Veeam Ransomware Resilience, Availability and Recovery

Executive Brief

Content

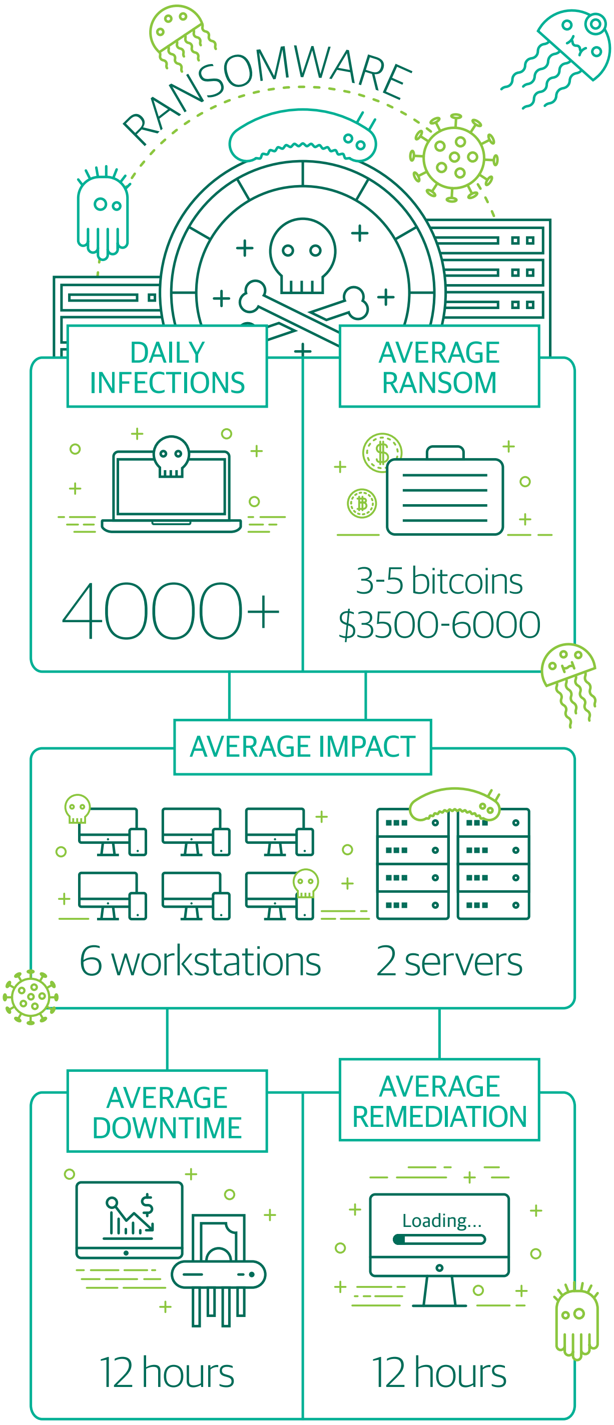
Introduction

Ransomware is a type of malicious software (malware) which restricts access to a computer and/or the files on a computer until a ransom amount is paid. Most commonly, ransomware spreads via cryptovirology, combining asymmetric and symmetric encryption to lock out users from managed file transfer or specific directories or files. It operates under the assumption that the encrypted data is important enough to users that they are willing to pay a ransom.

Originating in 1989, ransomware attacks have started spreading internationally around 2012, with infection approaches becoming more and more sophisticated and attack delivery getting easier and easier. Today, we hear about its gruesome effects and rapid spread impacting every industry worldwide.

Veeam® offers businesses and end users the confidence that their Digital Life will be Always-On™ and uninterrupted by ensuring they have the right ransomware resilience and recovery plans in place.

Everything you need to know about ransomware. Start the conversation today with [this FREE Conversational Ransomware Defense and Survival eBook](#).



Chapter 1: The true cost of ransomware

The U.S. Department of Justice recently referred to ransomware as a new business model for cybercrime and a global phenomenon. The frequency of attacks is alarming, increasing from 14% in 2016 to 27% in 2017, as noted by Accenture in a recent report on cybercrime. Looking further, Cybersecurity Ventures predicts that organizations globally will suffer a ransomware attack every 14 seconds by 2019.

