ForeScout Extended Module for CyberArk®

Defend against privileged credential misuse and rapidly respond to sophisticated privileged account threats

Highlights

See

- Discover devices and local privileged accounts without requiring agents
- Profile and classify devices, users, applications and operating systems
- Assess and continuously monitor devices and privileged accounts

Control

- Allow, deny or limit network access based on account activity, device profile and security posture
- Initiate threat mitigation actions on non-compliant or compromised endpoints
- Provide automated, policy-based compliance checks before allowing network access

Orchestrate

- Share device context, security posture and local privileged account information
- Gain holistic intelligence about privileged accounts and initiate automated actions to protect against credential misuse
- Leverage a centralized vault to store credentials for CounterACT and other network devices

The widespread use of privileged accounts across enterprise networks presents recurring security challenges. The proliferation of these accounts across multiple repositories and individual devices, combined with lack of holistic visibility, increases the likelihood of credential theft or misuse to exfiltrate sensitive data. Improved visibility and actionable intelligence about these accounts, especially those residing across individual devices on the network, can help disrupt privileged account compromise and greatly reduce the risk of data breaches.

The Challenges

Visibility. Privileged accounts represent a large, under-protected attack surface with tremendous risk to the enterprise. Often unmonitored, these unmanaged privileged credentials reside on many networked devices, applications and tools, and are frequently shared for everyday network operations management. The widespread use of these accounts, combined with a "governance gap" across various IT functions that leaves them unmonitored, provides attackers with easy access to exfiltrate sensitive information and remain unnoticed. Effective IT security programs must include real-time visibility of diverse devices on the network, their compliance with the security standards and an inventory of local privileged accounts to protect against advanced threats and data breaches.

Threat Landscape. Privileged credential abuse and data theft have heightened both awareness and concerns about the threats caused by privileged account compromises. In a recent study[1], 69 percent of respondents cited the inability of security tools to provide holistic contextual information about privileged account use. The study also cited use of manual or ad hoc processes such as email or spreadsheets to review and certify privileged user access as root causes of security challenges for organizations. Successfully governing, managing and controlling the use of privileged credentials requires systems that can automatically manage the lifecycle of privileged accounts. These systems must be supplemented with full network and device context awareness, combined with actionable intelligence, to detect and disrupt a compromise.

Response Automation. Insufficient privileged account analytics combined with manual and siloed processes to correlate heaps of information pose significant challenges for incident response. Additional factors such as mergers and acquisitions, an onslaught of unmanaged devices and compliance mandates exacerbate these challenges and can easily overwhelm manual response processes and render them ineffective. To combat today's cyberthreats, security teams must gain holistic intelligence across networks, devices and privileged accounts, and take automated response actions to minimize data breaches.

The integrated ForeScout-CyberArk solution allows you to:

- Gain enhanced visibility into privileged accounts on the network and protect against threats from undetected devices with privileged credentials
- Fortify credential management by centrally storing and managing privileged credentials, supporting a comprehensive audit trail for regulatory requirements
- Respond to threats based on comprehensive device security posture, network context, user activity and overall threat exposure

This helps to reduce your attack surface, prevent unauthorized access to sensitive resources and minimize data breaches.

ForeScout Extended Module

The ForeScout Extended Module for CyberArk is an add-on module for ForeScout CounterACT that is sold and licensed separately. It is one of many ForeScout Modules that enables CounterACT to exchange information, automate multivendor workflows and accelerate system-wide response. For details on our licensing policy, see www.forescout.com/licensing

Learn more at
www.ForeScout.com

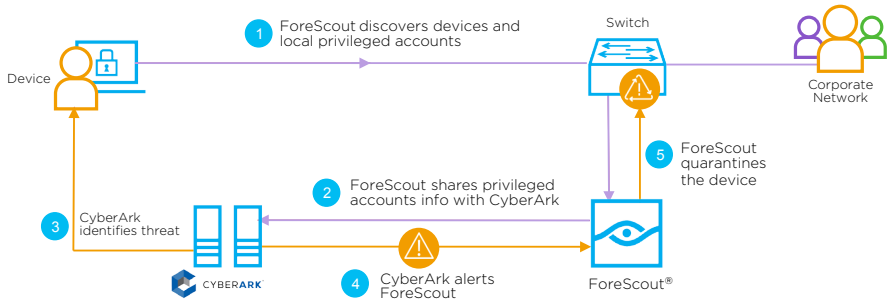

Figure 1: ForeScout Extended Module for CyberArk workflow.

How it Works

ForeScout CounterACT® is a network security solution that gives you the unique ability to see devices, including non-traditional devices, as they connect to the network. CounterACT provides policy-based assessment, monitoring and precise automated control of these devices.

The ForeScout Extended Module for CyberArk® leverages CounterACT's real-time agentless visibility to discover and classify a diverse set of devices, assess their security posture and gather intelligence about local privileged accounts. This enables you to get a current view of networked devices with privileged accounts, true-up your CyberArk account inventory and take precise, policy-based actions according to user activity, device security posture and recent threat exposure to allow or limit network access. As a result, you can more effectively manage privileged accounts and reduce your overall attack surface.

CyberArk leverages user activity and credentials usage of domain-managed devices as the source of intelligence. This allows CyberArk to detect a compromise and take domain-related actions, such as initiating password rotation or blocking access of suspicious or compromised accounts. In addition, the ForeScout Extended Module enables you to create compliance policies for real-time agentless security checks before allowing network access. This empowers you to control access of both domain-managed and unmanaged devices, and take automated actions to quarantine or remediate non-compliant or compromised devices.

When a credential theft or unauthorized use of credentials is detected by CyberArk Privileged Threat Analytics™, it associates a severity and certainty rating to the event. Based on this severity and certainty, the threat analytics platform can send an alert to the administrator or invalidate a suspected stolen privileged credential without requiring human intervention. With this joint solution, administrators can combine the device security posture and recent Indicators of Compromise (IOCs) discovered by CounterACT to gain comprehensive network awareness about the suspicious event and take policy-based network actions to quarantine and remediate the device with compromised credentials.

In addition, the Extended Module allows you to store credentials used by your CounterACT deployment in the CyberArk Enterprise Password Vault®. This enables you to use a centralized repository with automated options to store, rotate and monitor credentials across CounterACT and your other network devices, and assist with maintaining a comprehensive audit trail for regulatory requirements.

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

[1] http://www.raytheoncyber.com/rtnwcm/groups/cyber/documents/content/rtn_257010.pdf