TAG

SHARED CYBERSECURITY MODEL FOR MODERN ENTERPRISE SAAS DEPLOYMENTS

DR. EDWARD AMOROSO, CEO, TAG
RESEARCH PROFESSOR, NYU

RUSS SPITLER, CO-FOUNDER, CEO, NUDGE SECURITY

nudge

SHARED CYBERSECURITY MODEL FOR MODERN ENTERPRISE SAAS DEPLOYMENTS

DR. EDWARD AMOROSO, CEO, TAG[1] ,
RESEARCH PROFESSOR, NYU[2]
RUSS SPITLER, CO-FOUNDER, CEO, NUDGE SECURITY[3]

A shared cybersecurity model is presented for enterprise SaaS deployments using the Nudge Security platform to illustrate the concepts for practical application. The model is developed on four pillars of enterprise security including data and access, configurations, integrations, and identities and accounts. The responsibilities for each pillar are described in the context of the SaaS user, SaaS administrator, and enterprise security team.

INTRODUCTION:

For the past several decades, security protection of applications usually involved direct integration of any desired controls into software that was deployed onto operating systems running in data center-hosted servers. This monolithic approach was reasonably effective at dealing with threats, but it no longer applies to modern enterprise deployment of Software-as-a-Service (SaaS) applications running in hybrid cloud environments.

A challenge now emerges with application ownership and support shifting away from a single group, usually part of the enterprise information technology (IT) team. This group previously had full responsibility for the application, the operating system, and the underlying hardware. In contrast, modern applications are now generally SaaS-delivered and hosted across a hybrid mesh of heterogeneous environments, often delivered by different commercial providers.

In this report, we propose a new model for handling security responsibilities in this hybrid SaaS arrangement. It is a shared cybersecurity framework inspired by similar models for cloud such as from the Cloud Security Alliance (CSA).[4] The shared model presented here will be shown to apply to modern enterprise teams using SaaS applications and will be illustrated using the commercial platform solution from cybersecurity vendor Nudge Security.[5]

FOUR PILLARS OF SaaS SECURITY

Our industry certainly is at no loss for frameworks offering guidance on security prevention, detection, response, and governance. NIST, for example, publishes its Cybersecurity Framework (CSF 2.0) as well as a myriad of different Special Publications. These reports provide excellent guidance on how enterprise teams can reduce cyber risk, but like all government publications, they often lag current issues, usually by design, since standardization should follow innovation.

As a result, we view the transition of enterprise toward use of SaaS applications as demanding immediate guidance for practitioners. To illustrate the need, popular frameworks such as NIST 800-53 barely reference SaaS applications by name. Certainly, NIST offers related guidance such as SP 800-145 which covers SaaS, PaaS, and IaaS in a broad sense. Given the central role that SaaS plays in the enterprise, we choose to offer more focused assistance here.

The first step in establishing guidance is that a set of foundational pillars is needed – and these must reflect the actual manner in which SaaS applications introduce risk to the enterprise. Based on experience at Nudge Security deploying a platform that addresses SaaS security risk, as well as day-to-day work at TAG with many dozens of CISO-led teams working in this area, we present the following as a suitable set of foundational pillars for the proposed model:

- **Data and Access** – The challenge of controlling access to data through policies and controls is key to ensuring secure SaaS usage. Given the types of sensitive data that are commonly stored in SaaS applications today, it should be no surprise that significant cyber risks might be present.
- **Configurations** – Voiding misconfigurations in SaaS deployments is a key security objective. The underlying infrastructure is a lesser concern given the shared nature of SaaS deployments to the provider. Instead, the configuration of security features and security-relevant settings becomes the primary source of risk for applications.
- **Integrations** – The requirement to connect and integrate SaaS into a broader data environment is critical to security. SaaS applications rarely operate in data silos providing ample features for integration and automation across other SaaS offerings. This is especially true in hybrid environments where legacy resources, databases, and other systems (e.g., Active Directory) must be coordinated with SaaS applications.
- **Identities and Accounts** – The identities and accounts associated with SaaS applications are essential to proper security posture. This should also come as no surprise given the prominent role identity and access management (IAM) plays in reducing overall risk to the typical enterprise.

As suggested above, these four pillars were selected based on practical day-to-day interaction, technical support, and project engagement with enterprise teams deploying and securing modern SaaS applications. Our approach contrasts with more generic frameworks such as NIST CSF which are excellent resources, but which do not focus on the most essential aspects of securing SaaS in a typical hybrid network.

PROPOSED SaaS SECURITY MODEL

Our model presents the pillars in the context of the stakeholders of SaaS, each of which represents a unique set of security challenges. We do not include the SaaS provider because this part of the shared responsibility model is defined in their service level agreements (SLAs). That is, like most cloud environments, the SaaS hosting provider has the responsibility to tend to lower-level security issues such as patching servers, scanning local hosting networks, and other infrastructure roles.

