Hewlett Packard Enterprise

Business white paper

HPE SimpliVity Hyperconverged Infrastructure—Mitigate Ransomware Risks

Executive summary

Ransomware has quickly become one of the most pervasive and dangerous cyber-threats. The latest ransomware attacks can evade even the most stringent enterprise security systems and practices and quickly spread throughout an organization, disrupting user productivity and business operations.

Comprehensive **backup and recovery** plans are absolutely essential for combating today's sophisticated ransomware threats. By quickly restoring infected applications and data to their previous clean state, IT organizations can minimize the impact of a ransomware outbreak and limit revenue loss and customer frustration.

This paper reviews ransomware trends and implications and explains how **HPE SimpliVity hyperconverged infrastructure** accelerates data backup and recovery functions, mitigating ransomware risks.

Today's ransomware is sophisticated, destructive, and inescapable

Ransomware is a top concern for today's IT organizations. Across the world, ransomware attacks are growing in diversity, complexity, and severity. According to a 2016 report, ransomware "has quickly emerged as one of the most dangerous cyber-threats facing both organizations and consumers, with global losses now likely running to hundreds of millions of dollars."[1] It can impact any business, regardless of size or industry, causing downtime and financial loss.

A few years ago, ransomware was fairly primitive and benign. So-called "computer locker" attacks would seize a computer by disabling keyboard or mouse functionality. (Theoretically, the cybercriminal would unlock the keyboard upon receipt of ransom payment.) In most cases, IT professionals could simply ignore ransom demands and restore an infected computer to its previous working state using off-the-shelf malware removal tools.

Much has changed in the past several years. Today's ransomware attacks are far more advanced and invasive. The latest ransomware programs are capable of encrypting data files and locking users out of their own data. The encryption can spread throughout an organization, locking up data across the enterprise, and disrupting business operations. Some variants even threaten to post confidential data to the internet unless a ransom is paid.

These attacks are difficult to prevent or remediate. All are specifically designed to avoid detection by security applications, using techniques like polymorphism and throwaway command and control servers. Post-infection, the malware also impairs recovery efforts. Some encrypt native Windows® backup files, prohibiting restoration without a decryption key. Others simply delete native backup files altogether, making recovery impossible.

[1] Symantec ISTR Special Report: Ransomware and Businesses 2016

Ransomware is becoming more pervasive every month, putting an increasing number of businesses at risk. Contemporary ransomware attacks are aimed not only at Windows machines, but also at Linux® and Mac OS systems, and mobile devices. And new "ransomware-as-a-service" schemes allow any criminal with basic computer skills and internet access to get into the ransomware business. The ransomware author makes the malware available to other cybercriminals in exchange for a percentage of the ransom payment.

Paying ransom is not the answer

Some businesses may be inclined to simply pay ransom requests to restore normal operations as quickly and painlessly as possible. After all, the average ransom demand is only $679.[2] But law enforcement agencies like the FBI strongly encourage organizations not to pay ransom.[3]

According to the FBI:

- Paying a ransom does not guarantee an organization will regain access to their data; in fact, many businesses are never provided with decryption keys after paying a ransom.
- Some victims who paid the demand report being targeted again by cyber-actors.
- After paying the originally demanded ransom, some victims have been asked to pay more to get the promised decryption key.
- Paying could inadvertently encourage this criminal business model.

The true cost of a ransomware attack—system downtime and lost business

Ransomware attacks can wreak havoc on an organization's IT infrastructure. Prolonged system downtime can impair employee productivity and customer satisfaction, and impact a company's bottom line.

The true cost of a ransomware outbreak includes quantifiable costs like lost revenue as well as less tangible costs like damage to a company's reputation. The more widespread and drawn-out the disruption, the greater the costs. According to a Ponemon Institute study, the average cost of an unplanned data center outage approaches $9,000 per minute.[4] The same study puts the average cost of a cyberattack at $740,357.

Rapid data backup and recovery is fundamental for business continuity

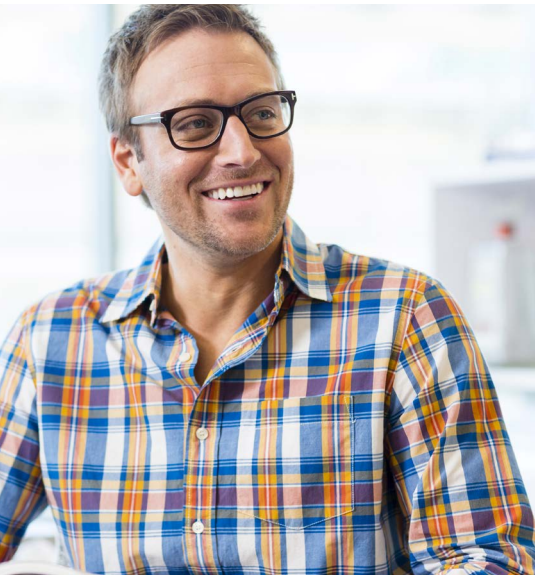
Unfortunately, even the best security systems and practices cannot fully protect against today's sophisticated ransomware attacks. The latest programs are specifically designed to evade signature-based detection. A comprehensive data backup and recovery plan is absolutely critical for restoring operations in the event of an outbreak.

