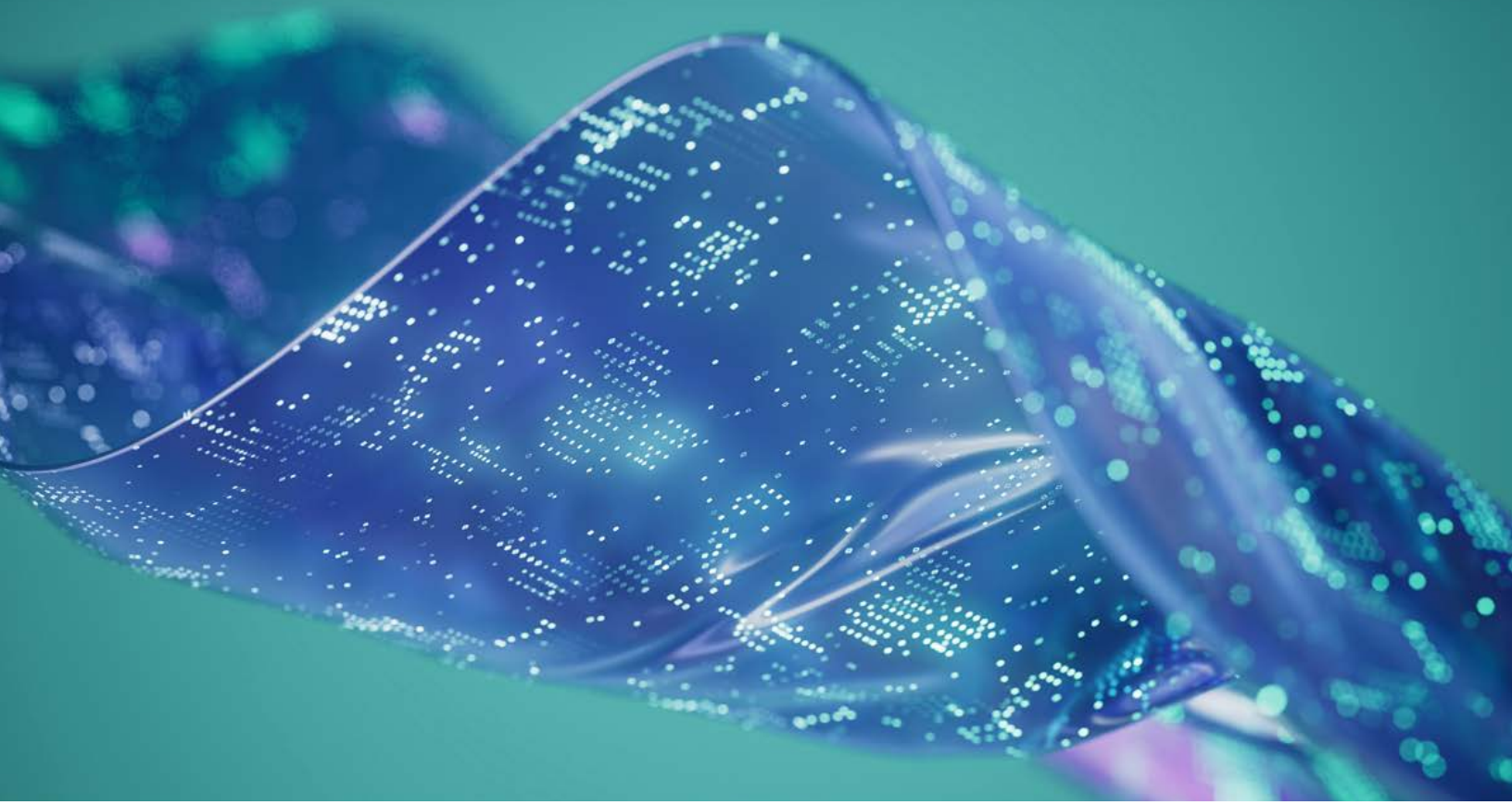
Enabling Zero Trust Using Forcepoint NGFW Endpoint Context Agent



