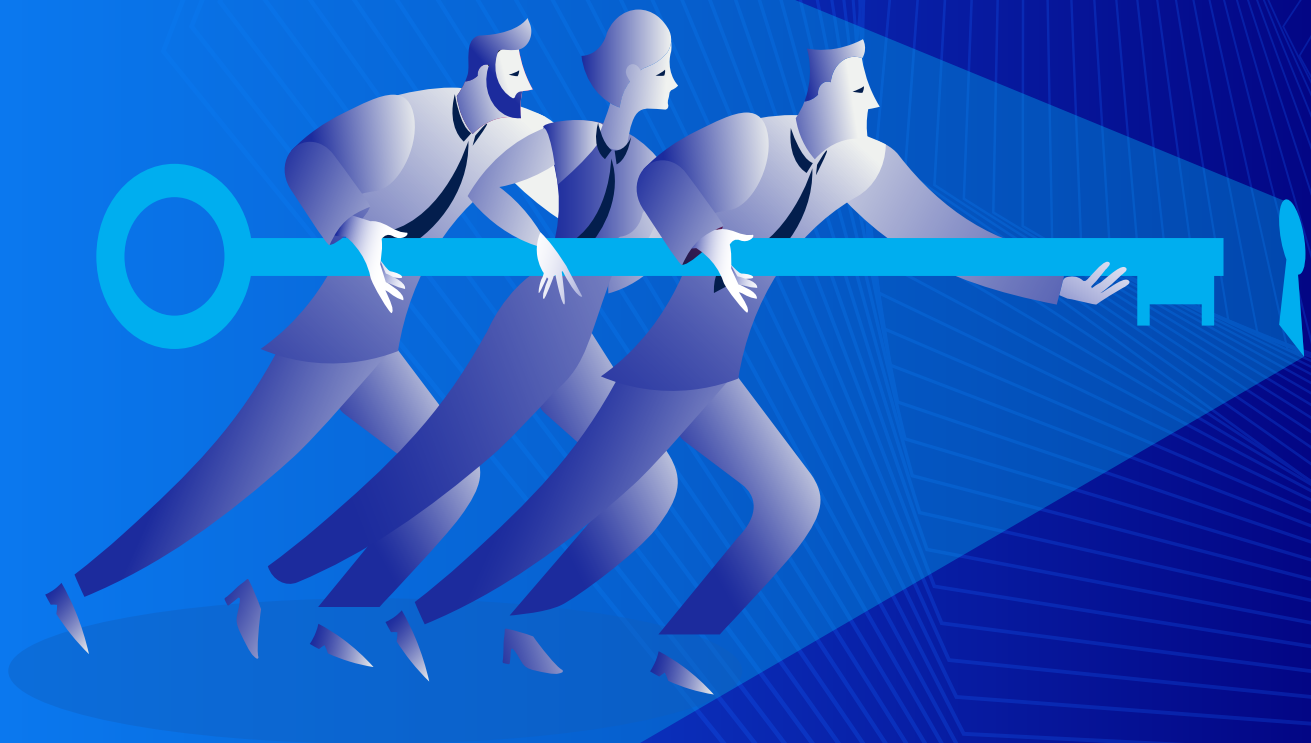
Kron TECHNOLOGIES

WHITE PAPER

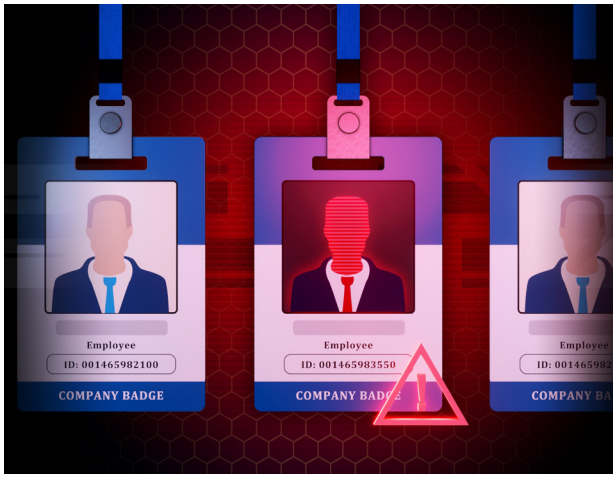
# MITIGATING
# Insider Threats with PAM



WHITE PAPER

# TABLE OF CONTENTS

Insider threats pose a significant cybersecurity risk for organizations today. According to the 2023 Insider Threat Report published by Cybersecurity Insiders, a staggering 74% of organizations are vulnerable to insider threats. These threats can originate from employees, contractors or other insiders who have authorized access to an organization's systems and data.




Insider threats can be malicious in nature, such as an employee stealing confidential data to sell tocompetitors. But they can also stem from careless or accidental behavior, like falling victim to a phishing scam and exposing login credentials. Regardless of intent, insider threats can lead to data breaches, loss of intellectual property, reputational damage, and financial losses.

Mitigating insider threats presents unique challenges. Unlike external hackers, insider threats involve people who already have trusted access built into their roles. Traditional perimeter defenses like firewalls are not effective against insiders. Organizations need visibility into how users are accessing data and systems, and the ability to control that access.

