FORESCOUT

Solution Brief

Forescout as a Zero Trust Platform

Protecting devices, networks and data across the business ecosystem

Zero Trust Model Defined

At its simplest, Forrester's Zero Trust Model of information security is a conceptual and architectural approach for redesigning networks into secure microperimeters, strengthening data security using obfuscation techniques, limiting the risks associated with excessive user privileges and access, and dramatically improving security detection and response with analytics and automation.[2]

Zero Trust Challenges:

- Lack of visibility into connected devices/lack of asset intelligence
- Limited insight into traffic patterns and system interdependencies
- Network segmentation is difficult to configure and maintain
- Little-to-no automation exists for firewalls to update policies as devices change and move
- Network access control doesn't map to specific user roles and business needs
- Security tool integration and information exchange from data center to cloud is less than seamless
- Constantly evolving heterogeneous networks lack centralized access control and asset managemement

Security and risk professionals the world over are coming to terms with the realization that maintaining perimeter defenses around a trusted network is no longer a viable security strategy. Forrester Research analysts anticipated the current reckoning and developed the Zero Trust Model of information security. Aptly named, the Zero Trust Model is built on the assumption that any person or device with access to an organization's data is a threat to the enterprise.

Forrester insists that 100 percent device visibility is a prerequisite for any effective security architecture.[1] Given the rapidly evolving enterprise environment, in which agentless IoT devices, virtualization and cloud computing have become prevalent, an enterprise that adheres to the Zero Trust Model must not only feature complete device visibility across the heterogeneous environment, it must also be capable of dynamic network segmentation and orchestrated incident response, as well as continuous monitoring and control of connected devices and workloads.

The Challenge

Networks are becoming increasingly complex and heterogeneous, the devices that are connecting to them are incredibly diverse, hackers are more devious than ever before, and security controls simply haven't kept up. Today more than ever before, every organization needs a way to continuously defend its network ecosystem and data in ways that actually work. This requires commitment to an enterprise-wide model of security in which nobody and no system is trusted by default.

Properly implemented, Forrester's Zero Trust Model provides the basis for knowing that an organization's sensitive data and intellectual property are protected according to policy requirements and are not being compromised by either internal or external threats.

Implementing Zero Trust across your digital business begins by recognizing network security as a fundamentally data-centric exercise and redesigning network security architecture accordingly. Note that each of Forrester's Five Steps to Zero Trust[2] focus on data in some way:

- Step 1: Identify your sensitive data
- Step 2: Map the data flows of your sensitive data

- Step 3: Architect your Zero Trust microperimeters
- Step 4: Continuously monitor your Zero Trust ecosystem with security analytics
- Step 5: Embrace security automation and orchestration

The Solution

The Forescout platform is a must-have for organizations seeking to implement a Zero Trust Model. It provides visibility into all IP-connected devices across all enterprise segments, including campus, data center, cloud and OT environments. It integrates with switches, routers and wireless controllers, and can dynamically segment the network. And because it can share intelligence and enforcement capabilities with third-party security and IT management tools, the Forescout platform is the core solution for protecting data, devices and infrastructure via granular policies, across-the-board compliance and ongoing endpoint control.

The complexity of enterprise networks—today and going forward—necessitates a security platform that can handle heterogeneous environments and constant change. The agentless Forescout platform can discover, assess and provision access to any legacy device or system through any IP-based network infrastructure (regardless of version level). The same can't be said for any other platform.

Continuous visibility and policy-based device control

Forrester analysts assert that a Zero Trust strategy requires continuously controlling ALL devices on the network.[3] In addition to "seeing" traditional servers, PCs, laptops and smartphones, the Forescout platform can discover IoT and OT devices, peripherals, network infrastructure components and rogue devices the instant they connect to the network—even if they don't have security agents installed. The same is true for virtual machines/workloads and cloud instances. The platform gathers detailed information about device types, users, applications, operating systems and more. Then it enforces expected behavior and policy compliance by allowing, denying or restricting access to internal network resources according to device/user roles. The platform can also issue notifications and initiate device remediation based on established policies. Post-connection, the platform continuously monitors endpoints to make sure that device behavior doesn't deviate from policies.

The Forescout platform serves as a centralized access broker in a Zero Trust architecture. It sees all devices, handles asset discovery, simplifies asset mapping and provides the device control enforcement mechanism.

