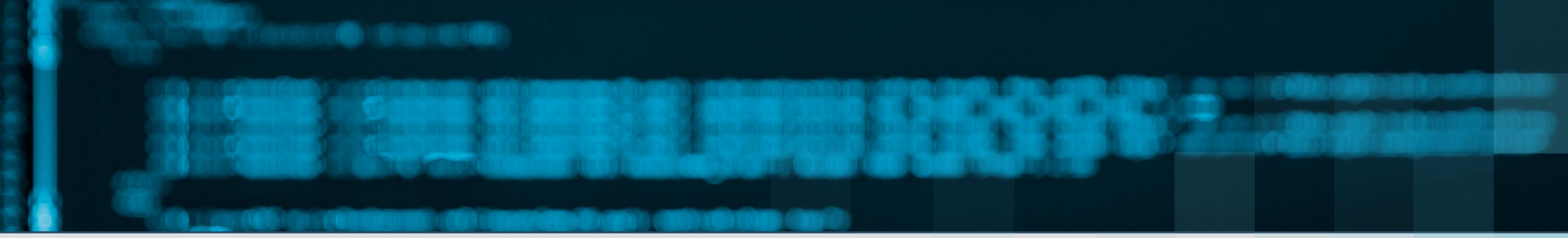
Using Threat Analytics to Protect Privileged Access and Prevent Breaches

ca technologies



Under Attack

Protecting privileged access and preventing breaches remains an urgent concern for companies of all sizes. Attackers are using a wider range of more sophisticated methods to infiltrate vulnerable systems. And although news of external breaches often dominates headlines, organizations must also be able to defend against insider threats.

In fact, given today's widespread use of outsourcing and partnering to support key functions, more users now have privileged access to critical business systems. Additionally, it's essential for today's system administrators to understand how systems are being used, who's using them and under what conditions.

Unfortunately, standard security solutions cannot secure internal/privileged access effectively and have serious gaps that put your organization at risk.

In recent years, well-publicized attacks at companies like J.P. Morgan, Anthem and Slack show that no industry is immune to the threat of external hackers. Yet, insiders like Edward Snowden, the U.S. National Security Agency analyst who leaked classified information, can be just as dangerous.

Static Controls Are Vulnerabilities

Like most organizations, you've deployed identity and access management tools over the years to support effective employee onboarding and provisioning of access and authentication capabilities.

Your goal has been to minimize privilege and ensure that people have the access they need and nothing more. But strict adherence to this principle can cause workflow issues that impede productivity. So, as a rule, users often receive wider access to enterprise systems and capabilities than they need.

Meanwhile, you're relying on your administrators to properly set up a set of access controls that are static, and you hope the attackers will not realize this. Because your administrators lack visibility into how systems are being used every day, they can't detect anomalies in user behaviors. That situation, combined with the expanded access granted to users, gives both external hackers and malicious insiders more pathways through which to exploit potential vulnerabilities.

Clearly, you need a better defense. But is it possible to secure your organization against both external and internal threats without causing undue friction? Let's take a look.

Many organizations have built an entire ecosystem to look for suspicious external behavior on the network or at exposed gateways—few are watching the actions of legitimate users.

A Model Use of Analytics

The credit card industry offers a great example of how organizations can effectively leverage analytics to strengthen their security posture. Credit card companies actively use analytics to monitor all transactions, flag unusual behavior, activate automated controls and reduce fraud.

Understanding the specific steps the credit card systems use to accomplish this are important. Specifically, they:

- Access the transactional data behind customer activities.
- Feed that data into the detection algorithm or model.
- Enable integrated mitigations that incur minimal friction on users, such as requiring cardholders to enter their zip code at the point of purchase.
- Support self-learning over time, so the system continually gets better at identifying and detecting new types of threats.

Enabling IT and data systems to benefit from this approach in a privileged access management (PAM) environment requires a multi-step process that hinges on the need to stay focused, enable insights, make informed decisions and mitigate risks.

