FORESCOUT

Enterprise-Wide Network Segmentation Use Case Overview

The Forescout platform addresses a wide array of network segmentation use cases. The flexibility of the Forescout platform helps to reduce the risk of business disruption and minimize operating costs related to segmentation projects.

Overview

Use Case Landscape

Figure 1 represents a logical depiction of an extended modern enterprise network. Different use cases span various domains, such as application-centric use cases in the data center (top left) as well as cloud environments (top right). Most organizations' environments begin and end in the data center, as this is where sensitive and regulatory data resides. Campus network use cases (bottom left) typically include managing knowledge-based worker access to devices. For example, IT admin access to printers or physical security admin access to cameras.

When discussing network segmentation, most organizations start and remain focused in an application-centric view (e.g., ring-fencing applications), with a combined north-south and east-west strategy in the data center. The problem is, from a Zero-Trust standpoint is that this use case needs to encompass east-west traffic between data center and cloud environments, north-south-east-west with privileged admins as well as north-south with users. The industry answer to this challenge, requires multiple types of enforcement technologies that include infrastructure-native controls and overlay controls such as next-generation firewalls, and agent-based controls, as indicated in Figure 1.

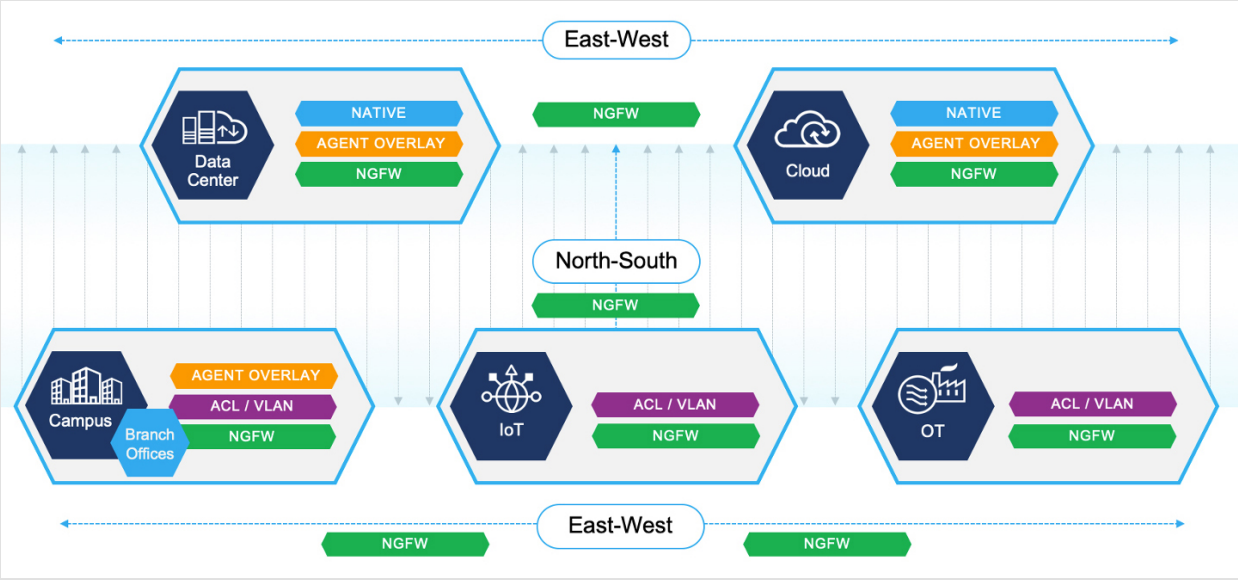

Figure 1: Modern enterprise network

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. Using a visibility-first approach, the Forescout platform bridges these disparate technologies to accelerate the design, planning and deployment of dynamic network segmentation across the extended enterprise.

Vertical	Use Case Category	Use Cases	Description
Financial	• Compliance Requirements	Meet compliance requirements and protect customer data: • Protecting critical business applications; payment systems and customer data • Ensure continuous environment separation; production vs. development	• Protect business-critical applications by ensuring that controls are effectively enforced, and continuous monitoring protection is maintained • Establish appropriate intra- and inter-business service controls across different services, applications and domains • Control user access to critical business services across different domains. Protect business-critical applications from misuse by users by effectively enforcing controls and continuously monitoring protection.
	• Regulatory Requirements	Meet regulatory requirements and protect customer data: • Protecting most critical assets • Protecting in-country data • Isolating SWIFT environments • Meeting Payment Card Industry (PCI) requirements	Every country has its specific regulations: • Alignment with FFIC; Implement network segmentation to protect the most critical assets that represent the highest risk • Protecting in-country data. • SWIFT – demonstrating isolation of your SWIFT environment (Bangladesh SWIFT breach). • Payment Card Industry (PCI) compliance is mandated by credit card companies to help ensure the security of credit card transactions in the payments industry.
	• Payments Platform and ATM Hygiene	• Non-PCI devices communicating with PCI devices • Payments/ATM network receiving communications from the internet • ATMs communicating outside of established traffic flow/behavior	Protect payment systems from cyberattacks and help ensure that they continue to operate.
	• Threat Exposure and Attacks in Branch Offices (Branch Hygiene)	Segmenting security cameras and other IoT devices from ATMs	Maintain branch hygiene by making sure branch security cameras and other IoT devices are segmented from ATMs
	• Outsourced IoT	Protecting outsourced enterprise IoT/OT devices (physical security, ATMs, building management, etc.)	Protect contractor-managed IoT devices across the extended enterprise

