CYBERARK®

CyberArk Privileged Threat Analytics™

Table of Contents

The New Security Battleground: Inside Your Network

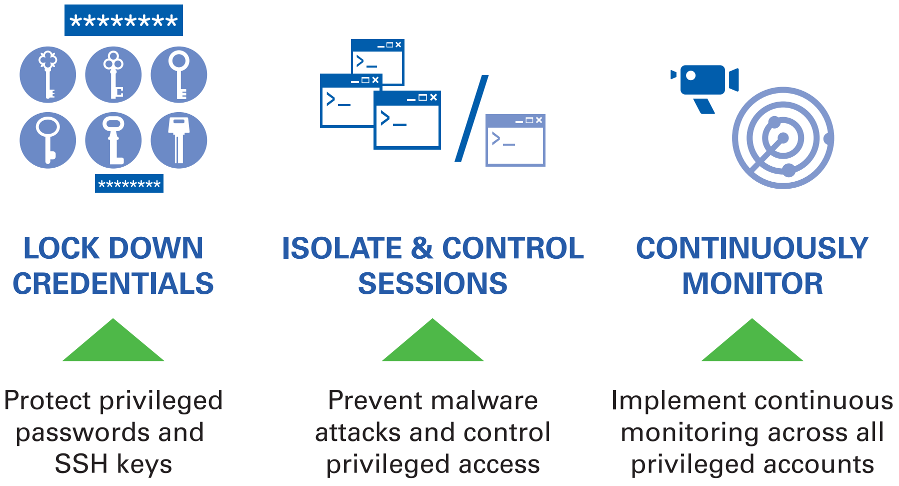
The new battleground for information security is inside your network. Perimeter security, such as firewalls and anti-malware, remain a necessary and important component of every security strategy. However, the perpetrators of advanced, targeted threats are aggressively breaking through the perimeter. Patient, cunning and armed with the resources to succeed, they will eventually find their way inside your organization. In addition, a "rogue insider" with legitimate access may abuse trusted privileges. Whether the threat originates externally or with a malicious insider, attackers will lay in wait as long as necessary to gain access to valuable assets, resulting in damaged reputations, financial losses and stolen intellectual property.

How do advanced attackers find their way to the heart of your enterprise? The pathway is the privileged account. According to information security firm Mandiant, advanced persistent threat attackers "prefer to leverage privileged accounts where possible, such as domain administrators, service accounts with domain privilege, local administrator accounts, and privileged user accounts."[1] Mandiant found that of 141 companies attacked by Chinese cyber attackers, 90% of breaches involved privileged pathways.[2]

Privileged account security

To help mitigate the risks of a serious breach, enterprises must adopt a security posture that specifically addresses their privileged account exposure. The key to privileged account security is to implement defense in depth: build layers of protection, recognizing that no single measure is enough to keep determined attackers out. Comprehensive controls on privileged activity include:

- Proactive protection of privileged credentials to manage and secure access to credentials
- Privileged session control and isolation to prevent the spread of malware to sensitive systems, and
- **Continuous monitoring with real-time analytics to detect in-progress attacks and enable immediate response to alerts of suspicious behavior.**



