DATA SHEET

CA Threat Analytics for PAM

At A Glance

The misuse or takeover of privileged accounts constitutes the most common source of breaches today. CA Threat Analytics for PAM provides a continuous, intelligent monitoring capability that helps enterprises **detect** and **stop** hackers and malicious insiders before they cause damage. The software integrates a powerful set of user behavior analytics and machine learning algorithms with the trusted controls provided by CA Privileged Access Manager

(CA PAM). The result is a solution that continuously analyzes the activity of individual users, accurately detects malicious and high-risk activities and automatically triggers mitigating controls to limit damage to the enterprise.

KEY BENEFITS

- **Reduced risk.** Detects and mitigates attacks via advanced behavior analytics.
- **Meaningful insight.** Simplifies incident response and compliance.
- **Immediate value.** Delivers detection capabilities, user experience and insights out of the box.
- **No special skills required.** Requires no expertise in algorithms, data science or machine learning.

KEY FEATURES

- **Advanced threat analytics.** Protects data via the same behavior analytics approach used by banks to defeat credit card fraud—machine-learning algorithms analyze historic and real-time activity, assess risk and trigger mitigations.
- **Automated detection of attacks and risk.** Provides a true continuous monitoring capability that uses automated analytics to quickly detect attacks, high-risk activities and breaches.
- **Response and mitigation.** Closes the door on insiders and attackers by automatically triggering mitigations like session recording and step-up authentication.
- **Complements existing systems.** As an integrated add-on, it complements existing operations, security information and event management and security operations center workflows by providing context-rich alerts and reporting.

Business Challenges

Attacks are on the rise against companies of all sizes. Even worse, these attacks often go undetected for weeks or even months, and result in significant financial or reputational damage—which is why protecting privileged accounts is critical to both prevent breaches and address compliance requirements. But static controls, such as traditional authentication and authorization solutions, aren't capable of stopping today's wily attackers, who may be external attackers or malicious insiders.

Successful breach defense today must be dynamic so that privileged user behavior is continuously analyzed to identify suspicious activity, assess risk and quickly detect issues such as compromised accounts or malicious insider activity. When high-risk activity or an attack is detected, there needs to be one or more mitigating controls that are automatically triggered to stop the attacker. By integrating privileged user behavior analytics with automated mitigations in this way, an enterprise can close the door on attackers and ensure protection of privileged accounts.

Solution Overview

CA Threat Analytics for PAM enables organizations to deploy user behavior analytics that detect and stop both external hackers and insider threats. The solution's advanced algorithms continuously assess the behavior of privileged users and compare their actions to historical observations and the behavior of other users. In this way, the solution accurately identifies attacks and high-risk activities, such as users observed surveying an environment in search of high-value assets or those who try to exfiltrate data off sensitive servers.

Unlike solutions that simply require alerts, CA Threat Analytics for PAM mitigates detected risks by automatically triggering controls to stop attacks and limit damage. For example, the system can generate additional authentication or automatically record suspicious user sessions.

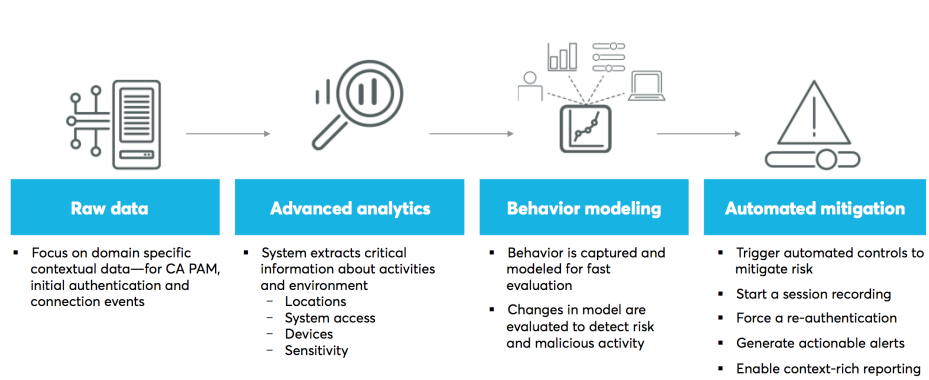
Plus, the solution is simple to deploy and doesn't require special skills for installation, configuration or operation.

Critical Differentiators

CA Threat Analytics for PAM provides robust protection against breaches and insider misuse beyond what competing solutions can provide. It collects domain-specific, contextual data from your CA PAM software, performs advanced analytics on this data, develops risk models based on previous behavior patterns and makes intelligent, risk-based decisions that in some cases will immediately trigger automated mitigation activities. These capabilities provide:

- **Advanced analytics:** The solution performs extensive analysis of each user action and evaluates it based on a user's previous behavior models.
- **PAM-specific analytics and capabilities:** Built specifically to protect privileged access, the solution goes beyond generic analytic tool kits that require significant time and effort to integrate, deploy and tune.
- **Automatic mitigation:** The solution mitigates detected risks by immediately triggering controls that stop and limit the damage that attackers can cause.
- **Context-rich views and reporting:** Robust reporting tools make it easy for administrators to investigate incidents, respond to inquiries for information and understand how their privileged accounts are being accessed.

CA Threat Analytics for PAM



Related Products/Solutions

- **CA Privileged Access Manager** is a simple-to-deploy, automated solution for privileged access management in physical, virtual and cloud environments.
- **CA Privileged Access Manager Server Control** protects critical business assets with fine-grained controls over operating system–level and application-level access.
- **CA Identity Suite** helps manage and govern user access across on-premises and cloud environments with a simple, business-oriented user experience.

Supported Environments

CA Threat Analytics for PAM is deployed as a virtual appliance and compatible with CA PAM versions v2.8 and later.

For more information, please visit **ca.com/PAM**

200-339748_0218