FORESCOUT

Total Visibility: The Master Key to Zero Trust

Forescout provides the device visibility platform for Zero Trust security

In None We Trust

The Zero Trust model of information security has become a fixture in both the strategies of enterprise security teams and the roadmaps of security solution developers, and for good reason. Perimeter-focused security architectures that default to high trust levels on the internal network continue to fail disastrously and expensively. A recent analysis by the Online Trust Alliance found that business-reported cyber incidents nearly doubled in 2017. In fact, in the first three quarters of 2017, data breaches exposed more than 7 billion records, a four-fold increase over 2016.[1] The Ponemon Institute puts a price tag on this carnage, estimating the cost of each stolen record at $141, and the average total cost of a data breach at $3.62 million.[2]

The Multiple Failures of Perimeter Security

Today's enterprise environments rely heavily on cloud-based services and infrastructure, which effectively erase the network perimeter. Workloads, data and the workforce itself are mobile now, and need agile security. Users also demand more access options to more accounts, data and resources. Concurrently, the volume and diversity of devices connecting to network resources overwhelms traditional endpoint management. Because many of these devices do not or cannot run corporate management agents (visitor devices, BYOD systems, IoT devices and operational technologies), security teams may be blind to many of the devices on their networks, unable to identify their users, assess their security state, or control their activities.

These systemic failings of perimeter-focused security led Forrester Research analysts to develop Zero Trust as an alternative. Introduced in 2010, Zero Trust is a conceptual and architectural model for how security teams should redesign networks into secure microperimeters, strengthen data security using obfuscation techniques, limit the risks associated with excessive user privileges and access, and dramatically improve security detection and response with analytics and automation.

Zero Trust: From Conceptual Model to Comprehensive Framework

In early iterations, the Zero Trust model focused narrowly on the concepts of protective segmentation and least-privilege access control, with little specific direction on how existing security controls could be leveraged in practical implementations. Over time, the basic model has evolved and matured into what Forrester calls the Zero Trust eXtended (ZTX) Ecosystem. This is a comprehensive framework that maps relevant security technologies to seven key dimensions of a typical enterprise environment where Zero Trust principles pertain: networks, data, people, workloads, devices, visibility and analytics, and automation and orchestration.

The ZTX framework helps security teams understand what a technology does to:

- Enable the principles of network isolation, segmentation and security
- Enable data categorization, isolation, encryption and control
- Protect the human users of network and infrastructure resources, while securing those resources from their users
- Protect workload application stacks in public and private clouds
- Automate and orchestrate Zero Trust controls and processes across heterogeneous environments
- Provide visibility and analysis to illuminate and secure every nook and cranny of the extended enterprise environment

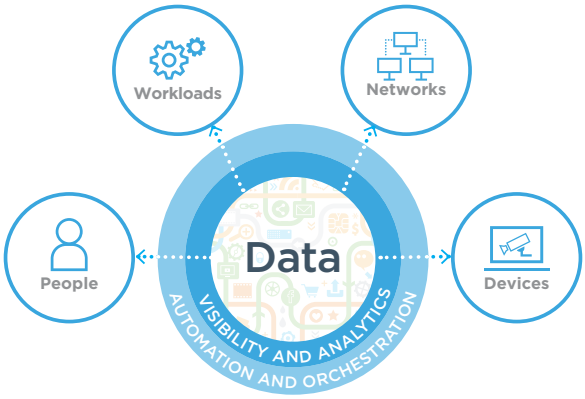

Figure 1: The seven dimensions of Forrester Research's Zero Trust eXtended Ecosystem Framework

If Visibility Is the Strategy, Forescout Is the Platform

One example of a Zero Trust strategy is the goal of discovering and classifying 100 percent of the devices that connect to the network—not just those with endpoint agents installed and operational—and to strictly enforce least-privilege access policy based on a granular analysis of the device, user identity and authorizations, software stack, configuration compliance and security state. To enforce restrictive access policy, one must see, assess and control everything on the network.

Forrester is emphatic on the topic of visibility in Zero Trust. According to Forrester analyst Chase Cunningham:

"Visibility is the key in defending any valuable asset. You can't protect the invisible. The more visibility you have into your network across your business ecosystem, the better chance you have to quickly detect the telltale signs of a breach in progress and to stop it."[3]

To realize such a strategy requires a comprehensive device visibility and control solution capable of seeing and controlling hosts that conventional endpoint management systems cannot: visitor and BYOD devices, corporate endpoints with disabled agents, rogue devices, IoT devices, network switches and routers, factory floor and other OT systems, and virtual machines in public clouds.