LOCK DOWN CREDENTIALS

Protect privileged passwords and SSH keys

ISOLATE & CONTROL SESSIONS

Prevent malware attacks and control privileged access

CONTINUOUSLY MONITOR

Implement continuous monitoring across all privileged accounts

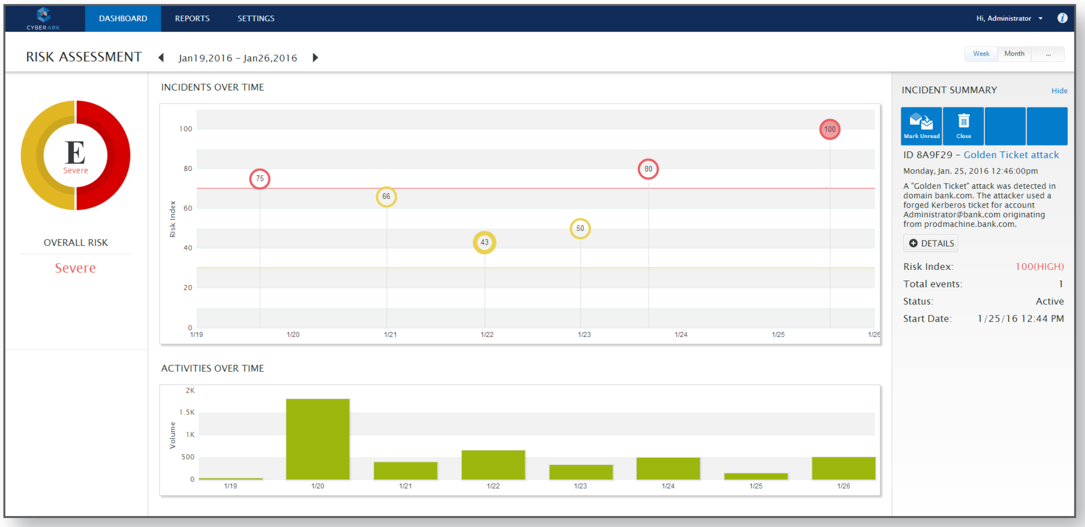
Figure 1: The CyberArk Privileged Account Security Solution includes proactive controls and threat detection

[1] Mandiant, "Exposing One of China's Cyber Espionage Units," February 2013
[2] Mandiant, "Exposing One of China's Cyber Espionage Units," February 2013

CyberArk Privileged Threat Analytics: Collect. Detect. Alert. Respond.

CyberArk Privileged Threat Analytics is an advanced system for privileged account security intelligence. The solution provides targeted, promptly actionable threat alerts by identifying anomalous privileged user and account activity.

CyberArk Privileged Threat Analytics calls an organization's attention to the most menacing of threats - those aimed at privileged accounts. By applying built-in analytics algorithms to a rich set of privileged activity data, the solution produces highly accurate and promptly actionable intelligence, allowing incident response teams to respond directly to an attack.



ID 8A9F29 – Golden Ticket attack

Monday, Jan. 25, 2016 12:46:00pm

A "Golden Ticket" attack was detected in domain bank.com. The attacker used a forged Kerberos ticket for account Administrator@bank.com originating from prodmachine.bank.com.

Risk Index: 100(HIGH)
Total events: 1
Status: Active
Start Date: 1/25/16 12:44 PM

Figure 2: The CyberArk Privileged Threat Analytics Dashboard: The analytics engine assigns a risk score to each individual detected security incident and generates an overall threat level for the environment as a whole.

Collect the right data

CyberArk Privileged Threat Analytics collects data from multiple sources across the IT infrastructure. Many analytics tools attempt to collect and analyze everything across an organizations' IT network and therefore easily become overwhelmed with too much data. CyberArk Privileged Threat Analytics collects data that contains a high risk for extensive damage: privileged account activity. With this rich and targeted data set, the analytics engine can quickly identify anomalous activities that could indicate an in-progress attack. As a result, incident response teams can prioritize incidents that involve privileged accounts, enabling them to stop damaging attacks before they stop business.

