DATASHEET

Revolutionizing Privileged Access Management with Adaptive MFA

In today's rapidly evolving digital landscape, internal threat detection is more crucial than ever.

Protecting your organization's sensitive data and critical systems from unauthorized access is a top priority, and that's where Kron PAM comes in. Kron PAM's groundbreaking Adaptive Multi-Factor Authentication (MFA) module is designed to enhance your security by adding an extra layer of security. Our innovative solution recognizes users' keystroke behavior, creating a unique user profile that helps identify potential threats before they can cause damage.

The Importance of Adaptive MFA Enterprises

Adaptive MFA is a game-changer for enterprises looking to bolster their security posture. By implementing Kron PAM's Adaptive MFA module, organizations can:

Strengthen Internal Threat Detection

Adaptive MFA helps identify potential insider threats by detecting unusual typing behavior, reducing the risk of data breaches and unauthorized access.

Boost Compliance

Adaptive MFA helps organizations meet regulatory requirements and industry standards, such as GDPR, HIPAA, and PCI DSS, by providing an additional layer of security.

Enhance User Experience

With seamless integration of Kron PAM, user can enjoy a frictionless authentication process without compromising security. This enables user to access various resources and applications with ease and confidence.

Future-Proof Security

Kron PAM's Adaptive MFA module ensures that your organization stays ahead of the curve with this cutting-edge technology. This enables you to leverage the latest innovations in the field of identity management.

How the Adaptive MFA Works

Keystroke Behavior Analysis

Kron PAM's Adaptive MFA module analyzes users' typing patterns, such as speed, rhythm, and pressure, to create a personalized profile for each use.

Continuous Monitoring

The system continuously monitors users' typing behavior, comparing it to their established profile to detect any deviations from the norm.

Real-Time Verification

If a user's typing behavior differs significantly from their normal profile, Kron PAM's Adaptive MFA module triggers a multi-factor verification process to confirm the user's identity.

Key Benefits

Utilizes sophisticated machine learning algorithms to create a unique user profile based on individual typing patterns, enhancing security without compromising user experience.

Dynamically adjusts the level of authentication required based on user behavior, providing a balance between security and usability.

Designed to grow with your organization, Kron PAM's Adaptive MFA module can easily accommodate an expanding user base and evolving security needs.

Continuously tracks users' typing behavior, detecting deviations from their established profile and triggering multi-factor verification when necessary.

DATASHEET

AI-Powered Threat Analytics with Kron PAM

Protect Your Enterprise from Internal Threats

Safeguarding your organization from external threats is Enterprises crucial, but it's equally important to address the risks posed by insiders.

With the ever-evolving landscape of cyber threats, it's time to take your Privileged Access Management (PAM) to the next level. Introducing Threat Analytics for Kron PAM, a powerful feature designed to detect and mitigate internal threats in real-time using advanced machine learning algorithms.keystroke behavior, creating a unique user profile that helps identify potential threats before they can cause damage.

The Importance of Threat Analytics for Enterprises

!

Proactive Security

Threat Analytics enables your organization to proactively detect and respond to potential insider threats before they can cause significant damage.

Compliance and Auditing

By continuously monitoring user activity, Threat Analytics helps your organization maintain compliance with industry regulations and simplifies the auditing process.

Enhanced Visibility

Gain a deeper understanding of user behavior patterns, allowing you to identify potential areas of risk and implement targeted security measures.

Reduced Response Time

Automated actions based on risk scores ensure that potential threats are addressed quickly, minimizing the potential impact on your organization.

How Threat Analytics Works

?

User Behavior Analytics

AI-Powered Threat Analytics utilizes machine learning algorithms to analyze user' session logs and create a comprehensive user behavior profile. Threat Analytics enables the system to establish a baseline of normal activity for each user individually.

Continuous Monitoring

Kron PAM continuously monitors user activity, comparing it to the established behavior profiles. This allows for real-time detection of any anomalies, such as abnormal session start and end times, unusual executed commands, or unusual connected target devices.

Risk Scoring

When an anomaly detected, AI-Powered Threat Analytics calculates a user risk score based on the severity of the deviation from the baseline behavior. This enables security professionals to prioritize their responses, focusing resources and efforts on addressing the most critical risks first.

Automated Actions

Depending on the user's risk score, AI Powered Threat Analytics can automatically take actions such as blocking the user, logging them out, or generating alerts for further investigation. This ensures that your organization maintains a high level of security and compliance.

Key Benefits

✓

Utilizes cutting-edge machine learning algorithms to analyze user behavior and detect anomalies in real-time

Continuously monitors user activity, providing up-to-date insights and rapid response to potential threats.

Calculates user risk scores based on the severity of deviations from baseline behavior, allowing for prioritized threat management.

Takes automatic actions such as blocking users, logging them out, or generating alerts based on risk scores, ensuring a swift response to potential threats.