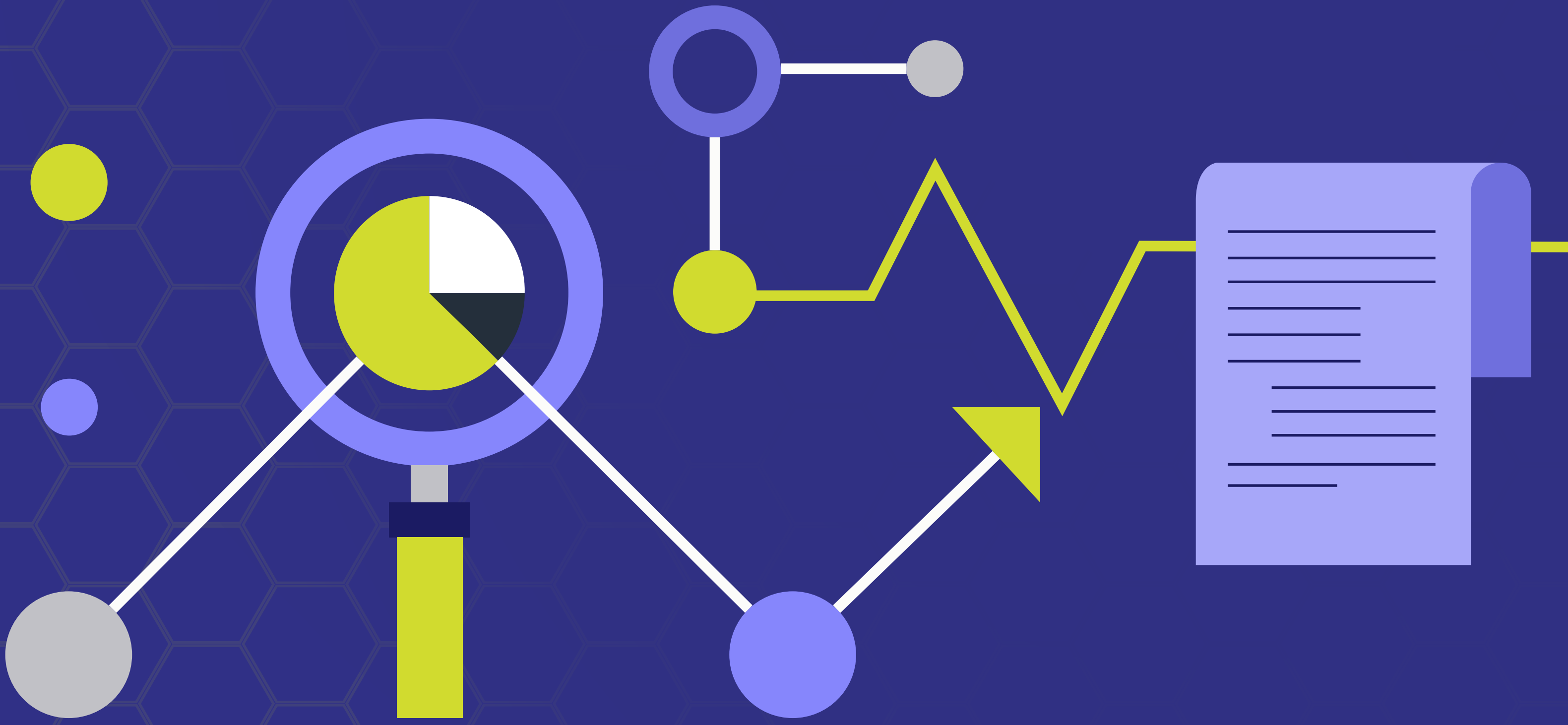
ManageEngine
PAM360

The business case for privileged access management

- Erin Casteel



www.manageengine.com/pam360

The business case for privileged access management

In 2020, the COVID-19 pandemic activated a global transition to remote work. Organizations that had been prioritizing a fortress approach to cybersecurity suddenly found themselves at a significantly higher risk and were scrambling to adjust. This recent transition, the increased threat to Internet of Things (IoT) devices, and the ever-increasing focus on digital transformation has accelerated the evolution in cybersecurity from perimeter-based security to the Zero Trust model.

With perimeter-based security, firewalls provide the first line of defence in almost every network. Today, with so many users and data sources in an increasingly complex environment, the move to a Zero Trust model means that rather than assuming a level of trust for users and devices within the firewall, organizations must authenticate every request coming in for access to a specific data source. A Zero Trust model also necessitates the use of multi-factor authentication to ensure that every user has legitimate access to the data in question. For a Zero Trust model to work, it's essential for organizations to have mature identity and access management (IAM) practices in place.