Over the last two years, the overall cost of cybercrime has achieved new heights - businesses worldwide ended up paying, on average,US$11.7 in 2017 alone. Specifically, global ransomware damage costs are estimated to exceed $11.5 billion annually by 2019. This figure takes into account much more than the ransom amounts, reflecting the wide range of possible ransomware outcomes. Indeed, technology and cybersecurity experts, as well as government officials worldwide, constantly remind us about the different dangers associated with this malware, from critical data loss to business operations disruption and reputational harm. Key ransomware damages include:

- Damage or loss of mission critical data
- Production downtime
- Lost productivity
- Post-attack disruption to the normal course of business
- Forensic investigation
- Restoration and deletion of hostage data and systems
- Reputational harm
- Loss of employee confidence

In many cases, victims of ransomware attacks who did not pay the ransom still faced massive direct and indirect costs, such as the ones listed above. More than half of respondents in a recent survey by Imperva of 170 security professionals at RSA admitted that the cost of downtime due to lack of system access was the most serious business impact of an attack. On average, downtime costs can range from $5,000 to $20,000 a day in lost business and damages.

As ransomware becomes a mainstream threat, cyberscurity spending forecasts show substantial growth moving forward. For example, Cybersecurity Ventures estimates the global spending on associated products and services will exceed $1 trillion in the period between 2017 and 2021. Another recent report by CyberEdge Group, showing the perceptions of 1,200 IT Security professsionals around the world, argues that the average IT security budget will rise by 4.7% in 2018, to constitute 12% of the total IT budget.

> "Whether companies choose to pay the extortion or not, the real cost of ransomware is downtime and lost productivity."
>
> — Terry Ray,
> Chief Product Strategist,
> Imperva

Even if Erie County Medical Center did not pay the requested ransomware of $30,000 following a cyberattack in April 2017, they ended up paying nearly $10 million in associated expenses. Approximately half of the sum was allocated to computer hardware, software and assistance needed in the aftermath of the attack. The other part resulted from a combination of increased expenses, such as staff overtime pay and lower revenues following the loss of business during the system downtime. Going forward, medical center officials also anticipated an ongoing additional expense of $250,000 to $400,000 a month for investments in upgraded technology and employee education to harden its computer system defenses to reduce the risk and impact of future attacks.

Chapter 2: Ransomware resilience, Availability and recovery

Ransomware resilience: Veeam best practices on data protection

Leveraging data protection and security best practices is crucial to protect your company's Digital Life. Veeam recommends a dual approach to combating ransomware: preparedness for what could be an inevitable attack and recovery. While no company or solution completely prevents ransomware, Veeam can deliver a backup and recovery solution that can ensure effective recovery from an attack when reccomended best practices are used.

Veeam Availability Platform offers you the most reliable solutions to quickly and effectively restore business operations and critical data across all workloads following a ransomware cyber-attack. By integrating Veeam Backup & Replication™ and Veeam ONE™ into your data protection strategy specifically for ransomware preparedness and recovery, you will remain resilient amidst an attack.

1. Patching

One of the most frequently recommended data protection best practices is patching. Every element of your IT infrastructure — operating systems, third-party applications such as antivirus solutions, as well as browsers and plugins — should be frequently updated. Most ransomware exploits succeed because they rely on vulnerabilities of endpoints, which can be easily addressed through patching.

2. Start using the 3-2-1 rule for data protection

This will help address any failure scenario without requiring specific technology:

- **Three copies of data:** In addition to the primary or production data, there should be a backup copy of the data and also a copy of the backup data. Ideally, these would be stored on different physical devices.
- **Two types of media:** It is imperative to use multiple forms of media to prevent ransomware to avoid drives in the same data center from being corrupted. Veeam natively supports backup to a variety of media types including disk, tape, backup appliances and the cloud.
- **One off-site copy:** Veeam's advanced backup and replication capabilities make it easy to have off-site, image-based replication and backup copies to a second location being offsite, tape or the cloud with Veeam Cloud Connect. With Veeam Cloud Connect you can store a backup copy offsite, to tape or in the cloud. Veeam offers WAN acceleration and encryption to provide fast and secure replications and backup copies.

Moreover, to effectively prepare in the advent of a ransomware attack, you should ensure that **one of the copies is air-gapped**, i.e., on offline media. The offline storage options listed below highlight many options where you can implement an offline or semi-offline copy of the data.

3. Have offline storage as part of the Availability strategy

One of the best defenses against the propagation of ransomware encryption to the backup storage is to maintain offline storage. There are numerous offline (and semi-offline) storage options with Veeam. These include:

- Tape: Completely offline when not being written or read from
- Storage snapshots of primary storage: A semi-offline technique for primary storage, but if the storage device holding backup supports this capability, it is worth leveraging to prevent ransomware attacks. It is important to consider that this strategy is not entirely failsafe and must be taken as only one of the key steps needed in ensuring ransomware preparedness
- Cloud: A great additional resource for resiliency against ransomware. For one, it's a different file system and secondly, it is authenticated differently. Backups in the cloud, whether it is Veeam Cloud Connect or object storage, are also off site. Veeam Cloud Connect provides a fully integrated, fast and secure way to back up, replicate and restore from the cloud
- Rotating hard drives (rotating media): Offline when not being written to or read from

4. Use different credentials for backup storage

Although this is a standard and well-known anti-ransomware best practice, it's crucial to follow. The username context that is used to access backup storage should be closely guarded and exclusive for that purpose. Additionally, other security contexts shouldn't be able to access the backup storage other than the account(s) needed for the actual backup operations. Do not use DOMAIN / Administrator for everything.

