SpinOne

A guide on protecting G Suite from ransomware

- The impact of ransomware
- Ransomcloud: ransomware is coming to the cloud
- G Suite native ransomware protection solutions
- Best practices to prevent ransomware attacks

Data loss, data breach, irreparable damage to your business reputation – those are frightening words for business leaders and stakeholders alike! Ransomware is a sinister threat to your business-critical data that can lead to all three outcomes.

In this G Suite ransomware protection guide, we will look at the ransomware threat to your G Suite environment as well as the tools available to secure your business-critical data.

SpinOne

Contents

WHAT IS RANSOMWARE? 01

RANSOMCLOUD 03

HOW G SUITE PROTECTS FROM RANSOMWARE 04

NATIVE TOOLS ARE NOT ENOUGH 07

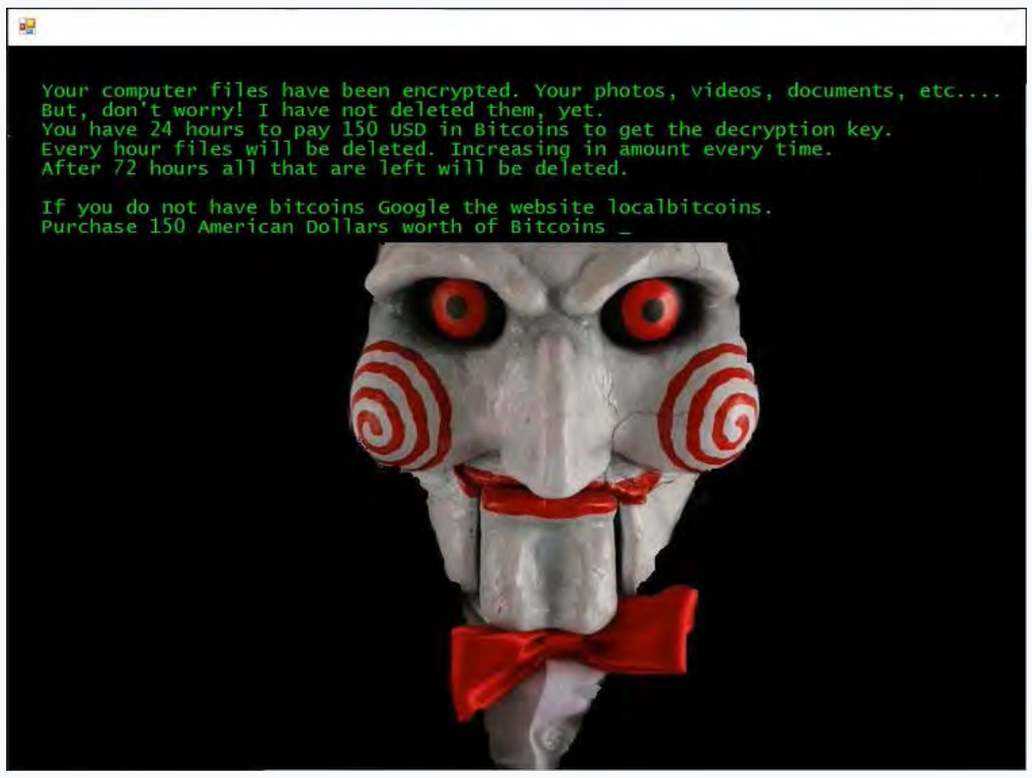
G SUITE SECURITY BEST PRACTICES 08

BEST-IN-CLASS RANSOMWARE PROTECTION 09

01

WHAT IS RANSOMWARE?

SaaS Data Protection Guide



[Jigsaw ransomware encrypts and deletes your data at specified intervals]

As the name implies, ransomware is a malware variant that demands a **ransom** payment in return for recovering access to your data. The ransom payment is generally demanded in the form of cryptocurrency such as Bitcoin.

How does ransomware prevent authorized users from accessing their own data?

Ransomware is a specific type of malware that uses file encryption in a malicious way to “lock” your files so they cannot be accessed without the attacker “unlocking” the files for you. Access to your data will only be returned by the attacker when the ransom is paid, but paying the ransom doesn't give you a 100% guarantee.

How is it possible for file encryption to be used on your own data without your consent?

Under normal circumstances, file encryption is a security operation implemented by a trusted system administrator to protect access to business-critical or sensitive data.

Ransomware uses this legitimate security tool against you. It is malicious software that infects an end-user, often under the guise of legitimate software installation, that assumes the permissions and rights of the user and encrypts all files the user has access to. Once user permissions are “hi-jacked”, it allows ransomware to encrypt files that are stored locally, on a network share, and even cloud storage, all without the consent of the end-user.

