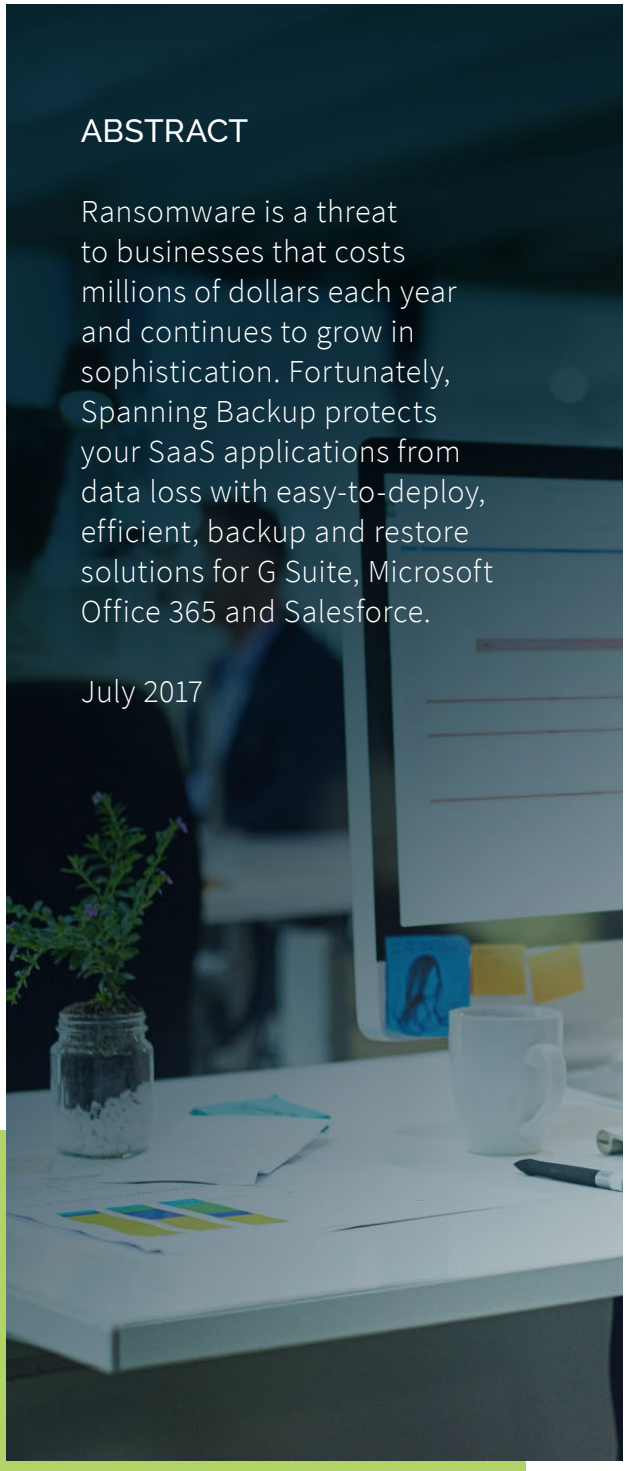
PREVENTING A RANSOMWARE DISASTER

Ransomware is not just another cyberattack; it can quickly proliferate through shared folders.

—

SPANNING



ABSTRACT

Ransomware is a threat to businesses that costs millions of dollars each year and continues to grow in sophistication. Fortunately, Spanning Backup protects your SaaS applications from data loss with easy-to-deploy, efficient, backup and restore solutions for G Suite, Microsoft Office 365 and Salesforce.

July 2017

CONTENTS

INTRODUCTION

Ransomware is a threat to businesses that costs millions of dollars each year and continues to grow in sophistication.

Using a variety of attacks, including targeted emails and infected websites, criminals can inject malware into your network, which then holds your data or other systems hostage until you pay a ransom. It's very difficult to block every ransomware attack, so many experts, including the FBI, advise organizations to have a layered defense with protected backups to enable a fast recovery.

Organizations following this advice often focus on key internal systems and forget about their endpoints—desktops and laptops—and SaaS applications, like G Suite and Microsoft Office 365, which contain data that is critical for employees to function. Fortunately, Spanning Backup protects your SaaS applications from data loss with easy-to-deploy, efficient, backup and restore solutions for G Suite, Microsoft Office 365 and Salesforce.

> "Never before in the history of humankind have people across the world been subjected to extortion on a massive scale as they are today."
>
> —
>
> Symantec Internet Security Threat Report

THE RISE OF RANSOMWARE

The first known ransomware was Trojan.Gpcoder, which was discovered in 2005 and affected Windows operating systems. More than 10 years later, there is little doubt that ransomware is on the rise. In fact, new ransomware antivirus detections increased by 36 percent during 2016, from 340,000 in 2015 to 463,000 during 2016. The daily rate of antivirus detections for ransomware also increased during 2016, averaging approximately 846 per day at the beginning of the year and rising to more than 1,539 a day at year end, according to the 2017 Symantec Internet Security Threat Report (ISTR).