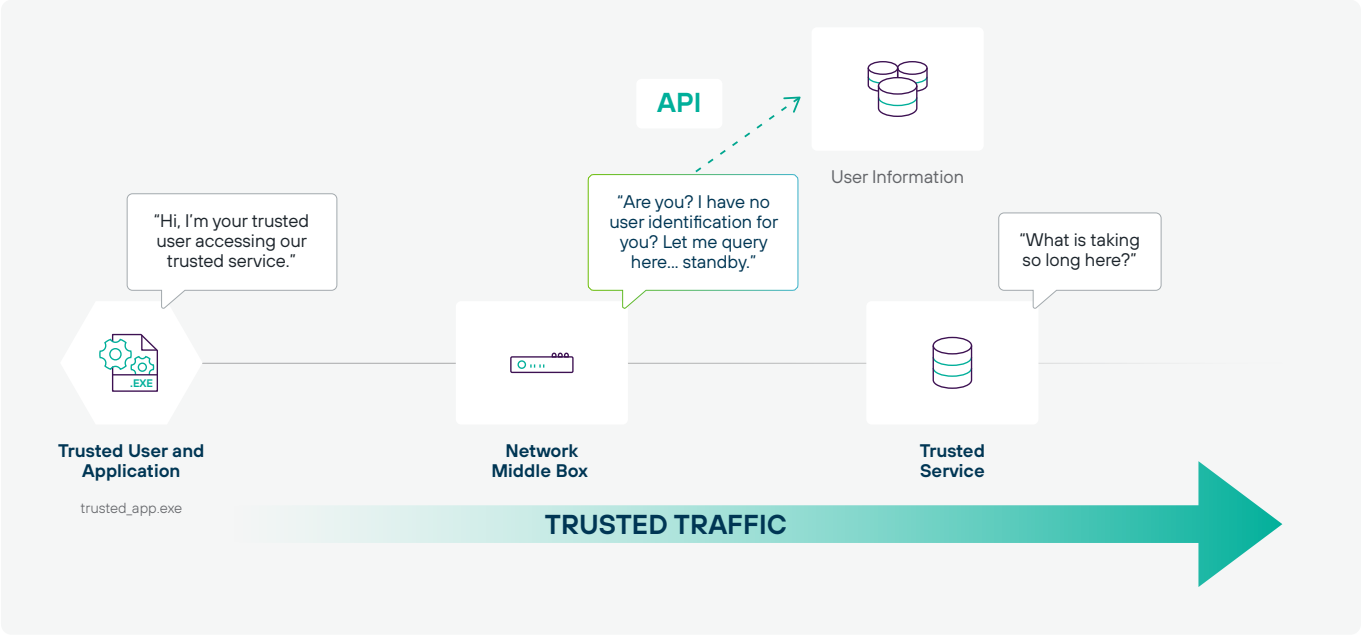
Forcepoint

Whitepaper

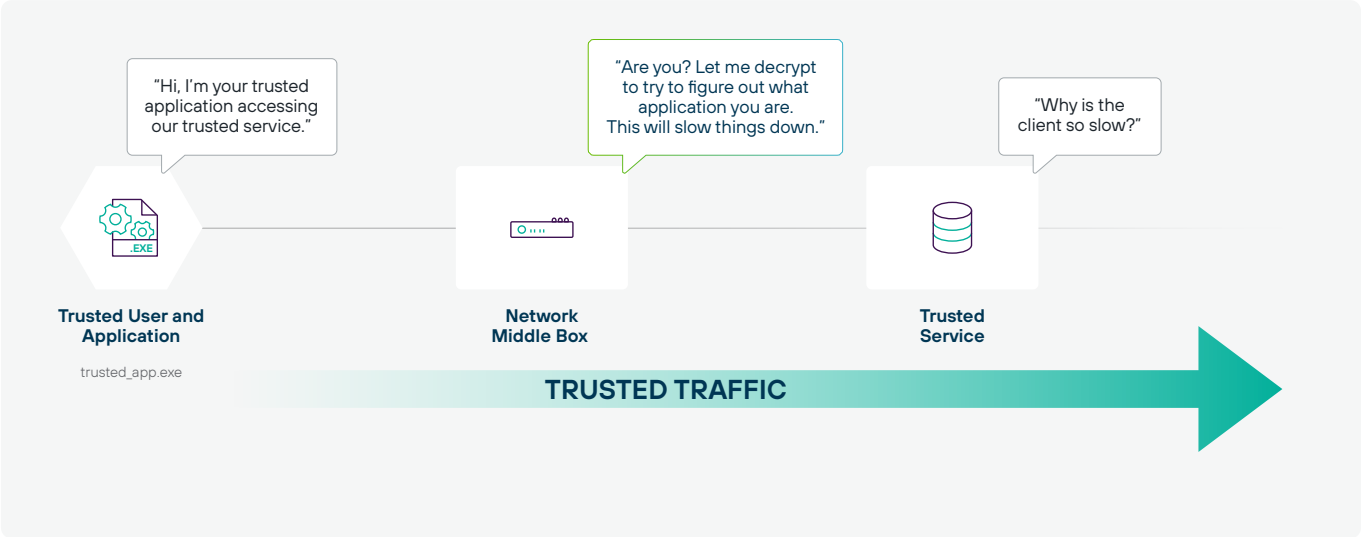
Background

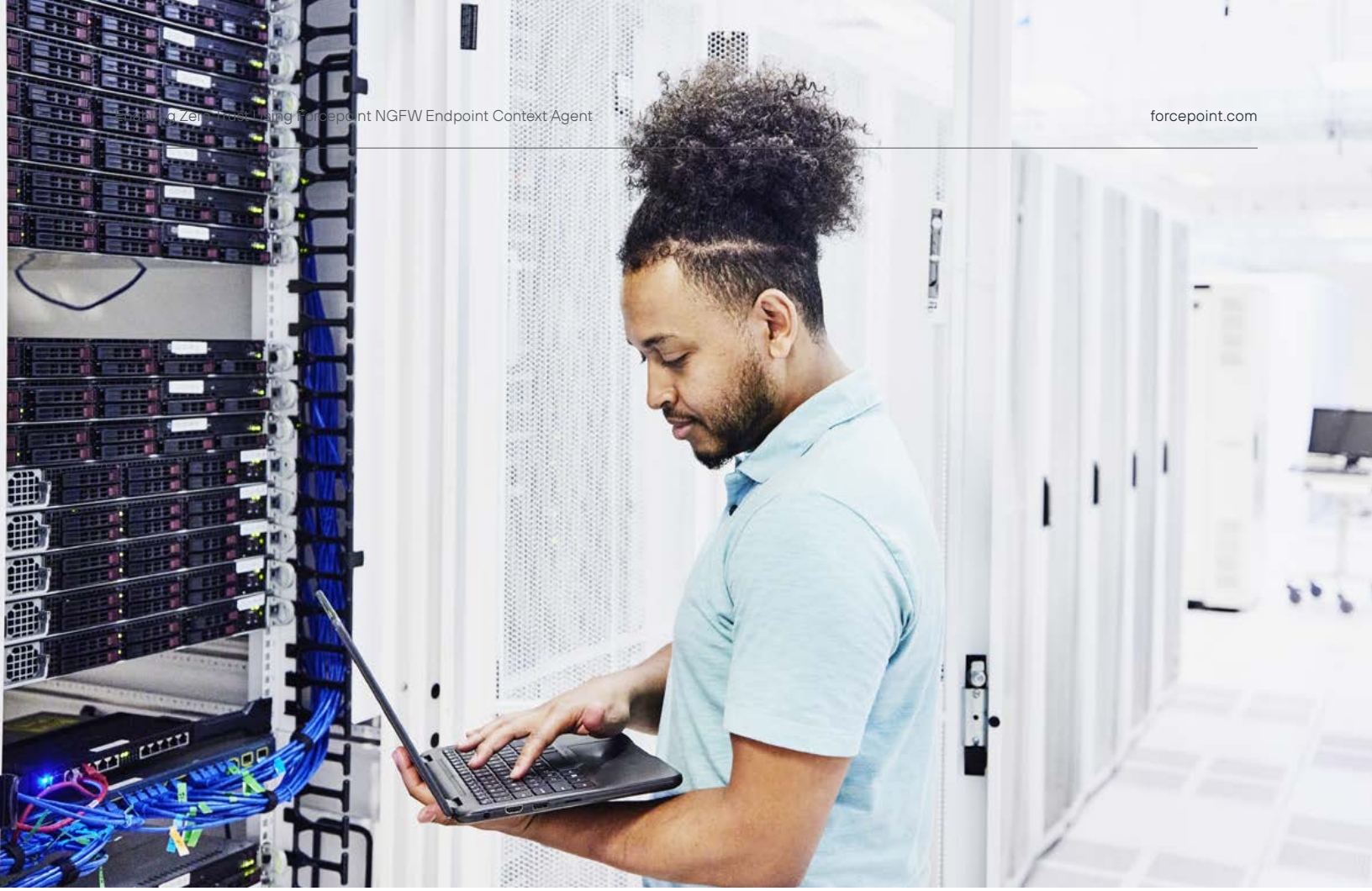
Network-level access control enforcement by products like Next-Generation Firewall (NGFW) has been the cornerstone of building cybersecurity architecture for years. Agencies and missions transforming into a least-privilege, Zero Trust approach to cybersecurity are creating challenges for the existing infrastructure. This is especially true for solutions that rely on information seen at the network level to make access control decisions.