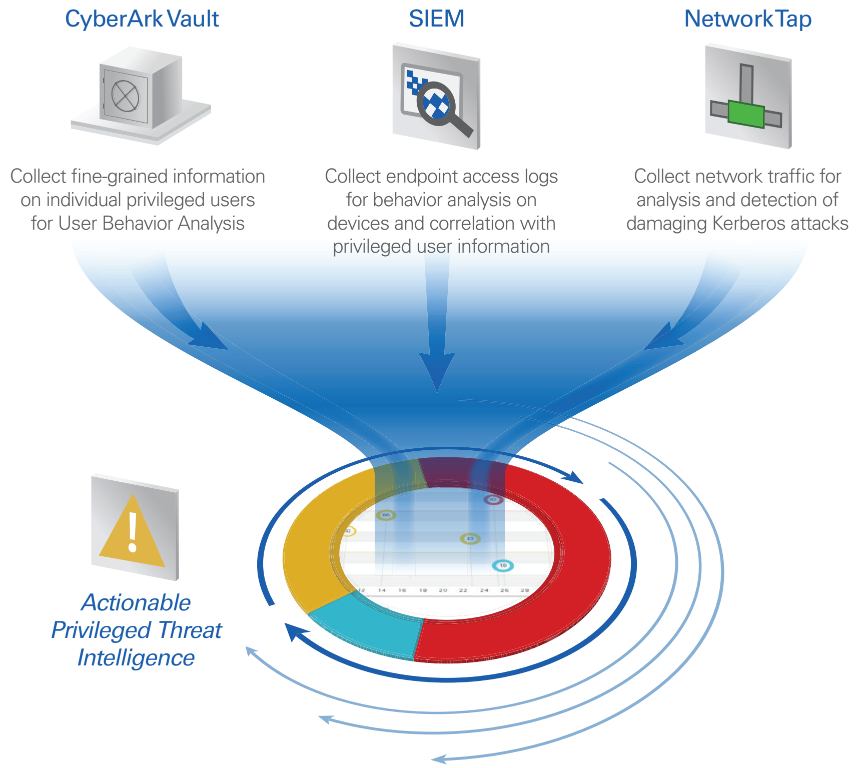

CyberArk Vault
Collect fine-grained information on individual privileged users for User Behavior Analysis
SIEM
Collect endpoint access logs for behavior analysis on devices and correlation with privileged user information
Network Tap
Collect network traffic for analysis and detection of damaging Kerberos attacks
Actionable Privileged Threat Intelligence

Figure 3: CyberArk Privileged Threat Analytics collects data from a variety of sources and leverages existing infrastructure including SIEM solutions and Network Taps.

Detect critical threats

With a comprehensive data set containing privileged activity, the analytics engine has robust information to help identify anomalous privileged activity. The solution includes a complex combination of proprietary algorithms including both deterministic algorithms and on-going behavioral analytics on users and entities, such as endpoints and servers. Using machine learning, the analytics engine calculates normal behavior for privileged users, privileged accounts, privileged access to machines and Kerberos authentication attempts. The analytics engine then identifies deviations from the normal profile using statistical modeling.

CyberArk Privileged Threat Analytics helps detect the most damaging attacks including:

Attacks abusing privileged accounts. Malicious insiders and external attackers often use privileged accounts to move laterally and escalate privileges, thus, not following normal behavioral patterns for account usage. CyberArk Privileged Threat Analytics conducts Privileged User and Entity Behavior Analytics (UEBA) in order to build behavioral profiles of all designated privileged users, accounts and systems. The analytics engine then looks for deviations from the baseline to detect and alert on anomalous behaviors that may indicate the credential has been accessed by an unauthorized user.

Leverage Existing Infrastructure

Integration with SIEM solutions

SIEM solutions are widely used to collect, analyze and alert on network activity. CyberArk Privileged Threat Analytics significantly enhances the information provided by SIEM solutions through a two-way integration. First, privileged account activity on network systems is collected by the SIEM and fed into CyberArk Privileged Threat Analytics. This data is processed by a set of complex algorithms in the CyberArk Privileged Threat Analytics engine and correlated with privileged user information. The analytics engine then detects anomalous activity and generates targeted, actionable alerts for high-risk incidents. Completing the integration, the alerts can then be sent to the SIEM solution, enabling an organization to efficiently prioritize and respond to the most serious threats.

Integration with Network Tap Aggregator solutions

CyberArk Privileged Threat Analytics integrates with network tap aggregators, switches, and switch mirror port solutions in order collect and analyze network traffic related to privileged activity. Analysis of network traffic provides organizations with visibility into malicious activities that are not detectable by log analysis alone, such as Kerberos authentication attacks. By integrating with existing network tap aggregators, switches and switch mirror ports, organizations can easily send relevant network traffic to CyberArk Privileged Threat Analytics, while not impacting network performance.

Example: Access at an unusual time of day

CyberArk Privileged Threat Analytics can detect a privileged account that has been accessed at an unusual time of day. By comparing the baseline behavior profile, which determines the regular hours that a user or application accesses the system, to real-time activity, CyberArk Privileged Threat Analytics will alert on any usage that occurs outside of regular hours.