There is no compelling reason to believe that the threat of this type of malware will not continue to increase dramatically. The reason is simple: "Ransomware is easy to develop, simple to execute, and does a very good job of compelling victims to pay to regain access to their precious files or systems." [1]

Although ransomware knows no geographical boundaries, the top six countries affected by this type of malware in 2016 were the United States, Japan, Italy, Canada, India, and the Netherlands.[2]

Consider the following ransomware attack that occurred in 2017.

WannaCry Decryptor Ransomware

WannaCry was first detected as cybercriminals manipulating tools called EternalBlue, a malware exploiting Windows Server Message Block (SMB) file-sharing services, and DoublePulsar, a backdoor, began propagating the ransomware via un-patched Windows computers. Once a computer was infected, it would scan the local network and the wider area network to find other vulnerable computers to infect. After infection, the ransom demanded was between $300-600 paid in Bitcoin.

On two occasions, since the infections started to spread, "kill switches" were discovered, but ultimately bypassed with newer, modified code. The most recent update suggests the WannaCry code has faults that could help potential targets. "After deeply analysing the WannaCry code, security company Kaspersky Labs found that the ransomware was full of mistakes that could allow some of its victims to restore their files with publicly available free recovery tools or even with simple commands." [3]

[1] Ransomware a Favorite of Cybercriminals, Matthew Rosenquist, McAfee Blog Central; September 1, 2015.
[2] The evolution of ransomware, Version 1, page 5; Kevin Savage, Peter Coogan, Hon Lau; Symantec; August 6, 2015.
[3] WannaCry Coding Mistakes Can Help Files Recovery Even After Infection, Swati Khandelwal, Hacker News; June 2, 2017.

WHAT IS RANSOMWARE AND HOW DOES IT SPREAD?

Ransomware is not just another cyberattack; it can quickly proliferate through shared folders, affecting both those within and outside the infected organization. Ransomware either locks the computer (locker ransomware) or encrypts the user's files (crypto ransomware) and then demands that the user pay a specified amount of money—usually a digital payment such as Bitcoin—in exchange for a decryption key that unlocks the computer or files.

Ransomware gains access to a computer system by way of a network's weakest link, which is typically a user's email or social networking site. Once a user clicks on a malicious link or opens an infected attachment, the malware spreads throughout the system.

Once opened, fake PDF files, fabricated FedEx and UPS notices, and fraudulent financial institution correspondence that are infected with malware can quickly bypass an organization's network security and spread beyond the local system through network drives and other endpoints tied to file sync and share tools such as Microsoft OneDrive, Google Drive and Dropbox.

According to the United States Computer Emergency Readiness Team (US-CERT), cybercriminals who use ransomware are so effective because they instill fear and panic into their victims, in part by displaying intimidating messages such as: "Your computer was used to visit websites with illegal content. To unlock your computer, you must pay a $100 fine." But ransomware has gained wide adoption among cybercriminals for other reasons as well: the ease by which it is created and deployed.

The gist of ransomware is simple: if you don't pay the ransom, you forfeit access to your computer and the data that's on it. And you further forfeit access for others to shared documents and data, compounding the impact exponentially. Unfortunately, victims who pay the ransom might still not get their files back.

The harsh reality is that the attacker might not supply the decryption keys. In fact, a recent survey found that of those victims of ransomware who paid the ransom, only 71 percent had their files restored.[4]

[4] Crypto-Ransomware: Survey of IT Experts, page 16, Jeffrey Henning, Researchscape International; February 4, 2016.

REALITY OF RANSOMWARE

The rise of ransomware has moved more from targeting consumers to organizations. Phishing campaigns were one of the biggest issues up to 21% (from 8% in the previous year), according to the 2017 Verizon Data Breach Investigation Report (DBIR).

Data that's key to an organization's daily operations or subject to regulatory compliance must always be protected. Hackers don't necessarily care who the information belongs to; they will do their best to exploit any weakness in the IT infrastructure to steal, damage, or hold for ransom an organization's data.

Businesses know that it's very difficult to protect against every threat, but ransomware is particularly challenging. Companies have to maintain focus on business continuity, which can lead them to be more likely to entertain paying a ransom.

Crypto ransomware, such as CryptoWall or Locky, account for the majority of all ransomware. The good news is ransomware, in general, dropped in 2016-17 due to variant decreases (number of unique, individual examples) and generic ransomware detections, but other actors like WannaCry continue to surface and plague users worldwide. According to the Symantec Internet Security Threat Report, new ransomware variants numbered 241,000 in 2016.

