FORESCOUT
Active Defense for the Enterprise of Things™

Total Visibility:

The Master Key to Zero Trust Security

In None We Trust

The Zero Trust model of information security is increasingly being adopted in both the strategies of enterprise security teams and the roadmaps of security solution developers – and with good reason. Perimeter-focused security architectures that default to high trust levels on the internal network are ill-suited for an edgeless enterprise that increasingly supports mobile and remote workers as well as vast numbers of IoT devices.

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. Also, digital transformation requires greater agility due to users, IoT devices and applications accessing more accounts, data and resources. According to Gartner, "As a result of

> **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.[1]**
>
> **FORRESTER RESEARCH**

digital transformation efforts, most enterprises will have more applications, services and data outside their enterprises than inside."[2]

Concurrently, the volume and diversity of devices connecting to network resources are overwhelming traditional endpoint management methods. Because many of these connected things, including BYOD and guest endpoints, IoT devices and operational technology (OT) systems, do not or cannot run corporate management agents, security teams may be blind to many devices on their networks and therefore unable to identify them or their users, assess their security state or control their network interactions.

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 to leverage existing security controls in practical implementations. Over time, the basic model has evolved and matured into what Forrester calls the Zero Trust eXtended (ZTX) Ecosystem. This comprehensive framework identifies seven

Components of the Zero Trust eXtended Ecosystem

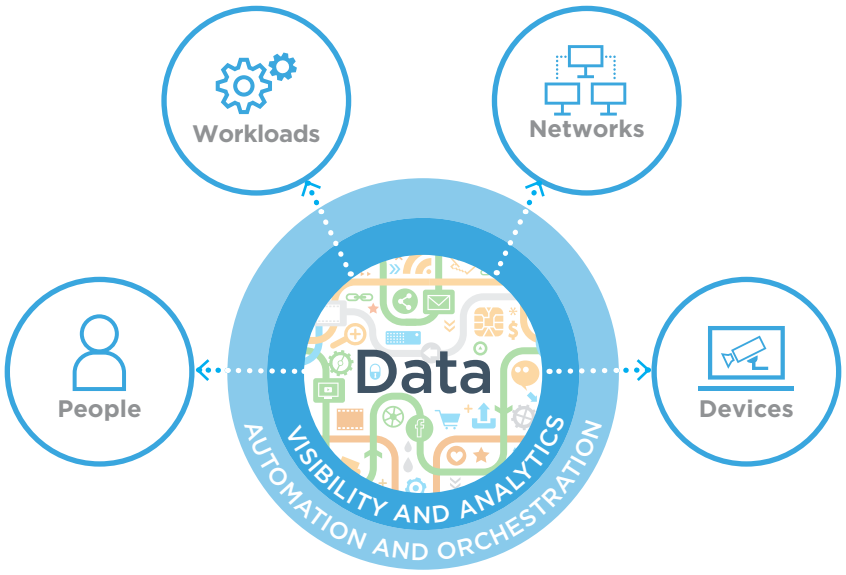

Figure 1: Forrester's Zero Trust eXtended Ecosystem comprises seven necessary dimensions.

key components of ZTX: 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 users (human and IoT) 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

Visibility Is Essential for a Successful Zero Trust Architecture

The foundational principle 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 posture. To enforce an access control policy, one must first see and assess 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. Zero Trust mandates significant investment in visibility and analytics across the business."[1]

To realize such a strategy requires a comprehensive device visibility and control solution capable of seeing and controlling all connected things, including devices that conventional endpoint management systems cannot: BYOD and guest 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 Solution: Complete Device Visibility and Control

Forescout's solution exemplifies the evolution of leading network technologies into Zero Trust platforms. In fact, **in its most recent Zero Trust Security Playbook,[1] Forrester named Forescout as a Zero Trust platform, thanks in part to foundational capabilities that align very closely with Forrester's ZTX framework.**

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 (or lack) of functional security agents. Next, it provides remediation, control and continuous monitoring of these devices.

The Forescout solution 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.

Zero Trust Platform Criteria

FORRESTER DEFINES A ZERO TRUST PLATFORM AS ONE THAT:
• Offers market-leading capabilities in at least four Zero Trust components
• Creates unique technical advantages to solution integration
• Develops and supports robust APIs and a partner ecosystem
• Maintains a center of gravity for visibility, analysis, policy and automation

"IoT and network-enabled device technologies have introduced potential compromise of networks and enterprises…Security teams must isolate, secure, and control every device on the network, continuously."[3]

FORRESTER RESEARCH

Enabling Zero Trust Security for the Enterprise of Things

Figure 2: The Forescout platform uses agentless visibility, access control, dynamic network segmentation and security orchestration to enforce Zero Trust security across your Enterprise of Things – regardless of where users or devices reside.

