ITPro Today™

EXECUTIVE SUMMARY

Data Protection, Disaster Recovery, and Ransomware Protection with DRaaS

- Ransomware attacks are common and costly, yet businesses are not prepared.
- Patching, layered security, and backups help protect businesses against attacks.
- Veeam helps IT teams follow the 3-2-1 rule of data protection with zero errors.
- KeepItSafe provides cloud-based ransomware protection featuring Veeam.

MARCH 14, 2018

Brandon McCoy, Inside Systems Engineer, Veeam Software
Michael Otey, Senior Contributing Editor, *Windows IT Pro* and *SQL Server Pro*
Patrick Rougeau, Senior Sales Engineer, KeepItSafe

in partnership with

KeepItSafe®

EXECUTIVE SUMMARY

Data Protection, Disaster Recovery, and Ransomware Protection with DRaaS

Overview

Ransomware is one of the biggest threats in the cybersecurity space today, and the number of ransomware attacks is expected to continue to grow significantly, impacting businesses of all types and sizes.

Businesses can best protect themselves against ransomware, as well as other virtual and physical disasters, by using data protection backup solutions. These disaster recovery (DR) and disaster recovery as a service (DRaaS) solutions allow organizations to back up systems and data in cloud datacenters so that they are available when a crisis, such as a ransomware attack, strikes.

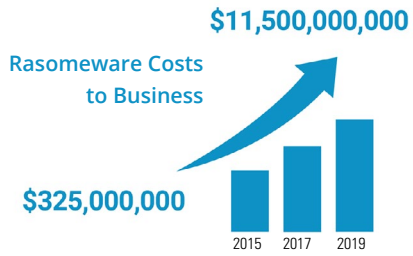
Context

These cybersecurity experts came together to discuss one of the most significant cybersecurity risks companies face today: ransomware. They described the challenges that ransomware poses to businesses and shared best practices for protecting against ransomware attacks. Among the best practices they discussed were Veeam's data protection solutions and KeepItSafe's cloud backup and recovery offerings.

Key Takeaways

Ransomware attacks are common and costly, yet businesses are not prepared.

Ransomware is one of the fastest growing threats in the rapidly expanding data protection space. Ransomware cost businesses $5 billion worldwide in 2017 and is projected to cost $11.5 billion in 2019. Despite the steep cost of these attacks, most businesses are still not prepared; only 38% of global businesses say they are ready for a sophisticated attack.



These malicious attacks spread in a number of ways, including email, social media, and system vulnerabilities. When ransomware gets into a system, it encrypts some portion of the data, requiring Bitcoin payment for an encryption key. Once the ransom is paid, however, the encryption key may not actually work.

The damage can be significant in that the business is noted as one that is seen as vulnerable, both by prospective attackers and—in some cases—by the media and consumers. Vulnerability to a ransomware attack can cost a business money, customers, and its reputation.

> *During the downtime [from ransomware], there's damage to your reputation, user confidence, and consumer trust. Ransomware costs are more than just straight-up dollars.*
>
> Michael Otey

Patching, layered security, and backups help protect businesses against attacks.

Some of the most common security risks that can expose a business to ransomware include missing system patches, weak passwords,

Data Protection, Disaster Recovery, and Ransomware Protection with DRaaS

excessive user permissions, unaccounted-for systems, and outdated software. Businesses can begin to protect themselves by tackling these common problem areas, implementing a layered security approach, and using backups.

Data Protection Best Practices

- Keep systems patched
- Use a layered security approach, including firewalls, perimeter security, antivirus solutions, and network segmentation
- Back up and replicate systems and data, offsite and in the cloud

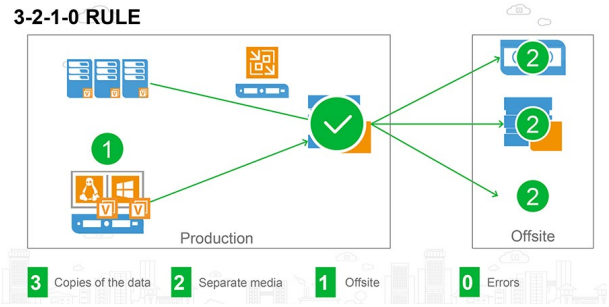
Backups are the foundation for all data protection and DR strategies. Storing backups offsite at a separated site or in the cloud further helps the business protect against ransomware attacks, since offsite backups are unlikely to be impacted by an onsite attack.

Hybrid cloud is an ideal solution for backups. Inexpensive cloud storage allows the business to reduce storage hardware and management costs. Additionally, since the backups are already located in the cloud, this ensures that copies are stored offsite in the event of a security attack.

