merlin cyber

FORESCOUT

FORESCOUT FOR ZERO TRUST ARCHITECTURE: 802.1X

Zero trust is front-and-center across the federal government thanks to the May 2021 Executive Order on Cybersecurity, CISA's Zero Trust Maturity Model, and OMB's Federal Zero Trust Strategy. This Solution Brief explains how Forescout applies zero trust to network security.

Current network access control falls short

The 802.1X authentication protocol that federal agencies and departments rely on to control network access only checks device credentials when users connect to the network. Because 802.1X is a boundary enforcement protocol, there's no endpoint monitoring after the network connection is established. This introduces network security risks because rogue or unauthorized users can:

- Escalate local privileges
- Launch unauthorized virtual machines that piggyback on their device's network connection
- Connect USB drives and copy sensitive data

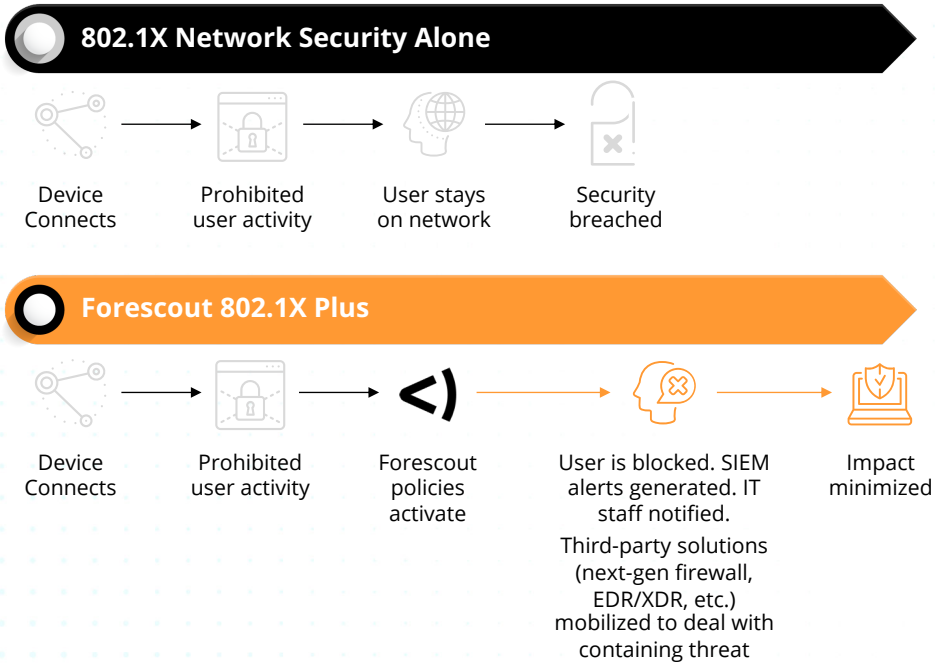
802.1X alone does nothing to prevent these scenarios. Something more is required.

Forescout is the zero trust solution for network security

Zero trust security requires continuous monitoring of all assets on the network, eliminating the security risks inherent with 802.1X. In addition to providing the necessary 802.1X network boundary admission services, Forescout's best-of-breed endpoint detection and response (EDR) capabilities close the gap around vulnerabilities arising from authenticated users performing unauthorized actions.

Forescout tracks what happens on endpoints in real-time. This includes Windows, MacOS, and Linux workstations. The active endpoint information is then checked against Forescout policies. When devices break the rules, the platform fires off network restrictions, alerts, notifications, and helps orchestrate responses across systems connected to Forescout.

