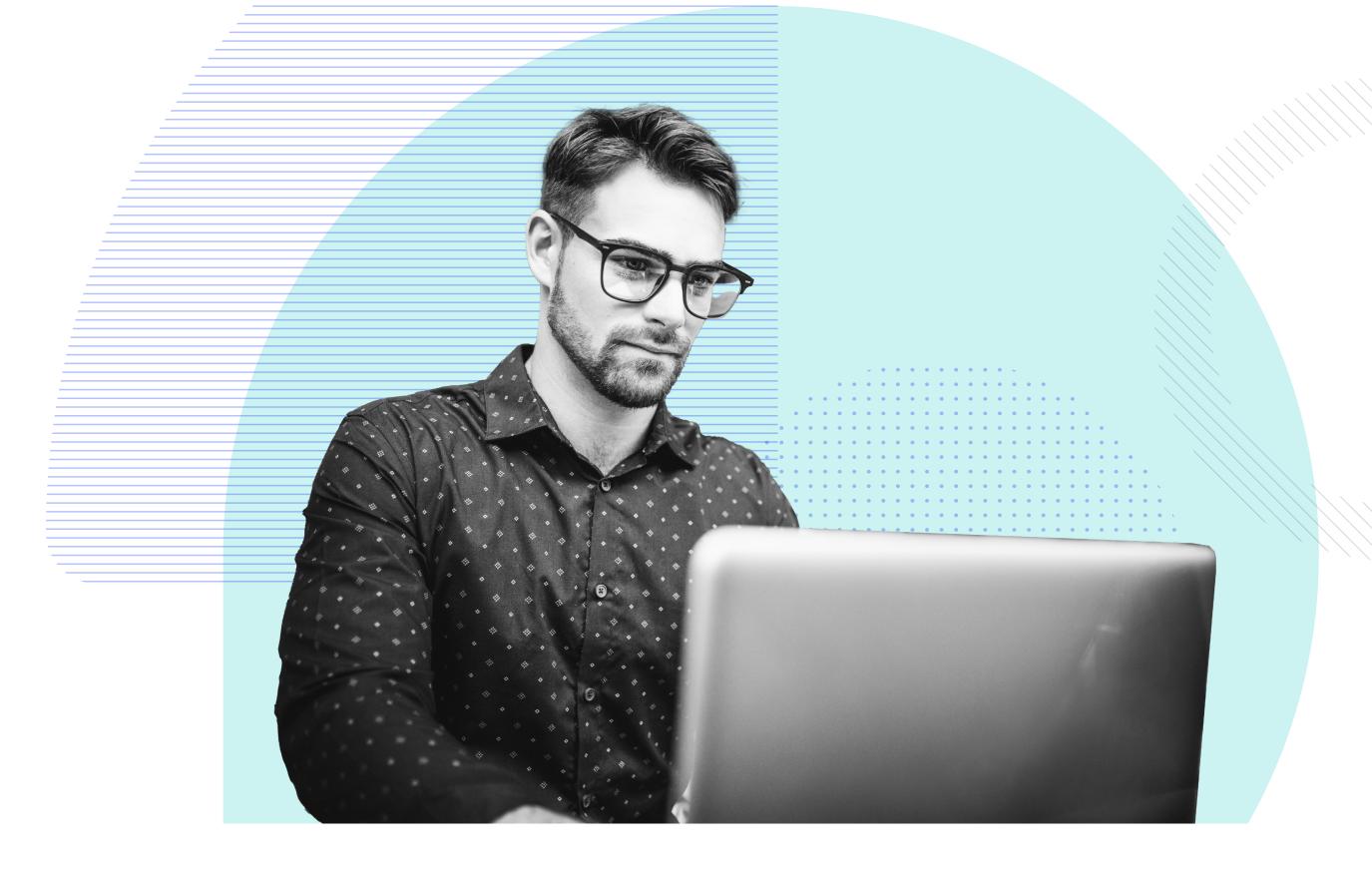
**EVALUATION GUIDE** 

## NIST Cybersecurity Framework Evaluation Guide

Building Cyber Resilience with Absolute



An estimated 68% of organizations suffered an endpoint attack in 2020. With the rapidly evolving cyber threat landscape, it's vital for companies to know where their endpoints are, take deep control of security actions on those devices, and ensure security controls repair themselves.

The NIST Cybersecurity Framework helps organizations understand their cybersecurity risks, and reduce threats, vulnerabilities, and impacts with customized measures. By implementing the framework, they can better respond to and recover from cybersecurity incidents, analyze root causes, and make improvements to security controls.