Privileged Access Management (PAM) solutions provide capabilities to help organizations manage insider risk. PAM allows organizations to secure, control and monitor access to critical assets and high-value data. By reducing excess access rights, enforcing multifactor authentication, monitoring activity, and setting up alerts for anomalous behavior, PAM limits the insider threat landscape.

This white paper provides guidance and best practices for using PAM technologies and strategies to mitigate insider threats. It outlines the types of insider threats, the risks they pose, and how implementing a comprehensive PAM program can help reduce organizational exposure. Case studies and recent statistics help illustrate the importance of addressing the human element in cybersecurity.

# Section 1: Understanding Insider Threats

Insider threats refer to risks posed by individuals within an organization who have authorized access to systems, networks or data. Employees, contractors, business partners and third-party vendors with inside access can potentially abuse their privileges, either maliciously or unintentionally.

According to the "2022 Cost of Insider Threats Global Report" by the Ponemon Institute, the average overall expense resulting from incidents caused by internal threats is $15.4. This indicates a 34% surge in internal threat costs compared to 2020 and a 75% escalation compared to 2018.

## There are three main types of insider threats:

### Malicious insiders

These actors deliberately steal data, sabotage systems, or commit fraud for personal gain or to harm the organization. Motivations may include financial gain, revenge, competitive advantage, or ideology.

### Accidental insiders

Well-meaning insiders who make mistakes or are careless with security policies and procedures. Examples include falling victim to phishing scams, misconfiguring access controls, or mishandling sensitive data.

### Negligent insiders

Insiders who disregard security best practices through apathy, laziness, or ignorance. This might involve using weak passwords, installing unauthorized software, or sharing their credentials.

As per IBM's "2023 Data Breach Report", the average duration to detect and manage data breaches caused by stolen or compromised credentials was approximately 11 months (equivalent to 328 days), while breaches triggered by an internal malicious actor took around 10 months (or 308 days) to be resolved.

## The significant risks posed by insider threats encompass:

Data Theft and Intellectual Property Leakage: This includes the unauthorized access or sharing of sensitive information, customer data, or proprietary trade secrets..

Disruption of Systems and Business Operations: Insiders may attempt to manipulate or sabotage organizational systems, leading to disruptions in normal business operations.

Reputation Damage and Eroded Customer Trust: Following a breach, an organization's reputation can suffer, and customer trust can be eroded, resulting in long-term consequences.

Financial Fraud: Insiders might orchestrate financial fraud through illicit transactions or embezzlement, causing monetary losses.

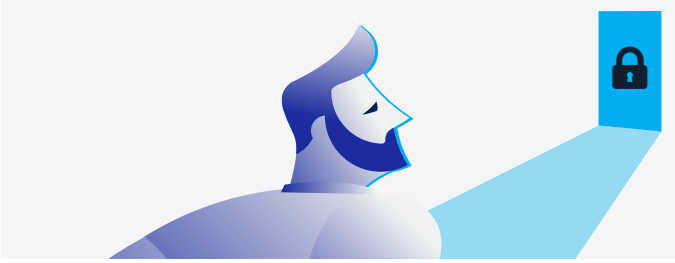
Physical Asset Theft: Insider threats can extend to the physical realm, including the theft of equipment, supplies, or inventory.

Given the potential for extensive damage, security teams prioritize mitigating insider threats. To achieve this, a multi-layered defense approach is crucial. This approach combines both technological controls and well-defined policies, working in tandem to minimize organizational risk.

In conclusion, comprehending and addressing insider threats is paramount for safeguarding an organization's assets, reputation, and operations. By recognizing the various categories of insiders and the potential risks they pose, organizations can tailor their security strategies to mitigate these threats effectively. Through a combination of robust technological measures and clear-cut policies, businesses can enhance their resilience against malicious, accidental, and negligent insider actions. As the landscape of cybersecurity continues to evolve, staying vigilant and proactive in countering insider threats remains an ongoing imperative for modern organizations.

# Section 2: The Role of Privileged Access Management (PAM)

PAM refers to the processes and tools used to secure, control, and monitor access to privileged accounts, systems, and data within an organization. Privileged access refers to extended levels of access beyond what regular users have, such as administrator, root, or service accounts.



**PAM solutions enable organizations to:**

- Establish least privilege access - Grant users only the bare minimum privileges needed to perform their work. This limits damage from malicious insiders or compromised accounts.

- Enforce strong access controls - Require approval and justification to gain privileged access. Place permissions expiry dates.

- Implement multifactor authentication (MFA) - Require an additional factor like an OTP code before granting privileged access. This prevents access with compromised credentials.

- Monitor activity - Record sessions and log actions taken during privileged access for auditing. Critical actions may require additional verification.

- Rotate credentials - Automatically reset passwords for privileged accounts on a frequent basis. This reduces the risk of stolen credentials.

- Manage secrets - Securely store and control access to passwords, keys, certificates in an encrypted vault.

- Detect anomalies - Use analytics like unusual access time, unfamiliar source IP, or abnormal resource access to detect potential threats.

