Ransomware in the Cloud: Challenges and Best Practices

The rise of SaaS ransomware is quickly becoming a prevalent issue in cybersecurity as it poses unique challenges and risks to businesses that rely on cloud-based data storage and management solutions.

In our latest webinar Director of Support at Spin.AI, Nick Harahill, we explored the intricacies of ransomware tactics within the SaaS ecosystem, discussed why traditional backup and disaster recovery methods must adapt in response to more sophisticated ransomware threats, and discussed why organizations should explore innovative approaches and solutions to fortify their data protection.

What's unique about ransomware in SaaS environments?

Ransomware in Software as a Service (SaaS) environments presents some unique challenges and considerations compared to traditional on-premises systems, making them a tempting target for adversaries as ransomware tactics evolve.

1. SaaS environments provide an expanded attack surface

Attackers will target where the data is - and, with most companies utilizing a wide variety of SaaS applications like Google Workspace and Microsoft 365, this provides a largely expanded attack surface. Moreover, the accessibility of your SaaS environment from anywhere with an internet connection further amplifies this risk surface.

2. SaaS environments promote collaboration and data sharing

While this aspect is what makes our lives easier, our jobs simpler, and enhances communications, it also poses a significant risk. When it comes to ransomware, multiple users often share access to files and documents - if one user’s account is compromised, that ransomware can spread quickly and easily throughout the SaaS environment.

3. SaaS environments host a proliferation of integrations and third-party applications

In your SaaS environment, users can install various applications and extensions spontaneously. If one of these integrations becomes compromised, it introduces a potentially disastrous vulnerability, offering a convenient target for ransomware attacks

What are the trends in ransomware attacks on SaaS environments?

1. Targeting weakly-secured administrator accounts

Administrator accounts overlook critical sections of your SaaS environment. In the absence of robust controls or authentication methods, such as Multi-Factor Authentication (MFA) or Two-Factor Authentication (2FA), these admin accounts become vulnerable targets for ransomware attackers.

2. Evading detection

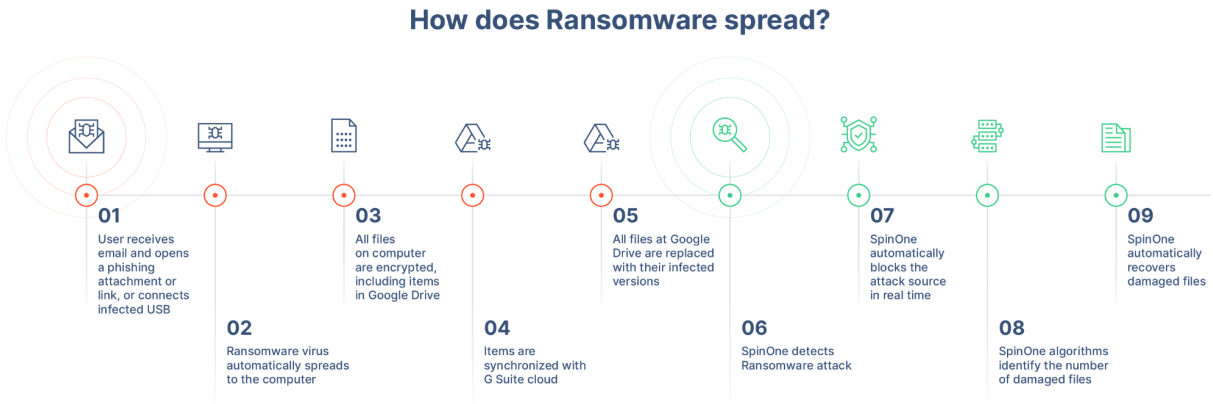
While this is nothing new to the cybersecurity industry, we're seeing a trend emerge for advanced, persistent threats. Attackers are increasingly adopting a "low and slow" method: gaining a foothold within an enterprise, then slowly spreading throughout the environment. This approach aims to evade traditional detection methods by encrypting a small percentage of files at a time or targeted files, making detection challenging.

