Five Steps to Combating Emerging Threats with Network Security



FORESCOUT®

FORESCOUT

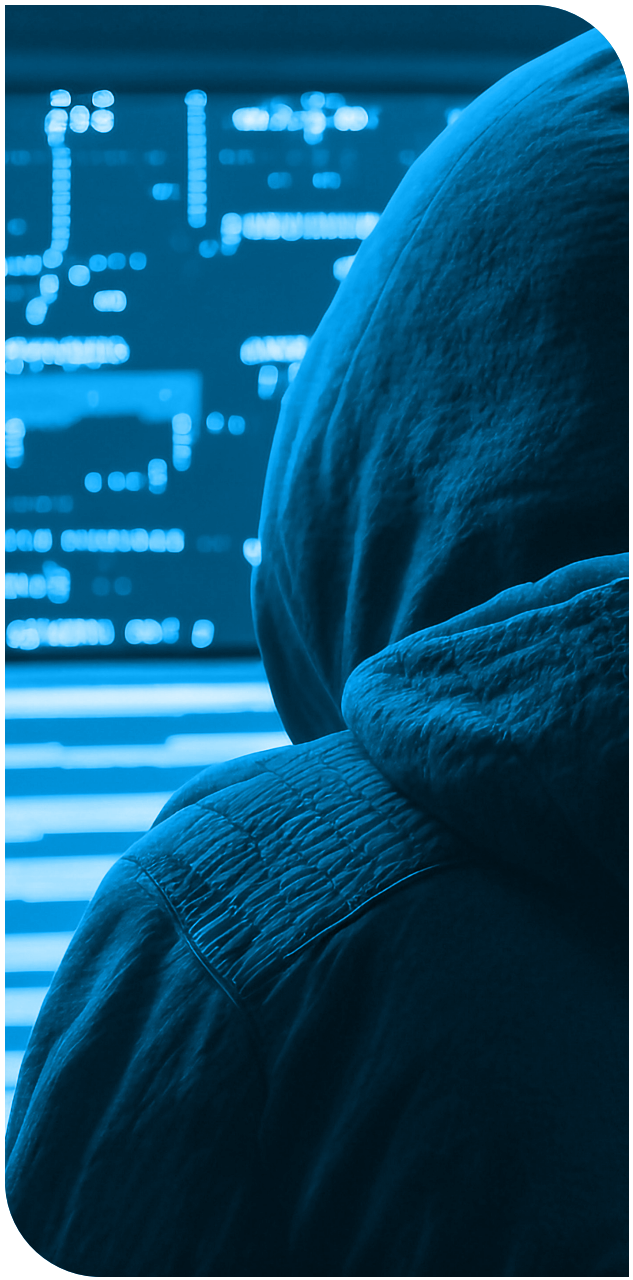


TABLE OF CONTENTS

Step 1: Know what you have 4

Case Study: “How big is my attack surface?” 5

Step 2: Control network access 6

Step 3: Limit movement and communication 7

Step 4: Leverage your existing investments 9

Step 5: Automate your response 11

Putting it all together 12

In today's rapidly evolving threat landscape, cybercriminals have become more sophisticated than ever, making it crucial to stay abreast of the latest trends and tactics. The challenge is exacerbated by the expanding attack surface as more devices and device types connect to enterprise networks: IT, OT, IoT and IoMT devices, all with known vulnerabilities that can be exploited. Managing this growing attack surface requires adopting measures like passive asset discovery, risk-based vulnerability prioritization and zero trust network segmentation, to name a few.

Organizations need to start thinking differently about how they approach network security to combat emerging threats. Unmanaged assets are hiding in the blind spots of the attack surface and are being targeted by attackers because they know that you can't secure what you can't see.

Recently, we've seen cyberattacks grow in sophistication and frequency, with malicious actors benefitting from growing geopolitical conflicts, economic uncertainty and rapid digitalization. One consequence of this digitalization is that organizations are more connected than ever. Many enterprise networks combine traditional IT devices with smart IoT sensors, and OT assets that interact with the physical world. This drastically increases the attack surface and creates new network blind spots.

Protecting ourselves from emerging threats means we can't continue using the same approach we've been taking to network security.

Here are five essential steps for combating emerging threats.