How does ransomware encrypt G Suite?

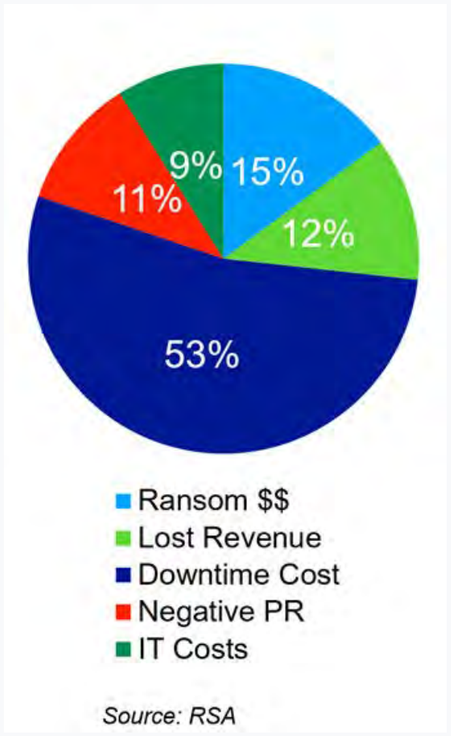
Data stored in the cloud such as in G Suite can easily be encrypted by ransomware via file synchronization. With file synchronization, files that are modified or created locally are synchronized to cloud storage. File changes are the trigger that initiates the synchronization process. When ransomware encrypts local files stored on an end user device, the malicious encryption process triggers file synchronization to cloud storage. Once files that are encrypted by ransomware are synchronized to cloud storage, both the local and the cloud copies of the files are now encrypted or “locked” by the ransomware.

What are the impacts of ransomware?

Impacts of ransomware are costly:

There are additional best practices and recommendations per Microsoft that can help protect your Office 365 environment from the threat of ransomware. These include:

- Current methods cannot detect, stop or remediate from Ransomware attacks
- Recovery, at best, can take many days
- Failures to recover/restore attacked files are very common
- Impact to organizations: millions of dollars in cost, lost operational time, lost data



03

RANSOMCLOUD

SaaS Data Protection Guide

The emerging cloud security threat

An alarming new variant of ransomware that has been demonstrated by security researcher Kevin Mitnick is called “Ransomcloud”. With a ransomcloud attack, it is not simply file storage that is the target of the ransomware, but rather cloud-based email.
In a ransomcloud infection, an unsuspecting end user receives an email requesting permissions to perform “security” updates. When the end-user grants permissions to the link contained in the email, ransomware begins encrypting the emails contained in the user’s inbox in real-time. Ransomware that can encrypt user’s cloud-based email is a dangerous threat to your data.

"While cloud providers are beginning to introduce features and services to help prevent or remediate a ransomware infection with file storage, very few if any of these protect cloud-based email."