The Forescout Platform: Gain Visibility and Control Risk

Forescout exemplifies the evolution of leading network technologies into Zero Trust platforms. The Forescout platform is an agentless security solution that dynamically identifies and evaluates network endpoints the instant they connect to your extended, heterogeneous, multi-cloud network. It quickly determines the user, owner and operating system, as well as device configuration, software, services, patch state and the presence of security agents. Next, it provides remediation, control and continuous monitoring of these devices.

Forescout exercises these capabilities on managed corporate devices, unmanaged visitor devices, physical and virtual servers, network infrastructure, industrial operations and control systems and IoT devices—without requiring software agents or previous device knowledge. It deploys quickly into your existing environment and rarely requires infrastructure changes, upgrades or endpoint reconfiguration. Critically, it functions seamlessly in physical, virtual and hybrid cloud environments.

The Forescout platform provides 100-percent discovery and classification of all IP-connected devices, as well as continuous, agentless risk and posture assessment to determine real-time situational awareness of every connected device. It then applies this intelligence to automate policy-based controls and orchestrate actions upon devices. These capabilities provide the basis for effective Zero Trust security.

Zero Trust Device Visibility, Analysis and Control

Agentless discovery of any device - The Forescout platform employs a combination of agentless active and passive methods to discover all of the devices on an organization's extended, heterogeneous network—from campus and data center to cloud and operational technology networks. It detects PCs and notebooks, physical and virtual servers, mobile and IoT devices, cloud instances and operational technology systems with no need for vendor-specific network equipment, upgrades of existing infrastructure or reconfiguration of switches and switch ports, with or without 802.1X authentication.

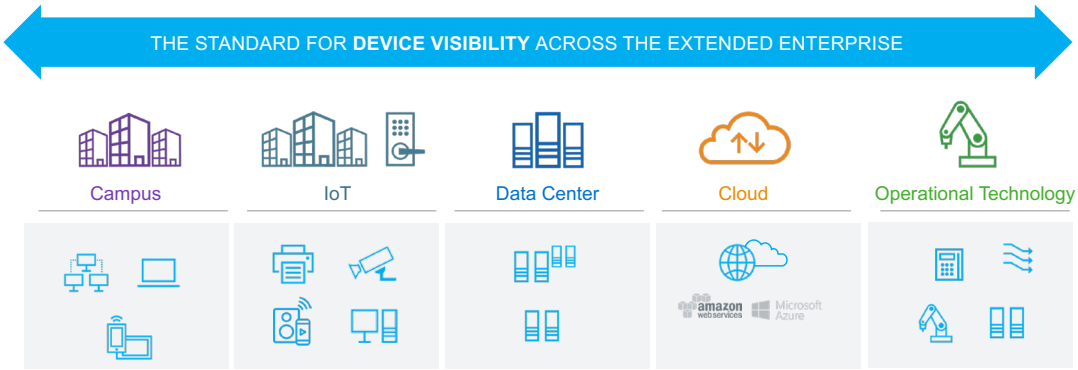

Figure 2: Forescout provides a device visibility and control platform for the extended enterprise.

From device discovery to asset intelligence – Forescout's varied discovery and profiling methods quickly produce and continuously refresh a vast amount of information on device identity, state and behavior. The platform's adaptive abstraction layer ingests billions of packets of raw data across a wide array of heterogeneous network systems. It correlates and consolidates this data, creating a unified view of the entire device population with granular drill-down detail into individual devices. The abstraction layer adapts and evolves with the IT environment, continuously enriching the device view as new data sources become available. Its data provides a richly detailed view of all the assets in the environment, empowering and informing a wide range of decisions and actions, and providing the basis for risk-mitigating controls.

In addition, the Forescout platform allows monitoring and visualization of communications between devices and data sources as well as system interdependencies. This is particularly important for segmentation mapping, planning and policy creation.

The Forescout platform allows monitoring and visualization of communications between devices and data sources as well as system interdependencies. This is particularly important for segmentation mapping, planning and policy creation.