The Forescout platform serves as a centralized access broker in a Zero Trust architecture. It sees all devices, handles asset discovery, simplifies asset mapping and provides the device control enforcement mechanism. Regardless of whether endpoints are associated with a Cisco switch, SDN network, wireless controller, VPN, application gateway or next-generation

Forescout Solution:

- See ALL devices and their compliance status in real time
- Map system dependencies across campus, data center, cloud and OT environments
- Enforce segmentation policies at network layer across heterogeneous infrastructure (switches, next-generation firewalls or software-defined networks)
- Correlate access and users (who is doing what, where, when and why) and provision them to dynamic network segments based on policies and real-time context
- Continuously monitor devices and enforce segmentation policies
- Orchestrate data sharing and enforcement actions across Zero Trust eXtended framework
- Configure/support leading security or infrastructure vendors' products running multiple technologies, including legacy systems and devices

Using rich endpoint data, the Forescout platform abstracts detailed policies to automate segmentation actions on VMware® NSX, AWS® EC2 instances, leading next-generation firewalls (NGFWs), software-defined security controls and ACLs/VLANs.

firewall, the Forescout platform sees and classifies them, then provisions them with access according to their identities and user roles.

From device discovery to asset intelligence

The Forescout platform turns asset discovery into real-time asset intelligence. Forescout's varied active and passive discovery and profiling methods quickly produce and continuously refresh a vast amount of information on device identity, state and behavior. By ingesting, correlating and consolidating billions of packets of raw data across heterogeneous network systems, it creates a unified view of the entire device population with granular drill-down detail into individual devices.

Initial deployment of the Forescout platform shows you the endpoints currently connected to your network and allows you to visualize communications between devices and data sources as well as system interdependencies. This is particularly important for segmentation mapping, planning and policy creation. Then, by implementing access control across all systems, the platform enables you to migrate up to dynamic segmentation and Zero Trust.

Dynamic, policy-based network segmentation

The Zero Trust approach calls for microperimeters that split the network into zones containing data with similar access and compliance requirements. The Forescout platform helps simplify segmentation modeling and policy creation. 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. Using this rich endpoint data, the Forescout platform abstracts detailed policies to automate segmentation actions on VMware® NSX, AWS® EC2 instances, leading next-generation firewalls (NGFWs), software-defined security controls and ACLs/VLANs.

By adding Forescout Base and Extended Modules, you can orchestrate dynamic segmentation enforcement across heterogeneous infrastructure and next-generation firewalls. One especially popular and effective integration is between the Forescout platform and next-generation firewalls such as those from Palo Alto Networks®. Sharing intelligence and policy enforcement between the two automates the process of perimeter and zone-based network segmentation assignment, as well as quarantining compromised endpoints until they can be fully scanned and cleansed. A concrete example of this type of dynamic segmentation is Forescout's ability to identify new IoT devices and automatically assign them to a restricted network segment. It's all part of helping you turn asset discovery into risk-mitigating controls.

Orchestrated asset protection and incident response

With an assist from Forescout Base and Extended Modules, the Forescout platform can share real-time device context, user information and device compliance status with more than 70 popular security and IT management tools.* By enabling integrations with these security solutions (ATD, AV, EMM, EPP/EDR, NGFW, VA, PAM, SIEM and more), Forescout extends the maturity level and value of existing solutions while enabling organizations

to strategically select integrated, best-of-breed enforcement solutions for Zero Trust across hybrid and disparate networks, including wired, wireless, virtualized on-premise data center, cloud IaaS and even passive OT segments.

Extending the value of legacy systems and environments

A critical advantage of the Forescout platform when it comes to real-world Zero Trust implementation is that it can discover, assess and control access to legacy devices or systems through legacy network infrastructure. In effect, the Forescout platform provisions legacy systems into a Zero Trust architecture. This is especially valuable in the context of merger and acquisition activity and legacy medical system integration.

With the acquisition of SecurityMatters, Forescout also extends its network-based situational awareness beyond IT to OT and industrial control system (ICS) environments. Combined capabilities now include deep packet capture/inspection of 100+ IT/OT protocols, network mapping, flow analysis, policy and behavior monitoring, network forensics, threat assessment and risk scoring.

Learn More

Zero Trust success begins with total device visibility and control. To learn more about how the Forescout platform simplifies planning and deployment of the Zero Trust Model, visit www.Forescout.com/zero-trust.

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
Fax 1-408-371-2284

*As of December 31, 2018
[1] Gauge Your ZTX Security Maturity, Forrester Research, July 2018
[2] Five Steps to a Zero Trust Network/Roadmap Report, Forrester Research, October 2018
[3] The Zero Trust eXtended (ZTX) Ecosystem/Strategic Plan: The Security Architecture And Operations Playbook, Forrester Research, January 2018