	• End-of-Life Business Systems	Windows 7, Windows Server 2008, systems running old OSes	These systems are critical to business continuity, but customers need to mitigate the risk.
Healthcare	• Protecting Customer Data	Eliminating the risk to PII and financial data • Segmenting all PII data from the rest of the network, ensuring only appropriate users have access • Protect back-end electronic health records	• Protecting sensitive customer data and make sure compliance and regulatory requirements are continuously met.
	• Outsourced Medical IoT	• Protecting third-party-managed medical IoT devices	• Protecting contractor-managed medical IoT devices across the extended enterprise • Laboratory devices are complicated and maintained by outsourcing
	• Legacy Application/OS Segregation	• Mitigate the risk of threats to devices running end-of-life operating systems	• Reduce the attack surface by segregating devices with legacy OSes and applications installed on them ○ Customers that have critical legacy systems that cannot be replaced (Example: $2M MRI machine running Windows XP)
	• Delivering Continuous Healthcare Services	• Segmenting end-of-life devices from the rest of the network	• Help ensure devices are limited to only what they should be communicating with (For example, radiology equipment only communicates with radiology and IoT imaging with IoT imaging. • Example: Legacy apps running end-of-life operating systems
	• Contain Vulnerable Devices	• Reduce the impact of known vulnerabilities on medical devices to prevent downtime	• Limit the access from/to vulnerable devices (due to WannaCry, unpatched, end of life, etc.) to the rest of the network
Manufacturing	• Cyber Resilience and Product Integrity	• Segmenting IT-OT boundary/environments • Separating facilities, plants, production lines, etc.	• Prove to auditors that backup systems are operational during the maintenance window for redundancy test • Help ensure that drug/food production lines are not impacted by cyberattacks to maintain product integrity
	• Reduce Business Disruption	• Prevention of downtime to reduce financial loss	• Downtime of production lines = loss of significant $$
Generic	• IoT Devices	• Protecting enterprise IoT devices (printers, cameras, VoIP phones, card readers, etc.)	• Best practice: All security frameworks recommend segmentation.

	• Enterprise-Wide Segmentation Assurance	• All segmentation use cases end up being north-south-east-west. Micro-segmentation is too limited in scope; it doesn't account for unmanaged devices or user access (north-south).	• Enterprise-wide segmentation planning, implementation and assurance; ensure continuous alignment across all enforcement technologies
	• Building Automation Devices	• Protecting building automation devices (surveillance cameras, elevator management servers, HVAC systems, etc.)	• OT networks are very often fragile with few security measures in place • eyeSegment ensures these systems are protected from outside interference by limiting communications to precisely what is required
	• Achieving Zero Trust	• Implementing Zero Trust across the extended enterprise	Zero Trust is a journey. Step one is to identify existing communications so organizations can understand the overall scope of the project. Then, based on use case priority, eyeSegment allows customers to re-design workflows, then simulate policy controls to align with Zero Trust enforcement. eyeSegment is the perfect tool to identify pain points customers are likely to encounter during the process: • Zero Trust has no answer for legacy applications, bare-metal servers, and unmanaged devices. Forescout is the solution here. • Forescout is the Zero Trust platform for IoT/OT (according to Forrester) • eyeSegment can help with enterprise-wide segmentation aspect of Zero Trust
	• eyeExtend Modules for NGFWs	• Implement dynamic network segmentation • Enhance firewall intelligence with real-time context for better policy creation and enforcement • Continuously assess device compliance and enforce network segmentation policies	Forescout eyeExtend NGFW modules help customers implement context-aware dynamic network segmentation. These integrations allow customers to create policy-based controls (leveraging eyeControl) to automate secure access enforcement to critical resources using their NGFWs (Palo Alto Networks, Check Point, Fortinet, Juniper) based on device context from eyeSight.