SOLUTION BRIEF

Fortinet and CyberArk Integrated Security Solution

Security Without Compromise for Privileged Accounts To Protect Critical and High-value Assets

Challenges

Business digitalization is impacting how companies do business, and how employees and consumers interact with organizations. As organizations adopt new technologies and solutions, their IT infrastructure and applications are becoming increasingly complex. Add to that, the organizational shift to cloud and DevOps methodologies is presenting attackers with newer pathways to exploit unprotected businesses. Adding to this complexity is the management of stringent mandates associated with regulatory compliance standards.

In the ever-widening attack surface, privileged accounts and credentials, which represent the most valuable core assets of any enterprise, are the most targeted and sought after. And, once these privileged accounts are breached, attackers can gain access to sensitive data or intellectual property that can cost companies their reputation and financial losses. Trying to manually manage and support all network and security devices to ensure business continuity and ensure compliance standardization can often be difficult, time-consuming, prone to error, and overwhelming for IT.

In order to safeguard the most critical assets and improve the productivity of users, organizations must adopt a privileged account security strategy that includes proactive protection and monitoring of all privileged secrets and credentials—a solution that can have the combined benefits of patented analytics, and the detection, alerting, and reporting required to stay one step ahead of the attackers.

Joint Solution Description

The Fortinet and CyberArk integrated solution addresses the above challenges by leveraging the Fortinet Security Fabric. The Fortinet Security Fabric is designed around a series of open application programming interfaces (APIs), open authentication technology, and standardized telemetry data to enable organizations to integrate existing security technologies via open interfaces and provide end-to-end security without compromise.

The combined solution of the Fortinet FortiSIEM security information and event management (SIEM) and CyberArk Application Identity Manager provides organizations with a simplified way to manage privileged application credentials while performing trusted discovery scans, without the need for stored credentials in the FortiSIEM solution. To ensure a comprehensive security and compliance strategy, organizations need to define and document a detailed inventory of all devices and assets connected to the network using a comprehensive, credential-protected discovery and mapping process. This is essential to define and document the baseline topology of the potential threat landscape.

Joint Solution Components

- Fortinet FortiSIEM
- CyberArk Application Identity Manager

About Cyber Observer

- Rapid detection and remediation of security events
- Identification of high-risk privileged account activity in real time
- Prioritization of alerts for privileged accounts, and quick investigation and response to critical threats
- Greater security, management, and control over privileged accounts across the organization
- Security, performance, and compliance management

FORTINET FABRIC-READY

FortiSIEM's centralized configuration management database (CMDB), an intelligent infrastructure and application discovery engine, is able to discover and map the topology of both physical and virtual infrastructure, on-premises and in public/private clouds simply without any prior knowledge of what the devices or application is. The FortiSIEM CMDB also self-learns and reports on any new devices that are added to the network, post the baseline snapshot.

Using CyberArk Application Identity Manager, FortiSIEM can perform secure discovery and assessment using privileged credentials securely stored and managed by the CyberArk Privileged Account Security Solution. This relieves the administrator from the responsibility of managing privileged account credentials at numerous locations, as well as reducing the risk of unauthorized use.

FortiSIEM also provides rapid time to value with out-of-the-box compliance reporting and analytics tools. Prebuilt reports are standard and help to manage a wide range of compliance needs, including PCI DSS, HIPAA, ISO 27001, FISMA, SOX, NERC, COBIT, ITIL, SOX, GLBA, GPG13, and SANS best practices. These reports can be customized to suit unique needs.

