AppOmni

SaaS Security Best Practices in #WFH World

> America has risen quickly to meet the work-from-home challenge. Within weeks of the COVID-19 outbreak 98 percent of companies had instituted a work-from-home policy, with 28 percent allowing all of their employees to work from home[1] .

While many businesses have been able to sustain productivity with a rapid shift to work-from-home modalities, the shift may have opened them up to new security risks. In this complex environment, with trouble tickets pouring in at an accelerated clip, thin-stretched IT departments and SaaS administrators need new, more effective and efficient means to secure and manage their SaaS deployments. The new work-from-home environment demands a sophisticated SaaS security and management platform for the enterprise.

Best Practices of SaaS Security

For enterprise IT leaders looking to secure their at-home workforce in a SaaS-driven world, a number of best practices can help to move the needle.

By adhering to a few basic principles, it's possible not only to ensure a higher level of security, but also to significantly reduce the workload on the IT team at a time when their talents are in high demand.

98%
of companies instituted a work-from-home policy

Enforce Multi-Factor Authentication (MFA) Predators are leveraging the fear and uncertainty of the moment to get more aggressive in their phishing expeditions and other social exploits. The U.S. Cybersecurity and Infrastructure Security Agency warned in the early days of the crisis that bad actors were already sending out emails with malicious attachments or links aimed at tricking victims into revealing sensitive information or donating to fraudulent charities or causes. According to a recent report from Google, the number of active phishing web sites grew by 350 percent from January to March, an indication that bad actors are actively looking to exploit the uncertainty surrounding this transitional time.

Multi-factor authentication or MFA offers a quick and ready defense against such activities. By requiring users to cross-authenticate their password against, for example, a text sent to their phones, IT can minimize the potential damage caused by compromised credentials. Even if a phishing scan were to succeed in compromising an employee's login information, the bad actor would be unable to make use of those stolen credentials without the secondary authentication.

A successful MFA implementation requires thoughtful management of SaaS applications. IT needs to ensure that MFA is required of all users and that exceptions are speedily corrected. Automated solutions can help to enforce this.

[1]Online survey of more than 250 companies conducted in late March 2020 by outplacement firm Challenger, Gray & Christmas

Say for instance the CEO doesn't have access to a phone: It's common enough for IT support staff to switch off MFA in order to grant the executive access to the system. Then, in the crush of other business activities, no one remembers to turn the safeguards back on. A platform approach to SaaS management can scan continuously for such lapses, notifying IT when a fix is needed or even automatically applying the correction when the gap is deemed serious enough.

Restrict Device Access Whenever possible, remote workers should be using dedicated work devices, separate from their home devices, especially in these early days when many are struggling to adjust to telework. This ensures they are working within your existing security constraints, using approved configurations and tools that are under the enterprise security umbrella.

Those running SaaS applications need to ensure that their applications are configured to only run permitted devices and permitted configurations.

As time goes on and telework becomes more the norm, enterprise IT may want to adjust those policies, allowing users to begin linking their own devices to the network. It's likely that this will happen as workers tire of small-screened laptops and request a desktop modality. This evolution takes advantage of the basic SaaS promise – any device, anywhere – but it will need to be managed thoughtfully. A platform approach to SaaS security ensures that the new rules will be automatically and appropriately enforced across all SaaS deployments.

Continuously Monitor Configurations In the full-speed push toward remote work, key settings and configurations may get tweaked or disabled, exposing data to possible breaches. It's understandable that user permissions will be reconfigured on the fly in order to allow people to do their jobs. The risk is that these changes will be forgotten over time, or will conflict with the business intent.

Number of phishing websites grew by

350%

from January to March

The remedy lies in the continuous monitoring of SaaS configurations, but that is neither practical nor feasible when approached as a manual task. The IT teams and SaaS administrators simply have too much else going on. Enterprise IT needs an automated solution for continuous monitoring to ensure all the settings in SaaS are correct and that they comply with the overall business need.

In addition, it can be easy to overlook the challenge posed by cloud-to-cloud access via APIs. All of that mission-critical data that is accessible to users is equally accessible by other applications. It's vital that administrators ensure each application has the appropriate level of data access. Here again, an automated solution is needed to satisfy what would otherwise be an overwhelming manual requirement.

Moving Forward

A SaaS security and management platform solution from AppOmni can help ensure the emerging work-from-home paradigm does not exacerbate the existing, and already significant, cyber-threat to the enterprise.

AppOmni empowers IT teams to scan, secure, and monitor SaaS applications, automatically and continuously enforcing rules for data access, data sharing and third-party applications. AppOmni technology deep scans APIs, security controls, and configuration settings to evaluate the current state of SaaS deployments and compare against both best practices and business intent.

At a time when many organizations are driving full throttle to enable work-at-home capacity, an automated, platform-based approach to SaaS management can help ensure security while freeing IT expertise from time-consuming manual management tasks, thus empowering them to more effectively support the pressing business needs of the day.

ABOUT APPOMNI AppOmni is the leading software as a service (SaaS) data security and management platform for the enterprise. AppOmni provides unprecedented data access visibility, management, and security of SaaS solutions, enabling organizations to secure mission-critical and sensitive data. AppOmni's patent-pending technology comprehensively scans APIs, security controls, and configuration settings to evaluate the current state of SaaS deployments and compare against best practices and business intent. With AppOmni, organizations can establish rules for data access, data sharing, and third party applications that will be continuously and automatically validated. The company's leadership team brings expertise and innovation from leading SaaS providers, high tech companies, and cybersecurity vendors.