"Never before in the history of humankind have people across the world been subjected to extortion on a massive scale as they are today."[5]

Effectively defending against ransomware requires not only threat detection and prevention, but a backup and recovery strategy. Failing to do so can result in significant costs. Recent research found that the average mean ransom demand seen in 2016 rose more than threefold from $294 to $1,077. [Symantec Internet Security Threat Report]

Finally, consider Ransomware-as-a-Service (RaaS); this is becoming the newest concept in the blackhat community as developers create tools that can be sold en masse to smaller criminals to then be launched against individuals and companies. This gives everyone involved a "piece of the action" and allows the dispersal mechanism to be co-opted out and decentralized.

[5] Internet Security Threat Report, Volume 21, page 58, Symantec, April 2016.

WHAT CAN BE DONE?

So how do companies mitigate the risk of ransomware attacks in their organizations? A consistent and defense-in-depth, multi-layer approach that involves software vendors, customers, ops, processes and security is critical.

It is important to note that common backup solutions such as a USB drive or network-attached storage device (NAS) are not reliable methods for backing up and safeguarding your data.

Ransomware typically spreads throughout an organization's entire file system, including an attached drive or network share, encrypting both production data and backup data.

The most reliable form of protection organizations can leverage to safeguard their data is backup. The more your backup supports fast, easy restore to the pre-infection state, the less likely you will be to suffer a massive failure of business continuity.

Like most criminals, cyber criminals are opportunists who seek out easy targets. Are you an easy target? For starters, consider these questions:

- Are you backing up your data?
- Are your employees aware of the risks of unsolicited emails?
- Are your firewalls and mail filters always up to date?
- Are you using expired antivirus software?
- Are you syncing data from endpoints up to cloud-based file sync share systems?

Having a viable backup and recovery plan is not just a sound operational practice, it is often required by law or regulation, depending on your organization's industry or type:

- HIPAA requires healthcare organizations to have and periodically test a viable data backup and disaster recovery plan for their electronic protected health information.[6]
- Two financing and banking enforcement arms, the OCIE and FFIEC, have made cybersecurity—including the ability to recover from incidents—a key part of their enforcement and audit priorities.[7]

The SEC has reminded public companies of their need for adequate cyber controls, which include backup and recovery functions, and responsibility to disclose material cybersecurity risks. In today's world, certainly the inability to recover from an increasingly common threat such as ransomware could rise to the level of disclosure.[8]

In the event of hardware failure, theft, virus attack (including a ransomware extortion plot), accidental deletion, or natural or manmade disaster, if you have the right backup and recovery solutions in place, you can ensure that your data will be available and can be restored to its original state, and that your organization is compliant with applicable regulations.

When looking for a backup solution, what should you evaluate to ensure that your data is protected? Consider the following:

- Do you have SaaS data that could be targeted?
- Is the backup off site (away from your primary site)?
- Can you verify that the backups are happening?
- Can you verify that data can be restored to its original state?
- How quickly can you restore data that's been taken hostage?
- Can you backup to a specific point-in-time?

[6] HIPAA Security Rule, 45 CFR 164.308(7).
[7] National Exam Program Risk Alert, Volume IV, Issue 8; September 15, 2016.
[8] Emerging SEC guidance and enforcement regarding data privacy and breach disclosures, Joseph D. Masterson, Inside Counsel; June 25, 2015; and Cybersecurity Update: Heightened Concerns, Legal and Regulatory Framework, Enforcement Priorities, and Key Steps to Limit Legal and Business Risks, Paul Weiss; September 30, 2015.

BACKING UP YOUR DATA WITH SPANNING

Implementing a backup system is a critical step in your data protection planning since it ensures you are well prepared to quickly recover from data loss—not just from ransomware attacks but also from other malicious attacks, end user errors, and configuration or sync errors.

Having a granular, complete and trusted backup service in place protects you in two ways:

