FORESCOUT
Active Defense for the Enterprise of Things™

eyeExtend

Bridge Privileged Access Management (PAM) Gaps

ACCELERATE TIME TO VALUE

Get Forescout built, tested, supported and ready to be deployed integration.

SHRINK THE ATTACK SURFACE

Continuously discover new devices and unmanaged privileged accounts without requiring agents.

ENHANCE AUDIT COMPLIANCE

Gain confidence in the accuracy of the privileged accounts inventory across the extended enterprise.

INCREASE OPERATIONAL EFFICIENCY

Automate workflows to onboard IT/IoT/OT assets and bring previously unknown privileged accounts under CyberArk management.

REDUCE MEAN TIME TO RESPOND

React instantly and automatically to malicious activity by isolating compromised devices, changing passwords and preventing malicious user access.

Expand visibility into privileged accounts, defend against privileged credential misuse and respond rapidly to threats

Forescout eyeExtend for CyberArk extends the power of CyberArk by closing gaps in privileged account management, device visibility and security in the privileged access management process. This eyeExtend integration enables robust, enterprise-wide device and privileged account detection, onboarding, risk management and network access control across IT, IoT and OT devices. IT and security administrators can now streamline the process of securing an ever-expanding privileged access environment.

- Discover and onboard sprawled unknown privileged accounts and increase operational efficiency
- Comply with corporate policies and regulations to minimize security risk and audit costs
- Accelerate response to threats to reduce mean time to response (MTTR)

IDENTIFY

Agentlessly discover and report IT/IoT/OT assets into CyberArk in real time

Onboard sprawled privileged accounts based on policy

Eliminate related risk of unsecured privileged accounts in multiple platforms

COMPLY

Retrieve credentials from the CyberArk Digital Vault for added security

Monitor credential usage across the enterprise

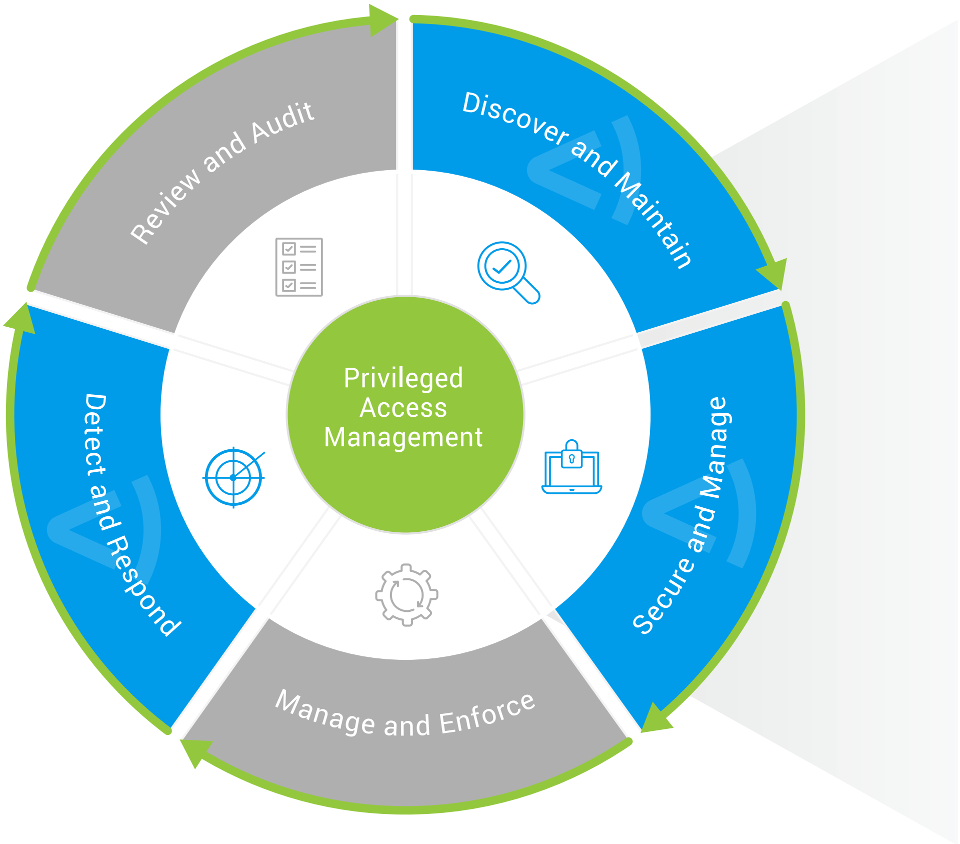
Maintain a comprehensive audit trail for compliance