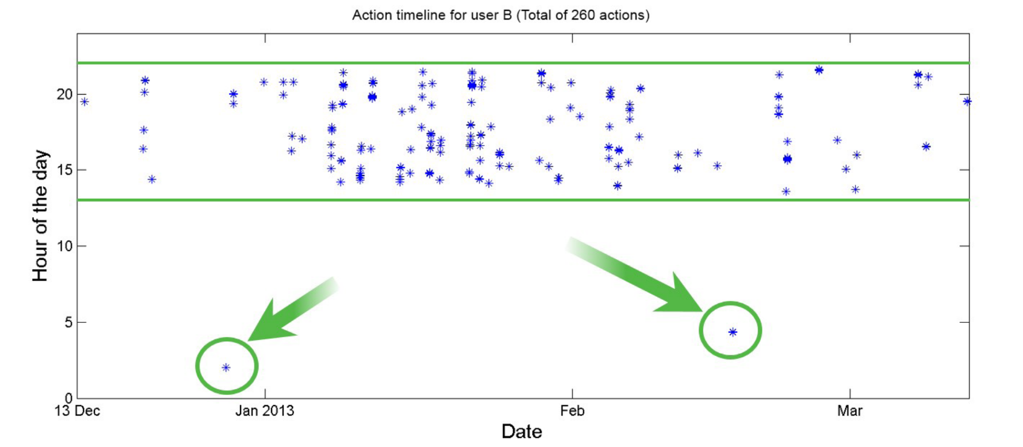


Figure 4: CyberArk Privileged Threat Analytics, illustrating anomalies in time-of-day access.

Attacks exploiting Kerberos authentication. Attackers exploit vulnerabilities in the Kerberos protocol (such as the poor protection of secrets i.e. password hashes) in order to manipulate and generate Kerberos tickets. These Kerberos-based attacks enable attackers to operate under the radar by impersonating authorized users. With the ability to anonymously impersonate any user, including privileged users, attackers are able to traverse the network for extended periods of time, likely without being detected by traditional security tools. As a result, these attacks can be extremely damaging. By conducting Network Behavior Analytics, CyberArk Privileged Threat Analytics is able to detect in-progress Kerberos attacks, including Kerberos Golden Ticket attacks.

Example: Kerberos Golden Ticket attack

CyberArk Privileged Threat Analytics can detect in-progress Kerberos Golden Ticket attacks by analyzing network traffic and identifying deterministic indications of compromise. With the potential to cause significant damage, these attacks must be detected quickly and responded to immediately by an organization. If CyberArk Privileged Threat Analytics detects a Golden Ticket attack, the security team will receive a prioritized alert that is automatically assigned the highest risk score possible empowering incident response teams to respond promptly.

Alert on critical incidents

When an anomalous privileged activity is detected, CyberArk Privileged Threat Analytics generates a targeted alert, which could indicate a very damaging attack. In addition, each security event is assigned a risk score based on the type of anomaly and the severity of the deviation from the normal behavior. Security events are also correlated with each other in order to determine whether a series of events relate to the same incident. Incidents with high risk scores generate an alert containing details of the security incident such as the impacted machine, user(s), and account(s) that were used in the suspected attack. The prioritized alert is sent to security teams via the CyberArk dashboard, email notification, and/or a SIEM dashboard.

Respond automatically

CyberArk Privileged Threat Analytics takes incident response one step beyond detection and alerting, and includes the ability to automatically respond to a detected incident. Once security teams detect a security incident, the next step is to contain the threat by cutting off an attacker's access. CyberArk Privileged Threat Analytics automates the containment step of incident response with a direct integration with the CyberArk Enterprise Password Vault. When the solution detects a suspected stolen privileged credential, it can promptly respond by rotating the credential in the CyberArk Digital Vault to stop an attacker from continuing to use the compromised credential.

Benefits of CyberArk Privileged Threat Analytics

An organization can

- Dramatically shorten an attacker's window of opportunity and reduce damage by focusing threat detection on privileged account activity and critical attack vectors
- Rapidly detect attacks with analytics based on built-in algorithms written by and continuously updated by experts in privileged account security
- Adapt threat detection to a changing risk environment with machine learning algorithms that continuously adjust the baseline behavior profiles as the authorized behavior changes over time
- Automatically respond to a suspected stolen privileged credential to stop an attacker from continuing to use a compromised credential further
- Accelerate remediation with prompt access to detailed information about an attack, including specific user, activity and current account state
- Receive quick time-to-value by leveraging existing network tap aggregators and end point connectors from SIEM solutions for integration with existing infrastructure

Conclusion

Recognizing that attackers are already on the inside, analyzing and alerting on unusual privileged activities is a critical component to protect against serious damage. CyberArk Privileged Threat Analytics provides targeted and promptly actionable threat analytics on privileged accounts, the number one critical attack vector[3], by identifying difficult to detect malicious privileged user and account activities. CyberArk Privileged Threat Analytics can be an essential part of an organization's overall security strategy that enables incident response teams to automatically respond to suspected stolen privileged credentials and block an attacker from continuing.

