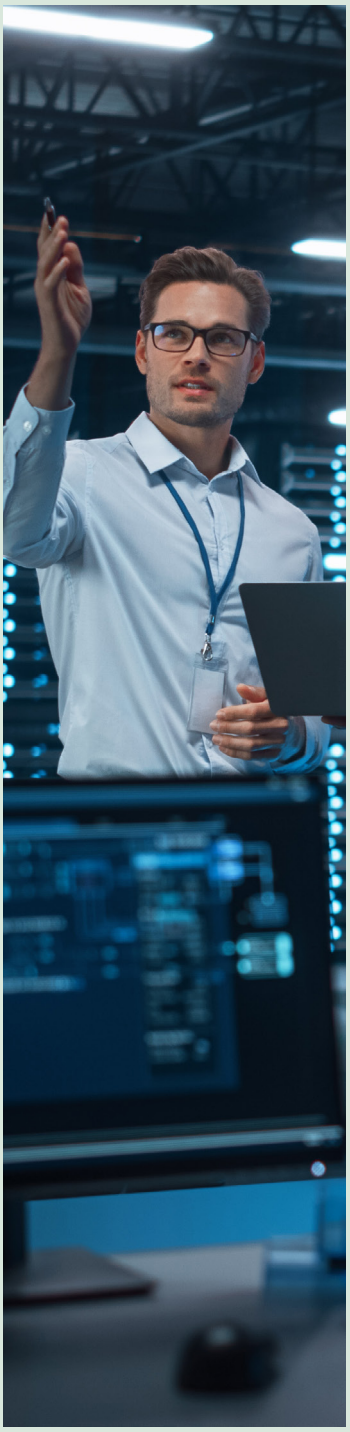
WHITE PAPER



ELEVATING SAAS SECURITY WITH PROACTIVE POSTURE MANAGEMENT

Abstract

The increasing dependency on Software-as-a-Service (SaaS) solutions for organizational productivity and innovation has rendered the security of these cloud environments. Traditional security measures have failed to address the evolving threats faced by SaaS platforms, thereby exposing organizations to data breaches, configuration errors, and regulatory challenges.

This whitepaper delves into the transition to proactive SaaS Security Posture Management (SSPM) - a forward-thinking strategy that enables organizations to detect, assess, and neutralize risks before they intensify. Through enhanced visibility, ongoing oversight, and automated corrective actions, proactive SSPM builds a strong and flexible security system that's ready for the future.

Infosys®
Navigate your next

Trends related to using SaaS applications

SaaS adoption has seen exponential growth as businesses seek scalable, cost-effective, and flexible software solutions. Organizations across industries are increasingly shifting from on-premises systems to cloud-based applications to improve productivity and collaboration. This trend is fueled by the upsurge of remote work, digital transformation initiatives, and ease of deployment.

80% of employees admit to using SaaS applications in their job without seeking authorization from their IT department, leading to various security risks and compliance failures.

52% of respondents believe SaaS providers are responsible for checking and maintaining cloud security, while businesses must research their SaaS service provider's policies on data security and compliance before signing up.

When it comes to SaaS app usage, the average employee is using 29 different applications.

Companies with over 1,000 employees use more than 150 SaaS applications on average, which increases the potential for security risks.

Overview

Many businesses use SaaS applications like Microsoft 365, Salesforce, and Workday to manage important tasks such as sales, communication, and collaboration. These applications store, process, and transmit sensitive data, including customer information, employee details, and more.

As a result, these applications have become a critical part of a company's IT infrastructure. However, security teams often struggle to keep up with the rapid growth of these applications and the sensitive data they handle. This creates a challenge for businesses to protect their critical data and applications

Key Challenges in Securing SaaS Platforms

The below figure depicts the main cybersecurity risks with using SaaS applications include a lack of awareness about the shared responsibility model, which can leave security gaps and increase the risk of breaches. Multiple third-party contractors and vendors, along with shadow IT make it harder to manage security across the organization. Weak access controls, insecure APIs, and misconfigurations also create more ways for attackers. Additionally, poor monitoring and data privacy practices can lead to undetected incidents and serious data loss.

