

Enterprise-Wide Network Segmentation

Simplify Zero Trust segmentation without disruption

The promise of digital transformation efficiencies, innovation and productivity has resulted in flat, interconnected networks that are susceptible to lateral movement of threats and unable to secure the growing numbers of connected Enterprise of Things (EoT) to the extended enterprise. As IT teams explore segmentation options to implement Zero Trust controls and increase security, concerns about complicated deployments and costly business disruption tax organizational confidence and stall progress. Challenges include:

- Lack of confidence to move forward on segmentation projects
- Threats and risk of exposure due to digital transformation
- Multivendor operational complexity and inconsistency in segmentation policies across multi-domain environments
- Lack of skills, resources and tools to effectively design, build and deploy network segmentation across the extended enterprise

Why Forescout: The best-in-class solution for non-disruptive Zero Trust segmentation

If these challenges sound familiar, now is an excellent time to evaluate the Forescout solution, which simplifies Zero Trust segmentation and optimizes risk management for your connected EoT in the extended environment. The Forescout platform accelerates dynamic, context-driven network segmentation without complexity, excessive cost or negative impact on business.

We'll meet your needs by helping you:

- **Accelerate Zero Trust segmentation** across the extended enterprise

“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.”¹

FORRESTER RESEARCH
June 2020

- **Gain an instant understanding of network segmentation state** in real time on any device, anywhere
- **Reduce the attack surface and maintain compliance** through dynamic segmentation across IT, IoT and IoMT (Internet of Medical Things) systems which can easily meet different vertical environments
- **Simplify threat analysis** with fewer tools, fewer dashboards and more actionable alerts
- **Reduce compliance risk and cost by efficiently managing cybersecurity detection and response**, requiring less skilled resources
- **Optimize cross-team workflows** and leverage existing investments with a consistent segmentation policy across the entire enterprise

Forescout recognizes 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. The Forescout platform, including Forescout eyeSegment, bridges these disparate technologies to accelerate the design, planning and deployment of dynamic network segmentation across the extended enterprise to implement effective Zero Trust policies, reduce regulatory risk and limit the attack surface.

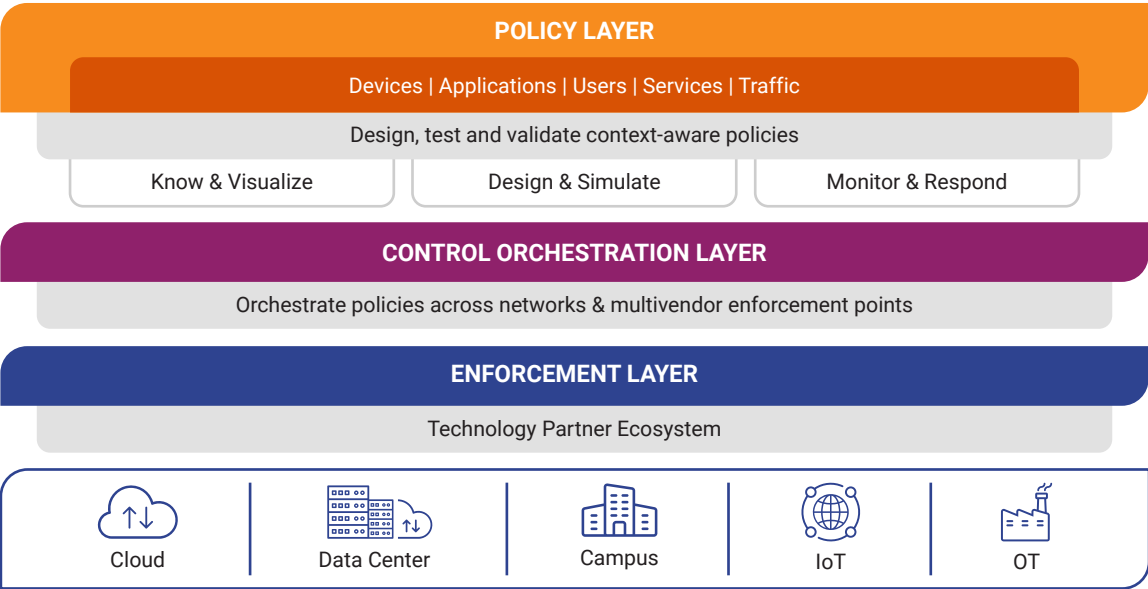
As shown in the below figure, enterprise-wide segmentation requires a context-driven, multilayered architecture to address today's broad diversity of device types—regardless of where they connect to the network. Forescout offers the platform, tools and expertise to help you efficiently plan and implement such a solution.