IAM is about defining and managing the roles and access privileges of individual users, systems, and devices across a variety of cloud and on-premises applications. Users can include employees, customers, and partners, so it's essential to have clarity about what access each user requires, to what data, and how that data will be used.

Effective management of risks also requires organizations to know which users and what data need to be prioritized based on the impact to the organization if compromised. These are business decisions based on the organization's risk profile.

Focus on managing privileged access

What is a privileged account?

Consider any account with access to monetizable data (protected health information, credit card numbers, Social Security numbers, or other personal identity information) as a privileged account. There are also privileged user accounts, which have administrative-level access to one or more systems, allowing these users to make configuration changes to devices.

Essentially, privileged accounts are prime targets, because these accounts have access to valuable data. This is why Forrester estimates that 80% of data breaches have a connection to compromised privileged credentials. Control of privileged accounts is also a major factor in compliance across all regulations in every industry.

Privileged access management (PAM) is a life cycle approach that can significantly improve the organization's risk posture. A key reason is that PAM is based on the principle of least privilege. This is the idea that all users should have access only to the information and systems they need to perform their job functions, regardless of job title or position in the organization's hierarchy. By following the least privilege approach, organizations can minimize the danger of insider and external threats, which can result in expensive data breaches. Privileged access can even be granted for a restricted period of time, such as a few hours or days.

PAM provides organizations with many key benefits:

- A reduced cyberattack surface protects against both internal and external threats. Limiting privileges for people, processes, and applications diminishes the opportunities for those privileges to be exploited.

- A good PAM solution creates a clear record of who accesses what and when, improving incident detection and resolution along with compliance.

- Many varieties of malware require elevated privileges to install or execute malicious activities. Removing excessive privileges using least privilege enforcement can reduce the threat of malware.

- By limiting the privileged activities that can possibly be performed, PAM helps create a less complex and more audit-friendly environment.

- Many compliance regulations (including HIPAA, PCI DSS, FDDC, FISMA, and SOX) require that organizations apply least privilege access policies to ensure proper data stewardship and improved systems security.

The risks and challenges of not having a mature PAM practice in place include:

- **Accumulation and over-provisioning of privileges:** Traditionally, IT aims to prevent an organization's access controls from being overly restrictive, because they can hinder productivity and frustrate users. Organizations have tried to address this by provisioning users with fewer restrictions to privileges, allowing more access to more users than is necessary. As an employee's role changes over time, they accumulate new responsibilities and corresponding privileges while often still retaining access from previous roles.

- **Lack of visibility or accurate, up-to-date information about users, accounts, assets, and credentials:** Without strict maintenance of privileged accounts, the number of these accounts can accumulate over time and provide dangerous backdoors for attackers, including former employees who have left the organization but retained access.

- Inability to effectively and efficiently detect and mitigate data breaches.

The costs of data breaches

PAM is considered by many industry analysts and technologists to be essential to reducing cyberrisk through limiting the organization's cyberattack surface, and has been found to achieve a high return on investment for organizations that have implemented it. The 2020 Cost of a Data Breach Report by the Ponemon Institute estimates that the average total cost of a data breach today is $3.86 million, although it found that these costs were much lower for some of the most mature companies and industries and much higher for organizations with less maturity and capability in areas such as security automation and incident response processes.

Additionally, having a remote workforce was found to increase the average total cost of a data breach by nearly $137,000 for an adjusted average total cost of $4 million. The study found that compromised credentials were the costliest and most frequent threat vector for data breaches.

The 2020 Cost of a Data Breach Report also found that the effectiveness of security automation in reducing the average cost of a data breach has continued to grow. Businesses that had not yet deployed security automation saw an average total cost of $6.03 million—more than double the average cost of a data breach of $2.45 million for businesses that had deployed security automation.

Another key finding was that the average time to detect and contain a data breach was 280 days while the average amount of time to contain a data breach caused by a malicious attack was 315 days. The average savings of containing a breach in under 200 days compared to over 200 days was $1.12 million.

This means that organizations with a mature PAM practice have significantly lower costs from data breaches, use less time and effort to contain a breach, and avoid longer-term adverse impacts on the organization, including loss of business and non-compliance with regulations. This information is vital when building a strong business case for PAM.

Why is a strong business case important?

Getting support for and approval of your PAM initiative is critical, both to receive the necessary funding and resources and to make it a priority in your organization.