Enterprise Awareness around Shared Responsibility

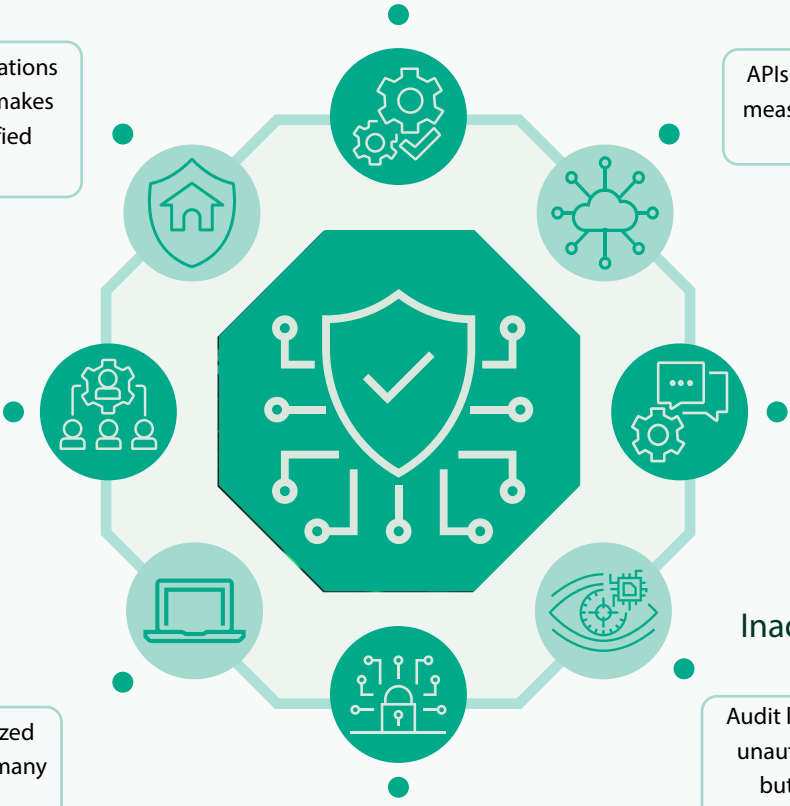
Enterprises may overlook critical security tasks, increasing the risk of data breaches and compliance failures.

Fragmented Platforms and Applications

SaaS often consist of multiple applications & service of various vendors which makes it challenging to implement a unified security approach.

Insecure APIs

APIs that lack proper security measures can be exploited by attackers.



Inadequate Access Controls

Weak authentication and authorization processes can lead to unauthorized access to sensitive data.

Increasing Misconfigurations

Organizations adopt more SaaS applications; misconfigurations are becoming a leading cause of security vulnerabilities.

Rise of Shadow IT

Where employees use unauthorized SaaS applications, is prevalent in many organizations.

Inadequate monitoring and logging

Audit logs are essential for detecting unauthorized or malicious activity, but many organizations fail to implement or check them in time to discover threats.

Data Privacy & Data Leakage Risks

Organizations must check if their SaaS providers follow compliance rules and handle data properly, because the risk of data loss is higher in SaaS environments.

Fig. Key Challenges in Securing SaaS Platforms

Enterprise Awareness around Shared Responsibility:

If enterprises are not aware of the SaaS responsibility model, they might assume SaaS provider/Vendor handle all their security and compliance needs. This can lead to critical gaps, such as misconfigured settings or unprotected data, which attackers can exploit.

Insecure APIs:

Insecure APIs in SaaS platforms pose a significant security risk, as they can be exploited by attackers to access sensitive data. Unsecured or poorly configured APIs can lead to data breaches, unauthorized access, and other security threats.

Misconfigurations in SaaS platforms:

Misconfigurations are increasing due to the complexity and constant evolution of cloud-based services. Manual configuration and lack of visibility into SaaS settings exacerbate the issue, making it challenging for security teams to detect and remediate misconfigurations.