Zero Trust Device Visibility, Segmentation and Control

The Forescout platform provides complete 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 the 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 uses this asset intelligence to continuously 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, the Forescout platform 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 re-scanning devices for vulnerabilities and indicators of compromise – in concert with third-party systems.

Forescout eyeControl can directly execute control actions upon the device or through the network infrastructure (as described below). Host-based controls include starting and stopping applications, updating antivirus security agents, disabling peripheral devices and requesting end-user acknowledgment. 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).

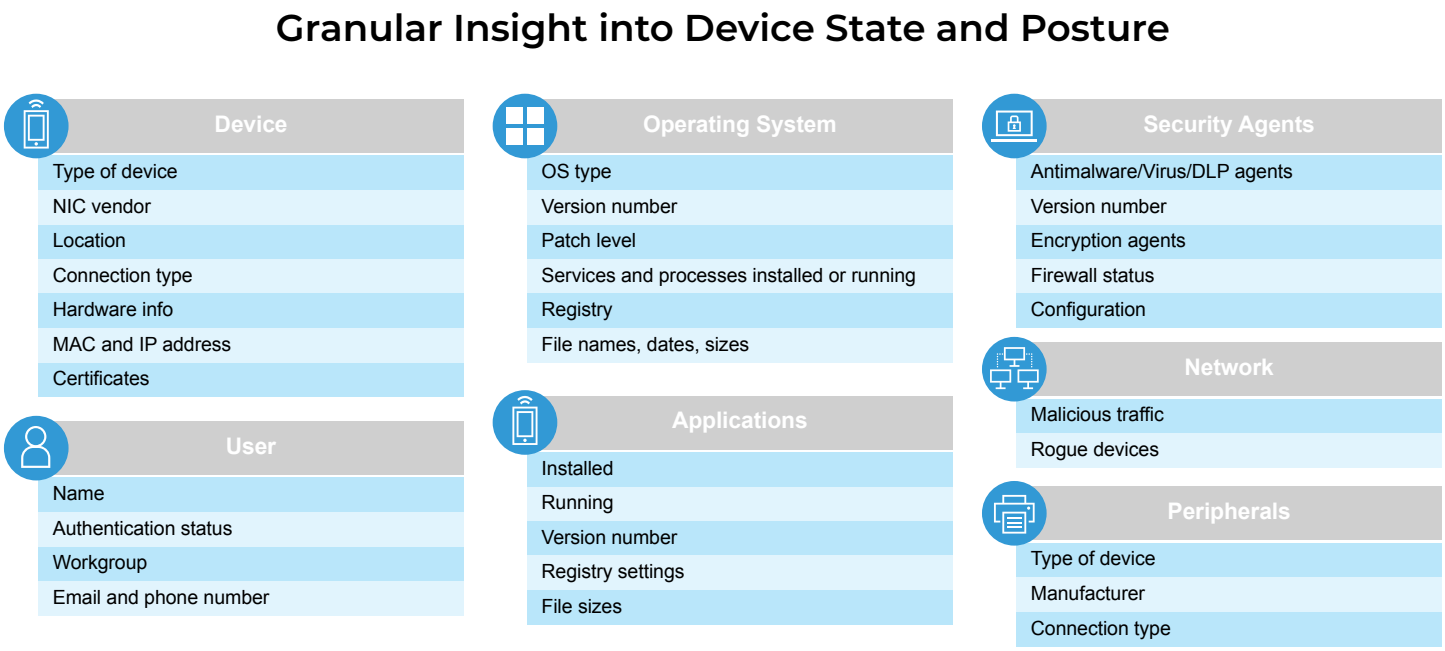

Figure 3: Forescout's classification process extracts detailed data on all IP-connected devices.

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."[3] 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 its 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 addition of Forescout eyeInspect to the product portfolio, 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."[4]

"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 capabilities for IoT/OT security shine above those of the competition."[4]

FORRESTER RESEARCH

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 occurs in complex, multivendor/multidomain enterprise environments, implementation becomes a massive undertaking.

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. This three-layer architecture enables the Forescout platform to actively identify, segment and enforce compliance of every connected thing.

