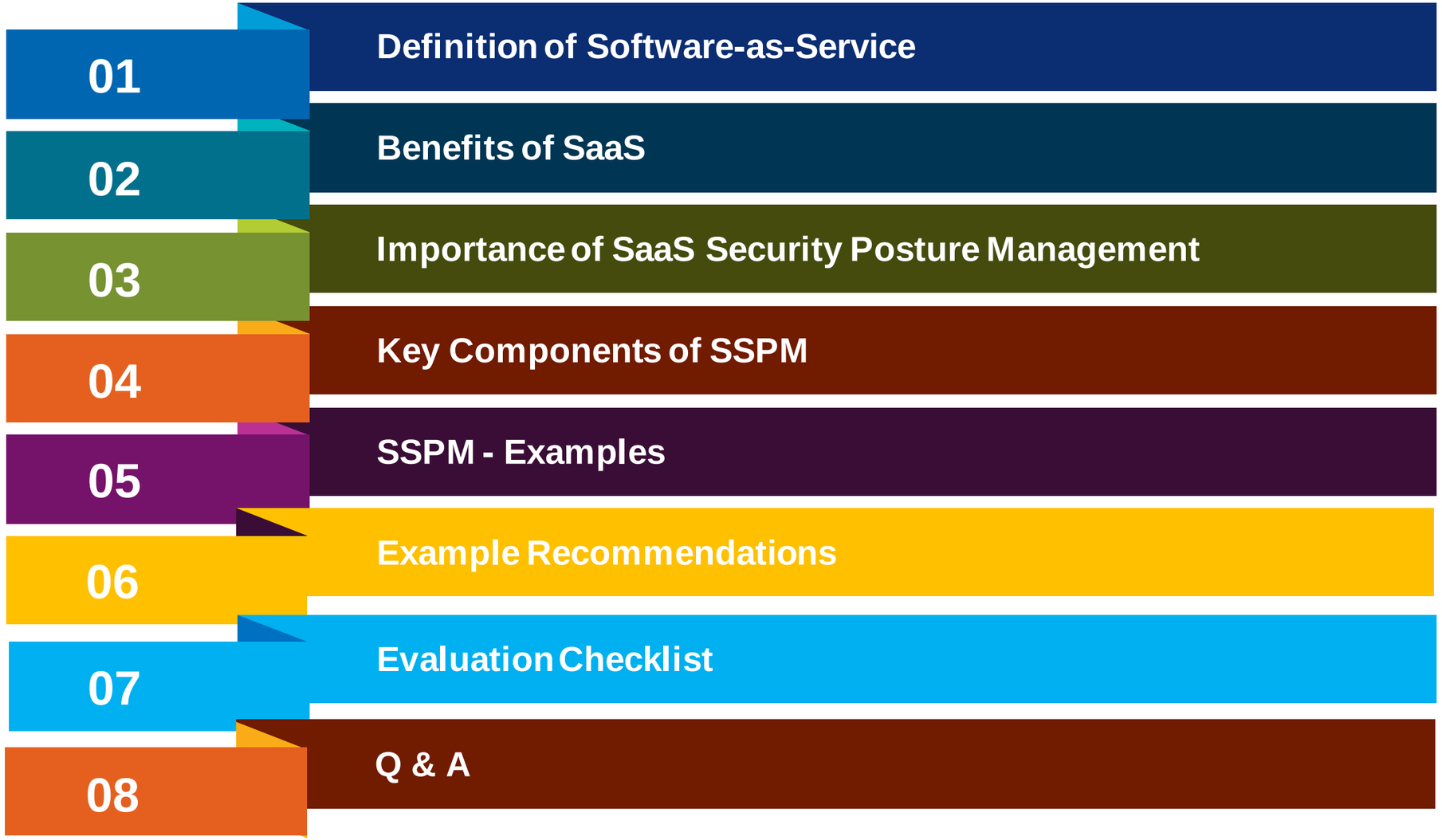
Gaining insights into SaaS vendor risk with Security Posture Management Solutions

Ashish P. Shah
Chevron
Team Lead – Information Risk & Strategy Management - IT Cybersecurity Engineering & Innovation

"Third-Party Risk Madness" Conference
Third Party Risk Association (TPRA)
April 9-12, 2024