- Alert on risks - Get notified of potential misuse of privileged accounts for prompt investigation. For example, alert on multiple failed login attempts.

Effective PAM takes a layered approach combining policies, access controls, monitoring, and automation. Benefits include reduced risk of insider threats, faster breach detection, simplified audits, and meeting compliance requirements. Ongoing reviews help prune unnecessary access while training improves security hygiene.

# Section 3: Best Practices for Insider Threat Mitigation With PAM


Conduct reviews of user access and rectify excessive authorizations- Routinely examine permissions and privileges to ensure that individuals only possess appropriate access according to their designated roles. Withdraw any redundant permissions.

Adhere to principles of minimal privilege - Furnish users with only the least amount of access imperative for executing their authorized responsibilities. Constrain privileges based on their job tasks.

Activate multi-factor authentication (MFA) - Demand an additional validating factor, like a singular token, prior to granting entry to sensitive data and systems.

Capture, oversee, and scrutinize system activity - Document user sessions, transactions, and additional actions to uncover questionable or unauthorized behavior.

Be vigilant for indications of discontent among personnel - Keep a close watch on individuals exhibiting unsettling demeanor, as they might have an escalated likelihood of engaging in malicious conduct.

Thoroughly scrutinize third-party entities-Meticulously assess external associates and suppliers requiring internal access in order to fortify protection against breaches originating from external sources.

Isolate sensitive data and environments - Partition and rigorously control entry to systems housing intellectual property, client information, and other imperative assets.

Apply encryption to data both at rest and in motion - Thwart unauthorized internal parties from pilfering data by executing robust encryption measures.

Deliver training on cybersecurity awareness - Educate end users on optimal strategies for managing credentials, fortifying email security, countering social engineering, and more.

Develop strategies for responding to incidents - Draft comprehensive schemes and protocols for promptly identifying and addressing potential threats arising from within the organization.

Instantaneously deactivate access for departing personnel - Rapidly rescind system access when employees depart from the company to avert actions stemming from dissatisfaction.

# Section 4: Building a Comprehensive PAM Program

**Secure executive approval** - Develop a compelling argument for leadership buy-in regarding the advantages of Privileged Access Management (PAM) in mitigating cyber threats and achieving compliance objectives.

**Engage relevant stakeholders** - Incorporate insights from multiple departments such as Information Technology, Security, Legal, Human Resources, Finance, and other pertinent units when crafting the strategy.

**Evaluate your requirements** - Perform an analysis of essential resources, systems, data, and potential vulnerabilities to clearly define the scope and prerequisites of the PAM initiative.

**Formulate comprehensive guidelines and protocols** - Create well-documented protocols covering aspects like access governance, monitoring, control, alert mechanisms, and response measures.

**Exercise prudence in tool selection** - Conduct a thorough assessment of available PAM solutions, aligning their capabilities with your specific needs and environment. Strike a balance between functionalities and intricacy.

**Implement phased deployments** - Adopt a gradual approach to deploying PAM controls, seamlessly integrating them with your existing IT infrastructure.

**Embrace process automation** - Leverage the workflow automation capacities of PAM tools for streamlining password administration, access requests, and provisioning processes.

**Provide effective training** - Educate both end users and administrators on updated policies, new roles, responsibilities, and the utilization of PAM resources.

**Monitor and encourage adoption** - Scrutinize adherence to policies, monitor key performance indicators of the program, and make necessary adjustments. Ensure transparency in dealing with any identified workarounds.

**Regularly assess access privileges** - Continuously evaluate roles, permissions, and entitlements to eliminate unnecessary access rights.

**Conduct incident readiness drills** - Organize simulated scenarios to enhance incident response readiness related to PAM, refining the program's incident management capabilities.

# Conclusion

In summary, the dangers posed by individuals with internal access bring forth notable vulnerabilities that may result in unauthorized data exposure, intellectual property misappropriation, deceptive activities, and disturbances in operations. All establishments necessitate intricate layers of defense to counteract the potential harmful exploitation of privileged rights, irrespective of whether it stemsfrom deliberate malice, carelessness, or inadvertence.

Privileged Access Management (PAM) solutions offer indispensable functionalities to establish safeguards, exercise command, and oversee privileged credentials and admittance. The deployment of the principle of least privilege, the utilization of multi-element authentication, vigilant supervision of activities, and other measures within the scope of PAM serve to diminish the potential avenues for internal hazards.

The formulation of an efficient approach to contend with internal threats entails the amalgamation of personnel, methodologies, and technological mechanisms. PAM utilities empower entities to enforce exacting boundaries on access, procure insight into the trends of access, and promptly pinpoint possible deviations or irregularities. Nevertheless, the utilization of PAM software in isolation proves insufficient. Establishments must also cultivate a climate that prioritizes security, provide persistent education, institute robust protocols, and engage stakeholders spanning the spectrum of enterprise activities.

By merging robust bedrock principles of security with suitable PAM technologies and protocols, corporations can enhance the fortification of their information, intellectual property, and essential infrastructure against internal vulnerabilities. PAM stands as a pivotal fragment of the larger mosaic that addresses the mitigation of threats originating from within.