Emerging threat examples

- Ransomware groups are using cross-platform malware to target network-attached storage (NAS) devices and hypervisors to exfiltrate data
- Hacktivists are targeting critical infrastructure to disrupt operations and grab media attention
- State-sponsored actors are creating wipers for the embedded firmware found in smart IoT devices

FORESCOUT

Active and passive discovery techniques

Forescout enlists various passive discovery and active scanning or integration techniques to identify all IP-connected devices on your network. The techniques fall into four categories:

- Network integrations – Connecting network routers, switches and WLAN controllers via SNMP, CLI or APIs enables asset discovery and provides critical contextual data for risk assessment and control. This is especially valuable for globally dispersed networks.
- Network traffic monitoring – Passive sensors can perform deep packet inspection (DPI), and identify HTTP user agents, DHCP and communications flows.
- Scanners – Scanners improve classification and actively probe for posts, banners and information that may not be seen passively.
- Third-party integration – Integration with third-party tools via APIs and SQL enables security products to enrich one another and improve overall defenses.

Step 1: Know what you have

Visibility and asset management lay the foundation for network security. You need to know what's connected, who uses it, where it's located, and what it communicates with. Preferably all this information is in one place. Unfortunately, that's usually not the case. Ask yourself: how many asset inventories do I have today?

If you're using tools for endpoint detection, vulnerability assessment and configuration management, each of them likely has an inventory or assets or IP addresses. And while there might be some variation between them, they probably overlap quite a bit since they're typically deployed on managed assets such as laptops and workstations. But today's attackers are targeting smart sensors in power generating stations, IP cameras in retail locations and industrial controllers on assembly lines. How can you know if there are more assets you're not seeing? To fully understand your attack surface, you must deploy multiple discovery techniques to uncover the unmanaged assets hiding in your blind spots.

Partial visibility = partial protection. If you want a single source of truth for 100% of network-connected devices, ask the network.

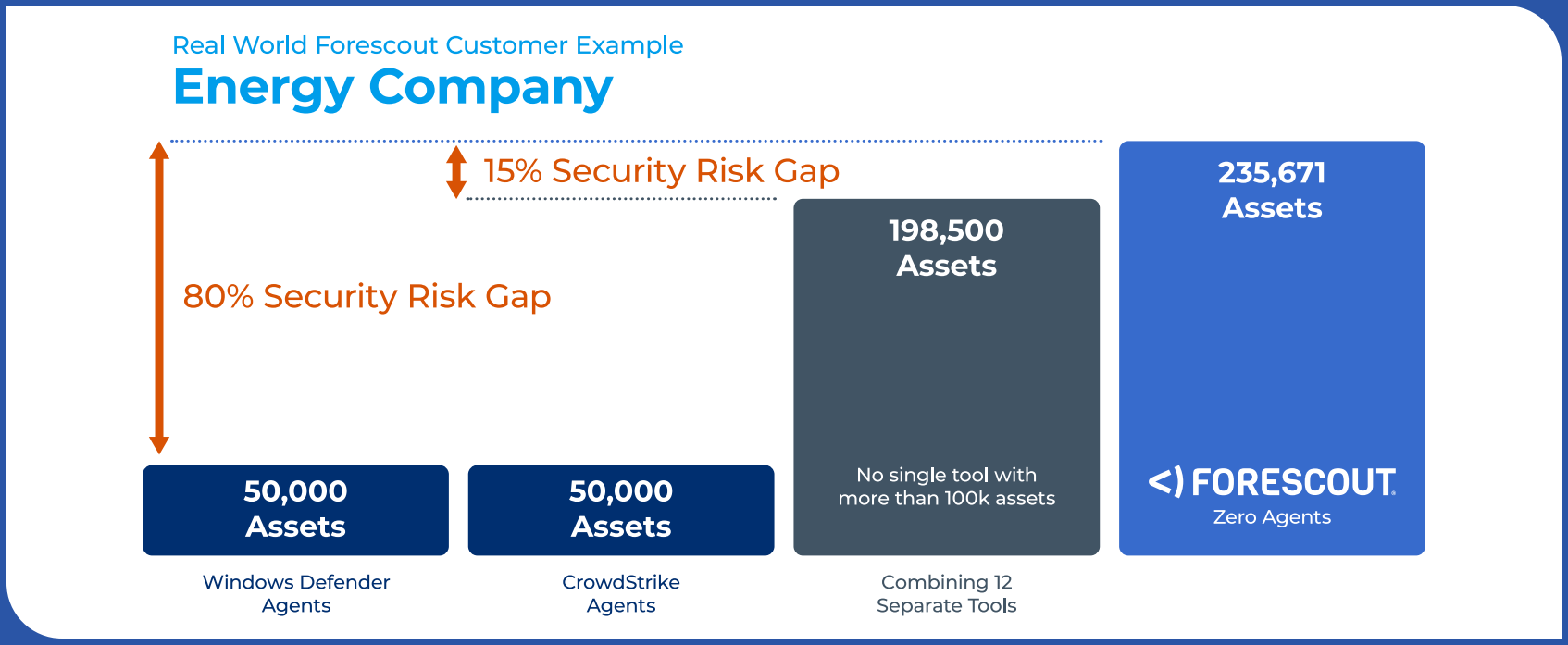
The Forescout® Platform uses more than 20 active and passive discovery techniques to deliver complete visibility of every connected asset. Certain types of assets require a specific approach to identify, classify and assess them without disrupting their operations. This is essential because some of these assets might monitor or perform critical processes that could severely impact your bottom line or reputation if they were compromised or taken offline.