5. Leverage different file systems for backup storage

Having different protocols involved can be another way to prepare for a ransomware attack. It's imperative that users add backups on storage that require different authentication. Having a Linux system functioning as a repository is a good example. The risk of ransomware propagation can arguably be reduced by using a different file system (ext3, ext4, etc.) and authenticating Veeam backup and restores over Linux. It must be noted, however, that this strategy is not failsafe either. For example, the Linux repository might be reachable through the SMB protocol. In this case, the ransomware on a Windows box could still encrypt the data on the Linux box.

6. Perform regular risk assessments

This should become an integrated step of your data protection strategy to ensure a proactive identification of potential risks and ensure you achieve complete visibility of your IT infrastructure. In order to get prepared for recovery in case of an attack, you need to be able to verify the recoverability of your data. Veeam Availability Suite™ contains a solution for precisely this purpose. Veeam ONE is a powerful monitoring, reporting and capacity planning tool for the Veeam backup infrastructure. It includes off-the-shelf reporting, which performs backup assessments to assure you are protected and also has a built-in alert to warn of potential ransomware activity.

7. Let the Backup Copy Job do the work for you

The Backup Copy Job is a great mechanism to have in order to create restore points on different storage and with different retention rules than the regular backup job. When the previous points are incorporated, the Backup Copy Job can be a valuable mechanism in a ransomware situation because there are different restore points in use with the Backup Copy Job. However, with the Backup Copy Job being a VBK file, it can also get infected with ransomware unless the copy is in a cloud, on tape or air-gapped.

8. Educate all employees on ransomware, not just your IT staff

Social engineering and phishing schemes are effective when companies do not educate employees on the dangers of ransomware nor the specific activities that leave the company vulnerable. Establish a strong source of education, communication and support to ensure the entire company is equipped to avoid propagating a ransomware attack.

Ransomware recovery: Veeam Availability and recovery solution

Protecting the data center

Veeam enables companies to quickly and effectively restore critical data infected by ransomware to a known good state. An essential part of the Veeam Availability Platform, Veeam Availability Suite provides a **turnkey solution to recover from ransomware as well as an enterprise-class data Availability solution for day-to-day operations** through:

- **Rapid restores from ransomware attacks through fast VM and granular recovery** to override encrypted ransomware databases, applications, files and operating systems. This is easily possible with Veeam Explorer™ for Storage Snapshots and 1-Click file restore scenario.
- **Rapid recovery and uninterrupted application performance with** tight integration with the word's leading storage vendors like Hewlett Packard Enterprise (HPE), Dell EMC, NetApp, IBM, Lenovo and INFINIDAT
- **Test and discover recovery points** to quickly and easily discover last good restore point using Veeam On-Demand Sandbox™.

Protecting the endpoint

In addition to including data center protection, an efficient Availability and recovery plan takes ensuring the protection of endpoint devices: Laptops and PCs. Ransomware can affect both Windows and Linux systems. Veeam Agent *for Linux* and Veeam Agent *for Microsoft Windows* essentially offer image-based Availability for non-virtualized systems. In order to avoid propagation in case of a ransomware attack, they offer the option of placing backups on different file systems through seamless integration with Veeam Availability Suite.

Despite having in place preventive practices and solutions, ransomware can still hit you. When this happens, a **quick and efficient response process** will ensure no or minimum impact on your business operations:

- Disconnect infected systems from the network, as well as disable Bluetooth and Wi-Fi to stop the malware from spreading further
- Quickly remove any USB sticks or external hard drives connected to an infected computer to prevent them from being locked and keep them unattached as long as possible
- Alert authorities before making any decision
- Do not pay the ransom! Paying the ransom will propagate the problem and provide the attackers with more resources to continue developing more advanced attacks and more manpower. They will most likely retain your system's vulnerabilities and continuously attack for recurring revenues. Moreover, according to research and marketing firm CyberEdge Group, half of organisations that pay ransoms never get their data back, while the other half acknowledged complete data loss.
- Use version history in online file services to recover to a previous version
- Recover from backups — your safe-haven

Chapter 3: Prepare for the future: Act now!