Step 1: **Stay Focused**

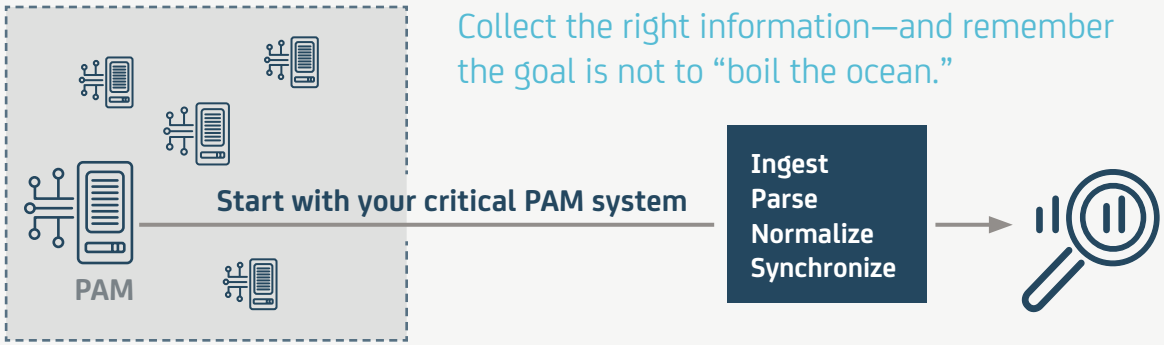
Adapting the credit card analytic model to your IT and PAM environment will immediately raise multiple questions:

- What's the right data to collect and can the machine understand it?
- And once you've determined which data to collect, what's the process for capturing it?

Collecting too much data will cause problems and make it harder for you to deploy an effective solution. For example, systems in place for security information and event management (SIEM) and big data are solutions that collect lots of data, but they're not well suited to deriving meaningful information about individual users and activities. Instead, they primarily provide a retrospective look at system threats.

Emulating the credit card model requires the ability to detect potential new threats in near real time and mitigate them quickly. In the end, you need to drive toward answering this question: "How do I detect high-risk privileged access activity and rapidly respond?"

Focusing clearly on data access activities and their context, such as the details of who's accessing your data, when and how, is essential to enabling threat analytics. Fortunately, all this information is visible to your PAM, so you don't have to engage in an endless integration project or sort through mountains of irrelevant data.



Collect the right information—and remember the goal is not to "boil the ocean."

Step 2: **Enable Insight**

Once you have access to the right data, you want to ensure that you can gain real insight from it. To do so, you need an analytics engine that can:

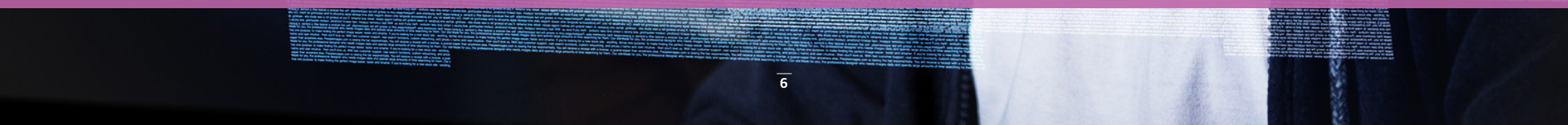
Extract essential "who, what, where, when and how" information for each transaction associated with an individual entity or identity.

Recognize characteristics about transactions so you can determine if they're common, first, frequent, only or new behaviors.

Learn by watching any changes or emerging patterns.

Store information in a meaningful way so that it can be quickly used and assessed.

With these capabilities, you'll be poised to act on insights that help you stop security threats in their tracks.



Value From an Entity and Relationship Graph

Your analytics model should provide the ability to automatically and easily map out characteristics about entities—such as users, devices, data repositories and access modes—and the relationships among them. In this way, your model will distill, over time, what a normal behavior looks like.

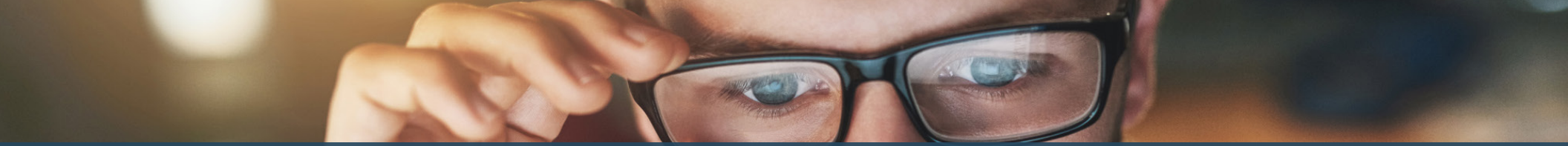
Through this approach, you'll benefit by knowing things like if it's normal for a user to access a particular server using a specified device and protocol—or whether that activity presents risks.

