SOLUTION BRIEF

Absolute Connector for Forescout eyeSight

Maintaining Compliance Across Remote Endpoints

Endpoint Visibility and Compliance for the Anywhere Work Environment

In today's work from anywhere environment, remote employees require uninterrupted access to critical business applications and corporate resources to remain productive. Not doing so can have a significant impact on the organization's business operations and ultimately its bottom line. $25 million is the average cost of mobile technology interruptions at the average 10,000-person company.[1] On the flip side, it is vital for IT and security teams to maintain the organization's security posture to protect against the ever-present scourge of today's complex cyberthreats and ransomware attacks. By 2031, it is estimated that ransomware will cost victims $265 billion annually, and will attack a business, consumer, or device every 2 seconds.[2]

Balancing end-user experience and security enforcement can be challenging for IT and security teams given the inconsistency in endpoint visibility and control across a distributed device population. Employees today access corporate resources from various locations including the office premises, their home office or public locations such as a coffee shop or the airport while in transit, leading to heightened endpoint complexity and the risk of devices being noncompliant. Patches may not be up-to-date, security applications such as Anti-Malware and Encryption fail over time, devices stray from approved geographical areas and potentially utilize unsecure public Wi-Fi networks to access corporate resources.

Granting noncompliant devices access to the corporate network can lead to dire consequences, as threats actors commonly look to exploit vulnerable devices, move laterally and take control of other critical systems on the corporate environment. Hence, it is critical for IT and security teams to utilize comply to connect policies to continuously assess the compliance of endpoints against specific policy benchmarks before granting access to the corporate network.

Challenges resulting from remote and hybrid work policies:

- Risk of endpoints going dark, being lost or stolen due to increased employee mobility
- Devices straying from approved geographical locations
- Devices utilizing unsecure public Wi-Fi networks to access corporate resources
- Lack of visibility into endpoint hardware, software and security issues
- Difficulty in deploying patches and enforcing security policies remotely
- Accumulation of sensitive data on remote devices over time
- Inability to continuously monitor endpoint security metrics to vet access to the corporate network

The Solution: Absolute Connector for Forescout eyeSight

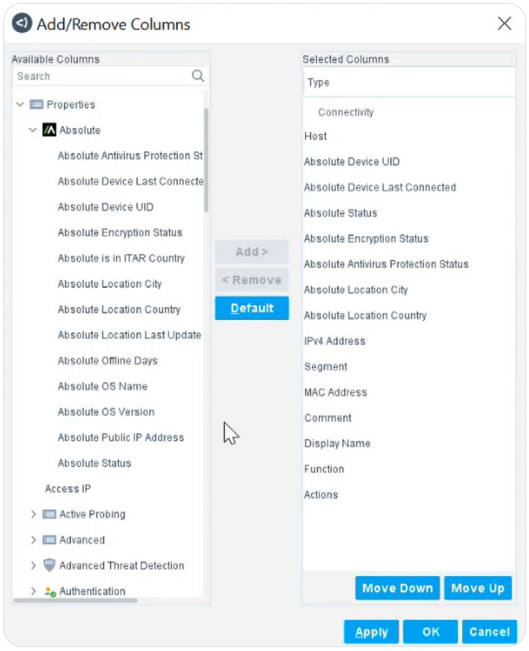
Absolute has partnered with Forescout to develop the Absolute Connector for Forescout eyeSight, combining Absolute's endpoint visibility and cyber resilience with Forescout's continuous network monitoring capabilities. This integration enables joint customers to build and configure policies to continuously assess device compliance before granting access to corporate resources. Absolute's telemetry captured from endpoints is utilized in the configuration of policies through the Forescout console. The integration also enables practitioners to execute remediation actions as part of their policies to secure devices whenever they stray from compliance.