3. Targeting mobile devices.

Mobile devices become an extension of your SaaS environment - this again notes the expanded attack surface that could affect the data stored on devices and the SaaS environment at large. This expanded attack surface not only encompasses potential vulnerabilities within the SaaS environment but also encompasses the data stored on these mobile devices. As these devices interact with the SaaS environment, they introduce additional entry points for potential threats, underscoring the importance of implementing robust security measures across both the SaaS platform and associated mobile devices to mitigate risks comprehensively.

How does ransomware infiltrate and spread within SaaS environments?

A common infiltration method is with phishing emails.



In this example, a user receives a phishing email and becomes compromised - now the ransomware virus can automatically spread to the computer.

At that point, all files on the computer are encrypted, including items within their Google Drive. Using Google Workspace as an example, many users will have active file sync from their end device to the Google G Suite cloud.

But in that case, synchronization can work against them - spreading that ransomware attack quickly and replacing files within Google Drive with their infected versions.

Why are backups alone not effective protection against ransomware attacks?

While 92% of businesses report having backups, more than 1 in 4 businesses fail to restore data from those backups during a ransomware attack.

This emphasizes the need to regularly test not just your backup processes, but also your restoration processes.

Despite having backup protocols in place, it's crucial to consider that data restoration takes time - and API limitations from your provider could impede that recovery time even further.

Note that the average downtime - even for companies with backups in place - averages about 3 weeks.

Taking this into consideration can help you minimize downtime and the impact it has on your business.

Why is automation critical to protecting your SaaS environment from ransomware attacks?

Automation plays a pivotal role in detection - first with monitoring. Automated monitoring not only detects known signatures of ransomware attacks but can also automatically detect behavior that mimics that - which is virtually impossible for a human to do alone.
Having automation in place to find different kinds of attacks - without placing that workload and responsibility solely on a security team - helps eliminate errors and detect a broader scope of potential threats.

Secondly, automation is instrumental in taking swift action once an attack is identified It facilitates the immediate identification of all impacted files and users, streamlining the restoration process for anything affected by the attack.

Lastly, utilizing automation helps to detect configurations that drift out of sync with control standards, and enhance posture management around any applications that may be a risk to your SaaS environment.

What are some proven strategies and best practices to defend SaaS data from ransomware?

1. Collaborating with your SaaS provider

Ensure you have a complete understanding of the native security features your SaaS provider has in place for SLAs. It's also critical to understand where their responsibility ends and yours begins - due to the shared responsibility model, you are most likely responsible for an extra layer of security that their features do not cover.

2. Develop an incident response plan

Ensure that all the key players in your incident response plan know what their responsibilities are, make sure they can execute those responsibilities, and have automation in place to assist where needed. Most importantly, regularly test this incident response plan to make sure your plan is both current and effective.

3. Security training and awareness for your end users

Limit your internal security risks with security training for your employees and all end users around phishing, social engineering, managing data within the cloud, and basic cloud security practices.

4. Ensure MFA is in place for all administrator accounts

As mentioned previously, your admin accounts hold potentially dangerous levels of access to your SaaS environment. Reduce your risk by making sure access controls are in place on all administrator accounts, log and regularly update/patch software, and ensure you have automation in place to detect potential attacks.

With all of these steps, it's important to continuously test your plans, processes, and backups with regular security audits.

How does SpinOne protect organizations from ransomware attacks on SaaS environments?

SpinOne is an all-in-one SaaS security platform that provides users with:

- 3x daily backups for fast, easy, accurate restoration
- Automated AI detection and response to finding the impacted files and restore these to the user quickly - drastically reducing downtime
- Automated monitoring of configurations and integrations within your SaaS environment
- Automated, customizable alerts for any detected risks
- 2-hour SLA from detection to restoration