04

HOW G SUITE PROTECTS FROM RANSOMWARE

SaaS Data Protection Guide

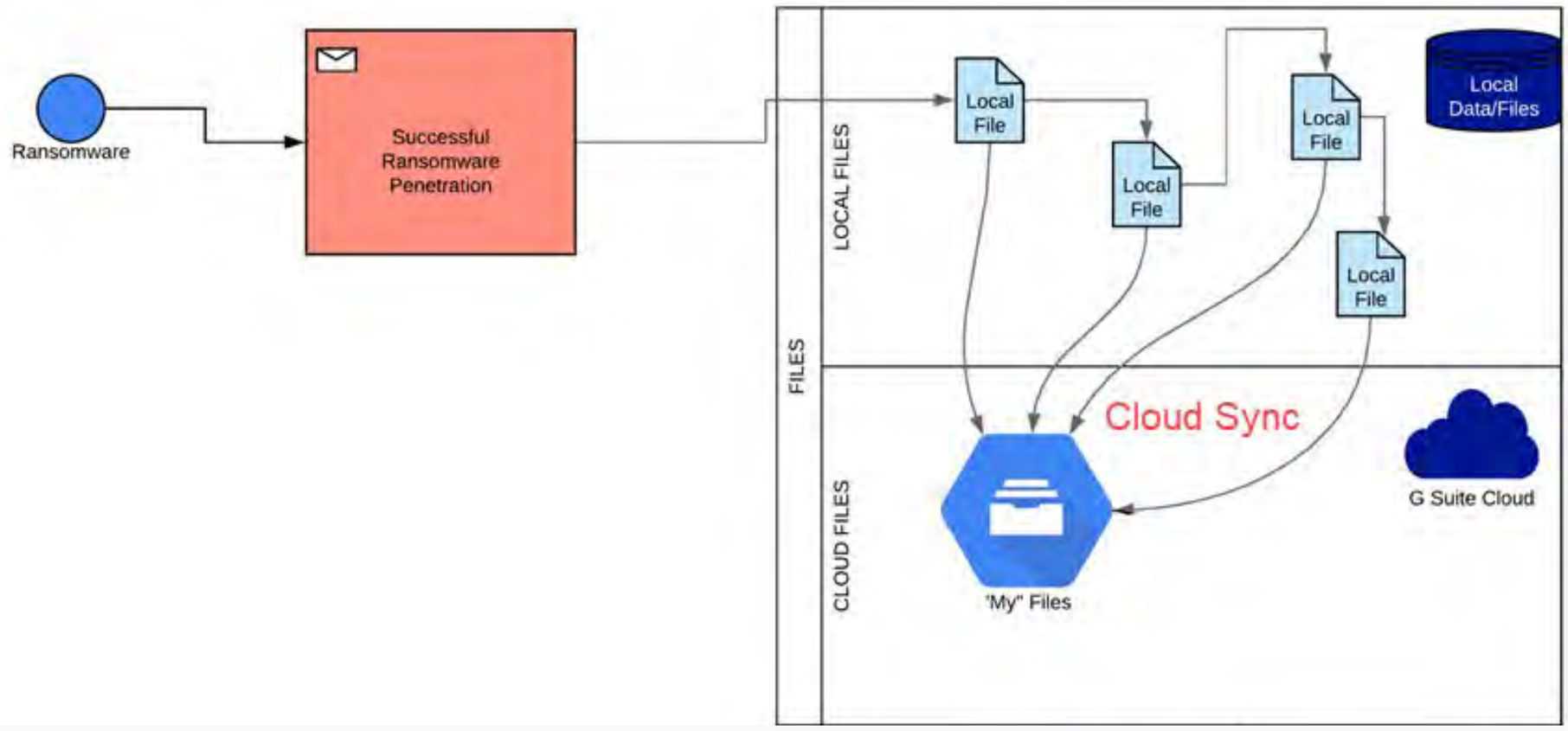
How can native tools help to reduce the risk of ransomware infecting your G Suite cloud environment?

There are a number of preventative measures that can be taken from a Google G Suite perspective that can help to protect your G Suite environment from ransomware. These include the following:

- Prohibiting access to Google Drive sync client
- Banning email attachments
- Preventing third-party apps installation

Prohibiting access to Google Drive sync client

File synchronization between local files stored on end user clients and your G Suite environment can be dangerous as noted earlier. File synchronization between on-premises clients and the cloud provides a fast path that can allow ransomware to easily destroy data in Google Drive storage.



Synchronizing on-premises files to G Suite can propagate ransomware

However, this risk can be minimized by prohibiting access to Google Drive sync clients so that end users cannot download and configure synchronization between their client and Google Drive storage in G Suite. By managing and controlling sync access for your organization, the threat of an on-premises ransomware infection overwriting files in Google Drive is greatly reduced.

- Check out Google's official guidance on turning on/off sync for your G Suite organization

Banning email attachments

Email is one of the most common threat vectors for ransomware. It continues to be a favorite among attackers to infect end users with ransomware. Ransomware payloads are dropped via malicious/infected email attachments. A malicious attachment generally masquerades as a legitimate file download. An end-user who unknowingly previews, downloads, or executes the malicious attachment, activates the malicious code and begins the ransomware infection.

An effective way for a G Suite administrator to eliminate malicious attachments as a possible attack vector for ransomware is to ban email attachments altogether. Banning G Suite email attachments prevents the possibility that an end-user receives a malicious attachment, opens it, and is infected with ransomware.

You may wonder – does Google not scrutinize and scan emails that you received into your G Suite environment? They do. However, there are ways that ransomware can still make it past malware scans and other security mechanisms. Attachments that are encrypted or compressed can often bypass security scanning measures.

While banning email attachments may present challenges for end-users accustomed to using email to send files back and forth, end users can be trained to use Google Drive to share files directly which eliminates the need to send attachments via email.

Preventing third-party apps installation

One of the benefits of using a Software-as-a-Service offering like G Suite is the massive number of third-party applications that can be used to extend the features and functionality of your G Suite environment. Third-party apps can provide capabilities to your organization that are not found natively in G Suite.