In contrast, the enterprise team will have different roles and responsibilities that reside more at the level of applications, workloads, and data. Some industry analysts have described the security task at this level using broad categories such as SaaS Security Posture Management (SSPM). Our choice is to focus in a more granular manner on the specific tasks that must be done for security – and by whom. As a result, the three types of relevant SaaS stakeholders that we've identified are as follows – and there certainly can be overlap between the roles:

- **SaaS End User** – The end-users of SaaS applications in the enterprise are ultimately responsible for the secure use of application features. A design goal for SaaS applications is to minimize the degree to which users can cause harm, but this remains a challenge for most applications, especially ones that include the use of sensitive or critical data. End-users are left with the security critical decisions of sharing data, integrating into other platforms, and often choices around authentication. Often, the end-users end up being responsible for technology selection with the common 'free-trial' and 'freemium' go-to-market models.
- **SaaS Administrator/Owner** – The administrators of SaaS applications, sometimes referred to as the owners (with the caveat that finance and business unit teams might also be involved as SaaS owners), will obviously have a significant impact on the overall cybersecurity posture of those applications. As shown below, configuration and other tasks will directly influence SaaS security.
- **IT/Security Team** – As one might expect, the IT and security team members, especially ones tasked with application security or cloud security, will play central roles in ensuring that SaaS applications are neither misused by bad actors nor allowed to operate with exploitable vulnerabilities. Such teams will oversee tasks such as integration of SaaS security with broader protection systems across the hybrid network.

By identifying these key players in the day-to-day administration, operation, usage, and protection of SaaS applications, we create a means for developing a richer security model. In the next section, we introduce this model by logically combining the four pillars with the three types of users. The result is a matrix that effectively summarizes how we recommend that SaaS security be employed across the typical enterprise.

SaaS SECURITY MATRIX

As suggested earlier, our objective is to create a useful model that is more specific to SaaS application security than general frameworks such as NIST CSF 1.0/2.0. As such, we present below the cross-product of SaaS security pillars with SaaS security actors. Within each element of the resulting matrix, we try to capture the essence of the responsibility for that cross-product entry in the model.

	Data & Access	Configuration	Intergrations	Identities & Accounts
SaaS End User "Be Responsible"	Comply with corporate policies when uploading or creating data in SaaS applications.	Ensure use of account-level security features versus potential user opt-out of controls.	Ensure integrations created are compliant with policies and corporate approved applications.	Coordinate deleting unused or abandoned accounts with application administrators.
SaaS Admin/Owner "Configure"	Configure SaaS data controls in compliance with corporate policies and user access controls.	Configure SaaS security features in compliance with IT policies and support required business functions.	Configure application controls for integrations with applications to prevent data sprawl.	Provision and deprovision access to applications with delegation to IT with use of SSO (if necessary).
IT Security Team "Verify"	Regularly verify SaaS data and access control configuration and SaaS app provider compliance.	Verify that SaaS security features are configured in compliance with applicable policies.	Verify integrations with an application are following applicable business requirements	Verifying user access to applications are following applicable business requirements.

Figure 1. SaaS Security Model

As should be evident, our proposed SaaS model involves shared responsibility, because it can essentially ignore the underlying lower-level security tasks that any hosting provider must attend to. This does suggest that enterprise teams must be discerning in their selection of SaaS vendors. Third-Party Risk Management (TPRM) should be in place to help reduce the risk of selecting an insecure SaaS provider.

It is also critical that enterprise teams select the right security platform to support the need for users, administrators, and security teams to secure their SaaS deployments. In the next section, we describe how commercial vendor Nudge Security was created for this specific purpose. We explain how the platform works, and we relate its operation to support for the shared SaaS security model presented above.

UNDERSTANDING THE NUDGE SECURITY PLATFORM

Nudge Security focuses on strengthening SaaS security by addressing SaaS-hosted data, configurations, integrations, and user identities. Their commercial platform is designed to support not only SaaS users and administrators but also the IT and security teams responsible for safeguarding and governing the integrity of SaaS applications. The platform's primary goal is to ensure that data, access controls, configurations, and identities remain secure across the SaaS ecosystem.

SaaS Users: Securing Data and Access

At the core of the Nudge Security approach is an identity and access management (IAM) framework that helps organizations enforce controls over user authentication and access permissions. It continuously monitors user activities, ensuring that users access the data and services for which they are authorized. This is achieved through real-time enforcement of access controls, minimizing the risk of unauthorized access or credential abuse.

In addition to access control, Nudge Security integrates data loss prevention (DLP) measures that track how data is accessed and shared within SaaS environments. This helps prevent data leaks by ensuring that sensitive information is only accessed by the right users under appropriate conditions. The platform identifies potential data exposure risks and works to mitigate them, ensuring that user interactions with the SaaS application do not compromise data security.

