Total Visibility: The Master Key to Zero Trust

Forescout provides the device visibility platform for Zero Trust security

"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." — Forrester Research, July 2019

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.

Perimeter Security Is Increasingly Irrelevant

Today’s enterprise environments rely heavily on cloud-based services, ecosystem partners and a mobile workforce, all of which live beyond the network perimeter. In addition, digital transformation requires greater agility with users and applications accessing more accounts, data and resources. According to Gartner, “As a result of digital transformation efforts, most enterprises will have more applications, services and data outside their enterprises than inside.”

Concurrently, the volume and diversity of devices connecting to network resources is overwhelming traditional endpoint management. Because many of these devices do not or cannot run corporate management agents (including visitor devices, BYOD systems, IoT devices and operational technologies), security teams may be blind to many of the devices on their networks and therefore unable to identify their users, assess their security state, or control their activities.

The 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 micro-perimeters, 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 as to 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

If Visibility Is the Strategy, Forescout Is the Platform

One key aspect 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.”

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 Device Visibility, 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 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 applies 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.

Forrester named Forescout as a Zero Trust platform within its Zero Trust eXtended ecosystem of vendors. According to the analyst firm, Forescout offers market-leading capabilities in five Zero Trust component categories. Forrester also highlighted Forescout as “The vendor for Zero Trust IoT/OT security” in its Q4 2019 Zero Trust Wave Report.

Zero Trust Device Visibility, Analysis and Control

The Forescout platform provides 100-percent discovery and classification of all IP-connected devices as well as continuous 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.

Agentless discovery of any device - The Forescout platform employs a combination of agentless active and passive methods to discover and classify 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.

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. This 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.
Continuous visibility and policy-based device control - The Forescout platform’s 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 (as elaborated on below). Host-based controls include starting and stopping applications, updating antivirus security agents, disabling peripheral devices and requesting end-user acknowledgement. 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).

Zero Trust Devices

One of the biggest challenges facing organizations is discovering and securing the vast numbers of unmanaged devices showing up on their networks. The IoT device explosion has left IT and security staff scrambling to address what Forrester describes as a "potential massive area of compromise." As IT-OT convergence continues unabated, there are no longer strict divisions in place between disparate technologies and areas of responsibility. Also, aside from being unmanaged, OT devices are no longer air-gapped for security purposes. CIOs are bearing the brunt of these structural changes, and they need sophisticated methodologies for gaining the upper hand over converged environments that are currently rife with vulnerabilities. Forescout’s agentless approach to device visibility and control and passive discovery techniques fit the bill. These capabilities have placed the company at the forefront of the IoT security market, and they are ideal for non-disruptive discovery and management of both IT and OT devices.

With the acquisition of SecurityMatters, Forescout extends its network-based situational awareness beyond IT environments—deep into OT and industrial control systems (ICS). 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.

This expertise in IoT and OT security is well recognized by Forrester. In fact, according to the analyst firm, “Forescout is the vendor for Zero Trust IoT/OT-focused security. 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. Maximum visibility, leading to maximum operational control and, ultimately, security, is the crux of Forescout’s approach to Zero Trust.”

---

Figure 3: Forescout’s classification process extracts detailed data on all IP-connected devices.
Zero Trust Network Capabilities

**Dynamic network segmentation** – Micro-segmentation is a core tenet of the Zero Trust framework. However, designing, applying and maintaining effective segmentation policies across distributed environments has been an arduous process at best. Conventional segmentation solutions have been labor-intensive, requiring manual analysis of traffic flows and logs to understand traffic dependencies. This manual approach increases the likelihood of human error, inconsistent segmentation policies, and even business disruption. When you factor in that most segmentation takes place in complex, multivendor/multidomain enterprise environments, implementation becomes a massive undertaking.

Forescout believes that there is no one-size-fits-all solution to network segmentation. All segmentation tools have specific strengths, use cases and areas on the network where they will be best deployed. Forescout's segmentation strategy supports application-centric, device/role-centric and boundary-centric approaches to policy-based Zero Trust segmentation that span all domains of enterprise network environments (campus, data center, IT/OT and cloud).

To simplify and accelerate segmentation adoption, Forescout has created a context-driven, multilayered architecture that embraces today's broad diversity of use cases comprised of applications, users, devices and services. By combining the Forescout platform and a multilayered approach to network segmentation, customers can gain complete situational awareness of their extended enterprise environment and can orchestrate segmentation to reduce cyber and operational risk across the board.

**Figure 4:** Forescout recommends a three-layered architecture as a best practice for enterprise-wide network segmentation, starting with “policy layer” powered by Forescout eyeSegment.

- **Policy Layer.** In 2019, Forescout unveiled its Forescout eyeSegment product to accelerate the design, planning and deployment of dynamic network segmentation across the extended enterprise. eyeSegment builds on the comprehensive device visibility and in-depth, real-time context provided by Forescout eyeSight. Because eyeSight doesn't require agents, it is equally adept at discovering and profiling managed, unmanaged and 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 you to visualize traffic flows and dependencies between users, applications, services and devices, and then design, simulate and monitor policies to understand the impact to your environment.
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 software 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.

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. This becomes critically important as more Windows operating systems reach end-of-life status.
Zero Trust Workload Capabilities

The Forescout platform discovers, classifies and profiles physical and virtual servers across hybrid data center/cloud environments, leveraging different infrastructure components and the workloads themselves. In addition, the Forescout platform tracks and monitors workloads as they spin up and down within hybrid data center/cloud environments, thus avoiding any visibility gaps. Forescout collects lower-level hypervisor or cloud properties all the way up to installed/running applications on the workloads, and then can use this context to ensure that only authorized users and devices are allowed access to specific workloads in support of Zero Trust policies.

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 September 30, 2019

*Notes

1 The Zero Trust eXtended Ecosystem Road Map: The Zero Trust Security Playbook, Forrester Research, July 11, 2019
2 Gartner Market Guide for Zero Trust Network Access, April, 2019
3 The Forrester Wave: Zero Trust eXtended Ecosystem Platform Providers, Q4 2019