EXTEND THE VALUE OF YOUR SECURITY & IT INVESTMENTS

- Enable non-disruptive and dynamic segmentation
- Accelerate network Zero Trust segmentation projects with confidence
- Reduce the risk of business disruption
- Reduce operational cost
- Rapidly adapt to compliance and regulatory requirements
- Leverage existing infrastructure investments

NETWORK SEGMENTATION WORKSHOP

Are you extending your Forescout deployment into advanced segmentation control scenarios? Forescout consultants now offer a network segmentation workshop to ensure that your network segmentation policies and implementation align with your business strategy. [Learn more.](#)



Solution Components

The Forescout platform helps organizations design their enterprise-wide network segmentation strategies and accelerate deployments. Here are the platform’s key products:

Forescout eyeSight: Rich context for every IP address

The eyeSight product provides unparalleled insight and context into the entire connected network from campus to data center to the cloud—transforming your connected inventory into a logical taxonomy of devices, applications, users and services. Use this taxonomy to group all connected devices into a logical business hierarchy for network segmentation. Visit <http://www.forescout.com/platform/eyeSight> for more details.

Forescout eyeSegment: Simplify Zero Trust segmentation for any device, anywhere

Forescout eyeSegment accelerates the design, planning and deployment of dynamic Zero Trust segmentation across the extended enterprise. It enables organizations to embrace Zero Trust principles for EoT security. eyeSegment enables rapid acceleration of segmentation projects across

the extended enterprise to reduce the attack surface, limit the blast radius and mitigate regulatory and business risk. Visit <http://www.forescout.com/platform/eyeSegment> for more details.

eyeControl/eyeExtend: Orchestrate consistent controls across network domains and multivendor environments

The Forescout platform lets you dynamically orchestrate segmentation policies and automate controls across heterogeneous enforcement technologies by leveraging Forescout eyeControl and eyeExtend products.

- eyeControl enables consistent enforcement of context-aware segmentation policies and controls to existing underlying technologies—eliminating the need for agents. Learn more at www.forescout.com/platform/eyecontrol
- eyeExtend products orchestrate controls via out-of-the-box integrations with leading next-generation firewall (NGFW) vendors. Learn more about Forescout NGFW integrations at www.forescout.com/platform/eyeextend



The Forescout segmentation solution allows you to focus on what is important to you so that you can analyze and investigate a particular traffic pattern in your environment, as shown in the above figure. You can instantly understand the current state of communication flows and create desired Zero Trust segmentation policies. This visibility-first approach allows you to easily build micro-segmented zones and protect your business while ensuring business continuity.

Use Cases

The Forescout network segmentation solution addresses a wide array of use cases across different verticals such as Healthcare, OT (operational technology), Financial Services, Government, Retail and more. In every case, the Forescout platform's flexibility helps to reduce the risk of business disruption and minimize operating costs related to Zero Trust implementation and segmentation projects. To learn more about use cases, visit Enterprise-wide network segmentation use case overview.

Summary

Segmentation projects are currently managed in silos due to the complexity of cross-domain technologies. Additional factors such as Zero Trust security, digital transformation and regulatory compliance require a more holistic and systematic approach. The Forescout solution address organizations' cross-domain, multi-use-case segmentation challenges across extended enterprises. Through an instant understanding of your "current-state" segmentation in real time, context-aware policies, business-structured groups and proactive policy simulations, the Forescout platform enables Zero Trust segmentation controls that span diverse enforcement technologies and validate expected outcomes. The net result is a rapid acceleration of Zero Trust segmentation projects that include more granular controls and reduced risk across the organization.

1. Mitigating Ransomware With Zero Trust, Forrester Research, Inc., June 8, 2020

**Don't just see it.
Secure it.**

**Contact us today to actively
defend your Enterprise of Things.**

forescout.com/solutions/network-segmentation

salesdev@forescout.com

toll free 1-866-377-8771



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](https://www.forescout.com)

© 2020 Forescout Technologies, Inc. All rights reserved. Forescout Technologies, Inc. is a Delaware corporation. A list of our trademarks and patents can be found at <https://www.forescout.com/company/legal/intellectual-property-patents-trademarks>. Other brands, products, or service names may be trademarks or service marks of their respective owners. Version 08_20