AppOmni

Treating SaaS as the Critical Infrastructure It Is

The modern enterprise has made SaaS a part of their critical IT infrastructure, enhancing productivity in day-to-day operations by empowering users and providing them with almost unlimited access to data. If they are to continue taking advantage of SaaS, it should be treated as critical infrastructure and must be given the same security consideration as the rest of the stack.

WHITE PAPER

Treating SaaS as the Critical Infrastructure It Is

Software as a Service (SaaS) is a rapidly growing segment of the it market as enterprises rush to take advantage of the flexibility and economy offered by the cloud. According to Gartner's latest forecast of Worldwide Public Cloud Revenue, spending on cloud application services is projected to grow from $99.5 billion in 2019 to $116 billion in 2020, and increase to more than $151 billion by 2022. Not only is SaaS becoming more common in the enterprise, it is becoming increasingly important in their day-to-day business operations.

Applications such as Salesforce, Workday, Microsoft 365, GSuite, Box and Slack support the vital activities of every line of business within the organization. Their ubiquity and convenience make these applications almost invisible to those who rely on them and they are used almost without thought. This transparency creates a paradox, however. By almost any objective criteria—sensitivity of data, importance to business operations, need for data integrity, etc.—these applications and the data they contain are part of the critical IT infrastructure stack. But they receive little attention from administrators responsible for managing and securing critical enterprise IT.

"We have not, as an industry, given the same level of due diligence to SaaS as we do to IaaS, bare metal, and other elements of the IT infrastructure stack", said Tim Bach, VP of Engineering at AppOmni. This leaves organizations vulnerable to leaks and breaches that can compromise the integrity of sensitive information, disrupt operations and damage reputation and market value. "We have to treat SaaS as critical infrastructure," Bach said. "As a security leader, if I don't, it's my fault when data gets breached."

$99.5
2019

$116B
2020

$151B
2022

SHARED RESPONSIBILITY

SaaS is in part a victim of its own success. The use of cloud-based applications has grown quickly and often they are acquired and managed by individual lines of business rather than centrally under the eye of the CIO or CISO. Ease of use has also led to the democratization of administration. While democracy can be a good thing, in this case it often means that lines of business rather than security professionals end up making decisions which have a significant impact on critical security posture controls.

Vendors have done a good job of positioning their applications as turnkey solutions with security built in. And in truth, the applications are secure. It is unlikely that the application itself will be compromised, or that a bad actor will steal data directly from the service provider's infrastructure. Cloud service providers also protect their infrastructures, and the federal government has established a framework for verifying the security practices of service providers under its FedRAMP program. Consequently, customers use these platforms with a high level of confidence.

> *"Most cloud security failures are the fault of customers failing to live up to their portions of the shared responsibility model."*
>
> Gartner

Ultimately, it is not the SaaS software or the supporting hardware that must be protected to safeguard the enterprise. The crown jewels of any organization are its data, and it isn't necessary for a server or the cloud infrastructure to be hacked in order for data to be compromised. The customer has ultimate responsibility for the security of its critical data, and misconfigurations and lax controls on SaaS applications can expose it to theft, manipulation or other threats.

Government and industry best practices call for a shared responsibility model for cloud security, with the cloud provider, product vendor and the customer each assuming responsibility for those portions of the infrastructure under their control. Organizations ignore this responsibility at their own peril, Bach said. "It is entirely the customers' right to shoot themselves in the foot," by neglecting proper security practices.

Ensuring that proper security procedures are being followed is not a simple task when the typical enterprise is using an average of 15 clouds with resources continually spinning up and spooling down on demand. "The scale and dynamism of cloud computing complicate visibility and control over all workloads, storage and processes performed in hybrid and public cloud computing environments," Gartner says in its most recent cloud security report. "Consequently, most cloud security failures are the fault of customers failing to live up to their portions of the shared responsibility model."

SaaS applications are not exempt from the requirements of shared responsibility. Under its implementation of the model in its Azure cloud, Microsoft assumes responsibility for the physical hosts, network and data centers hosting SaaS applications, but leaves responsibility for data, endpoint management and access, and identity management to the customer.

In its cloud security report, Gartner found that many organizations struggle to meet these responsibilities. "SaaS control remains elusive even for the most conscientious of enterprises."