Presentation Agenda



Software as a Service (SaaS)

Problem Statement

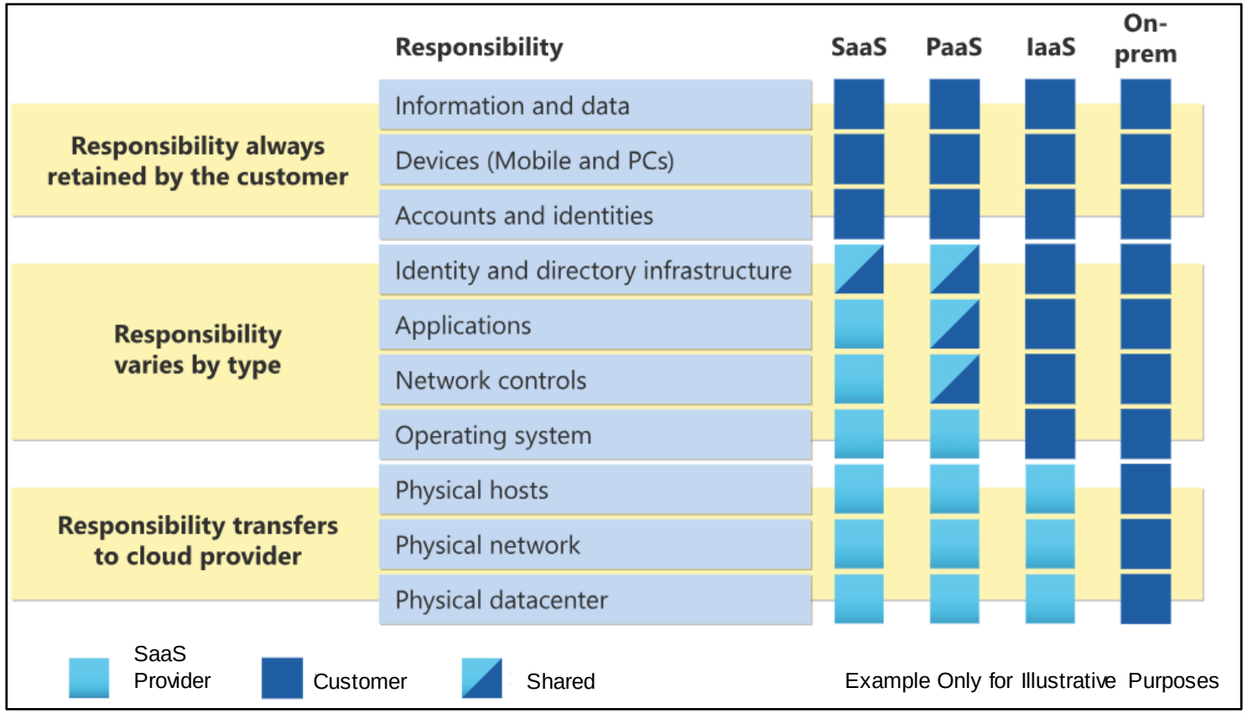
- Sensitive data at risk in SaaS environment
- Lack of visibility for day-to-day management of apps
- Organizations are at risk of sensitive data exposure within SaaS environment due to lack of visibility for day-to-day management

Software as a Service (SaaS) Definition

- In the simplest terms, SaaS solutions reside outside of an organization's technical environment and are accessed via the internet. The vendor provides and manages the application, platform and infrastructure.
- Software as a Service (SaaS) is one of three cloud computing service delivery models. The figure on the right, describes how SaaS compares to PaaS and IaaS.

Common SaaS Solutions

- Microsoft Office 365 (for example: Teams, Outlook, SharePoint, PowerPoint and Word), ServiceNow and Workday are all enterprise examples of Software as a Service solutions