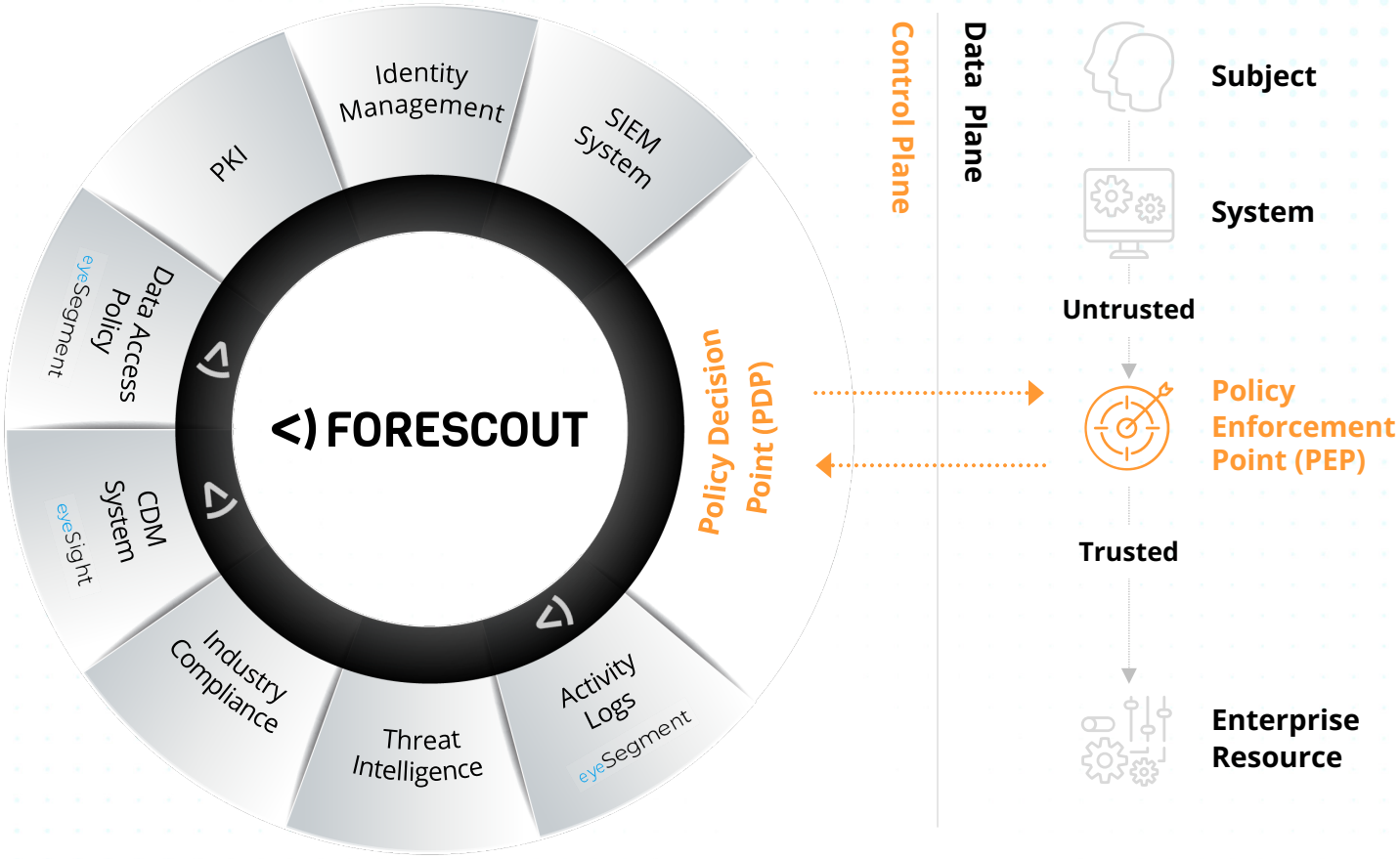
By providing real-time policy decision point engagement, Forescout ensures that systems are constantly checked for compliance. When systems fail a compliance check, Forescout engages with network devices and other security tools to surround the non-compliant system with policy enforcement points, thereby containing the threat posed by non-compliant systems.



Forescout provides both 802.1X network admission security and enables the kind of constant endpoint awareness and response that today's zero-trust environments require. Centrally placed in your security architecture, it acts as a coordinating system to keep all your security tools on the same page. This results in a toolkit that's ready for action any time an endpoint goes rogue—not just when it connects to the network.

Zero Trust Architecture

Forescout Roles



About Forescout

Forescout, the preferred solution for CDM hardware asset management (HWAM), actively defends the Enterprise of Things by identifying, segmenting, and enforcing compliance of every connected device. Federal agencies and Fortune 1000 companies trust Forescout as it provides one of the most widely deployed, enterprise-class platforms at scale across IT, IoT, OT and IoMT managed and unmanaged devices. Forescout arms customers with extensive device intelligence, data, and policies to allow organizations to accurately classify risk, detect anomalies, and quickly remediate cyberthreats without disruption of critical assets.

About Merlin

Merlin is the premier Public Sector growth acceleration platform for cybersecurity companies seeking to rapidly scale their businesses within the U.S. Federal and State, Local and Education (SLED) markets. Merlin's one-of-a-kind business model leverages innovative technologies, trusted relationships, and capital to develop and deliver groundbreaking security solutions that help Public Sector agencies minimize risk and simplify IT operations. Merlin selectively represents prominent cybersecurity brands and invests in visionary, emerging technologies. By bringing select partners and portfolio companies together into Merlin Labs, cybersecurity engineers integrate, test, and deliver more holistic security solutions that are entrusted to solve the Public Sector's most complex cybersecurity challenges. This approach helps the U.S. Public Sector save time, money, and other resources while more effectively securing its systems, data, and users no matter how requirements evolve.