Application data, in most cases, does not include user or group information and must be provided from other sources. This API-based user identification is prone to delays that can cause misidentification, leading to incorrect access control decisions.

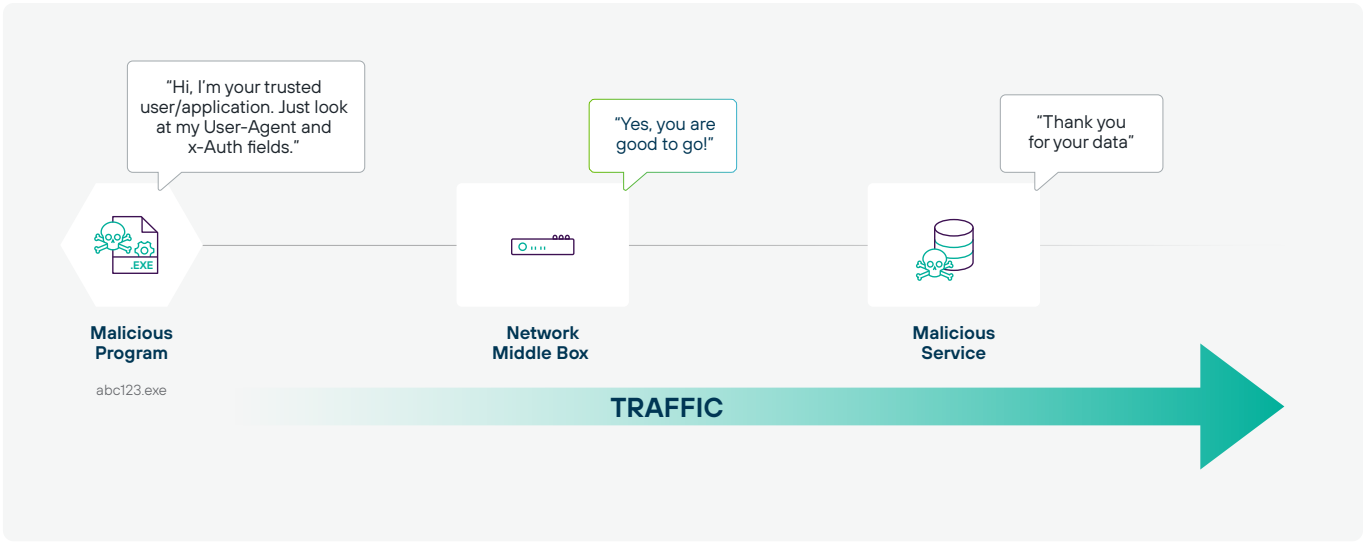


The trusted application can be encrypted, making detection difficult and taxing for the device, as the traffic must be decrypted on the fly.





User-Agent-based browser control is not reliable, as it is trivial to spoof malicious activity as an up-to-date Chrome browser. The X-Auth field can be manipulated by malicious programs, creating false positives for Zero rust.