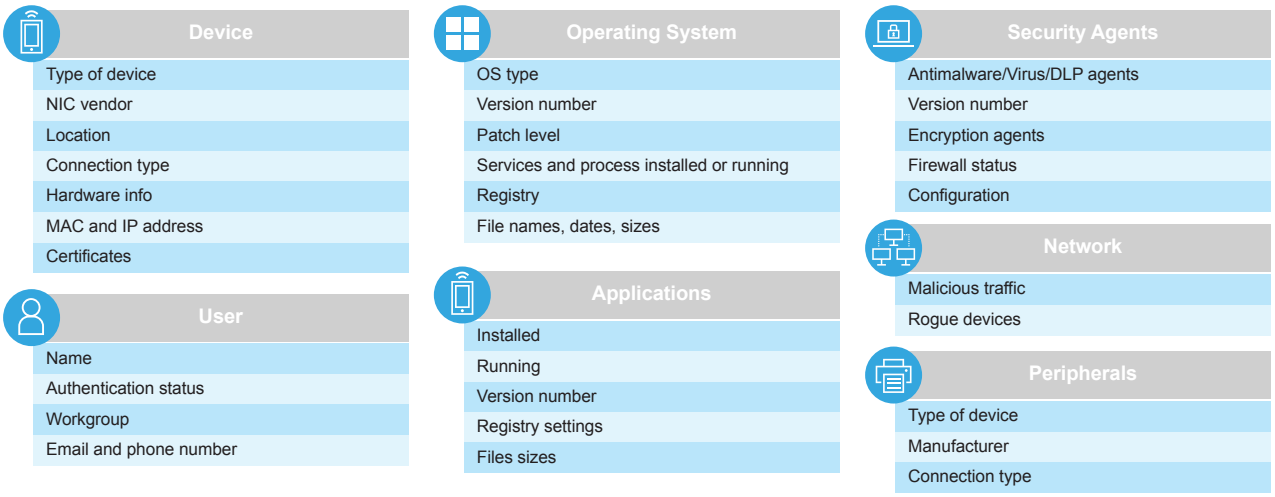

Figure 3: Forescout's classification process extracts detailed data on all IP-connected devices.

Continuous visibility and policy-based device control - The Forescout platform's real-time policy engine utilizes this asset intelligence to continually assess devices against policies that enforce expected behavior. It triggers policies in real time based on a device's network admission, authentication and other customizable attributes. For example, Forescout can identify a new IoT device with outbound internet access and automatically assign it to a restricted network segment. It can detect changes in a device's security state, such as antivirus agents or encryption software that have been disabled or become dysfunctional. The platform re-assesses devices while they are on the network and each time they come and go. It shares real-time device context and initiates posture-assessment actions—such as rescanning devices for vulnerabilities and indicators of compromise—in concert with third-party systems.

Forescout can execute control actions directly upon the device or through the network infrastructure (discussed below). Host-based controls include starting and stopping applications, updating antivirus security agents, disabling peripheral devices and requesting end-user acknowledgement. The policy engine applies these policies automatically regardless of a device's location. When necessary, the Forescout platform can automate remediation actions, such as device patching or reinstalling vulnerability assessment, endpoint protection, encryption or other security software through orchestration with third-party tools (also covered in greater detail below).

Customizable device intelligence for security operations and incident response - Security operations teams lack a comprehensive view into connected devices and their classification, connection and compliance context. This hampers incident response and compliance reporting. In addition to the platform console, the Forescout platform now includes a customizable web dashboard that provides a consolidated view of your device landscape and compliance status across the extended enterprise. The dashboard works in concert with the Forescout eyeManage and provides insight into the diverse types of devices connected to your heterogeneous network.

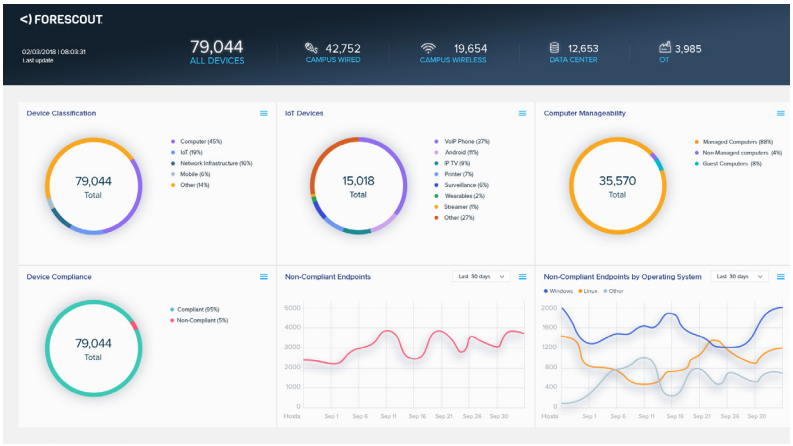

Figure 4: Consolidated view of device landscape for security operation centers.