[3] CyberArk Threat Report: Privileged Account Exploits Shift the Front Lines of Cyber Security

CyberArk Privileged Account Security Solution

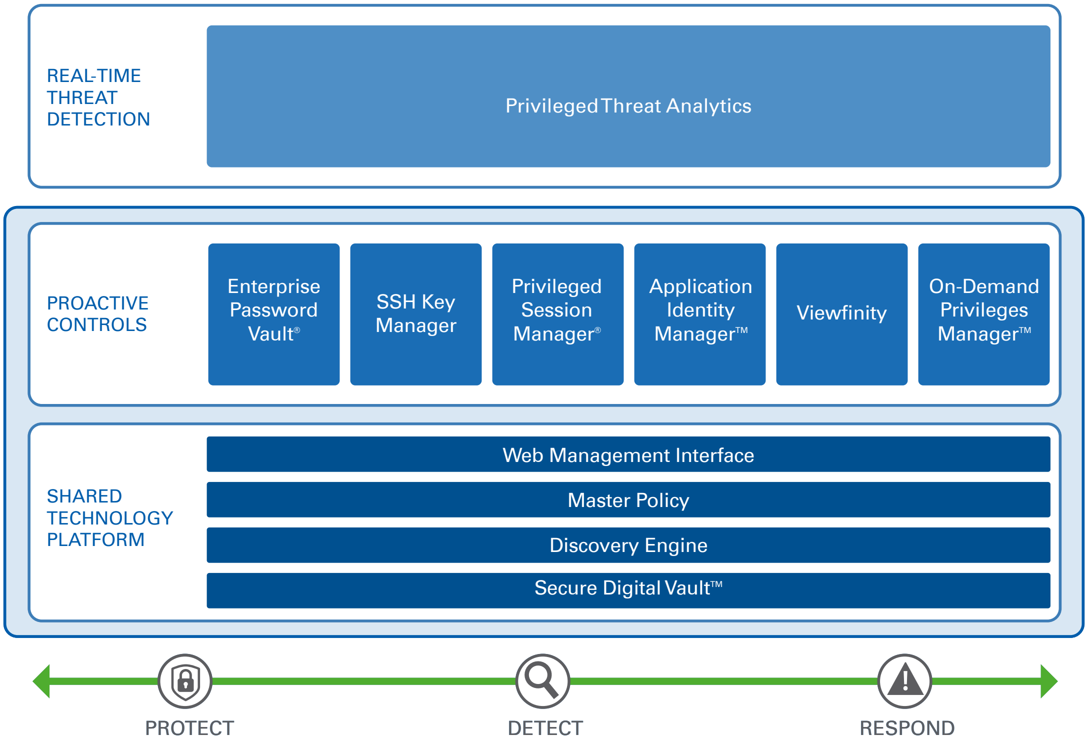

REAL-TIME THREAT DETECTION
Privileged Threat Analytics
PROACTIVE CONTROLS
Enterprise Password Vault®
SSH Key Manager
Privileged Session Manager®
Application Identity Manager™
Viewfinity
On-Demand Privileges Manager™
SHARED TECHNOLOGY PLATFORM
Web Management Interface
Master Policy
Discovery Engine
Secure Digital Vault™
PROTECT
DETECT
RESPOND

Figure 6: CyberArk Privileged Account Security Solution

In addition to CyberArk Privileged Threat Analytics, CyberArk offers the following products designed for proactive privileged account security. The products provide the comprehensive protection, monitoring, detection, and reporting that enable organizations to thwart the malicious insider and advanced attacker.

Enterprise Password Vault® - Protection, management and audit of privileged passwords

SSH Key Manager™ - Protection, management and audit of SSH keys

Application Identity Manager™ - Protection, management and audit of embedded application credentials

Privileged Session Manager® - Isolation and control, session recording and live session monitoring

Viewfinity – Least privilege enforcement and application control for endpoints and servers

On-Demand Privileges Manager™ - Least privilege access control for Unix, Linux

About CyberArk

CyberArk is the only security company laser-focused on striking down targeted cyber threats; those that make their way inside to attack the heart of the enterprise. Dedicated to stopping attacks before they stop business, CyberArk is trusted by the world's leading companies – including 40 of the Fortune 100 – to protect their highest-value information assets, infrastructure, and applications.

For additional information, visit **www.cyberark.com.**