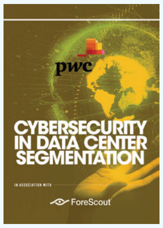
FORESCOUT

Published In:



Rethinking Segmentation

WannaCry. NotPetya. SamSam. It's not a question of ***if*** your network will be breached, but ***when***. You take all the usual protective measures: antivirus, intrusion prevention, firewalls, etc. But the best thing you can do to mitigate the risk and demonstrate security compliance is segment your network.

With segmentation, you logically separate your network into secure zones, each of which is compartmentalized and isolated from all others. For example, the server on which your all-important intellectual property (IP) is stored can be placed in one segment, and the part of the network your security cameras are attached to can be another segment. There's a wall between the two.

The benefit of this? If—or rather, when—a device like a security camera is hacked, what goes on in that segment stays in that segment. Containing the malware or cybercriminal to just one localized portion of the network minimizes potential damage. Your IP stays safe.

Not incidentally, segmentation also guards against insider threats because sensitive data and systems can be isolated from "curious" employees attempting to venture where they don't belong.

Win the compliance game

Segmentation also helps you more efficiently comply with regulations that otherwise can be burdensome—and costly if you fail the audits. Take the PCI Data Security Standard (PCI-DSS). Adhering to PCI-DSS means protecting the entire cardholder data lifecycle as it flows to and from payment devices, applications, infrastructure and customers.

This is so difficult that only 52.5 percent of businesses surveyed in 2017 were fully compliant with their annual PCI-DSS audit, according to the Verizon 2018 Payment Security Report.

Segmentation can reduce the areas of your network that come under audit and thereby increases your odds of being compliant.

Why segmentation hasn't caught on—yet

Segmentation isn't new. Traditional methods for segmenting networks such as virtual local area networks (VLANs) and access control lists have been around for decades.

But most segmentation projects never get off the ground. They're too complex and labor intensive given the heterogeneous nature of most enterprise network environments, and have traditionally required learning multiple tools from different vendors. The fact that most of these environments are now distributed across data centers, campuses and the cloud doesn't help.

Then there's the potential to disrupt your business. How do you write business policies so precisely that each of your employees has access to the exact network resources they need to do their jobs—but no more? You don't want to prevent a senior engineer from meeting a critical deadline because the data she needs is on the other side of a segment wall. Neither do you want her wandering freely through sensitive HR data.

The biggest challenge in segmentation is that you don't really know your network. You don't have sufficient context to build intelligent policies.

But the bottom line is, if you can't answer simple questions about what's connected to your network, you can't hope to protect your business.

Segmentation—do it right with Forescout

Forescout is focused on making segmentation an attainable reality for businesses.

Deploy the Forescout platform, and you immediately know what's connected to your network.

Everything. PCs. Servers. Printers. Internet of Things (IoT) devices like medical equipment and lighting systems. Operational technology such as manufacturing equipment and building automation systems. The instant something—anything—attaches to your network, you know about it. No manual scans or software agents required.

Because we're vendor agnostic, we work across heterogeneous environments and legacy networks and with other technologies such as next-generation firewalls (NGFWs.)

Then, we work hand-in-hand with your current solutions to automate your defenses.

Forescout: Security at First Sight™

Device visiblity is foundational to segmentation. It's non-negotiable. You can't protect what you can't see.

Forescout addresses the barriers to effective segmentation: complexity, high cost, vendor lock-in, and, most importantly, lack of device transparency. With Forescout, intelligent segmentation is a security strategy that is now achievable.

Pedro Abreu
Chief Strategy and Product Officer
Forescout Technologies, Inc.

FORESCOUT

Forescout Technologies, Inc.
190 West Tasman Drive
San Jose, CA 95134 USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support 1-708-237-6591