Reducing Complexity for Zero Trust Segmentation

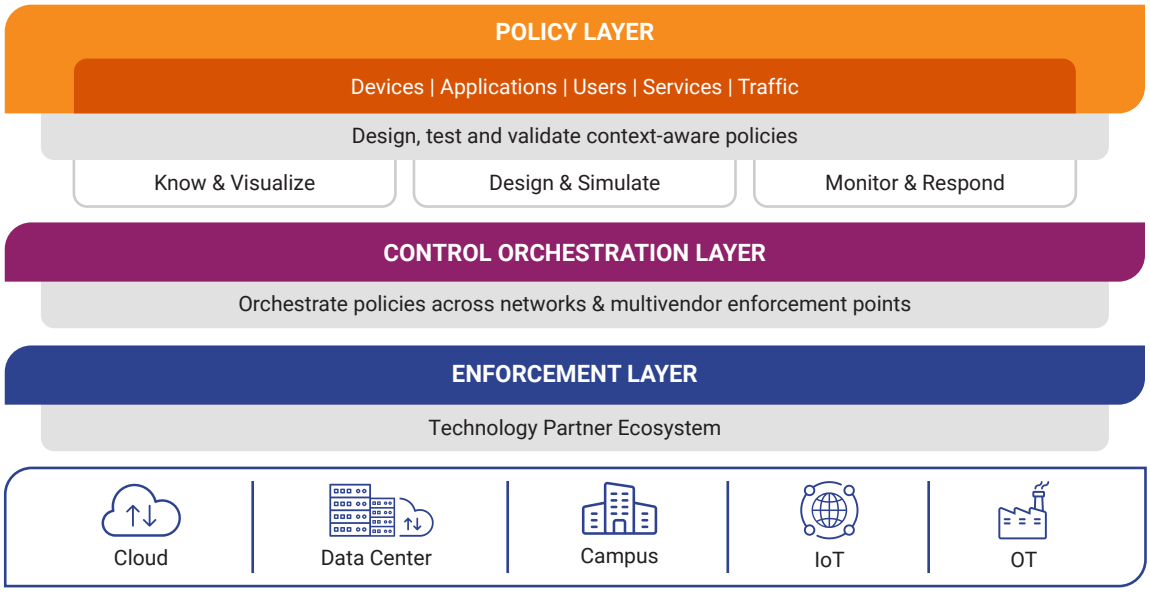

Figure 4: Forescout recommends a three-layered architecture as a best practice for enterprise-wide network segmentation, starting with the "policy layer" powered by Forescout eyeSegment.

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.

- **Policy Layer.** Forescout's eyeSegment product accelerates 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 on your environment.
- **Control Orchestration Layer.** The second layer helps to orchestrate policies across underlying enforcement technologies and network domains with a vendor-agnostic approach. As today's leading solution for network access control, Forescout eyeControl provides policy-based segmentation assignment working in concert with leading switches, routers and enforcement points in campus, data center and cloud environments. Forescout eyeExtend products help to streamline the integrations within the orchestration layer.
- **Enforcement Layer.** The third layer coordinates multivendor enforcement points, enabling the execution of segmentation controls across physical and virtual networks. This architectural layer also allows customers to continue leveraging their existing enforcement-technology investments.

One critical distinction for real-world Zero Trust implementation is that the agentless Forescout platform can discover, assess and provision the network access of any legacy IP-connected device. This becomes critically important as more Windows operations systems reach end-of-life status.

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 and segmentation assignment 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. 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 the network access of any legacy IP-connected device. Forescout products see and control every IP-connected device and integrate with all IT and OT network infrastructure.

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.** The Forescout platform 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's policy engine 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. What sets the Forescout platform apart is its ability to instantly apply 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

The Forescout platform discovers, classifies and profiles physical and virtual servers across hybrid data center/cloud environments without requiring agents by leveraging different infrastructure components and the workloads themselves. In addition to visualizing east-west and north-south traffic, the Forescout solution tracks and monitors workloads as they spin up and down within hybrid data center/cloud environments, thus avoiding any visibility gaps. It collects lower-level hypervisor or cloud properties all the way up to installed/running applications on the workloads and 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 authentication and access decisions based on both device and user insights. Insights provided by the platform can guide the creation of trust zones that incorporate directory services and business taxonomy. Access control and segmentation enforcement mechanisms ensure that only authorized on-campus or remote users and devices gain access to resources appropriate to their role or function. User behavior is monitored continuously, and integration with privileged access management systems enables discovery of user accounts with noncompliant permissions.

Zero Trust Data Capabilities

Forescout's solution 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 required by policy. If such applications are missing or inactive, it can take policy-based actions such as alerting the user, notifying an administrator or quarantining the device until it has been remediated. The solution enables real-time mapping of data flows between users, devices, services and applications. Also, it helps you understand data at rest and in motion across the extended enterprise.

For Zero Trust Success, Start with Total Device Visibility

Forescout products can accelerate a non-disruptive implementation of Zero Trust security that builds upon its visibility-first approach. To learn more, check out these resources:

- **Enterprise-Wide Segmentation Solution Brief:** Discover how to simplify Zero Trust segmentation and optimize risk management across heterogeneous networks.
- **Zero Trust Segmentation for OT Networks Solution Brief:** Learn how to safely secure extended OT networks with advanced risk management and dynamic segmentation.
- **Take a Test Drive:** Experience the before-and-after difference of the Forescout platform with a hands-on test drive that takes you through powerful use cases and highlights new capabilities of Forescout 8.2 and Forescout eyeSegment.
- **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, 2020

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. Mitigating Ransomware with Zero Trust, Forrester Research, Inc., June 8, 2020
4. The Forrester Wave: Zero Trust eXtended Ecosystem Platform Providers Forrester Research, Q4 2019