Even though third-party apps can greatly extend the functionality of your G Suite environment, they represent security risks to your organization. This includes the risk of becoming infected by ransomware that is laced inside the third-party app downloaded by an end-user.

G Suite administrators have the ability to ban third-party apps installation. While banning all third-party apps may not be feasible or desirable, having an approved list of third-party apps that are allowed for installation can help to bolster the security of your G Suite environment and help protect against ransomware.

07

NATIVE TOOLS ARE NOT ENOUGH

SaaS Data Protection Guide

Native Google solutions don't protect from emerging threats and deteriorate the user experience

While using the native tools found in G Suite for protecting your environment from ransomware is a good start, the native tools are not enough in themselves for completely protecting business-critical data from ransomware. There are a couple of reasons for this:

- Ransomware is becoming much more sophisticated
- G Suite administrative user interface design issues lead to configuration vulnerabilities

Ransomware is becoming increasingly more sophisticated and robust. It is finding new ways to infiltrate cloud environments like G Suite and prey upon end-user actions (blindly granting permissions requests and others) to allow unauthorized access to your data. In the near future, attacks will initiate with Apps connected to G Suite. These are 100% cloud to cloud attack pathways. Current native G Suite tools do not protect you 100% when it comes to these new cloud-to-cloud attack vectors.
Businesses must match sophisticated ransomware with tools that employ machine learning and other “intelligence” to remain effective in the battle to protect cloud SaaS environments like G Suite effectively.

Bad user interface design is another vulnerability to native tooling. This is a challenge with G Suite and other public cloud environments where UX design and administrative workflows are constantly changing. Google has had UX design issues **blamed for customers** inadvertently leaking company data in times past.

Even if built-in tools can help organizations protect against ransomware and other security threats, UX design implementation issues and misconfiguration by customers due to those design flaws can prevent native tools from being implemented effectively. More protection is needed, and this often means making use of effective third-party security tools.

08

G SUITE SECURITY BEST PRACTICES

SaaS Data Protection Guide

Make sure you implement ransomware preventive measures

Since native G Suite tools alone may come up short in the fight against ransomware, G Suite administrators need to implement other best practices and security tools to secure G Suite. These include:

- **Make use of an API-based CASB** – Cloud Access Security Brokers allow implementing and enforcing the same organizational policies you have in place on-premises, in the cloud. API-based CASBs are the preferred way to implement CASB technology in public cloud environments like G Suite as they provide seamless and powerful capabilities to secure the cloud.
- **Control risky third-party apps** – Aside from blocking third-party applications, organizations today must scrutinize the behavior of third-party applications integrated in their G Suite environments. If a once trusted third-party app starts to exhibit risky behavior, you want to have visibility to those behaviors and prevent malicious actions on your data
- **Prevent sensitive data leak with role-based access controls** – Modern ransomware variants are beginning to use the threat of data leak and data deletion as a means to force paying of the ransom demanded. The Maze ransomware releases hostage data to the Internet at specified intervals if the ransom is not paid. Jigsaw ransomware deletes data at intervals leading up to 72 hours when all data is deleted. By using G Suite's role-based access control and API-driven CASB controls, policies to prevent data from leaking outside of your G Suite environment can be enforced and prevent your data from falling into the wrong hands.
- **Use G Suite security policies** – G Suite security policies provide a specific scope of rules, exceptions, and notification settings applied to specific users, departments, and business entities. This provides a customized security approach to different groups of users.
- **Enforce compliance and regulatory standards** – Regulatory and compliance concerns are becoming an increasingly critical aspect of doing business. You must comply with regulations such as GDPR, CCPA, PCI-DSS, and others. This is accomplished by leveraging the right security tools to protect, backup, and secure your data.