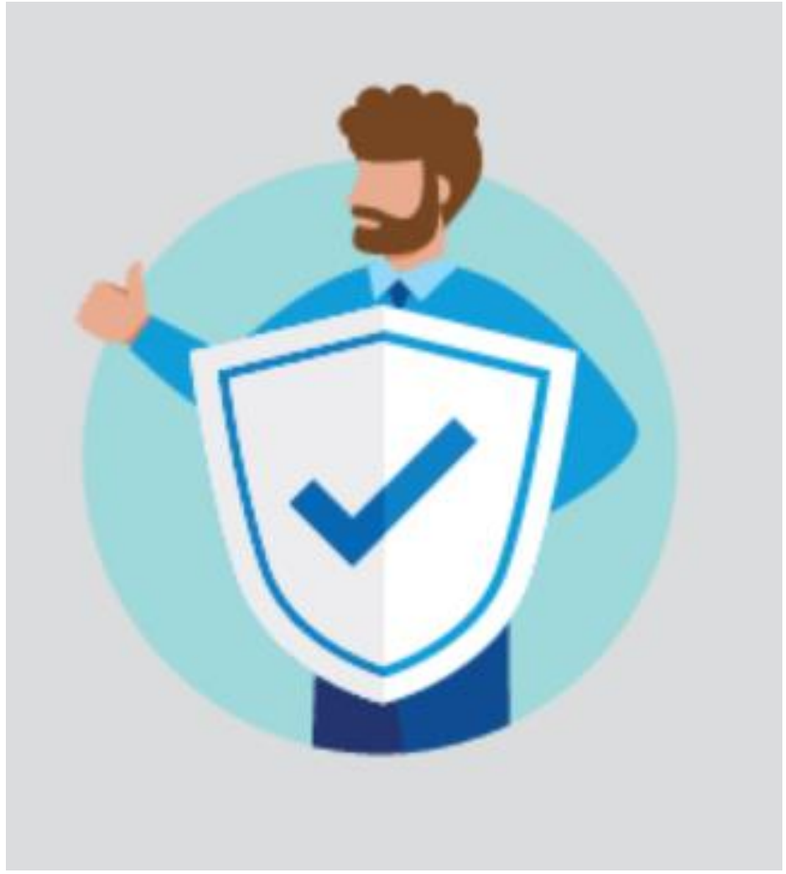


Detailed technical industry SaaS definitions are bulleted below:

- Definition of SaaS - IT Glossary | Gartner
- Software as a Service (SaaS) - Glossary | CSRC (nist.gov)

Benefits of SaaS

SaaS empowers organizations with:



- Reduced time to benefit
- Lower costs
- Accessibility from Anywhere
- Scalability
- Automatic Updates

Importance of Software-as-a-Service Security Posture Management (SSPM)

SSPM is a term created by Gartner in 2019 to describe an emerging set of tools, designed to help organizations gain visibility into the risk and maintain the security of their SaaS applications and services.

Rapid proliferation of SaaS environments increases an organization's exposure to attack vectors for applications accessed and used over the internet.

Traditional security practices leaves organizations blind to activity within applications and presenting a target rich environment for attackers.

Essential for enterprises to have robust SSPM practices in place to ensure the security and integrity of their data and systems.

Misconfigurations in SaaS environment exposes organizations to cyber threats such as data breaches, malware attacks, and unauthorized access to sensitive data.

SSPM is a critical component of an organization's overall security posture, helping to protect against potential threats, automating compliance and ensuring the continued operation and integrity of SaaS applications.

Key Components of SSPM

- **SSPM helps organizations maintain a secure SaaS environment through the following:**

- Assessment & Visibility
- Remediation & Mitigation
- Risk Identification
- Compliance & Auditing
- Continuous Monitoring
- Integration with CASB

SSPM – Examples

SaaS Security Posture Management plays a crucial role in preventing data breaches, misconfigurations, and unauthorized access in SaaS environments. By proactively monitoring and enforcing security best practices, organizations can enhance their overall security posture and protect critical data.

Data Leakage

CRM Platform: In 2021, a CRM platform, experienced a data leak where sensitive customer data was exposed due to misconfigurations.

Mitigation: SSPM solution that is implemented effectively would continuously monitor SaaS vendor configurations, detect misconfigurations, and enforce secure settings. This could have prevented the data leak by identifying and rectifying the misconfigured access controls.

Account Credential Takeover

Global Technology Provider: Cybercriminals gained unauthorized access to identity accounts through phishing attacks, weak credentials and exploiting MFA.

Mitigation: SSPM tools can enforce least-privileged access controls, monitor user permissions, and detect suspicious activities. By proactively managing access, organizations can prevent unauthorized takeovers.