Inadequate monitoring and logging:

Inadequate monitoring makes it harder for security teams to find and fix security problems. Audit logs are crucial for identifying unauthorized or malicious activities within systems, serving as a key tool for security teams to detect potential threats. However, many organizations often overlook the importance of implementing these logs or fail to review them in a timely manner

Data Privacy and Compliance Challenges:

This is a top concern since SaaS platforms handle sensitive data. Regulations like GDPR, HIPAA, and CCPA impose strict data protection requirements, which can be difficult to meet.

Data leakage risks:

This risk arises where sensitive information is exposed or stolen unintentionally. Data leakage can happen through user error, misconfigured settings, or malicious intent. This can lead to financial loss, reputational damage, and regulatory penalties.

The rise of Shadow IT:

When employees use unauthorized SaaS applications, it poses a significant security risk. These unauthorized apps can introduce malware, data breaches, and compliance issues, going unnoticed by IT teams

Inadequate access controls:

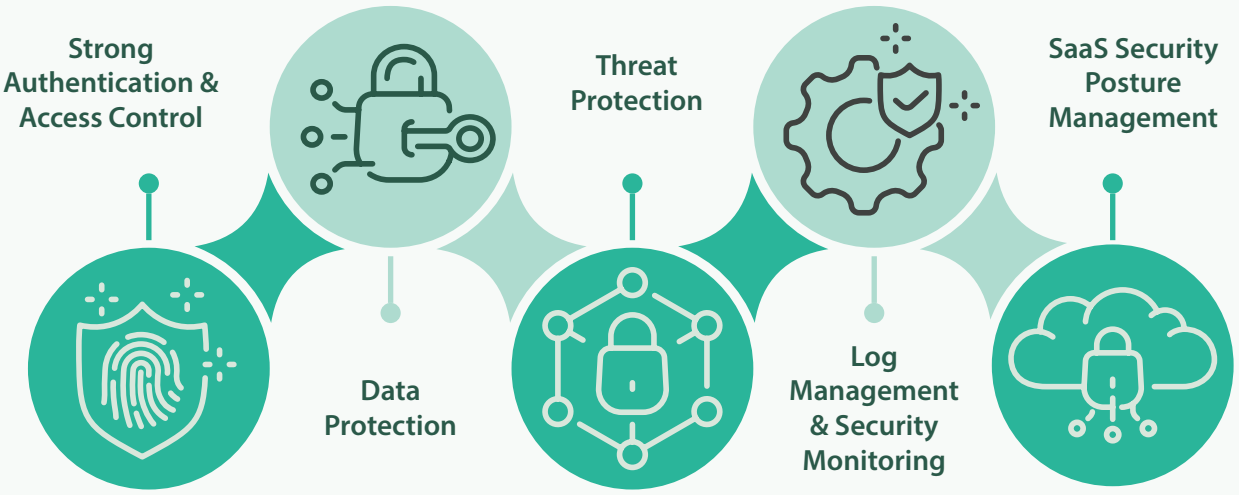
Inadequate access controls in SaaS platforms can lead to unauthorized access to sensitive data. Weak authentication and authorization processes make it easy for hackers to gain access, compromising data security.

Fragmented Platforms and Applications:

Since SaaS platforms typically consist of multiple applications and services sourced from different vendors, they contribute to a fragmented security landscape. This heterogeneity makes it challenging to implement a unified security approach, and as a result organizations struggle to maintain consistent security controls and policies across their SaaS ecosystem.

Pillars for Securing SaaS Environment

Securing a SaaS environment relies on the key pillars, which starts from strong authentication and access control, like Multi-Factor Authentication ensures only authorized users access data; Data Protection secures information at rest and in transit through encryption, audit trails, and enforces privacy rules to prevent data loss and reduce breach risks; Threat protection detects and blocks cyberattacks in real-time; and Log management with security monitoring provide visibility to spot and respond to risks quickly. In the end, SaaS Security Posture Management (SSPM) continuously checks configurations and compliance to reduce vulnerabilities.