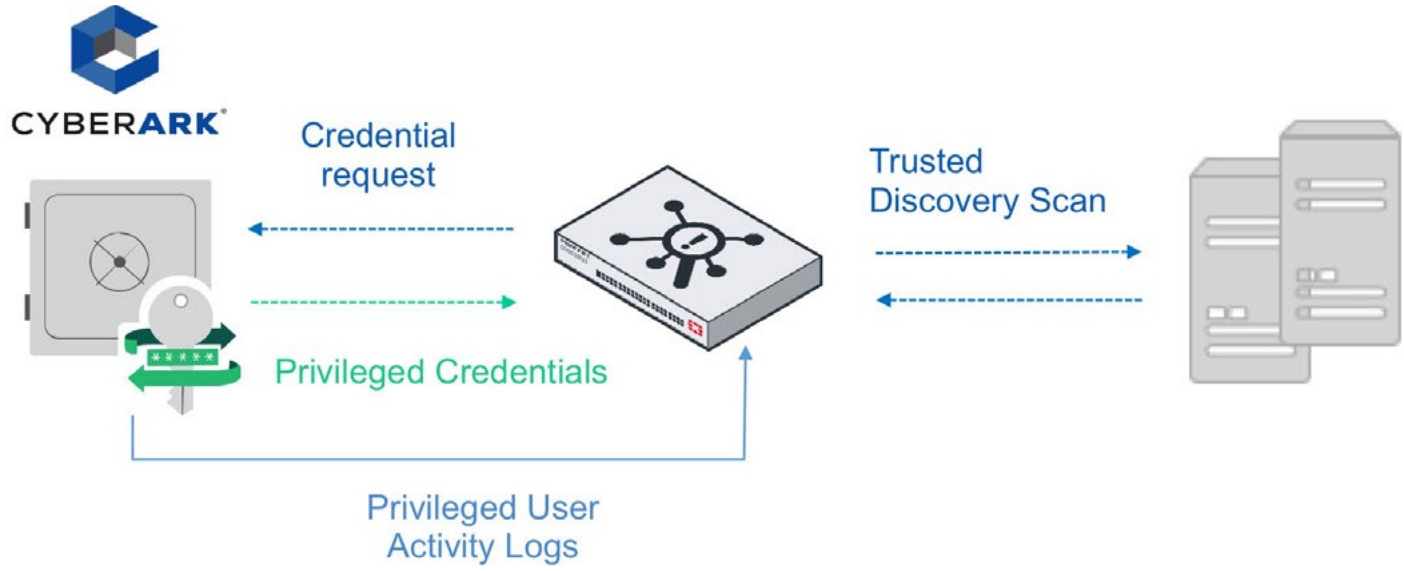

Figure 1: Integration of Fortinet and CyberArk to secure privileged credentials used by Fortinet and offer integrated privileged threat intelligence.

FortiSIEM: Powerful Security Information and Security Management

FortiSIEM expands the Fortinet Security Fabric beyond Fortinet devices to support the complex needs of security operations with a powerful and scalable solution that provides single-pane-of-glass visibility of the entire threat landscape, including asset self-discovery and cross-correlated network operations center (NOC) and security operations center (SOC) analytics for more rapid detection and remediation of threats. This next-generation SIEM solution leverages data from security solutions, performance, availability, change monitoring, and compliance; delivers cross- correlated analytics and intelligence in real time, and provides tools to address incidents completely and swiftly.

Summary

The FortiSIEM and CyberArk integrated solution allows customers to reduce the risks associated with unauthorized access to privileged accounts without overburdening IT teams and organizations with tools to proactively secure, automatically rotate, and control access to privileged account credentials, which serve as the keys to the IT kingdom.

About CyberArk

CyberArk is the global leader in privileged account security, a critical layer of IT security to protect data, infrastructure and assets across the enterprise, in the cloud and throughout the DevOps pipeline.

CyberArk delivers the industry's most complete solution to reduce risk created by privileged credentials and secrets. The company is trusted by the world's leading organizations, including more than 50 percent of the Fortune 100, to protect against external attackers and malicious insiders. To learn more, visit us at www.cyberark.com.

September 14, 2021 2:38 PM

Macintosh HD:Users:austin:Dropbox (Red Rider):Clients:Fortinet:Solution Brief Updates:Working Group 2:sb-fortinet-cyberark:sb-fortinet-cyberark_2021

429117-A-0-EN