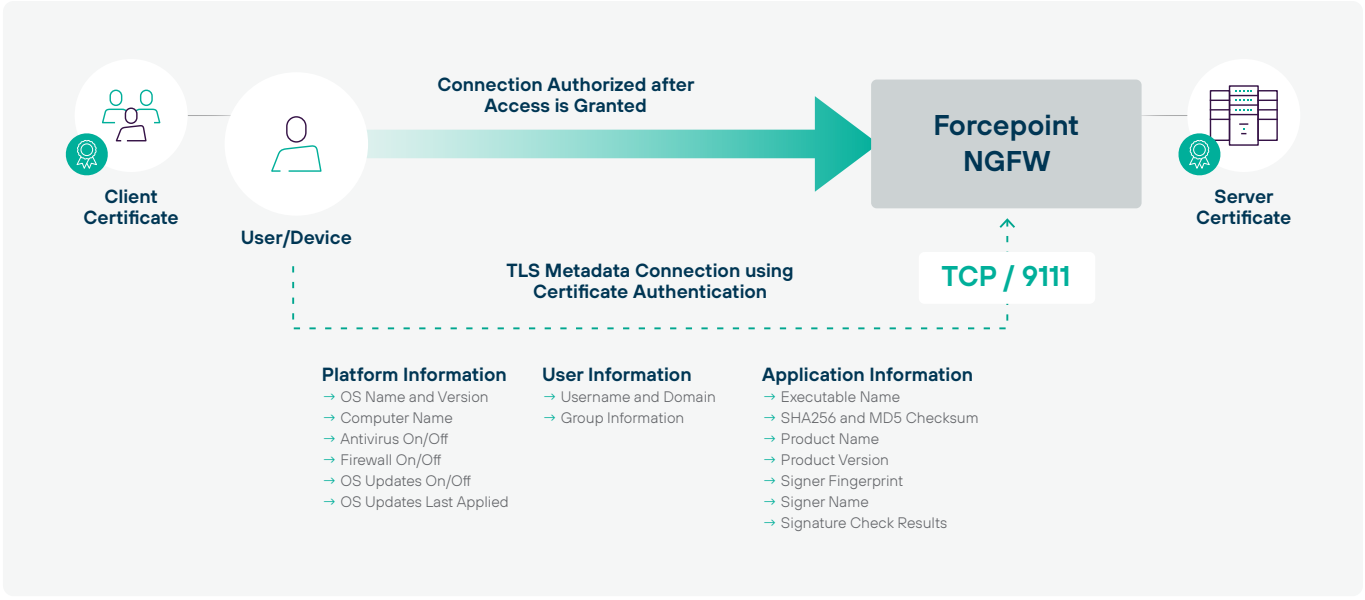


There are also certificate-pinning thick applications that can bypass inspection completely. TLS/SSL inspection is not possible due to the certificates being stored inside the application itself.

Forcepoint Endpoint Context Agent (ECA) Architecture

Forcepoint Endpoint Context Agent is a Windows-based software that observes the endpoint's executable applications, logged-in user and network details of the connection being used by the application. This information is communicated via an out-of-band, encrypted and authenticated metadata connection to the Forcepoint NGFW. This ensures accurate application and user identification, enforcing Zero Trust at the application level.

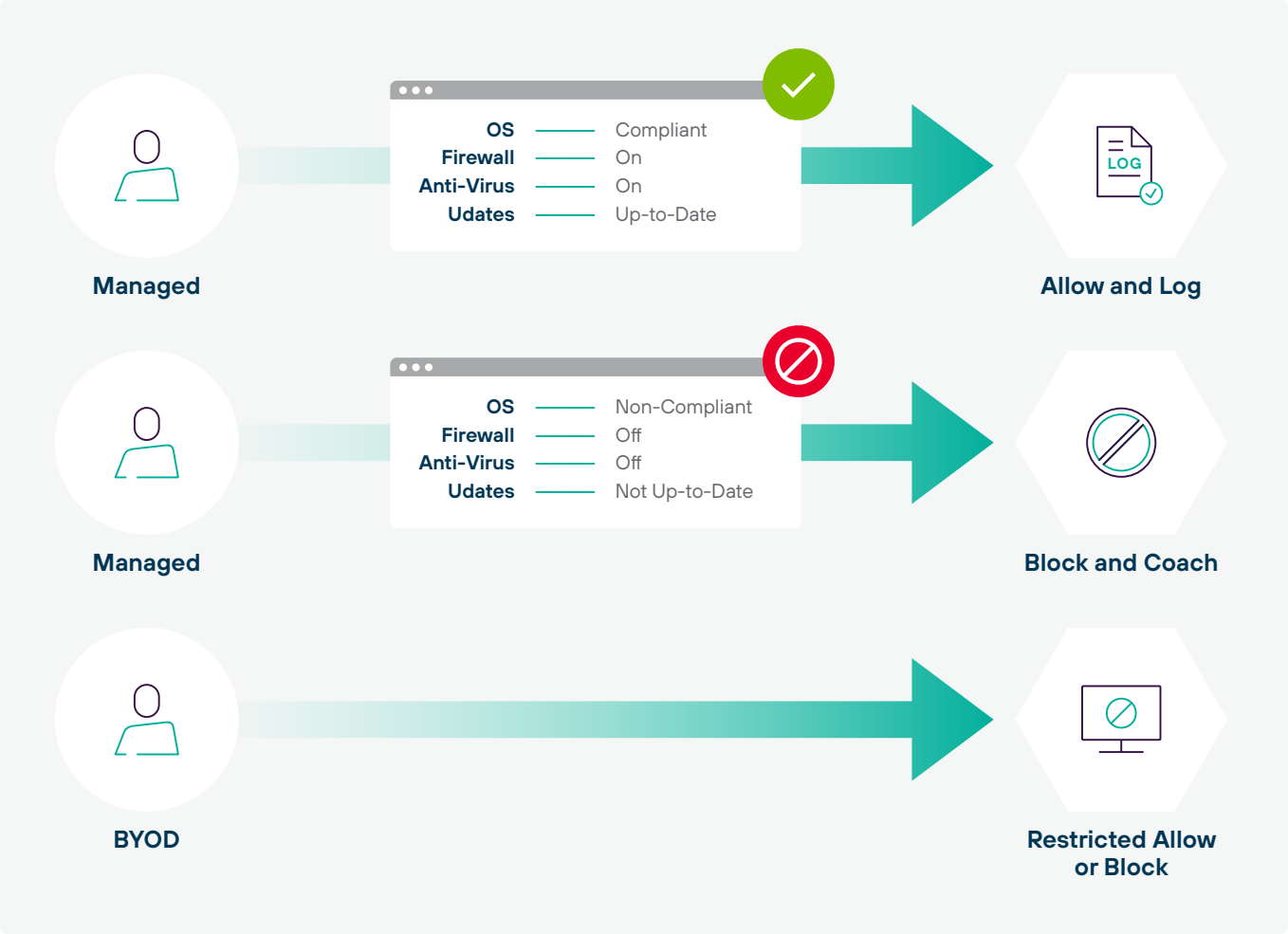
ECA ARCHITECTURE



Use Case – Security Posture Check

The Forcepoint ECA authenticates itself using a machine certificate. The certificate can be issued by a trusted domain CA, ensuring that only domain-joined machines can connect. Furthermore, the OS version can be validated to ensure that the operating system is compliant and that the firewall, anti-malware and automatic updates are enabled and up to date. Since you can easily identify managed devices using the ECA, this also gives you the ability to apply different controls to the same resource based on whether the device is BYOD or managed. For example, you can block non-managed devices or apply more controls to those devices.