These entity relationships and characteristics provide the true power of analytics. They make it possible to understand behaviors observed over time—and quickly recognize what's truly unusual, risky and malicious.

ENTITY & RELATIONSHIP GRAPH

Track → Test → Inspect → Measure

Unlike threat analytics systems, SIEMs and firewalls don't have the ability to model and build the deep understanding of individual entities necessary to help proactively prevent fraud.



Step 3: **Make Informed Risk Decisions**

To apply the insights you've captured to reduce risk, you must be sure that your threat analytics system is flagging the right transactions.

It's not enough to flag activities that are simply different than past activities or slightly unusual. Flagging and alerting on minor changes will create an avalanche of false positives for you. What you're looking for and care about is activity that poses real risk.

That said, your threat analytics system needs to make risk decisions based on both recognizing when multiple factors change and the difference between a minor change that's common and one that's highly unusual or risky.

Consequently, you should avoid systems that either rely on specific predefined thresholds to recognize issues or trigger alerts. These systems fail to use analytics and create brittle defenses that attackers will quickly characterize and side-step. Look for systems that scan the entire user population and use information regarding which characteristics are trending or rare to assess risk.

A good threat analytics solution employs context to **enable the detection of true risk**.

Significant change?

Consistent with their own past behavior?

Current trends across user population?

Step 4: **Mitigate Risks Appropriately and Automatically**

Rapidly closing the door on attackers requires automated response capabilities. But different types of threats require mitigations that are appropriate, meaningful and effective. So what's the best way to handle these differences?

Insider Threat	External Threat
DON'T: Enable an automated mitigation that alerts the hostile insider.	**DON'T:** Worry about alerting the bad guy.
DO: Activate an invisible tracking mechanism, such as heightened logging or session recording, to collect enough data to act upon.	**DO:** Automatically initiate actions that slow or stop the attacker, such as triggering step-up authentication.

Automated responses are critical—but so is the ability to provide reporting. Being able to automatically generate reports when something is flagged as risky improves the speed and effectiveness of your company's response capabilities. Ideally, these reports will enable you and members of your compliance or incident response teams to quickly inspect both the context and full background associated with the suspicious user you're investigating.

Complement existing PAM and SIEM workflows.

You've made significant investments in your infrastructure—and your threat analytics solution should add value to those efforts. The work you do to enable threat analytics should enhance existing capabilities, such as your SIEM, security operations center (SOC) and incident response workflows. You can accomplish this by selecting a threat analytics solution that feeds new visibility into risk and analytic insights to your SIEM, so it can be used to improve your company's broader security posture.

Protect Privileged Access

As the threat landscape continues to evolve, you **need a practical and robust way to protect privileged access** in your enterprise. Analytics that detect new threats and automatically mitigate them are a great way to achieve this.

By following these four key steps as you build a PAM threat analytics solution, you'll be able to establish a more comprehensive and effective approach for addressing internal and external security threats.

FOUR KEY STEPS AS YOU BUILD A PAM THREAT ANALYTICS SOLUTION

1. **Stay focused:** Determine the data you need to collect in order to detect high-risk privileged access activity and rapidly respond to it.
2. **Enable insight:** Employ an analytics engine that can extract essential contextual data, recognize and assess different types of behavior, learn over time and store information for later use.
3. **Make informed risk decisions:** Avoid raising unnecessary flags through a system that can recognize when behaviors are highly unusual or risky.
4. **Mitigate risk appropriately and automatically:** Enable automated mitigations that are appropriate based on risk, so you can close the door on attackers.

For more information, see **CA Threat Analytics for PAM.**

For more information, see CA Threat Analytics for PAM.

CA Technologies (NASDAQ: CA) creates software that fuels transformation for companies and enables them to seize the opportunities of the application economy. Software is at the heart of every business, in every industry. From planning to development to management and security, CA is working with companies worldwide to change the way we live, transact and communicate—across mobile, private and public cloud, distributed and mainframe environments. Learn more at **ca.com**.

CS200-251836_0117