API Token Exposure

Collaboration Platform: Tokens (used for integration) were exposed in public repositories on the internet, leading to unauthorized access to collaboration workspaces.

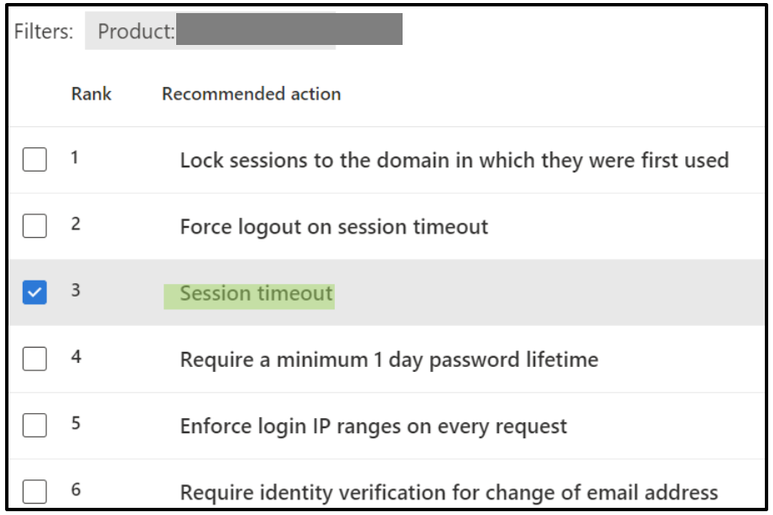
Mitigation: SSPM tools can scan for exposed tokens, enforce secure token management practices, and provide visibility into risky integrations. Proper monitoring and remediation can prevent such incidents.

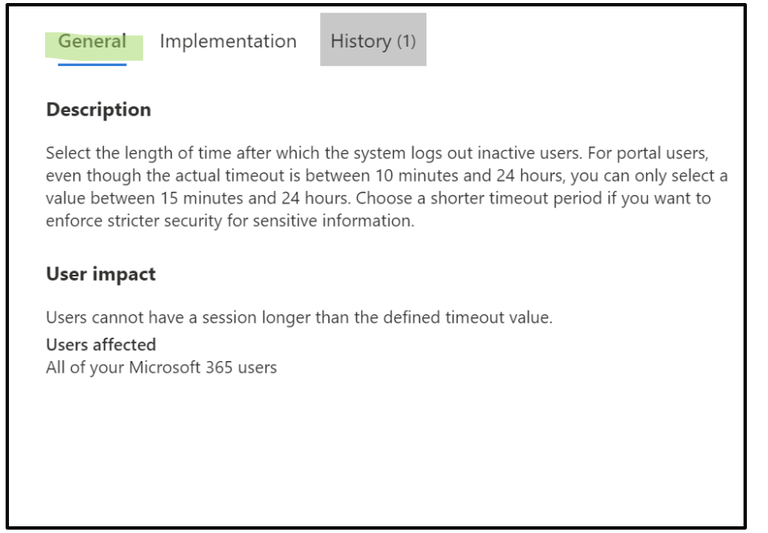
Privacy & Security Issues

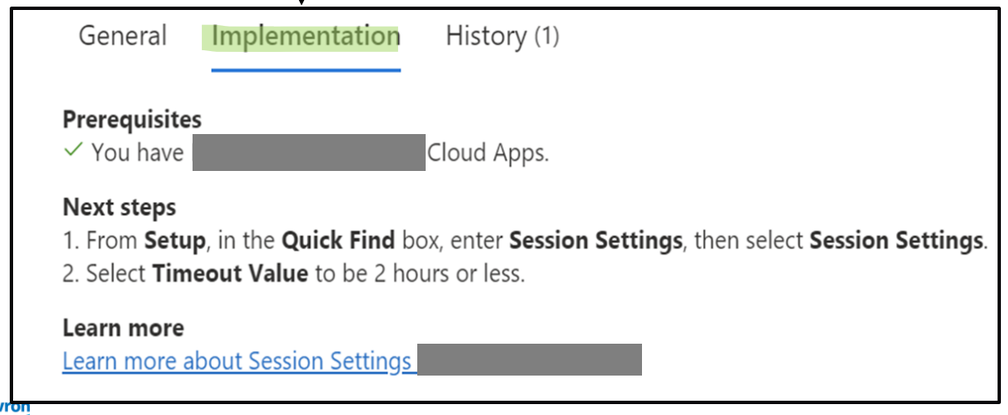
Web Meeting Platform: Technology faced privacy and security challenges during the surge in remote work. Issues included uninvited guests in meetings and data leaks.