Case Study: "How big is my attack surface?"

A U.S. energy company came to Forescout trying to answer the question, "How big is my attack surface?"

As a baseline, the company only had visibility into its 50,000 agentable assets using Windows Defender and CrowdStrike. Over two years, they spent countless hours combining inventories from 32 separate security and IT tools. From this fragmented approach, they could identify closer to 200,000 connected devices – a substantial increase, but what if there was still more to discover?

Forescout was able to deploy in this environment and identify just over 235,000 total assets without deploying software agents, providing a single source of truth in only a few weeks' time. These previously unknown assets represented a 15% visibility gap over all previous security tools combined and an 80% gap over agent-based solutions. A gap like this poses a significant security risk that attackers can use to exploit vulnerabilities and infiltrate networks.



FORESCOUT

Step 2: Control network access

The next step in combating emerging threats with network security is controlling which assets should and shouldn't be on your network. But controlling network access isn't just about authentication. Many unmanaged or unagented assets don't have the concept of a "user" or "identity" to authenticate with.

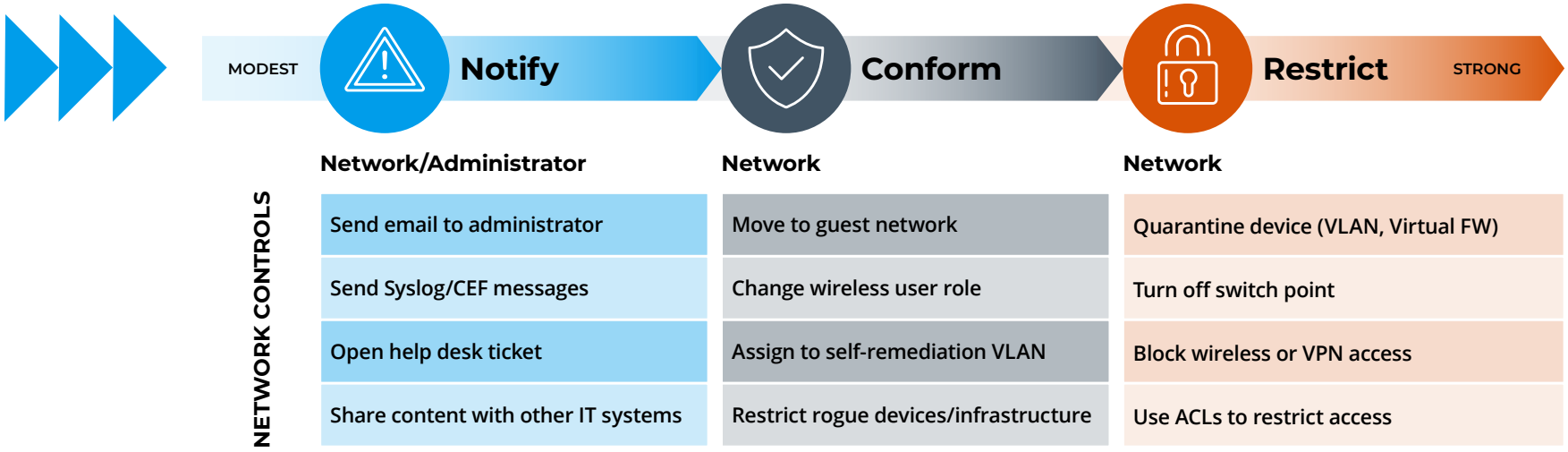
So how do you handle these assets when you want to enforce pre-connect authentication like 802.1X? Typically, security teams end up with a bypass list that connects anything with an allowed MAC address onto the network. This puts attackers one spoofed MAC address away from gaining access to your network.