Veeam helps IT teams follow the 3-2-1 rule of data protection with zero errors.

The 3-2-1 rule of data protection helps businesses ensure that they have good, accessible copies of their critical data in the event of an emergency. Veeam's backup, recovery, and data management solutions help IT teams follow this best practice:

- Having (at least) **3** copies of the data . . .
- On **2** separate media . . .
- At (at least) **1** offsite location
- Ensuring **0** errors if a restore is necessary



Veeam offers additional solutions and features that help businesses protect against ransomware, both on-premises and in the cloud. Veeam's solutions include:

- **Veeam® Backup & Replication™** delivers Availability for ALL workloads—virtual, physical, cloud (including VMware vSphere and Microsoft Hyper-V)—from a single management console.
- **Veeam Cloud Connect** provides a fully integrated, fast, and secure way to backup and replicate to a service provider's cloud repository.
- **Veeam SureBackup** creates a virtual lab that lets you test VM backups and make sure that you can recover data from each backup without disruption to production.
- **Veeam ONE Monitoring and Reporting** performs a backup assessment to ensure production, backup, and replication environments are protected.
- **Veeam Backup for Microsoft Office 365** recognizes that cloud services are not immune to ransomware attacks. This solution backs cloud-based Microsoft Office 365 data, such as Outlook mailboxes, to an on-premise location so they can be restored if an attack occurs or the data is otherwise corrupted.

Data Protection, Disaster Recovery, and Ransomware Protection with DRaaS

A lot of customers think that Office 365 is a backup and that all of their data is safe because it's in the cloud with Microsoft. But at the end of the day, it's just a service.

Brandon McCoy

KeepItSafe provides cloud-based ransomware protection featuring Veeam.

KeepItSafe offers cloud backup and recovery solutions that feature Veeam to deliver disaster recovery as a service and other file backup solutions. With 20+ global data center locations, KeepItSafe provides global cloud data availability for cloud backup, disaster recovery, endpoint protection, and SaaS application backups, such as Office 365. This comprehensive backup and recovery suite of solutions enables organizations of all sizes and across any vertical to protect their business-critical data. Ransomware protection is built into each solution so that businesses are able to quickly protect against and recover from an attack. KeepItSafe delivers a holistic data protection strategy that combines security and compliance with custom managed and monitored services including 24/7 support.

Ransomware protection with KeepItSafe	
Unlimited file versioning	Go back to a specific point in time to restore unencrypted files
Data protection for all data sets	Organization-wide visibility of all corporate data, regardless of where it resides
Granular restore	File-level restore capabilities for endpoints and cloud applications to ensure information on traveling devices is never lost
Delta blocking	Activate your organization's recovery time objective (RTO) through delta blocking and bandwidth throttling
256-bit advanced encryption standard (AES) encryption	Military-grade, 256-bit AES encryption, both at rest and in flight
Redundant tier-IV data centers	Data stored in multiple geographically strategic data centers for both easy access and failover

[Ransomware] is really scary. But one of the main ways we protect at the end of the day is with backup: being able to recover an entire system that's been encrypted.

Patrick Rougeau

Biographies

Brandon McCoy
Inside Systems Engineer, Veeam Software

Brandon McCoy is an inside Systems Engineer at Veeam Software. Before Veeam, Brandon worked at Arrow Electronics as a lead sales rep for Fujitsu's X86 business. He currently serves as Veeam's dedicated VCSP & Cloud engineer for the entire U.S. as well Federal end users. His background and current position allows him to bring a unique perspective of sales-driven approaches to complex I.T. solutions in the public and private cloud space as well as security considerations for the federal government.

Michael Otey
Senior Contributing Editor, *Windows IT Pro* and *SQL Server Pro*

Michael Otey is a senior contributing editor for *Windows IT Pro* and *SQL Server Pro* and is president of TECA a technical writing, content creation, software-development and consulting company in Portland, Oregon. Michael is a former SQL Server Microsoft MVP. He covers data center, SQL Server, Windows Server, virtualization, hardware, storage, Azure, the hybrid cloud, systems management, VMware vSphere, containers, and PowerShell.

Patrick Rougeau
Senior Sales Engineer, KeepItSafe

information technology space. With a background in IT consulting, IT management, and disaster recovery planning. Patrick currently serves as a Solutions Engineer at KeepItSafe®, helping IT departments achieve their backup and recovery goals. Through speaking engagements, webinars, meetups and blogging Patrick spreads the word on what technologies best serve KeepItSafe®'s ever expanding client base.