DEFEND

Prevent privileged credential misuse and unauthorized network access

Automate credential change per policy for compromised devices

Automate a diverse range of network and device actions in response to privileged credential threats



Defend against privileges credential misuse and respond rapidly to privileged account threats.

IDENTIFY

Discover all networked devices agentlessly and report their local privileged accounts to CyberArk the moment they connect:

- Increase CyberArk's privileged accounts management coverage with complete visibility into:
  - Privileged accounts on Windows-, Linux- and Apple OS-based devices
  - IoT, OT and network infrastructure devices
- Share privileged account information with CyberArk for placement in the Vault Pending Accounts List
- True-up your CyberArk account inventory and delete stale or illegitimate privileged accounts

COMPLY

Follow security best practices and enforce system-wide security policies to minimize risk:

FORESCOUT ADDS VALUE:

Discover and Maintain

- Real-time and agentless discovery of devices with privileged accounts
- Policy-based onboarding of IT/IoT/OT assets

Secure and Manage

- Privileged account credentials retrieval from the vault to access various resources as a security best practice

Detect and Respond

- Automate Forescout actions based on Forescout or other third-party detected suspicious user behavior and PSM violations
- Apply diverse range of network actions to quarantine and remediate risks
- Automatically change passwords on risky endpoints

eyeEXTEND FOR CYBERARK SOLVES FOR:

Security risk and audit costs introduced by lack of awareness of unknown privileged accounts across the enterprise – a visibility gap that increases the likelihood of credential theft or misuse that can lead to exfiltration of sensitive corporate data.

Ever-increasing operational costs, inefficiencies and errors due to manually managing and securing privileged credentials.

Slow mitigation caused by inadequate network and device intelligence with limited response options for granular and precise actions. Lack of automated response actions against devices with malicious activity results in increased security risk and potentially severe business impacts.

- Enhance security by eliminating the need to save or manage login credentials locally and by leveraging the sensitive credentials stored in the CyberArk Digital Vault for endpoint inspection
- Monitor credential usage across the enterprise and maintain a comprehensive audit trail for compliance
- Identify devices with a Privileged Session Management (PSM) requirement and enter them into a policy that will ensure continuous compliance

DEFEND

Receive and respond to alerts from CyberArk Privileged Threat Analytics and/or other third-party threat-detection tools:

- Automatically respond to PSM violations by providing a network-level response to noncompliant devices
- Prevent credential abuse in real time by automating password change for compromised devices as identified by Forescout and other integrated third-party threat intelligence solutions such as leading ATD, EDR and SIEM tools
- Foil lateral threat propagation by automating policy-driven threat response actions such as blocking, limiting or quarantining noncompliant and compromised devices' access to the corporate network. Based on policy, Forescout can also trigger remediation of the endpoint or notify the security authority

Refer to the Forescout Compatibility Matrix to view the complete list of supported partner products and versions.

Don't just see it.
Secure it.™

Contact us today to actively
defend your Enterprise of Things.

forescout.com/platform/eyeExtend/ salesdev@forescout.com toll free 1-866-377-8771

FORESCOUT
Active Defense for the Enterprise of Things™

Forescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

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

Learn more at Forescout.com