A better approach is to go beyond basic authentication and assess an asset's compliance and risk posture before granting access to the network.

If you can't verify an asset's compliance with your security policies, it doesn't belong on your network.

This doesn't apply only during network admission, either. Assets must be continuously assessed to watch for changes in configuration, communication and behavior that goes against your policies. This best practice comes directly from one of the core principles behind zero trust security: never trust, always verify.

The Forescout Platform features an intuitive and flexible policy engine that enables you to automate and apply targeted control actions, from moderate to stringent, based on your needs and priorities. You can apply policy-based controls that enforce device compliance to proactively reduce your attack surface or quarantine an infected endpoint to rapidly respond to incidents.



Step 3: Limit movement and communication

Another core principle of zero trust is to assume you've been breached.

When an attacker exploits a vulnerability in an IP camera, their end goal isn't to simply kick back and watch the video feed; they want to move and propagate across the network in search of something worth extorting.

What are attackers looking to extort?



Customer data



Financial results

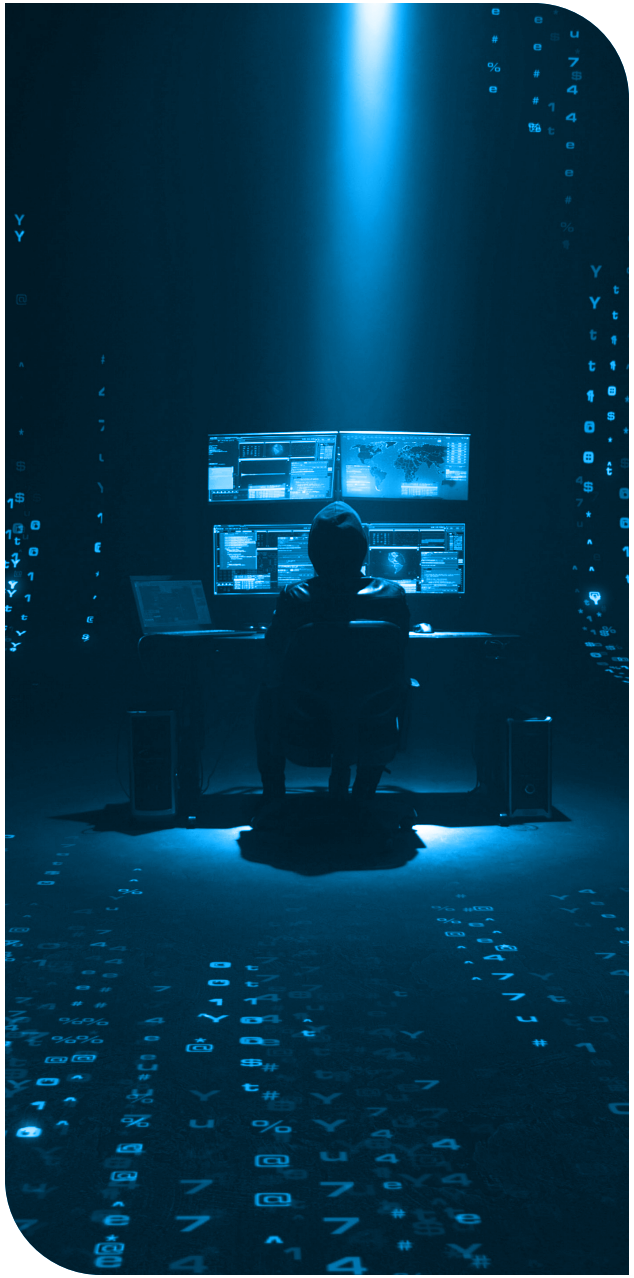


Patents and other intellectual property

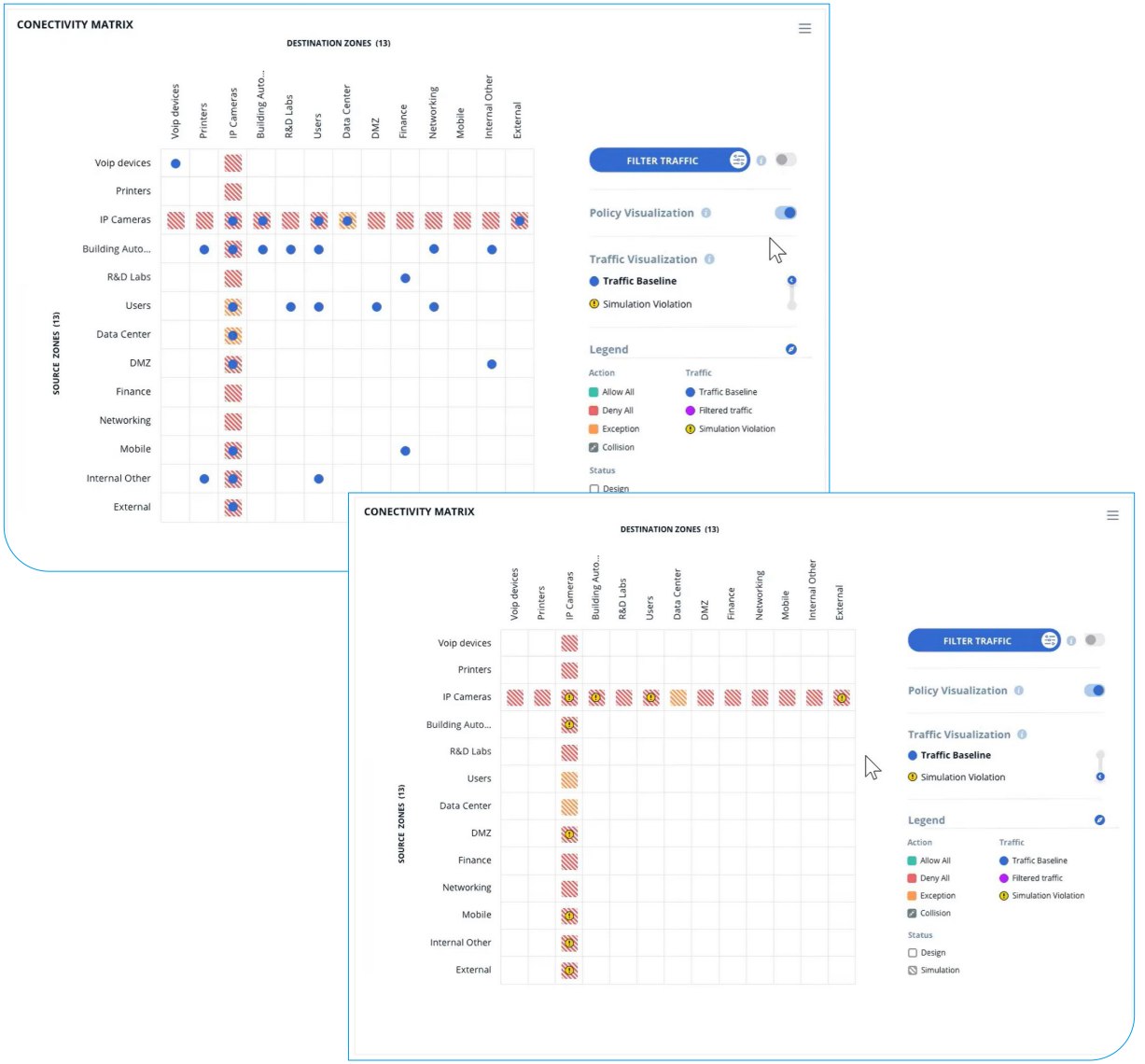
The best way to fight extortion is before it happens. That means enforcing least privilege access through segmentation and access controls that restrict unauthorized communication and shrink the blast radius if someone gets in. Flat, undersegmented networks allow emerging threats to propagate, increasing risk and exposure.

First, you need to analyze how assets are communicating. Being able to map the connections between assets allows you to effectively implement policies to block communication over certain protocols or to certain IPs, while allowing normal business operations to continue. This might sound straightforward, but if you've worked on a segmentation project you know that if you can't visualize traffic flows and simulate policy changes, your project is likely doomed to fail.





With Forescout's traffic matrix and segmentation simulator, you can test policy changes and see how they impact communication flows before implementing them to minimize risk and the chance for costly disruptions or project delays.