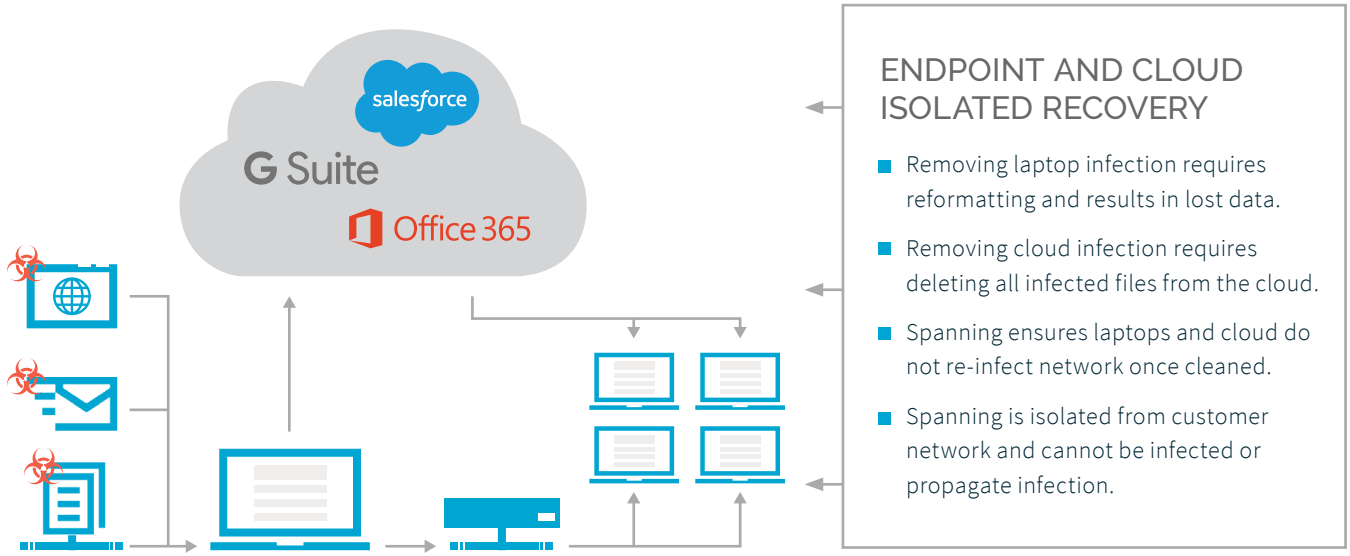
- First, your data is safe and can be restored from any point in time, easily by your IT admin.
- Second, you won't have to consider paying ransom to hackers, as you still have access to an unencrypted version of your data.

IT STARTS AT THE ENDPOINT

Recovering servers doesn't guarantee you've removed the infection from your network because it probably started at the endpoint as illustrated below.

Data that's backed up by Spanning is isolated from the customer network and cannot be infected or propagate an infection.

SaaS office productivity platforms such as G Suite or Microsoft Office 365 are also vulnerable to malware attacks, and Google or Microsoft may not be able to roll back your files to a pre-infected state.



Infected endpoint devices can sync with these platforms, and in some cases the malware can automatically proliferate through shared drives and folders, encrypting files shared within your and even outside of your organization.

Spanning Backup fully protects data that is stored and generated in G Suite and Office 365 and enables you to rapidly recover data from a previous point in time, before the files were encrypted by ransomware.

That means your data is safe, secure, and always available. These solutions ensure that you can respond and recover from an attack, and rapidly restore your data to its original state for business continuity and to meet recovery time and recovery point objectives.

Recent research found that the average mean ransom demand seen in 2016 rose more than threefold from $294 to $1,077.

—

Symantec Internet Security Threat Report

CONCLUSION

According to Symantec and Verizon, ransomware is utilizing many new avenues for infection: email, brute force, self-propagation, OS vulnerabilities, and third party app stores. Although prevention and detection are critical, a regularly updated backup that enables rapid, accurate restores is the last line of defense.

"The use of backup files is an effective way to minimize the impact of ransomware and… implementing computer security best practices is the most effective way to prevent ransomware infections. Individuals or businesses that regularly backup their files on an external server or device can scrub their hard drive to remove the ransomware and restore their files from backup. If all individuals and businesses backed up their files, ransomware would not be a profitable business for cybercriminal actors."[9]

Organizations rely on digitized data more than ever. As such, all organizations—from the smallest business to the largest enterprise—must take the necessary steps to ensure that their data is securely backed up and quickly restorable to its original state.

Spanning Backup solutions provide peace of mind, knowing that you can quickly and easily restore your data exactly the way it was at any point in time should a data loss event strike.

Backup is one thing. Restore is everything. We deliver the most fine-tuned and user-friendly restore process available for Office 365, Salesforce and G Suite.

To learn how to protect your SaaS data, visit Spanning.com, and follow us on LinkedIn or Twitter.

[9] U.S. Department of Justice, Federal Bureau of Investigation, Letter to Senator Ron Wyden, February 8, 2016.

SPANNING

Spanning is a leading provider of SaaS data protection solutions, helping organizations to protect and manage their information in the cloud. We provide powerful, enterprise-class backup and recovery for G Suite, Salesforce, and Office 365. Spanning Backup is the most trusted cloud-to-cloud backup solution for thousands of companies and millions of users around the world.

501 CONGRESS AVE, SUITE 200
AUSTIN, TEXAS 78701
P 512.236.1277

SPANNING.COM