A. Strong Authentication & Access Control

I. Authentication and Single Sign-On (SSO) protect SaaS applications by ensuring that only authorized users can access company data and resources. Strong authentication methods like MFA make it hard for attackers to break in. SSO streamlines access by letting users sign-in once to use multiple apps which helps in reducing password fatigue and minimizing security risks from weak or reused passwords. Centralized management with SSO allows security teams to monitor, control, and quickly revoke user access when required. Together, these tools strengthen security, improve compliance, and offer better user experience in SaaS environments.

II. Least Privilege Access: Implementing the principle of least privilege means giving users only the access and permissions they need to do their jobs. This reduces the risk of data breaches by limiting the areas that can be attacked. By restricting access to sensitive data and systems, organizations can prevent unauthorized access, stop attackers from moving laterally within the network, and prevent them from gaining higher levels of access.

III. Conditional Access & MFA: Conditional access policies along with MFA secure SaaS applications by allowing organizations to set rules on when and how users can access data, such as requiring trusted devices or blocking risky locations. When paired with Multi-Factor Authentication (MFA), users must provide additional proof of identity when certain conditions are met, like logging in from a new device. This approach stops most unauthorized access, even if a password is stolen. Conditional access and MFA together ensure security without inconvenience to the users, as extra verification is only required in higher-risk situations. They provide stronger and enhanced protection for SaaS environments.

IV. Regular User Reviews: Regularly reviewing user access ensures that access rights are current and match the changing roles, responsibilities, and business needs. This process helps identify and eliminate unnecessary access, which reduces the risk of insider threats, data breaches, and unauthorized changes to sensitive data and systems.

B. Data Protection

I. Data Encryption at Rest and in Transit: Ensuring that SaaS provider encrypts data both when it is stored and when it is being transmitted adds a vital layer of security. Encryption converts sensitive information into an unreadable format, making it useless to hackers even if they intercept or steal it. This protects the integrity and confidentiality of the data, thereby safeguarding it from unauthorized access.

II. Data Classification: Data classification involves categorizing data based on its sensitivity, such as personally identifiable information (PII), financial data, or intellectual property (IP), to determine the level of protection required. By applying restrictions based on data classification, organizations can ensure that only authorized users with a legitimate need-to-know can access sensitive data, thus minimizing the risk of data breaches and unauthorized disclosure.

III. Data Loss Prevention (DLP): Implementing data access controls block unauthorized access to sensitive information, preventing malicious activities like unauthorized uploads, downloads, and sharing. This also protects against insider threats and accidental data leaks. Advanced monitoring tools track data usage in real-time, detecting and alerting suspicious activities, such as unusual login attempts or large data transfers; allowing for quick action to address potential security incidents.

C. Threat Protection

Threat Protection is vital for SaaS security, defending applications against threats like malware, phishing, and account takeovers. It continuously monitors SaaS activity to detect and block suspicious behavior in real time, thus preventing the breaches. Cloud Access Security Brokers (CASBs) play a key role by identifying and stopping threats - including malware and data exfiltration, across all connected cloud services

D. Log Management & Security Monitoring

I. **Log Management:** Gathers logs from SaaS applications, and captures security events, system activities, and user behavior. Examines logs to identify potential security threats, anomalies, and trends, providing valuable insights into SaaS application usage and security. Triggers alerts and notifications for suspicious activity, enabling swift incident response and minimizing the risk of security breaches.

II. **Security Monitoring:** Continuously monitors SaaS applications to detect security threats, vulnerabilities, and suspicious activity in real-time. Identifies potential security threats, including malware infections, phishing attempts, and unauthorized access attempts, to prevent security breaches and protect sensitive data.