1 Vanson Bourne, The Experience 2020 Report: Digital Employee Experience Today, 2020

2 Cybersecurity Ventures, Ransomware Will Strike Every 2 Seconds By 2031, 2023

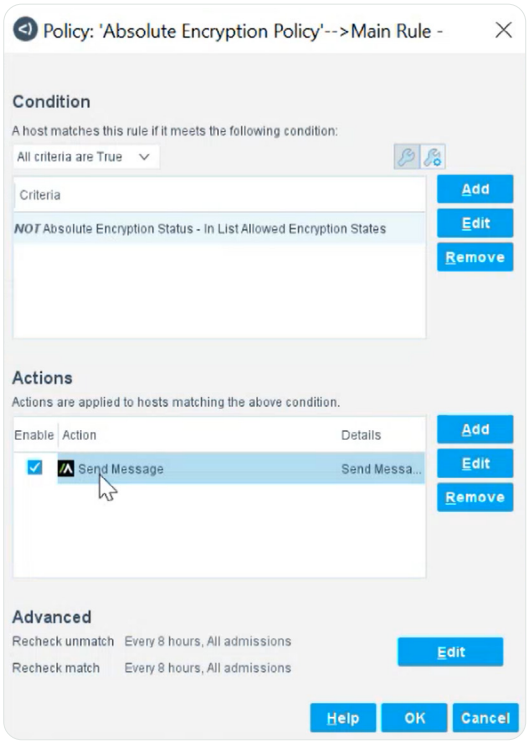
Key Capabilities:

- Configure policies to assess the compliance status of devices before granting access to corporate resources.
- Utilize endpoint telemetry such as geolocation, the health of critical security applications such as antivirus and encryption to gauge device compliance as part of the policies.
- Manually execute or integrate automated remediation actions across non-compliant devices including sending custom messages to end users or freezing a device when required.



Potential Use Cases or Scenarios:

- Flag a device as being non-compliant whenever it enters a prohibited geographical area (e.g. an International Traffic in Arms Regulations, or ITAR, listed country) and block access to the corporate network. In addition, freeze the device to protect it and any residing data from falling in the wrong hands.
- Continuously monitor the status of security controls such as anti-malware, encryption status, Endpoint Detection and Response and VPN and block access to the network whenever the apps are non-compliant. Attempt to remediate by repairing or reinstalling the application(s).
- Track installed software to identify whenever suspicious or banned application (e.g. consumer VPN, P2P Files Sharing, known spyware or malware) is installed on a device and block access to the network. Remediate the scenario by sending an end-user message informing to uninstall the software.
- Adhere with government regulations to adopt Comply to Connect (C2C) policies that discover and categorize every connecting device, run them through inspection layers and assess them against security benchmarks.



The Absolute Connector for Forescout eyeSight is accessible to joint (i.e. Absolute and Forescout) customers. It will soon be available as a consolidated solution for Forescout customers to utilize. For more information on the Connector and how to set it up, check out the Connector's listing on the Forescout Marketplace.

About Forescout

Forescout Technologies, Inc., a global cybersecurity leader, continuously identifies, protects and helps ensure the compliance of all managed and unmanaged connected cyber assets – IT, IoT, IoMT and OT. For more than 20 years, Fortune 100 organizations and government agencies have trusted Forescout to provide vendor-agnostic, automated cybersecurity at scale. The Forescout® Platform delivers comprehensive capabilities for network security, risk and exposure management, and threat detection and response. With seamless context sharing and workflow orchestration via ecosystem partners, it enables customers to more effectively manage cyber risk and mitigate threats.

About Absolute

Absolute Security is partnered with more than 28 of the world's leading endpoint device manufacturers, embedded in the firmware of 600 million devices, trusted by 21,000 global enterprises, and licensed across 14 million PC users. With the Absolute Security Cyber Resilience Platform integrated into their digital enterprise, customers ensure their mobile and hybrid workforces connect securely and seamlessly from anywhere in the world and that business operations recover quickly following cyber disruptions and attacks.