Absolute Connector for Forescout eyeSight

This document addresses a few commonly asked questions about Absolute Connector for Forescout eyesight

What is the Absolute Connector for Forescout eyeSight?

The Absolute Connector for Forescout eyesight is an integration developed by Absolute and Forescout offering joint customers the ability to build and configure policies to continuously assess the compliance of devices in their environment 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.

What pain points or challenges does the Connector solve for joint (i.e. Absolute and Forescout) customers?

The Connector enables organizations to solve pain points and challenges that their IT and security teams typically encounter in managing and securing remote devices in today's work from anywhere environment. Some common challenges encountered for practitioners include the following:

- 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

What specific capabilities does the Connector offer to joint customers?

The Connector offers the following capabilities for joint customers to access through the Forescout console.

- Configuring policies to assess the compliance status of devices before granting access to corporate resources.
- Utilizing 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 executing or integrating automated remediation actions across non-compliant devices including sending custom messages to end users or freezing a device when required.

How does the Connector work?

The Connector transfers specific datapoints that Absolute collects off an endpoint device to be viewable through the Forescout console. Examples of the datapoints collected include Antivirus Protection Status, Encryption Status, Location City/State/Country, OS Name and Version among others.

These datapoints can then be leveraged to build policies through the Forescout console so that whenever a device is in a state of non-compliance (e.g. encryption is disabled or the device is in an unauthorized location), its access to the corporate network will be blocked. In addition, a user can invoke an Absolute action (e.g. to Freeze a device or send an end-user message) either manually through the console or as part of a policy.

Are there any prerequisites/requirements needed to install and utilize the Connector?

Organizations need to be joint customers of both Forescout and Absolute and thus have applicable subscriptions of both to utilize the Connector. On Absolute's side, customers with Absolute Visibility, Control and Resilience can view Absolute's collected datapoints through the Forescout console and leverage them as part of policies. Customers with an Absolute Control or Resilience subscription can also invoke Absolute actions (e.g. Device Freeze and End-User Messaging) either manually through the Forescout console or as part of policies. On Forescout's side, customers must have access to the Forescout eyesight product to utilize the Connector.

Where can the Connector be downloaded and installed from?

The Absolute Connector for Forescout eyesight can be downloaded from the **Forescout Marketplace**.