CASE STUDY

A cautionary tale securing SaaS apps

SaaS apps have redefined how we work and enabled organizations to stay nimble and better adapt to change. 70% of the apps used are IT-sanctioned SaaS apps and businesses use an average of 80 SaaS tools.[1] SaaS has impacted every aspect of work: communications, productivity, operations management, project planning, and more...

70% of the apps used are IT-sanctioned SaaS apps and businesses use an average of 80 SaaS tools.[1]

Businesses that take the approach of establishing basic security practices for creating passwords and sharing files help to reduce business risks when using SaaS services. At the same time, they may give little thought to how the data is generated, collected, and backed up by their favorite SaaS apps, which can be problematic, as it does not guarantee protection when cybercrime strikes.

Cybercriminals realize application vulnerabilities happen and work tirelessly to exploit them, exploited an vulnerability is the most common root cause of ransomware attacks.[2] As they harvest information through social engineering efforts, or mine for latent loopholes in systems, they find ways to hack company networks and inject malware. Once the malware gets into a network, it corrupts machines and/or encrypts data. The attackers then extort the business.

Unfortunately, this is when companies discover there is unmanaged risk in using SaaS apps, and that data protection is their responsibility.[1] Especially since many mistakenly believed out-of-the-box backup capabilities were enough to make cyber recovery possible.

THE SAD TALE OF XYZ COMPANY

XYZ Company experienced a sophisticated zero-day attack on their environment. The malware rapidly encrypted their SaaS app data and rendered it useless. Day-to-day operations came to a halt, as workers, company-wide, could not access their critical applications.

XYZ made repeated attempts to restore the SaaS data and avoid paying the ransom. Because they believed (as many do) that SaaS app vendors are responsible for securing their data, XYZ Company did not have a 3rd party backup and recovery solution in place. They had assumed the native controls built into their SaaS applications would be sufficient.

Eventually, XYZ learned all the redundant backup copies living within the source SaaS app environment were also encrypted by the malware. After days of outage, XYZ paid a lofty 7-digit ransom for a decryption key.

Luckily, they were able to recover most of the data and resume some operations, though it will take them many weeks to fully recover. They are currently taking steps to improve IT security, train employees on how to spot suspicious communications, appropriately handle information access, and find a trusted partner to manage their back up and disaster recovery program.

WHAT IF XYZ COMPANY HAD PARTNERED WITH COMMVAULT?

When the zero-day threat happened, they were prepared. The combination of awareness and the right suite of tools and processes from Commvault® Cloud gave XYZ Company the ability to succeed and swiftly combat a successful ransomware breach.

XYZ Company understood that cyber resilience was their responsibility and engaged Commvault to deploy a robust, dedicated solution to safeguard SaaS app data well before the attack occurred. They chose Commvault for its unique, multi-layered security. Data was stored in virtually air-gapped locations, outside of source environments. Advanced AI and real-time insights and tools helped with early detection of anomalous and ransomware activity. And flexible controls made it possible for admins to recover data fast, to the right location, at the right time.

Because XYZ Company used Commvault as their last line of defense to secure their SaaS app data, the IT administrators were able to recover data quickly and avoid costly downtime and payouts. Data was restored to a pre-infected timeframe without hiccups to any business operations.

1 The shared responsibility model explained and what it means for cloud security | CSO Online | 2021
2. State of Ransomware Report | Sophos | 2023

To learn more, visit **commvault.com**