Zero Trust Network Capabilities

A Zero Trust access broker - The Forescout platform enforces device control actions through the network infrastructure, providing a centralized brokerage service and decision point for network access provisioning based on its integrated view of user identity, role, authentication and device state. It integrates natively with products from more than 30 switch and wireless vendors and provides direct integration with routers that run the Linux operating system. Depending on the vendor, various methods are used individually or in combination, including SNMP, CLI and NETCONF. Working at a network switch, this technology can change a VLAN assignment, add an ACL or disable a switch port. At a wireless controller, it can blacklist a MAC address or change the role of a user. In addition, our technology can restrict remote VPN users.

One critical distinction for real-world Zero Trust implementation is that the agentless Forescout platform can discover, assess and provision access to any legacy IP-connected device. Forescout sees and controls every IP-connected device and integrates with all IT and OT network infrastructure without exception.

One critical distinction for real-world Zero Trust implementation is that the agentless Forescout platform can discover, assess and provision access to any legacy IP-connected device.

With the acquisition of SecurityMatters, Forescout also extends its network-based situational awareness beyond IT—deep into 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.

Dynamic network segmentation - Forescout also works with next-generation firewalls, providing the decision and enforcement points for dynamic, policy-based segmentation. Next-generation firewalls provide network control based on user, device, application and traffic classification. They leverage user and device context from a variety of sources, including the Forescout platform, to enforce granular access policies with precise and flexible control over resources. This enables IT organizations to implement dynamic network segmentation and create context-aware security policies within their next-generation firewalls based on endpoint context information from Forescout.

Zero Trust Automation and Orchestration Capabilities

The Forescout platform orchestrates infrastructure-wide security management to make formerly disjointed security products work as one. Its unique set of network, security and management interoperability technologies is extended and amplified through API integration via Forescout eyeExtend products to more than 70 third-party security and IT management products*, allowing the combined system to accelerate response, achieve major operational efficiencies and provide superior security.

Forescout enables security automation and orchestration in three ways:

- **Sharing real-time contextual insight** - Forescout continuously monitors and dynamically shares endpoint device identity, configuration and security details with other security and management systems you own and use. This bidirectional data exchange adds to the overall properties that can be applied to the rules engines of other tools, enhancing policies and actions.
- **Automating workflows** - Forescout allows systems to share policy-based decisions that previously required manual analysis and application across systems. Automating these workflows and processes results in coordinated, instantaneous response.
- **Automating response actions** - Many security products such as advanced threat detection systems, security information and event management and vulnerability assessment tools can inform IT staff about security issues. Forescout instantly applies this security insight to trigger an automated response and enforce its broad range of policy-based controls, such as isolating the device and remediating the endpoint to eliminate threats.

Zero Trust Workload Capabilities

Because the Forescout platform discovers, classifies and profiles physical and virtual servers anywhere on an extended network, it can track and monitor workloads as they migrate between private and public cloud environments. Forescout can identify the entire application stack running on each server and can ensure that only authorized users and devices are allowed access.

Zero Trust User Capabilities

The Forescout platform integrates with leading directory and identity systems to acquire available user information, including role and resource access authorizations. It correlates this information with discovered data on device configuration, security state and compliance, allowing resource access decisions based on both device and user insights. User behavior is monitored continuously, and integration with privileged access management systems discovers user accounts with noncompliant permissions.

Zero Trust Data Capabilities

Forescout supports data security across all IP-connected devices by providing visibility into the presence and operational state of encryption, obfuscation, and other information security software that is required by policy. If such applications are missing or inactive, Forescout can take policy-based actions such as alerting the user, notifying an administrator or quarantining the device until it has been remediated.

For Zero Trust Success, Start with Total Device Visibility

Forescout offers many ways to gain greater insight into the Forescout platform, including:

- **Take a Test Drive:** Experience the before-and-after difference of the Forescout platform with a hands-on test drive that takes you through five powerful use cases.
- **Request a Demo:** Visit the Forescout demo page to request a personal demo and access a full complement of on-demand demos and video options.
- **Use the Forescout Business Value ROI Tool:** Quantify the business value the Forescout platform can provide to your organization (as calculated by IDC's Business Value Model) in just 10 minutes.
- **Contact Forescout Consulting Services:** Are you in the process of architecting your environment to the Zero Trust model? Forescout consultants are thoroughly trained, experienced and certified in product implementation, process development and systems integration, as well as network access and endpoint compliance best practices.

*As of December 31, 2018

***Notes**

1 Online Trust Alliance, Cyber Incident and Breach Trends Report, January 2018
2 Ponemon Institute 2017 Cost of Data Breach Study, June 2017
3 The Zero Trust eXtended (ZTX) Ecosystem, Forrester Research, January 2018

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

Learn more at Forescout.com