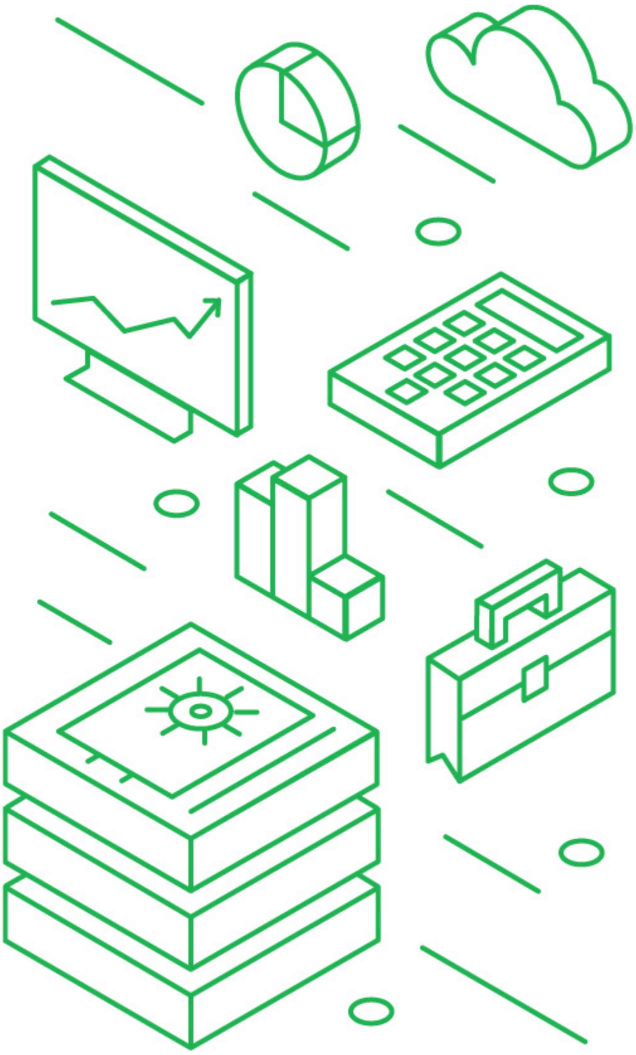
The cyberthreat landscape has transformed considerably since the surge of ransomware around five years ago. In response, the majority of businesses have re-designed and strengthened their security strategies. Those who have failed to do so have paid the consequences.

Looking forward, we envision a multitude of new opportunities and revenue streams for the Always-On Business™. For example, the Internet of Things has been transforming our lives for the last two decades, ultimately paving the way to innovative methods of conducting business and delivering new insights. Although such innovations imply endless benefits for business and consumers, they also bring many new security challenges.

Cybersecurity Ventures predicts that there will be six billion Internet users by 2022. Cisco also reports that global IP traffic grew fivefold over the past five years and predicts that it will continue to grow threefold over the next five years. While we become increasingly connected, cybercriminals will continuously find more vulnerabilities to exploit. Consider this: 111 billion lines of new software code are produced annually, introducing numerous vulnerabilities along the way. Recent increases in BYOD and mainstream IoT adoption are further contributing to the increasing complexity of securing an IT environment by creating new system and human vulnerabilities that can be easily exploited.

The rate of digital transformation is outpacing our ability to secure our increasingly digital lives. In the aftermath of previous years' attacks and giving the gloomy future expected, organizations and end users will likely pay more attention to security in 2018. They have learned the hard way that ransomware is a highly expensive threat to ignore. Organizations and their customers require 24.7.365 access to account information and mission critical data and thus to protect it at all costs.

By using Veeam and our recommended best practices you will be prepared and ready to recover should your data get infected by ransomware. The Veeam Availability Platform **is the most reliable solution to support businesses and end users on their journey to ransomware resilience, recovery and Availability across all workloads.**



Learn more

All capabilities shown are standard with **Veeam Availability Platform** combined integration with modern storage.

Get a **free 30-day trial key for Veeam Availability Suite** for ransomware preparedness and recovery.

Learn how Bedford School recovered ransomware encrypted files without any impact with Veeam.

VEEAM IS VERY PROUD OF OUR

1 000 000 USERS

53 000 PARTNERS

282 000 CUSTOMERS

80 TOP INDUSTRY AWARDS

About Veeam

Veeam® has pioneered a new market of *Availability for the Always-On Enterprise*™ to help companies solve the challenges of keeping their businesses up and running at all times. Veeam enables the Always-On Business™ with solutions that provide recovery time and point objectives (RTPO™) of less than 15 minutes for virtualized applications and data.

www.veeam.com