FORESCOUT

Zero Trust

Frequently Asked Questions

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-bread 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 operational technology (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, data center, 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, the Forescout platform continuously monitors devices, so should the device change (network location, security posture, logged-on user, etc.), the Forescout solution 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: How does Forescout simplify micro-segmentation planning within the context of the Zero Trust framework?

A: Micro-segmentation is a core tenet of the Zero Trust framework. However, designing, applying and maintaining effective segmentation policies across distributed environments can be an arduous process. With the introduction of its eyeSegment product, Forescout has accelerated and substantially simplified the process of designing, planning, testing and deploying dynamic network segmentation across the extended enterprise. eyeSegment builds on the comprehensive device visibility and in-depth, real-time context provided by the Forescout platform. Because this platform doesn't require agents, it is equally adept at discovering and profiling managed, unmanaged and Internet of Things (IoT)/OT devices, as well as virtual instances and cloud-based workloads. This allows organizations to embrace Zero Trust principles for all IP-connected systems. eyeSegment allows customers to visualize traffic flows and dependencies between users, applications, services and devices, and then design, simulate and monitor policies to understand the impact to their environment.

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. This helps organizations understand devices, users, applications and workloads that need to be protected. With eyeSegment, Forescout helps organizations map data flows to marry user/device/application context with network traffic, allowing them to understand the business context and interdependencies of devices prior to establishing segmentation policies. Organizations can simulate segmentation policies prior to actually deploying them in the production environment—avoiding potential disruption of critical services.

Once Zero Trust segmentation policies are established, the policy engine evaluates the device state and posture of devices, then passes specific configuration commands to enforcement products, allowing network segmentation using switch ACL/VLANs, NGFW dynamic address groups, cloud security groups and 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: 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 the Forescout platform 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's solution and 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 data center 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 SIEM, ITSM, EPP, EDR, CMT, PAM, NGFW, ATD and EMM products.

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 data center, 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 micro-segmentation 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 and SDN data center, 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, Cisco DNA Center, 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 micro-segmentation of applications and workloads as well as isolation or quarantine of networked endpoints in the event of an incident.

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

A: The Forescout platform incudes 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, data center, cloud and OT). The Forescout platform also allows you to demonstrate MAC spoofing resilience to auditors and improve audit compliance.

Q: What capabilities does Forescout provide within Forrester's Zero Trust eXtended ecosystem?

A: Forescout offers several capabilities that are foundational to Zero Trust architecture. In July 2019, Forrester named Forescout as a Zero Trust Platform and highlighted the Forescout platform's market-leading capabilities in the following Zero Trust eXtended Ecosystem categories: Security Visibility and Analytics, Device, Network, and Security Automation and Orchestration. Forrester also highlighted Forescout as "The vendor for Zero Trust IoT/OT security" in its Q4 2019 Zero Trust Wave Report. According the report: "IoT/OT device security is one of the hardest problems to solve within the enterprise. This is Forescout's sweet spot, and the vendor's platform and capabilities for IoT/OT security shine above those of the competition."

FORESCOUT

Forescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

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