This challenge is complicated by the fact that many organizations are only now beginning to understand the criticality of these applications and the need to fully manage them.

Best practices for managing and securing servers, endpoints, operating systems and networking elements are well established. Continuous monitoring and automated remediation have replaced static point-in-time certification of security status. Security vendors have provided tools to enable these practices, and no CIO would consider deploying servers or endpoints without products for monitoring and automated management that interoperate to work across product and platform types.

But that is exactly what is being done with SaaS applications. Users are taking advantage of out-of-the-box functionality while trusting the vendor and the cloud provider for security.

THE CHALLENGES

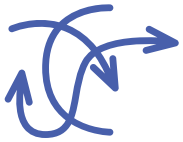
Applications offered as a cloud service provide rich functionality to enhance productivity in the day-to-day operations of different offices and lines of business within an organization. The flexibility of the cloud and the ease of access by multiple types of devices from any location, coupled with economies of scale, make SaaS an attractive and customizable solution. And therein lies the challenges.

DECENTRALIZATION

Simplified licensing, task-specific functionality and ease of provisioning via the cloud make SaaS affordable and practical for individual lines of business. Applications often can be acquired and deployed with local budgets without centralized authorization. This is a boon to businesses by enabling offices and teams to rapidly deploy tools supporting productivity and customize them to meet specific needs. This is an upside that is easy to see.

The downside is not always immediately obvious. Executives not well-versed in security are content to depend on vendors and cloud providers to secure their products and services, often ignoring their responsibility for seeing that the applications function not only effectively, but securely.

The CIO, CISO or enterprise security team might not be aware of all SaaS applications deployed, and when they are aware, they often do not have the access needed to fully monitor and manage them. An evaluation of the tools might consist only of a point-in-time assessment of configuration and controls, which is likely to be out of date as soon as it is completed. Without centralized visibility and the ability to automatically manage these applications, they can quickly evolve—or devolve—to open breaches in the enterprise IT infrastructure.



COMPLEXITY

This challenge is compounded by the complexity of the SaaS environment. Enterprises deploy multiple applications, and each one can have hundreds of controls and settings that can be continually adjusted and tweaked to adapt to changing needs.

Configuring these applications manually can be an overwhelming job. Each organization—and each group within an organization—has its own needs, so there is no set default that can be relied upon out of the box to provide the necessary accesses and functionality while maintaining the required security. An initial set-up can attempt to balance these competing needs, but must be carefully monitored to ensure that the balance between functionality and security is indeed being met, and that the balance is not shifting as needs and threats change over time.

Dynamic business environments mean that needs can change on a daily basis. Personnel and their business roles frequently change, requiring new privileges for users, and administrators must have access privileges to make these changes as the environment evolves. The easiest way to ensure that administrators have the access they need to do their jobs quickly and efficiently is to allow broad privileges in accessing and changing settings. However, broad access compromises security. Good security practices call for limiting access privileges to only those that are immediately needed, and revoking them when they are no longer needed. This can delay necessary actions and requires that a constant watch be kept on all temporary changes to ensure that they do not become permanent, something that local administrators of SaaS applications might not be qualified or have the time to do.

The result is that locally, manually managed applications are likely to drift out of security compliance over time, leaving data exposed to internal and external threats. Cloud and application security measures might be perfectly adequate, but will not protect data on an application that has been misconfigured to allow public access to sensitive data or in which access privileges for former employees have not been revoked.

An effective solution to these challenges must support the speed and flexibility that makes SaaS attractive without sacrificing security. Local administrators should be able to configure applications to keep them useful, while security professionals get the level of visibility and control they need to ensure that security is not compromised.

SOLUTIONS

Organizations have made SaaS a part of their critical IT infrastructure stack, enhancing productivity in day-to-day operations by empowering users and providing them with almost unlimited access to the data they need. If they are to continue taking advantage of this power, SaaS must be treated as critical and should receive the same security considerations as the endpoints, servers and network elements that make up the rest of the stack.

While the security of the applications themselves and supporting infrastructure is the responsibility of vendors and service providers, users have the responsibility for securing access to the data and understanding the security posture of applications at all times. This means applying the same security best practices to SaaS as to the rest of the IT infrastructure.