ECA SECURITY POSTURE CHECK



Use Case – Browser Control

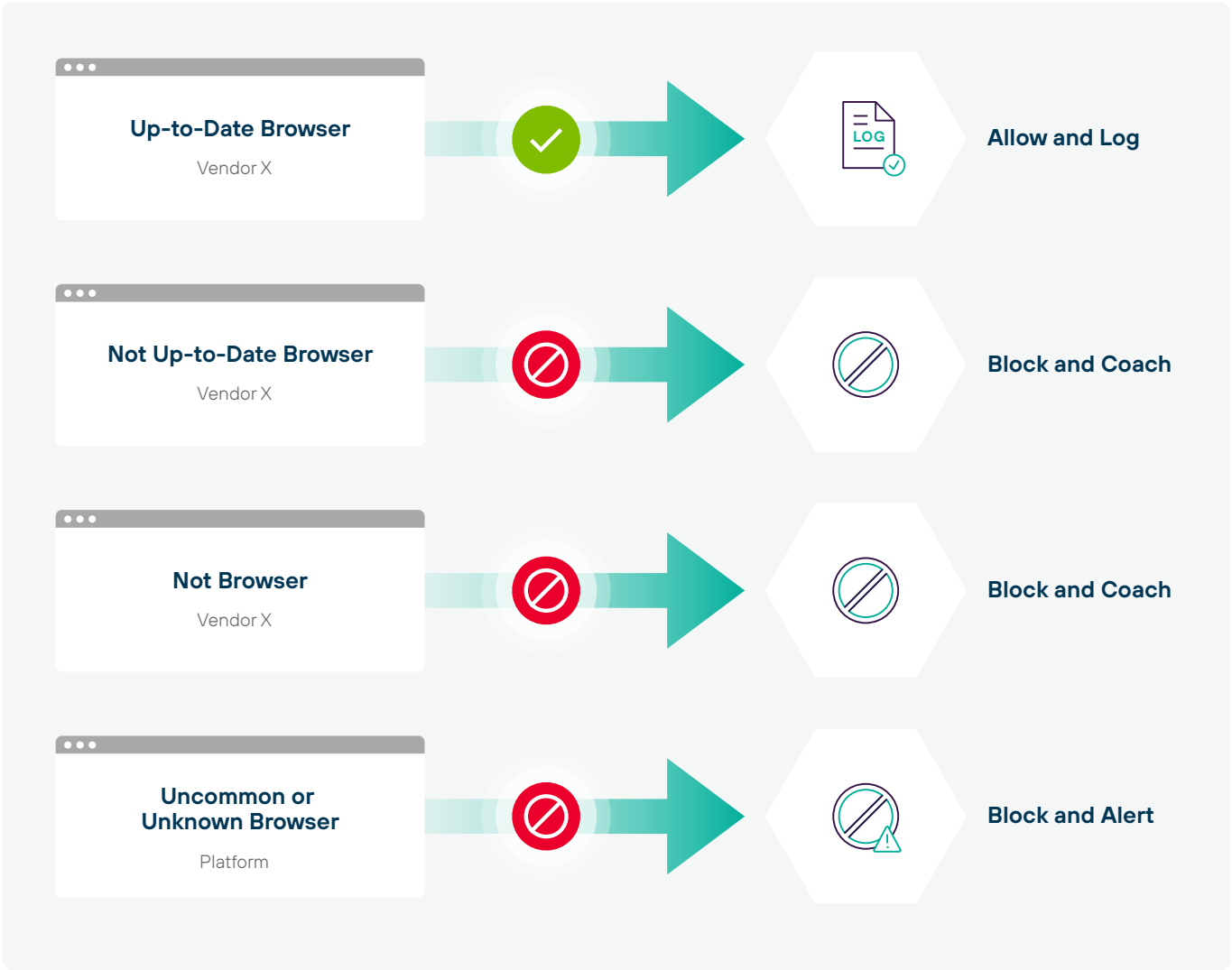
Traditional browser control solutions rely on the HTTP User-Agent field to identify the browser platform, version and operating system. This method is prone to evasion, as the User-Agent can be easily spoofed by a malicious actor, bypassing the browser enforcement.

Forcepoint ECA's unique approach provides the ability to easily enforce up-to-date browser platforms, reducing the overall attack surface in the environment.

Forcepoint NGFW can be configured to employ user responses, meaning that coaching can be used to ensure out-of-compliance users know how to correct their browsers to be fully compliant. This also addresses issues with users using the wrong browser platform or an out-of-date version of the approved browser platform.

Unknown and uncommon browser platforms should be automatically blocked and investigated for possible malicious activity.