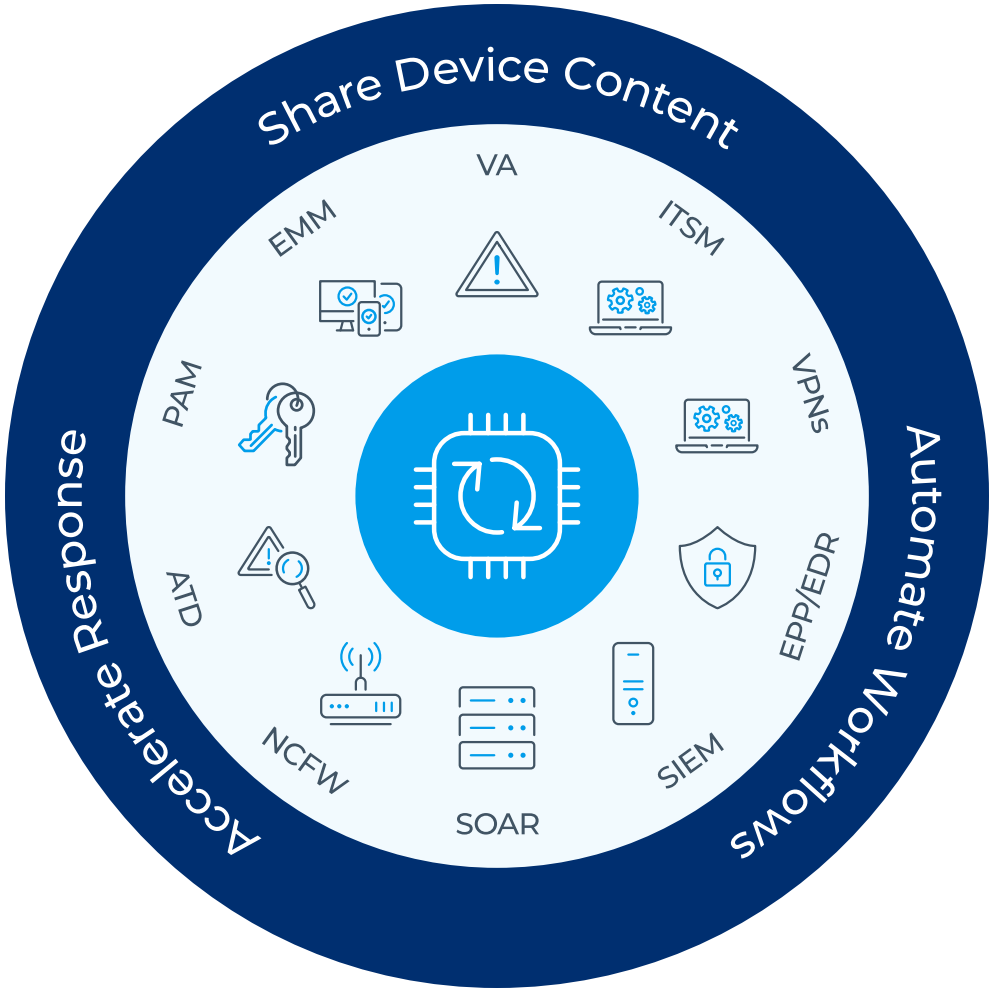


Step 4: Leverage your existing investments

It's no secret that there's a major cyber skills shortage, not to mention the alert fatigue and burnout experienced by many security teams. To manage this, you must integrate your existing cybersecurity investments to deliver even more value than they are today. Doing so enables you to share information and orchestrate workflows, which can drastically reduce the resources and time needed to maintain your security posture.

For example, you could trigger a scan from your EDR tool whenever a transient device rejoins the network instead of waiting for the next scheduled scan. Or you could update your CMDB whenever a new asset is identified and classified.

Just because you know a device exists doesn't mean it can be secured like a traditional asset. Take patching vulnerabilities, for example. When Microsoft releases a new patch, deploying it across affected devices is relatively easy. But what about smart devices or IoT sensors? Their embedded firmware will rarely see an update; even if they do, many perform critical functions and can't easily be taken offline for the update to be applied.



When dealing with thousands of these unmanaged devices, combined with the skills shortage and alert fatigue, a risk-based approach to prioritizing your efforts is essential. Sharing asset information via integrations lightens the load on security teams.