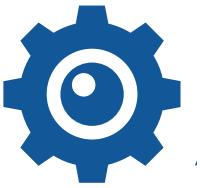
BEST PRACTICES

The standard for cybersecurity has shifted in the last decade from static and reactive to proactive. Periodic point-in-time assessments of security status have been replaced by continuous monitoring, analysis and remediation, with the goal of identifying and correcting potential threats before they result in a breach.

The security industry has responded to this shift by developing suites of tools, often interoperable, that give security operations centers (SOC) visibility into the IT infrastructure. This includes not only monitoring network activity and traffic, but also the configuration and state of devices to ensure that they are in compliance with industry and government regulations as well as organizational requirements. Effective monitoring requires not only visibility into elements of the IT infrastructure, but the ability to correlate data from different elements to identify problems. A particular type of activity on the network might not be problematic in itself, but could indicate a threat when associated with a specific vulnerability or a pattern of data access.

This capability has evolved based on a deep understanding of the traditional hardware and software elements of the critical IT infrastructure. But the fairly recent and rapid development of SaaS has only recently allowed the enhancement of similar technology for critical SaaS application security. There are many different applications developed by various vendors to perform unique functions. Each has its own controls and tools that allow it to operate with multiple endpoints and back ends.

This has made it difficult to bring SaaS applications into the same security regime as the rest of the IT infrastructure until now.



TOOLS

The AppOmni solution provides monitoring, visibility and policy-based controls to enable continuous and automated management of critical SaaS applications. Security teams are able to understand and manage the security posture of applications, respond to and remediate vulnerabilities and threats in real time, and ensure continuous compliance with security requirements.

The solution is created specifically for critical applications, with an understanding of the software that allows security teams to monitor and manage across multiple applications. This together with the flexibility to drill down into each application provides a comprehensive solution.

“We go very deep into each application,” Bach said. “We understand how the system works.” This understanding is coupled with established best practices so that SaaS security can be brought into the SOC, allowing it to detect misconfigurations, monitor user activity, normalize event logs from a variety of applications and detect anomalous activity. Security professionals can establish the parameters for secure operation of critical applications, allowing day-to-day administration to remain with individual lines of business while constantly validating the security posture.

ELEMENTS OF THE SOLUTION ENABLE

- Monitoring and detection, with real-time visibility into actions in SaaS environments. Events are normalized across the cloud and delivered to existing SIEM or SOC infrastructure for analysis without requiring another "single pane of glass."
- Data access monitoring to provide an immediate, comprehensive understanding of who has access to what data and why, whether they are employees, contractors or external third parties. This access modeling allows administrators and security personnel to understand why access has been granted, reducing time to remediation. Improper data exposure can be quickly detected and fixed before it leaks, with policies to monitor and prevent recurrence.
- "Guardrails" can be put in place to allow rapid SaaS application development without sacrificing security or functionality.
- Continuous security posture monitoring to manage configuration and vulnerabilities in critical SaaS applications across multiple deployments and clouds. Third party applications connected to SaaS platforms are detected, inventoried and monitored. Sensitive configurations and administrator actions are monitored and audited to allow automatic remediation of configuration errors and enforce critical security controls. Security baseline requirements can be deployed across multiple instances of an application simultaneously.
- Continuous compliance of SaaS applications with regulations. This includes out-of-the box mappings for SOC 2, ISO 27001, NIST CSF, NIST 800-53 and other industry and government requirements, including PCI, HIPAA and GDRP. Reports can be automatically generated to support audit activities.

Organizations deploying critical applications can only meet their shared responsibilities with tools that enable the use of best security practices in the SaaS environment. These tools, purpose built for critical SaaS, provide proactive solutions in this new space with continuous monitoring and automated response to leverage existing in-house resources and expertise.v

AppOmni

SaaS Security Management

To learn more, email us at **info@appomni.com** or visit **appomni.com**.

AppOmni is a leading provider of SaaS Security Management software. Its patented technology scans APIs, security controls, and configuration settings to compare the current state of enterprise SaaS deployments against best practices and business intent. AppOmni makes it easy for security and IT teams to protect and monitor their entire SaaS environment from each vendor to every end-user.

AppOmni