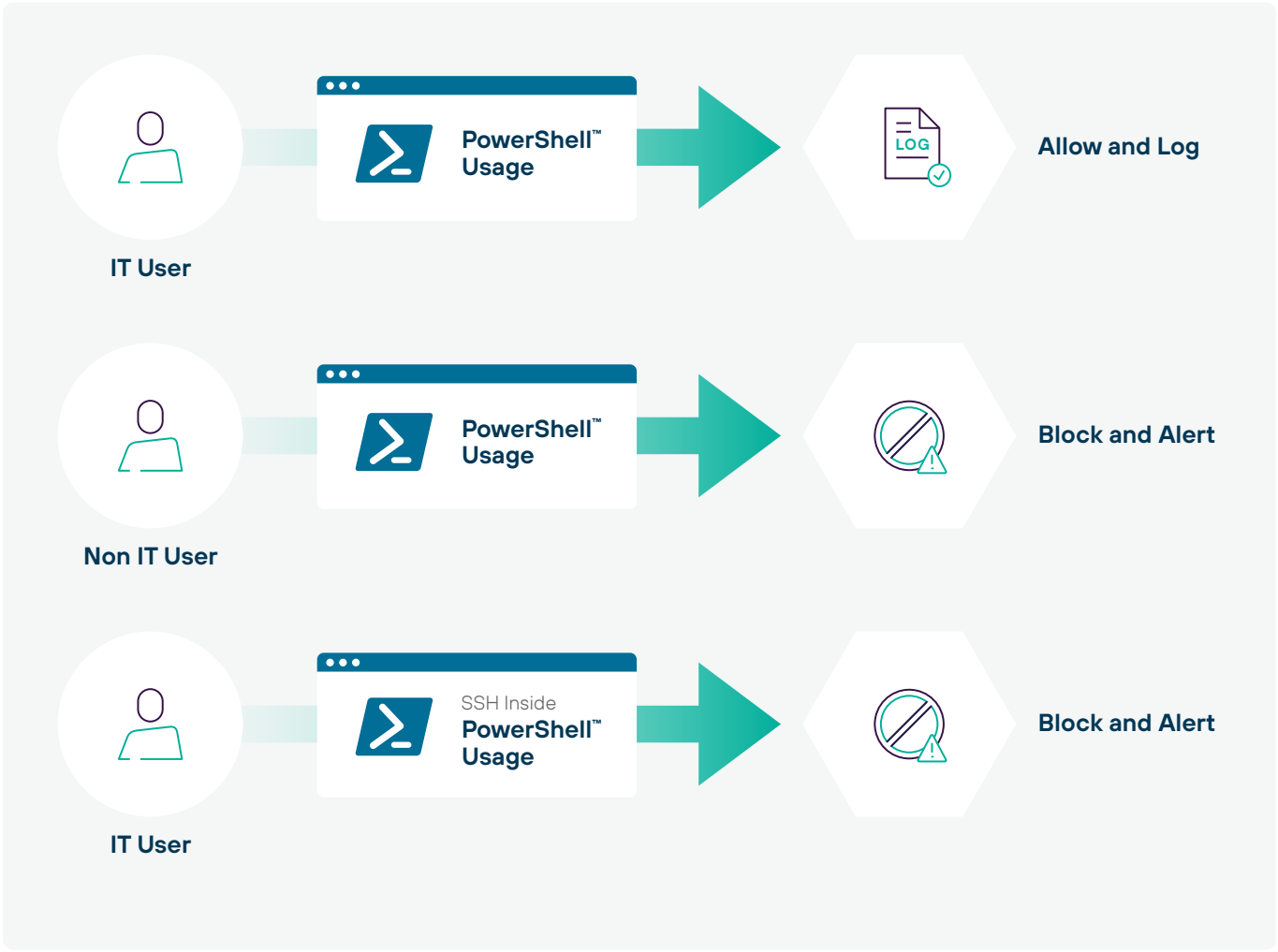
ECA BROWSER CONTROL



Use Case – Control Microsoft PowerShell™

Microsoft PowerShell is an immensely powerful administrative tool that is also favored by malicious actors. Forcepoint ECA endpoint executable detection, combined with user identification, can ensure that only authorized IT administrators can use the tool, while unauthorized or malicious software will be blocked and alerted. Furthermore, tools like SSH launched inside PowerShell can be detected and blocked, even for authorized users.