The Forescout Platform has a multifactor risk score that analyzes multiple aspects of an asset's configuration, function and behavior so you can prioritize remediating the assets that pose the greatest risk to the organization. You can also use the risk score in network control policies to dynamically block risky assets from joining your network.

Forescout Multifactor Risk Score

1 Configuration:

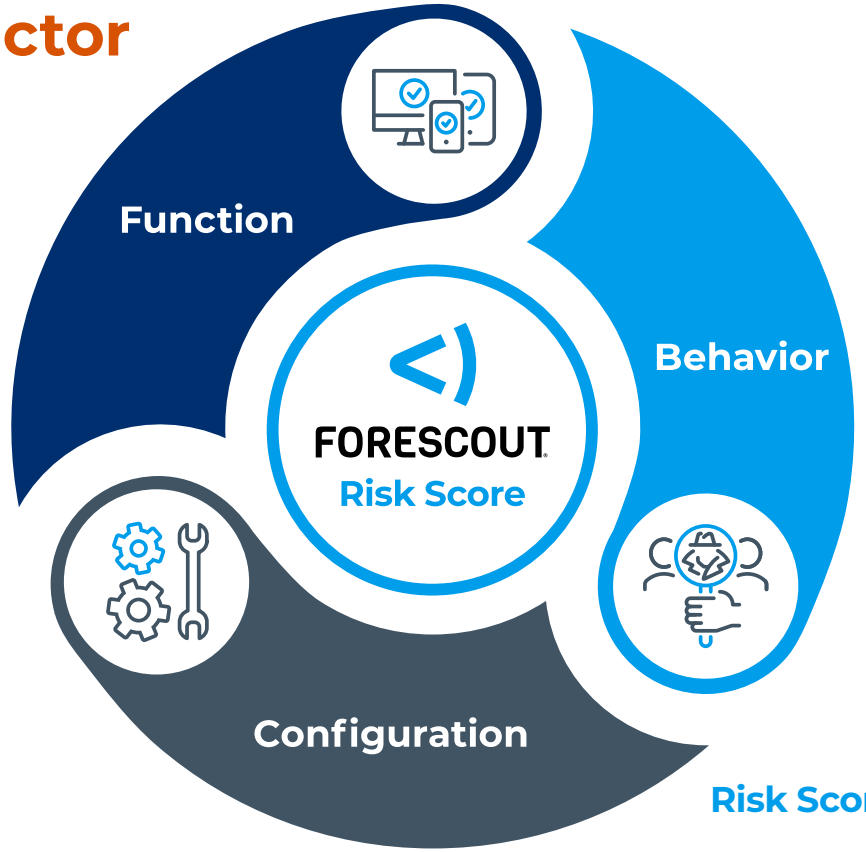
- Vulnerabilities (CVE's)
- Exploitability (EPSS)
- Exposed Services