E. SaaS Security Posture Management (SSPM)

Provides a complete view of potential risks, allows for the enforcement of security policies, and ensures compliance with regulatory requirements, all of which helps to maintain a strong security posture. The activities include:

- Identifying and mitigating security risks within SaaS applications
- Monitoring for misconfigurations and vulnerabilities
- Enforcing security policies and controls
- Protecting sensitive data
- Ensuring compliance with industry standards and regulations

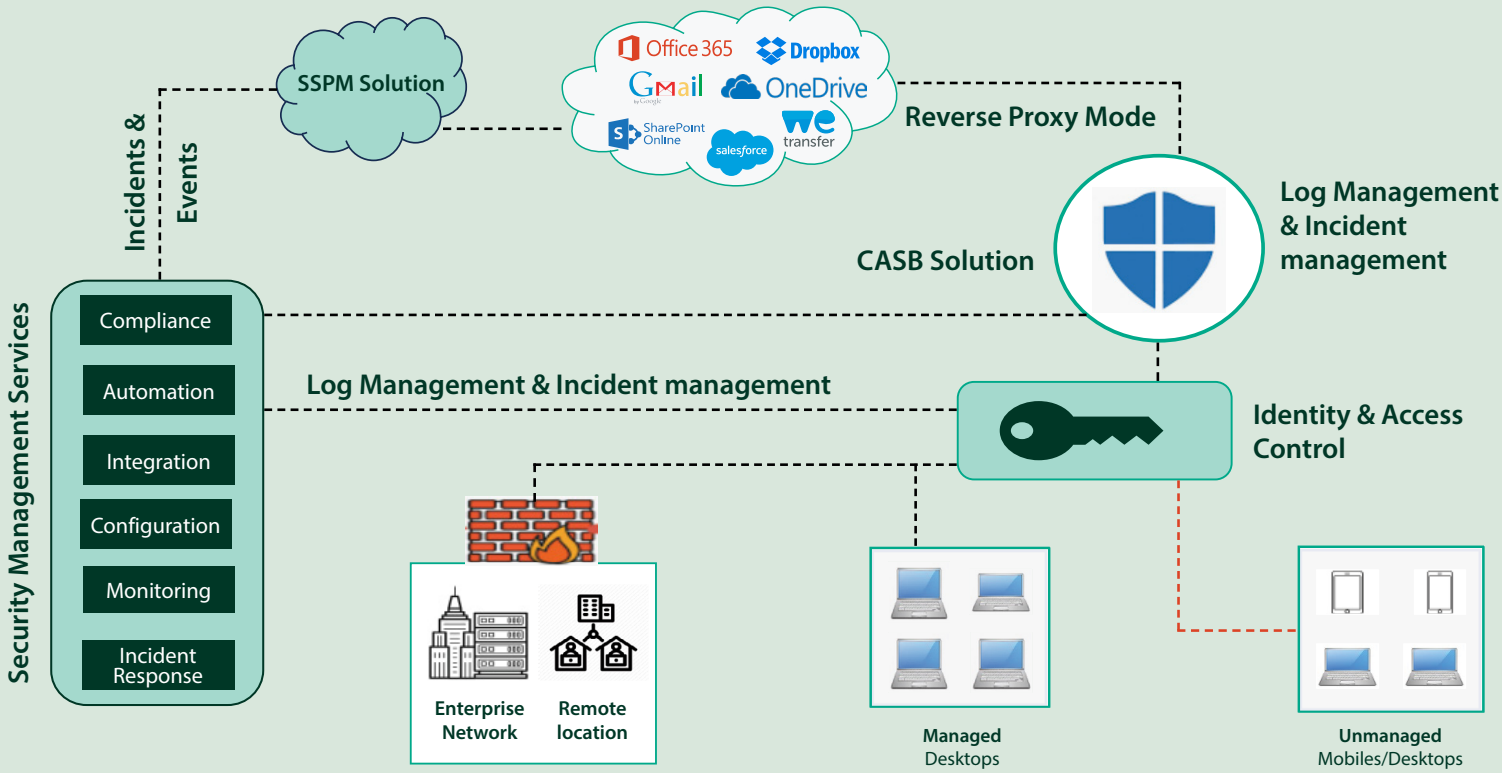


Fig. SaaS Security Reference Architecture

Best practices

As the organizations depend more on SaaS applications, securing them is essential to prevent data breaches, unauthorized access and compliance issues. By following security best practices, organizations can protect their data and adhere applicable regulations for SaaS.level of protection required. By applying restrictions based on data classification, organizations can ensure that only authorized users