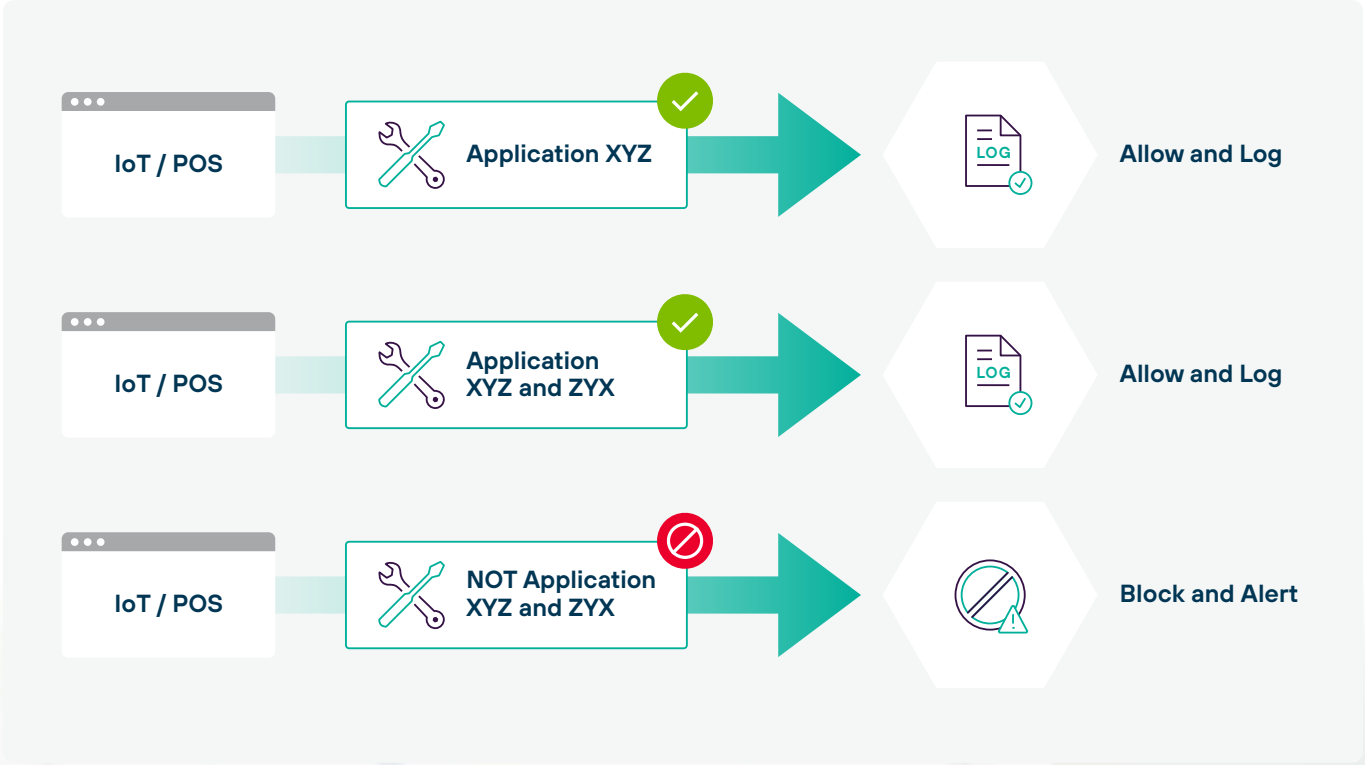
ECA CONTROL MS POWERSHELL™



Use Case – Application/Service Whitelisting

As demonstrated previously, Forcepoint ECA can accurately detect endpoint executables and make access control decisions based on security posture and user/group information. Using signer certificate validation, entire groups of trusted applications can be authorized. It is extremely easy to whitelist all Microsoft Windows applications signed by Microsoft. For unmanned devices with no user logged in, the controls can be pinpointed to specific executables used by that device. Any other activity would be considered malicious and automatically blocked by the Forcepoint NGFW.

ECA APPLICATION WHITELISTING

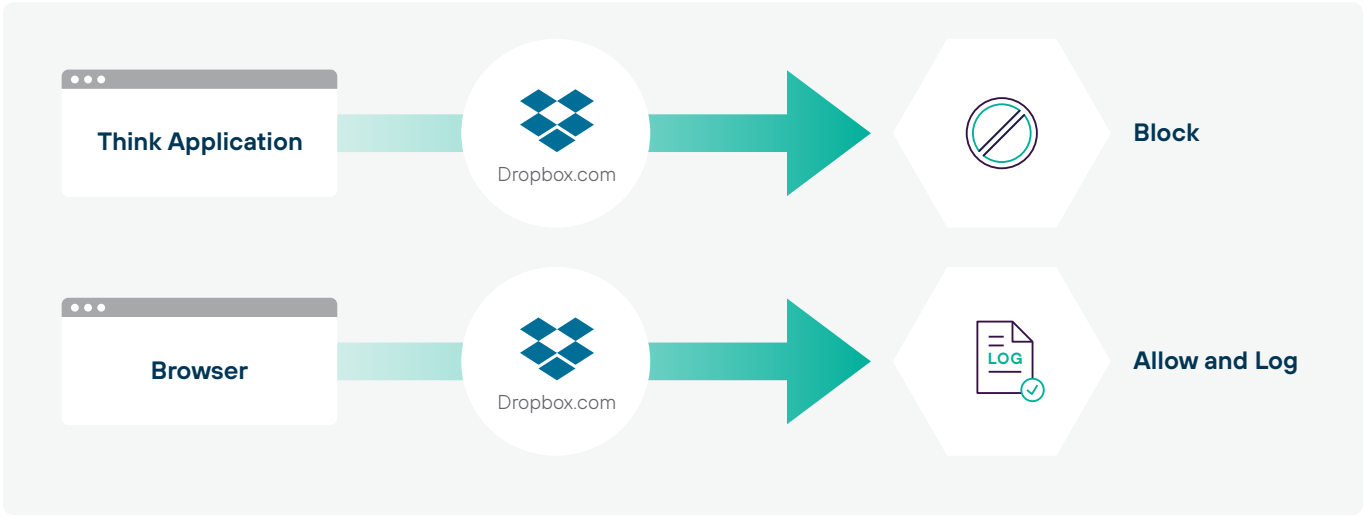


Use Case – Control Certificate Pinning Thick Application

Certificate pinning thick applications pose a challenge to network-level inspection devices as SSL/TLS inspection is not possible. This can lead to blind spots where security controls cannot be applied.

Forcepoint ECA can detect the thick application and force the user to use a browser instead where security controls can be applied.

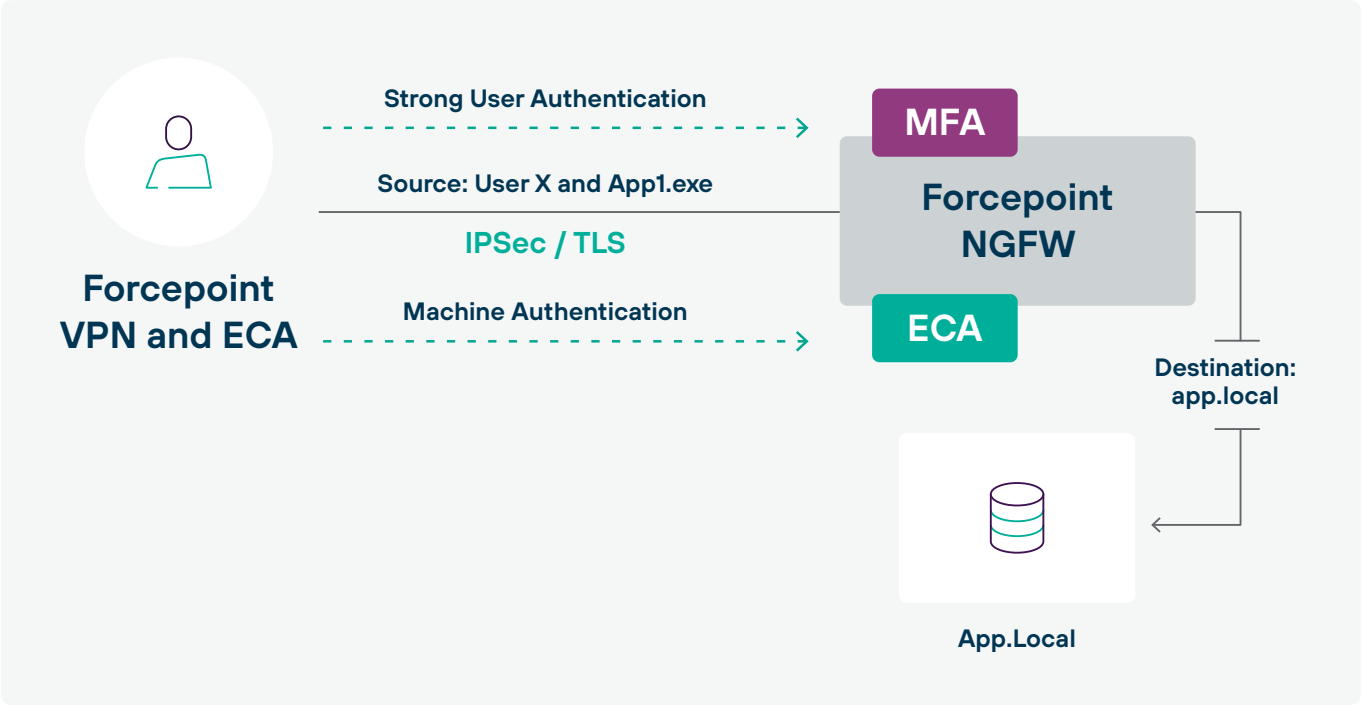
ECA CERTIFICATE PINNING THICK APPLICATIONS