The NIST CSF outlines specific actions that help organizations address cybersecurity challenges. Think of it as a blueprint: follow the architect's plans and you'll have a well-engineered structure. The five pillars or actions of the NIST CSF are:

- 1. Identify
- 2. Protect
- 3. Detect
- 4. Respond
- 5. Recover

Leading organizations rely on Absolute's persistent connection to devices, apps, and data to accelerate and improve their implementation of each pillar. The chart below identifies actions that all organizations must be able to perform, on all their devices, to comply with the NIST CSF.



absolute.com 2



## NIST Cybersecurity Framework | Endpoint Resilience

The Absolute platform delivers a comprehensive suite of capabilities that let you remotely and reliably implement each pillar of the NIST CSF.



Identify	<b>Absolute Capability</b>
Pinpoint each endpoint for a comprehensive inventory	
Identify authorized and unauthorized hardware and software	
Prioritize endpoints based on classification, criticality, and business use	
Benchmark device controls against security standards and policy	
Quantify risk based on device vulnerabilities and exposures	
Catalog device, data, user, and application relationships across the endpoint population	



Protect	<b>Absolute Capability</b>
Gain physical access control and geofencing for distributed endpoints	
Freeze, delete, and wipe devices remotely	
Persist remote access systems (e.g. VPN) on all endpoints	
Remotely wipe encrypted devices when lost or stolen and produce a certificate of sanitization	
Automatically check for data integrity in software, firmware, and cloud storage apps	
Control communication from endpoint to corporate network or domain	
Enable telemetry analysis and remote command for maintenance and repair	





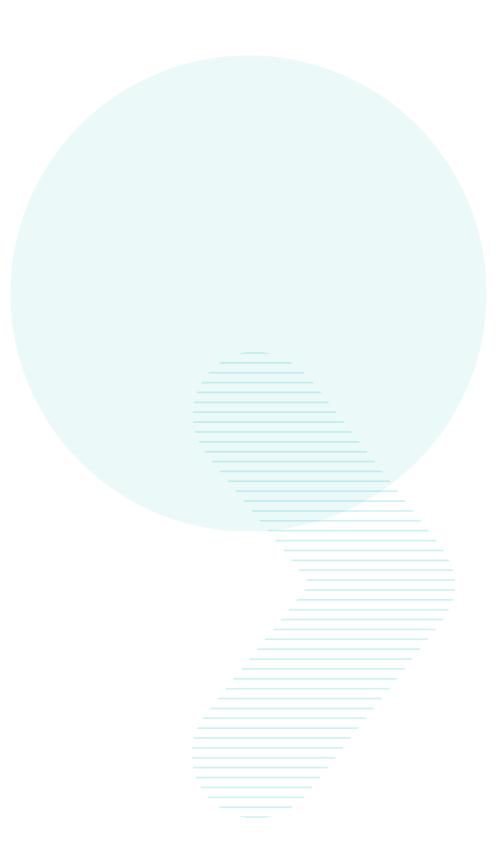
Detect	<b>Absolute Capability</b>
Establish baseline behaviors for users, data, devices, and applications	
Unify asset intelligence across the device population	
Monitor user activity and enforce role-based security controls	
Score high-risk users with access to ePHI	
Access geotracking and user-device awareness	
Detect and log configuration changes	



Respond	<b>Absolute Capability</b>
Utilize dynamic remediation and control changes	
Perform role-based access control for in-console response commands	
Deliver continuous device logs and forensic documentation	
Isolate a device or group of devices for containment	
Push control changes to prevent spread of detected compromise	
Command hotfixes to mitigate indicators of exposure (IOEs)	



Recover	<b>Absolute Capability</b>
Enforce policies within device controls	
Monitor device use and locally accessed sensitive data	
Control incident investigations, digital forensics, and documentation	
Augment and push new controls for endpoint hygiene	
Instantly access documentation for continuous improvement to endpoint hygiene and data protection	





## ABSOLUTE®

Absolute Software makes security **work**. We empower mission-critical performance with advanced cyber resilience. Embedded in more than 600 million devices, our cyber resilience platform delivers endpoint-to-network access security coverage, ensures automated security compliance, and enables operational continuity. Nearly 21,000 global customers trust Absolute to protect enterprise assets, fortify security and business applications, and provide a frictionless, always-on user experience.

Request a Demo