1. **Inventory All SaaS Applications:** Conduct a thorough discovery process to identify all SaaS tools in use, including shadow IT (unapproved apps). Use tools like CASB (Cloud Access Security Broker) or SSPM (SaaS Security Posture Management) solutions.

2. **Monitor User Access:** Track who has access to what applications, including third-party integrations and permissions levels.

3. **Assess Configurations:** Regularly audit app configurations to ensure they align with security benchmarks (e.g., CIS benchmarks).

4. **Enforce Multi-Factor Authentication (MFA):** Mandate MFA across all SaaS platforms to reduce the risk of credential-based attacks.

5. **Adopt Single Sign-On (SSO):** Centralize authentication to streamline access management and reduce password fatigue.

6. **Least Privilege Principle:** Grant users and apps only the permissions they need for their roles and review access rights regularly.

7. **Continuous Configuration Monitoring:** Use SSPM tools to detect misconfigurations (e.g., overly permissive sharing settings, disabled encryption) in real time.

8. **Automated Remediation:** Set up automated workflows to fix common issues like public file-sharing links or unused accounts, wherever possible.

9. **Baseline Standards:** Establish and enforce security baselines tailored to each SaaS app (e.g., Salesforce, Microsoft 365, Slack).

10. **Classify Sensitive Data:** Identify and tag sensitive information (e.g., PII, financial data) stored in SaaS apps.

11. **Enable Encryption:** Ensure data is encrypted both at rest and in transit, leveraging native SaaS encryption features or third-party solutions.

12. **Data Loss Prevention (DLP):** Deploy DLP policies to monitor and prevent unauthorized data exfiltration.

13. **Integrate with SIEM:** Feed SaaS logs into a Security Information and Event Management (SIEM) system for centralized monitoring and correlation.

14. **Conduct Risk Assessments:** Perform periodic reviews of your SaaS stack to identify vulnerabilities and compliance gaps (e.g., GDPR, HIPAA).