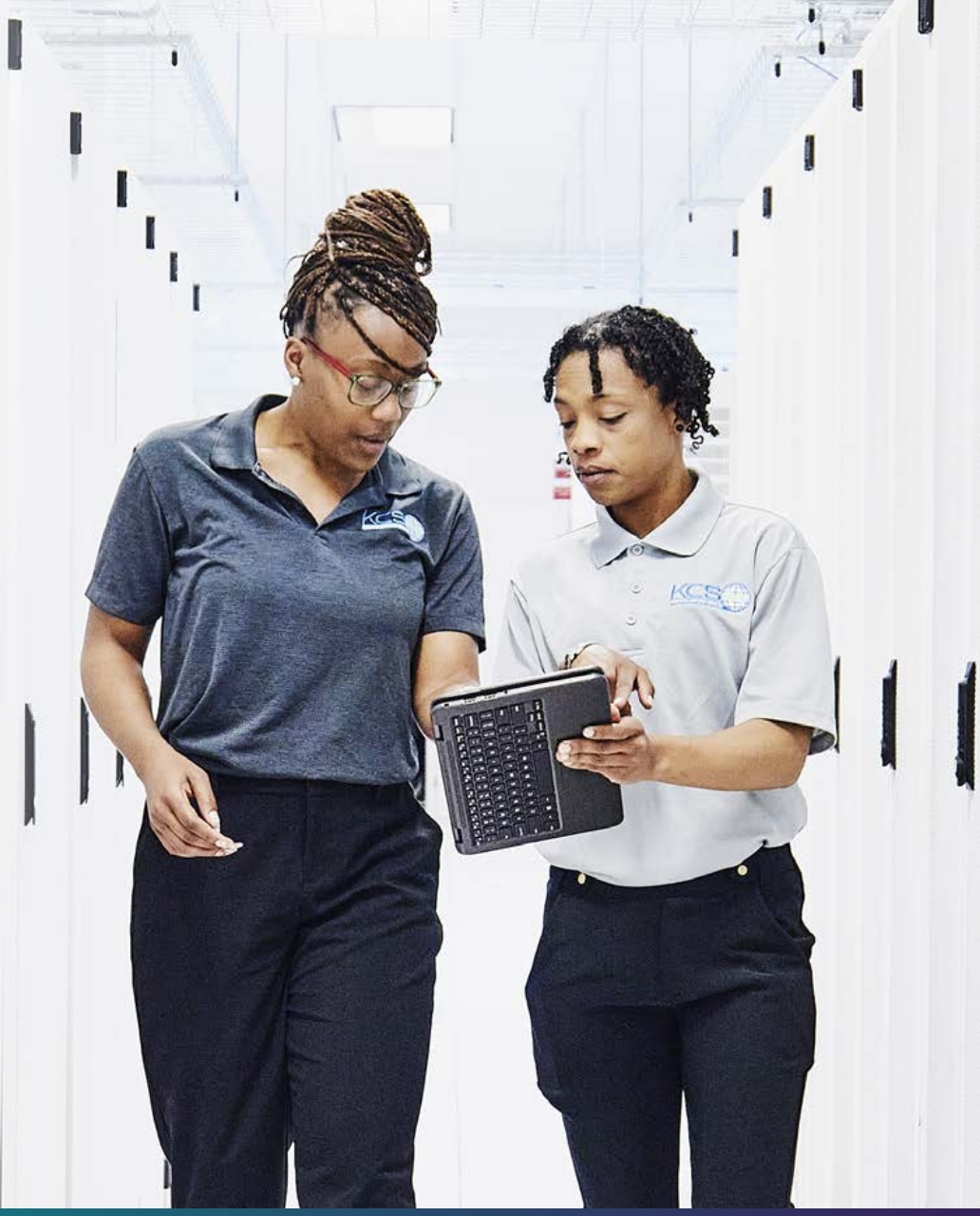


Use Case – Integration with Forcepoint VPN Client

Combining Forcepoint ECA with Forcepoint VPN Client creates a true Zero Trust network access control. The combination of ECA machine authentication, security posture check and the MFA in the VPN Client ensures that only compliant managed devices are authorized to connect to the specific internal resources. Combine this with ECA's endpoint application authorization and user identification to ensure true least-privilege access control when accessing the resources.

ECA FORCEPOINT VPN CLIENT INTEGRATION





Conclusion

Forcepoint ECA enables agencies and missions to extend Zero Trust to include endpoint application information. Forcepoint NGFW access control can be expanded to incorporate trusted information from the endpoint, aiding in the enforcement of Zero Trust principles.

Forcepoint

forcepoint.com/contact

About Forcepoint

Forcepoint simplifies security for global businesses and governments. Forcepoint's all-in-one, truly cloud-native platform makes it easy to adopt Zero Trust and prevent the theft or loss of sensitive data and intellectual property no matter where people are working. Based in Austin, Texas, Forcepoint creates safe, trusted environments for customers and their employees in more than 150 countries. Engage with Forcepoint on www.forcepoint.com, X and LinkedIn.

[Enabling Zero Trust Using Forcepoint NGFW ECA-Whitepaper] 09Jan2025