09

BEST-IN-CLASS RANSOMWARE PROTECTION

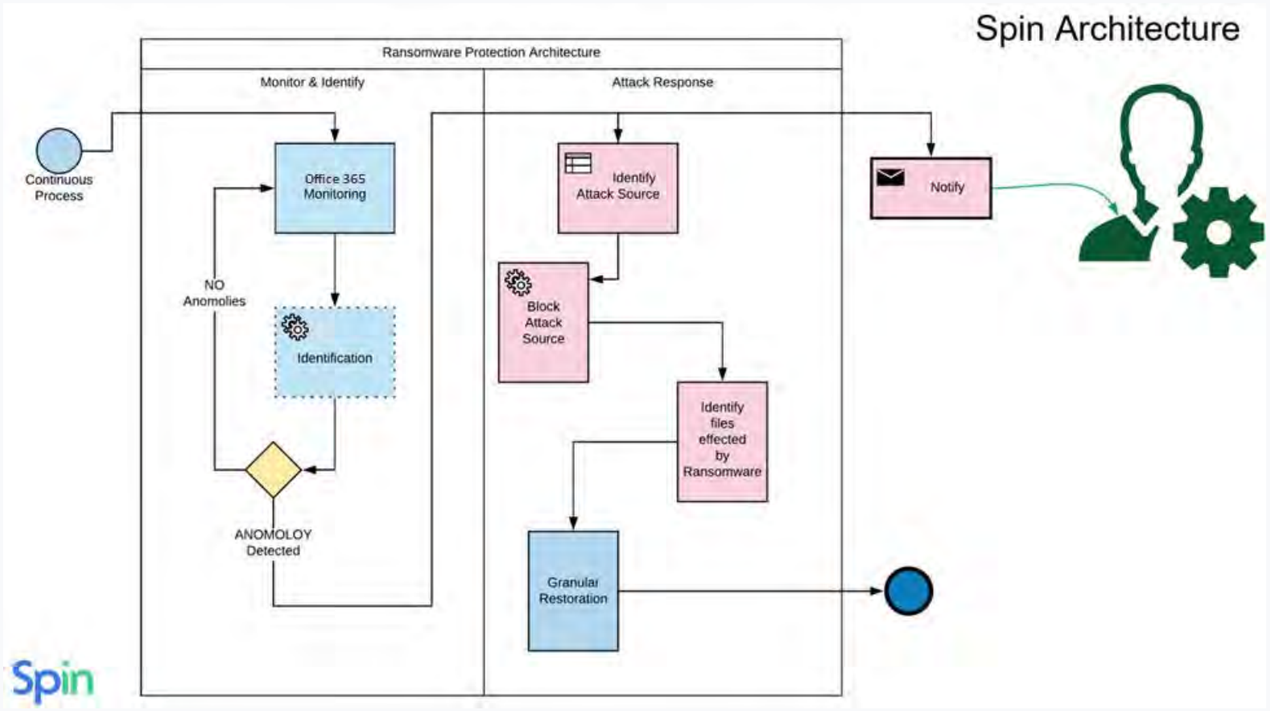
SaaS Data Protection Guide

SpinSecurity

When the very livelihood of your business is at stake (your business-critical data), you need to use the best solution available to safeguard your data from attack by ransomware. SpinSecurity from SpinOne is a “best-in-class” solution that provides the tools and capabilities needed to safeguard your data from the dangers of ransomware.
SpinSecurity is a modern API-driven CASB solution that makes use of machine learning to provide automated intelligence to fight today’s security threats such as ransomware. It does this by using a powerful two-fold ransomware protection architecture that can detect and remediate 99% of all ransomware infections.

Ransomware Protection by SpinOne includes the following four stages:

- **Detect** – Machine learning algorithms monitor G Suite for any anomalies that indicate a ransomware attack.
- **Stop** – SpinSecurity provides a quick and effective attack response. The attack source is identified and stopped immediately by blocking the ransomware process.
- **Remediate** - Once the attack is identified and stopped, any files affected by the ransomware attack are identified.
- **Recover** - SpinSecurity automatically restores the files that have been identified as affected by the ransomware attack. G Suite administrators are notified of the attack and the automatic recovery.



SpinOne provides automated ransomware protection and remediation

SpinOne's two-fold, automated ransomware protection is unique among its competitors. Not only does SpinOne backup your business-critical data, it proactively monitors and secures your data against the very threats that often require data recovery such as ransomware.

SpinOne

ABOUT SPINONE

SpinOne is a multi-tenant platform created by Spin Technology and designed to simplify the complexity of cloud data security. As an all-in-one platform, SpinOne combines three solutions that make business data bulletproof from the security breach and insider threats: SpinSecurity, SpinAudit, and SpinBackup.

SpinOne is trusted by over 1,500 organizations worldwide including HubSpot, Vopak, IBT Industrial Solutions. We have more than 1,200,000 business users in more than 100 countries.

Try SpinOne Free →

Spin Technology Inc

2100 Geng Rd Suite 210

Palo Alto, CA 94303, USA

USA and Canada Toll Free:

+1-888-883-2993
(9am to 5pm PST)

EU, CIS and Asia:

+48-22-602-2440
(7am to 4pm GMT)