SaaS Administrators: Managing Configurations and Enforcing Best Practices

Nudge Security provides SaaS administrators with tools that help effectively manage SaaS configurations. The platform continuously assesses the configurations of SaaS applications, ensuring that they are aligned with best practices, security frameworks, and regulatory compliance requirements. By automating the process of configuration management, Nudge Security helps administrators identify and remediate misconfigurations that could introduce security vulnerabilities.

Misconfigured SaaS settings can leave sensitive information exposed to unauthorized users or enabling attackers to exploit weak points in the system. Nudge Security proactively identifies these configuration issues and provides administrators with actionable insights to resolve them. Whether it's ensuring that proper encryption protocols are in place or limiting unnecessary user privileges, the platform enforces configurations that protect data and mitigate risks.

SaaS Integrations: Securing Third-Party Connections

Enterprise SaaS applications frequently rely on integrations with third-party services, which can introduce additional attack vectors if not properly secured. The platform addresses this common threat by ensuring that all third-party integrations are monitored and secured against vulnerabilities. It assesses the security posture of these integrations and flags any weak points that could be exploited.

The platform ensures that data exchanged between SaaS applications and third-party services follows secure protocols and is protected from interception or tampering. This includes enforcing secure API configurations, monitoring data flows, and ensuring that only authorized systems can interact with the SaaS application. By addressing the security of these connections, Nudge Security helps maintain security in the presence of multiple external services.

Security Teams: Monitoring and Incident Response

For security teams, Nudge Security offers a centralized platform that provides visibility into the entire SaaS environment. It allows security teams to monitor user activities, SaaS configurations, and integrations from a single dashboard, making it easier to identify potential threats or anomalies. The platform's incident response capabilities are integrated into this monitoring system, allowing security teams to respond quickly to any security incidents that arise.

Nudge Security supports the detection of both internal and external threats. Its threat detection capabilities are designed to identify suspicious behavior, such as unauthorized data access, unusual user activity, or attempts to exploit vulnerabilities in the SaaS platform. In the event of a potential breach or attack, Nudge Security provides security teams with real-time alerts and detailed information on the incident, allowing for rapid response and mitigation.

SaaS Identities and Accounts: Securing the Foundation

SaaS identity and account security are additional critical components of any SaaS environment. The platform continuously monitors the security of user accounts, ensuring that identities are verified and protected from compromise. This includes enforcing multi-factor authentication (MFA) and providing ongoing monitoring for account takeover attempts or suspicious login activity.

By providing proactive measures to secure both SaaS identities and accounts, Nudge Security helps enterprise organizations reduce the risk of unauthorized access or insider threats. The platform's emphasis on identity security ensures that users are properly authenticated and that account activities are secure. Any practitioner will agree that this risk is all too common in modern environments.

ACTION PLAN AND NEXT STEPS

Our recommended next steps for enterprise security teams who must contend with SaaS application protection would be as follows: First, review the shared model we propose above to determine if the three actors match up with the security team's view of relevant individuals and groups involved in SaaS usage, administration, and security. This can be adjusted if some additional granularity is needed (e.g., different groupings of SaaS users).

Next, the four pillars should be reviewed to determine local relevance to the specific duties that are owned by the enterprise – versus the underlying shared responsibility of the SaaS application provider. Again, assuming the pillars line up with local views, then the enterprise would be wise to be in touch with a suitable commercial vendor for support. As should be obvious from our report, we believe Nudge Security to be an excellent choice in this regard.

Readers interested in more information on Nudge Security should feel free to reach out to the company using their website or the contact information of the authors listed at the top of this report. Alternatively, TAG Research as a Service (RaaS) customers or prospects interested in this service should be in touch with TAG for vendor guidance or they can reach out to the TAG author listed at the top of this report.

---

[1] TAG Infosphere provides research and advisory in cybersecurity, artificial intelligence, and climate science/sustainability for enterprise teams, government agencies, public policy lawmakers, academic researchers, and commercial vendors. See https://www.tag-infosphere.com/.

[2] NYU's Center for Cybersecurity (CCS) is an interdisciplinary academic center in which leading edge cybersecurity research, teaching, and scholarship are directed into meaningful real-world technology, platforms, and policies. See https://www.cyber.nyu.edu/.

[3] More detailed information on cybersecurity vendor Nudge Security and their approach to SaaS security and governance is available on their public website at https://www.nudgesecurity.com/.

[4] See https://cloudsecurityalliance.org/blog/2023/10/17/the-importance-of-the-shared-responsibility-model-for-your-data-security-strategy for information on the Cloud Security Alliance Shared Responsibility Model for cloud security.

[5] Information on cybersecurity vendor Nudge and its approach to security protection of SaaS applications in enterprise can be obtained at their website: https://www.nudgesecurity.com/.

ABOUT TAG

Recognized by Fast Company, TAG is a trusted next generation research and advisory company that utilizes an AI-powered SaaS platform to deliver on-demand insights, guidance, and recommendations to enterprise teams, government agencies, and commercial vendors in cybersecurity and artificial intelligence.