Mitigation: SSPM solutions could have assessed platform's security posture, identified vulnerabilities, and enforced secure settings. This would improve privacy controls and reduce the risk of unauthorized access.

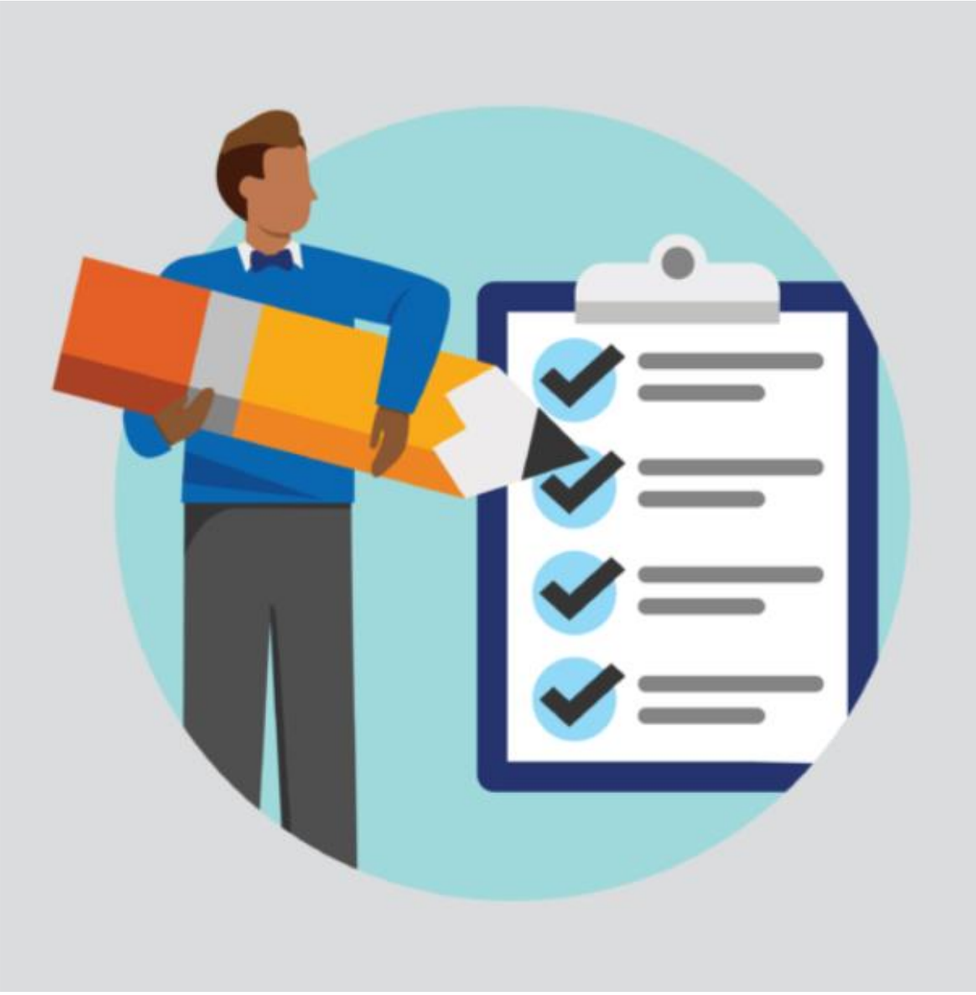
SSPM - Example Recommendations







SSPM Evaluation Checklist



- Ensure wide range of coverage across critical SaaS apps
- Provides visibility into SaaS apps being used across organization, including Shadow IT
- Security Posture Assessment – risk identification, misconfiguration, vulnerability identification, and remediation recommendations
- Integration with other Security Tools – Cloud Access Security Broker (CASB), Extended Threat Detection & Response (XDR)
- Data Protection & Compliance with applicable Regulations
- Capability to monitor SaaS to SaaS app access
- Ease of Deployment & Management

Q&A


the
human
energy
company®
Chevron