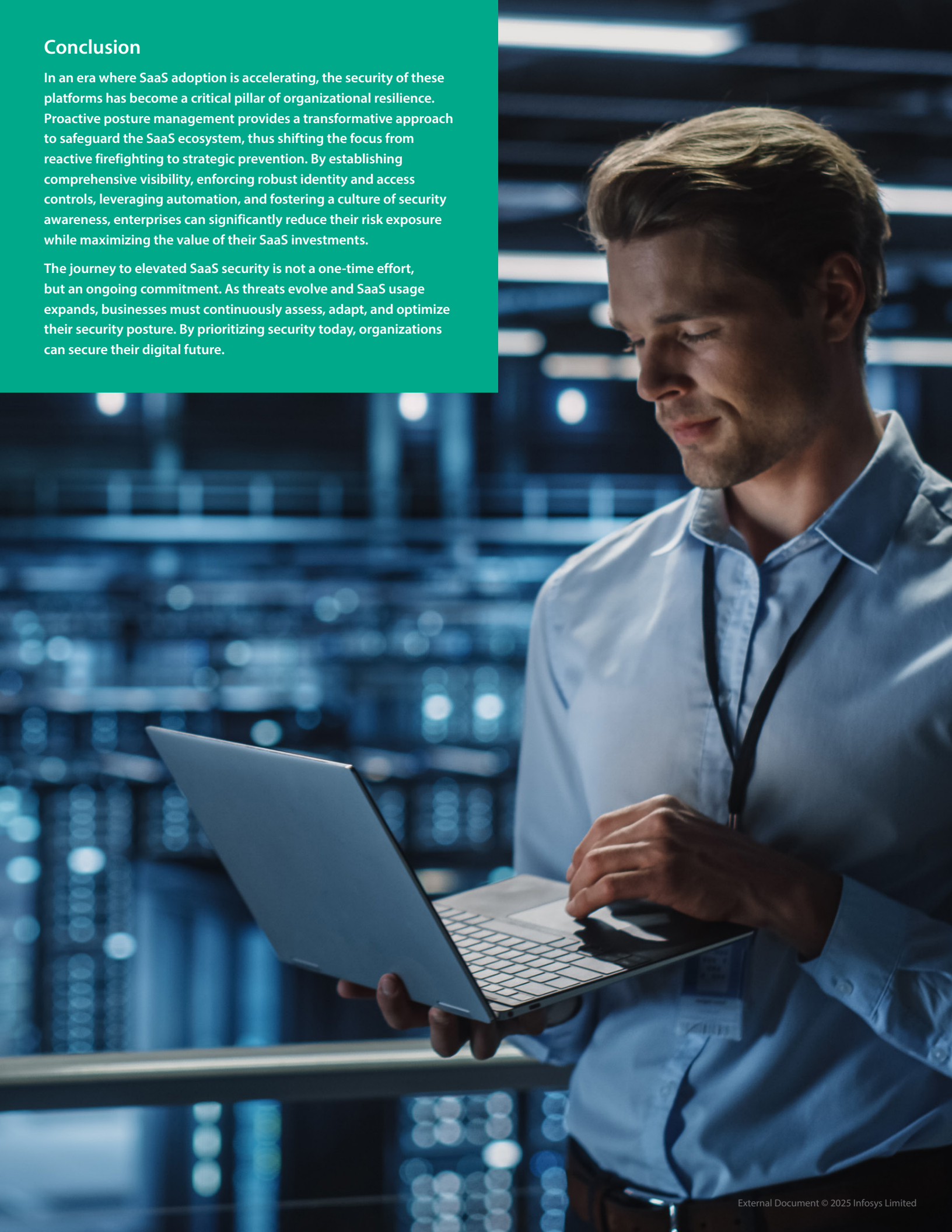
15. **Vendor Risk Management:** Evaluate the security practices of SaaS providers, including their SOC 2 reports or ISO certifications.

16. **Backup and Recovery:** Test data backups and restoration processes regularly to ensure resilience against ransomware or data loss.

Conclusion

In an era where SaaS adoption is accelerating, the security of these platforms has become a critical pillar of organizational resilience. Proactive posture management provides a transformative approach to safeguard the SaaS ecosystem, thus shifting the focus from reactive firefighting to strategic prevention. By establishing comprehensive visibility, enforcing robust identity and access controls, leveraging automation, and fostering a culture of security awareness, enterprises can significantly reduce their risk exposure while maximizing the value of their SaaS investments.

The journey to elevated SaaS security is not a one-time effort, but an ongoing commitment. As threats evolve and SaaS usage expands, businesses must continuously assess, adapt, and optimize their security posture. By prioritizing security today, organizations can secure their digital future.



References

- https://www.cloudflare.com/en-gb/learning/cloud/what-is-sspm/
- https://martech.org/new-blissfully-report-most-companies-have-orphaned-saas-apps-in-their-stacks/
- https://chiefmartec.com/2020/04/saas-adoption-trends-start-2020/
- https://wing.security/
- https://www.wiz.io/

About the Author

Saurabh Sharma

Principal Consultant

Saurabh Sharma is a Cyber Security Consultant at Infosys, and a part of the Cyber Consulting and Advisory Team. With 15 years of experience, he focuses on cutting-edge cybersecurity solutions, excels in consulting, assessing, and implementing Data Protection and Infrastructure Security Solutions, and brings deep expertise in OT and Cloud Security.

For more information, contact askus@infosys.com

Infosys®
Navigate your next