Establishing or optimizing a PAM practice will encompass multiple changes impacting technology, people, and processes. A strong business case sets the right expectations and justifies the appropriate scope.

It's essential that an organization and its stakeholders—from executive management to employees and IT security staff—understand the purpose and the priority of PAM and how it can address the organization's business risks.

The business case should clarify these points and ensure justification for sufficient funding to not only implement technical solutions and automation, but for the ongoing resources to manage, run, and continually improve the PAM practice.

When determining return on investment and total cost of ownership for the PAM solution and establishing and managing the PAM practice, the following should be considered:

- The estimated impact of data breaches on revenue, costs, reputation, and organizational productivity. This estimate need not be comprehensive—even an indicative estimate can make a powerful statement.
- The benefits of a PAM program, including improved product and service delivery, faster time to market, and competitive advantages.
- The risk and costs of non-compliance.
- The value of mature IAM to support increased agility and resilience in our digital age.

Choosing a robust technical solution to support PAM is critical. The more automated and mature a PAM implementation, the more effective an organization will be in reducing its cyberattack surface, mitigating the impact of attacks, enhancing operational performance, and reducing organizational risk.

The business case must also clarify that the PAM practice will require people with the right skills, whether these are internal to the organization or provided as a service through a third party. PAM also needs an adaptable strategy that can evolve with the changing needs and priorities of the organization, ongoing operational management, and continual optimization aligned with business priorities and the organization's information security management system.

Organizations that have been less successful with PAM initiatives over the last few years have likely implemented it as a siloed program, defined it as a purely technical solution, or given it the wrong scope.

IoT and privileged access

It's also important to consider that privileged access is not just for humans, but also for systems. IoT-connected devices are increasingly prevalent and can pose a significant risk to all types and sizes of organizations without privileged access controls in place. However, these devices can often slip under the radar without the same security controls that protect the rest of the organizational network. For example, industrial control systems may be maintained for 10 to 15 years before being replaced or updated. Attackers know this and are increasingly exploiting the weaker security associated with IoT devices to compromise them and use them as launching platforms to gain unauthorized access to network systems.

The increase in IoT devices leads to a larger network of devices that can create a target-rich environment for hackers. Having a strong PAM solution that can not only efficiently regulate access to these devices but also rapidly monitor and detect anomalies in device access and usage patterns will help prevent compromise. PAM will address the IoT machine-to-machine connectivity issue. If a device is not recognized, it will not be allowed to access the network, system, or any information. It'll become much easier to identify a breach or unauthorized access in real-time and lock systems down quickly.

Organizational integration

IAM has become increasingly essential since remote working and other aspects of digital transformation have made physical boundaries irrelevant. More organizations today are giving users outside the organization greater access to their internal systems. IAM now facilitates customer acquisition, management, and retention—its importance will only continue to increase over time. As organizations improve their maturity and capability in managing identity and access, they'll also increase velocity, customer satisfaction, and value realization. On the other side of the coin, organizations that don't embrace these changes will find themselves at a disadvantage and may not be able to compete.

In order to be truly effective, an organization's IAM practices must also be connected with all parts of the business, including integration with analytics, business intelligence, customer and partner portals, and marketing solutions. This integration will not happen all at once, but the organization's strategy should consider how and over what time period it will evolve.

Conclusion

Organizations that prioritize mature PAM capabilities as part of their larger cybersecurity strategy can experience a number of organizational benefits. These include improved understanding and management of security risks along with reducing the overall cyberattack surface, reducing operational costs and complexity, enhancing visibility of vulnerabilities, gaining situational awareness across the enterprise, and improving regulatory compliance.

Many organizations follow a similar path to a mature PAM practice, prioritizing easy wins and the biggest risks first, and then incrementally improving privileged security controls across the enterprise. However, the optimal approach for any organization will be best determined after performing a comprehensive audit of privileged access risks, mapping out the steps it will take to get to an ideal state, and building a strong business case for PAM.

About the author:

Erin Casteel is a strategic advisor, governance and management system expert, and business architect, helping organizations transform and thrive at velocity in the digital age. She works with organizations to design, implement, run, and improve organizational governance and management systems, cybersecurity, and agile service management to create and preserve value.

Erin is a lead architect and author of ITIL 4® and an editor of/contributor to a number of international (ISO) management system standards, including the ISO/IEC 27000 family of standards for information security management.

www.manageengine.com/pam360

4141 Hacienda Drive Pleasanton,
CA 94588, USA
US +1 888 204 3539
UK : +44 (20) 35647890
Australia : +61 2 80662898
www.manageengine.com/pam360

ManageEngine
PAM360