2 Function:

- Device Criticality

3 Behavior:

- Internet Exposure



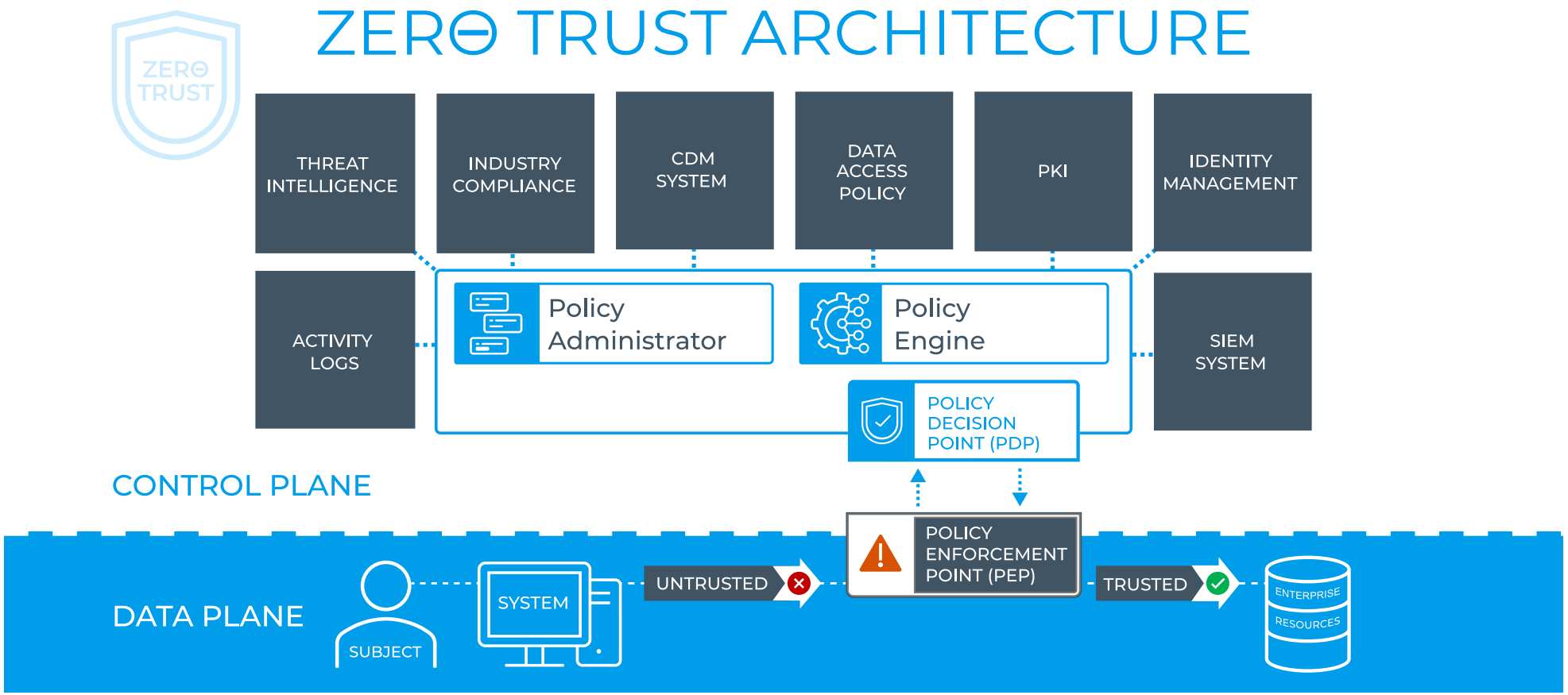
$$\text{Risk Score} = f(\text{Detected Risk Indicators}, \text{Device Criticality})$$

Step 5: Automate your response

Attackers can move at machine speed because they deploy automation to test and exploit vulnerabilities at scale. To effectively combat this, you must automate your response, too.

This includes everything from automatically remediating noncompliant assets so they can quickly and safely connect, to dynamically quarantining risky assets so attackers can't use them to infiltrate the rest of the network.

Here's what that may look like within a zero trust architecture (ZTA).



01 **Know what you have**
Ensure coverage of managed & unmanaged assets.

02 **Control network access**
Continuously assess & enforce asset compliance.

03 **Limit movement & communication**
Grant least privilege access & shrink the blast radius.

04 **Leverage existing investments**
Share information & orchestrate cybersecurity workflows.

05 **Automate your response**
Remediate at-risk assets & respond to emerging threats

Within a ZTA, it's the policy decision point, or PDP, that orchestrates the enforcement of security controls and responds to threats through your various enforcement points. The PDP is the central repository for your security policies, making managing and auditing your practices easier. It collects multiple intelligence sources to make decisions carried out by the enforcement points. That's why there's no such thing as a single-vendor, all-in-one zero trust solution. Each piece of the architecture plays a vital role in keeping your network, assets, applications and users secure.

Forescout's flexible policy engine has fully customizable policy templates for discovering and assessing unmanaged assets and automating your response to threats. A robust PDP that centralizes your security policies builds a strong foundation for your ZTA.

Putting it all together

It's become a common refrain in cybersecurity: you can't secure what you can't see. And that's because you can't. Attackers know this too. Traditional ways of identifying devices using point-in-time scans or software agents don't cut it with today's rapidly evolving threat landscape. Any asset that goes undiscovered on your network introduces potential risks to your organization. That's why total visibility is essential to hardening your security framework against emerging threats.

Think about how much of your attack surface you can see today – 20%? 50%? 85%? How confident are you in your coverage and intelligence on unmanaged, non-traditional assets? If you don't like the answer, follow these steps to modernize your network security to combat emerging threats.

Request a Demo

FORESCOUT®

Forescout Technologies, Inc.

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

Learn more at Forescout.com

©2023 Forescout Technologies, Inc. All rights reserved. Forescout Technologies, Inc. is a Delaware corporation. A list of our trademarks and patents is available at 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 01_02