

Why ForeScout for Zero Trust

Q: How does the ForeScout solution map to the Zero Trust framework?

A: The ForeScout platform aligns directly with the Zero Trust framework from the top down. It enables organizations to strategically select best-of-breed enforcement for Zero Trust across all portions of their enterprise networks. ForeScout starts with full visibility for all IP-connected devices across enterprise segments, including campus, data center, cloud and OT environments. The solution provides deep inspection of device security and configuration state to determine the device risk posture. The ForeScout policy engine translates the enterprise's security policies and segmentation strategy into the rules applied by individual enforcement products based on the device's risk posture. Specifically, ForeScout allows translation of Zero Trust strategy to enforcement across wired, wireless, DC, cloud, and OT portions of enterprise networks using switch, FW/NGFW and SDN products. Additionally, ForeScout includes an open integration capability to allow field-built integrations with any product that offers REST APIs.

Q. How does the ForeScout solution enable your organization to achieve Zero Trust at the network layer?

A: The ForeScout platform uses a combination of passive and active methods to discover and provide detailed classification of devices upon connection to the network. The device type and classification is fed into the solution's policy engine so customers can define the business' security risk and Zero Trust segmentation policies. Based on the type, state, location, etc. of the device, ForeScout translates the matching Zero Trust policy to the specific commands necessary to configure that policy on a broad range of network devices (switch, router, WAP, FW, SDN, etc.). The commands are executed by ForeScout and the wide array of enforcement products to enact the Zero Trust policy without IT administrators manually configuring each product. Finally, ForeScout continuously monitors devices, so should the device change (network location, security posture, logged-on user, etc.), ForeScout will re-evaluate the new state of the device and enforce the Zero Trust rules in real time, if necessary, without any IT Staff intervention.

Q: What specific capabilities does the ForeScout solution enable Zero Trust networking?

A: The ForeScout platform conducts detailed device classification and assessment of devices upon connection. The evaluation of the device state and posture by the policy engine then passes specific configuration commands to enforcement products, allowing network segmentation using switch ACL/VLANs, NGFW dynamic address groups, cloud security groups, software-defined security controls. ForeScout also has API integrations with multiple endpoint management products in the EPP, EDR and CMT categories. These integrations pull detailed device-configuration-state data, as well as orchestrate remediation responses to correct security posture deficiencies, and subsequently enforce the Zero Trust policy associated with the endpoint after successful remediation. ForeScout does this agentlessly and continuously across heterogeneous networks that use a variety of network vendors, without requiring network changes in the campus (wired/wireless), data center/cloud and OT environments.

Q: What ForeScout features specifically power Zero Trust within the solution?

A: The ForeScout platform's robust policy engine is the core element that enables your organization to implement your Zero Trust strategy. It combines ForeScout's detailed device classification and posture assessment with assignment of segmentation policies. The policy engine allows creation of rules to identify devices connecting to network, interrogation of a device's state, including security posture and user of the device. The policy engine then provides product-specific enforcement commands that are unique to each network infrastructure vendor, allowing policy-based control of what that device can access. Additionally, should the state of any device change, the policy engine reassesses that device in real time and informs the network architecture of any Zero Trust changes necessary to dynamically adapt.

Q: In a Zero Trust network, how does the ForeScout solution enable a Zero Trust strategy across the enterprise?

A: ForeScout's agentless data collection capabilities use a combination of both active and passive methods to discover and classify device type, user identity, location, etc. of each device, as well as assessing its security posture. With these rich data sets, the solution leverages its built-in translation integrations with over 70 network enforcement vendors across wired, wireless, SDN, cloud and OT environments. This allows the customer to define

a unified ZT strategy across their environment and leverage Forescout to perform the individual enforcement-product configuration. These integrations use a variety of methods including SSH/CLI, SNMP, Syslog or custom API services to communicate between Forescout and the enforcement products.

Q: How does the Forescout complement other security solutions and/or services in pursuit of a Zero Trust network?

A: The Forescout real-time policy engine continuously checks devices against a set of policies that control how devices are expected to behave on the network. Acting as an abstraction layer, it enables orchestration between network security and device posture assessment point products. By leveraging data and context from both the network and device, Forescout allows automated implementation of enterprise business, risk and security policies to drive the organization's Zero Trust strategy. Forescout's integrations with NGFW, Cloud IaaS, SDN and DC solutions enable the creation and management of device assignment to dynamic Zero Trust enclaves (dynamic MCAPs for source and destination). The visibility and wealth of device data coupled with business policy housed in the policy engine rules have allowed Forescout to build over 70 bi-directional data sharing and control enforcement integrations with third-party tools across the SIEM, ITSM, EPP, EDR, CMT, PAM, NGFW, ATD and EMM product categories.

Q: What effect does the solution have on hybrid networks (cloud and on-premise)? Does the solution work seamlessly across disparate networks?

A: The Forescout platform provides comprehensive coverage across hybrid and disparate networks, including wired, wireless, virtualized on-premise DC, cloud IaaS and completely passive OT segments. Forescout provides a unified user experience to implement Zero Trust across all of these components of an enterprise because it has been engineered to provide the translation from the policies defined in the platform to a very large range of network infrastructure and security products. The Forescout platform was built from the beginning to thrive in heterogeneous networks.

Q: At what layers of the OSI model does the Forescout solution make the most impact?

A: The Forescout platform operates at levels 2-7 of the OSI model for different aspects of the platform. The lower layers are used when inspecting raw traffic to identify and classify devices as they connect to the enterprise network. Endpoint device assessment and inspection is done at the application layer using remote access protocols. After the solution has identified, classified and determined which Zero Trust policy applies to a device, Forescout uses various application-level protocols to configure the individual enforcement rules on the individual enforcement components in the network.

Q: How does the Forescout solution enable microsegmentation or isolation of network assets?

A: The detailed visibility capabilities of the Forescout platform allow dynamic identification of both source and destination assets on any network (campus, physical & SDN DC, cloud and OT) within the customer environment. Using the rich endpoint data (device type, user identity, location, compliance, application, etc.) the solution provides granular and detailed policy translation to the specific commands necessary to configure VMware NSX, AWS, NGFWs and over 15 switch vendors' ACLs/VLANs for dynamic MCAPs (source and destination) segmentation, allowing dynamic ZT enclaves to be defined across multiple enforcement products. This capability allows for automated microsegmentation of applications and workloads as well as isolation or quarantine of networked endpoints in the event of an incident.

Learn more at
www.Forescout.com



FORESCOUT

Forescout Technologies, Inc.
190 West Tasman Drive
San Jose, CA 95134, USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support 1-708-237-6591

Q: How does the Forescout solution enable compliance control at the network layer of your organization?

A: The Forescout platform includes the capabilities to do deep agentless inspection of device posture (configuration state, agent-based control state, SCAP-based profile compliance) upon initial connection to the network (wired or wireless network informs Forescout in real time of connection) through remote access protocols (SSH, RPC, WMI, proprietary third-party product APIs). Network segmentation policies can be created using over 900 different attributes of an endpoint as decision criteria for how the device will be segmented at the network layer, leveraging multiple enforcement points and methods across any network (campus, physical, SDN DC, cloud, and OT).

© 2019 Forescout Technologies, Inc. All rights reserved. Forescout Technologies, Inc. is a Delaware corporation. A list of our trademarks and patents can be found at <https://www.Forescout.com/company/legal/intellectual-property-patents-trademarks>. Other brands, products, or service names may be trademarks or service marks of their respective owners.

Version 01_19