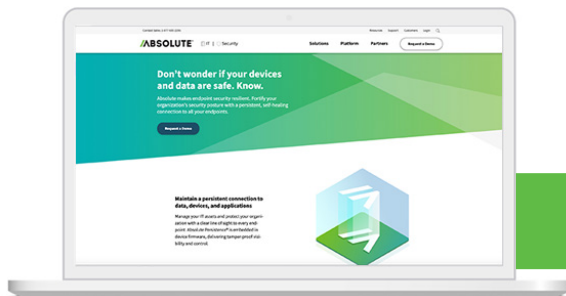
SALES:
absolute.com/request-a-demo



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



WEBSITE:
absolute.com



REQUEST A DEMO

Find out how our solutions can benefit your organization.

[REQUEST DEMO](#)