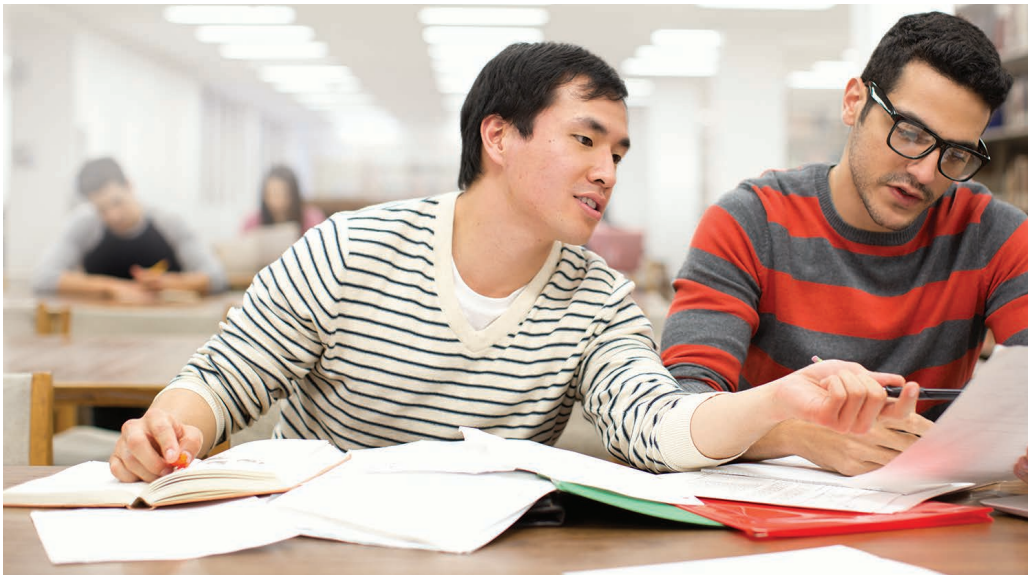
The best way to minimize the impact of a ransomware attack is to restore services as quickly as possible, with minimal data loss. A fast and efficient offline backup and recovery solution is paramount.

[2] Internet Security Threat Report, Volume 21, Symantec, April 2016

[3] Ransomware Prevention and Response for CEOs, Federal Bureau of Investigation, 2016

[4] Cost of Data Center Outages, Data Center Performance Benchmark Series, Ponemon Institute, January 2016





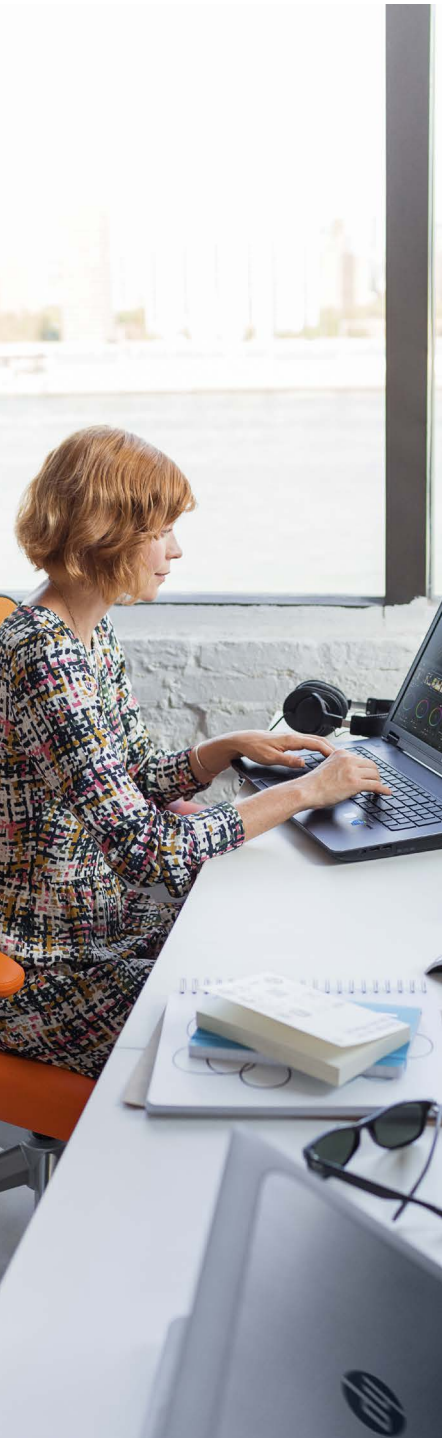
HPE SimpliVity accelerates data recovery and mitigates ransomware risks

There are steps a business can take to minimize data loss and company downtime brought on by a cyberattack. An important first step is defining the recovery time objectives (RTOs) and recovery point objectives (RPOs). IT administrators need to determine how long the business can afford to be shut down while waiting for the restore to take place, and how many hours of business-critical data the company can afford to lose.

Then, focus the data protection strategy around a solution that is capable of getting the infrastructure running again in the time provisioned. An HPE SimpliVity hyperconverged solution consolidates the IT infrastructure and simplifies both the data protection scheme and the recovery process, particularly for businesses with multiple remote offices to support. Solutions that offer integrated functions, such as built-in data protection, help to ease the burden at remote offices and provide better protection across the company.

HPE SimpliVity hyperconverged infrastructure provides a scalable, modular, 2U building block of x86 resources that offers all the functionality of traditional IT infrastructure—including hypervisor, compute, storage, and data protection capabilities—in a single device, with a unified VM-centric administrative interface. The HPE SimpliVity built-in data protection functionality accelerates data backup and restoration operations, helping IT organizations rapidly recover from ransomware attacks. The solution reduces equipment and operations expenses and complexity by eliminating or drastically reducing special-purpose data backup and recovery tools, data deduplication solutions, and WAN optimization appliances.

The HPE SimpliVity data efficiencies enable more frequent backups for near-continuous data protection, longer retention periods, and faster recovery. With HPE SimpliVity, terabyte-sized VMs can be backed up and restored in less than a minute—even over bandwidth-constrained WAN links. In the event of a ransomware infection, a VM and all its data can be restored quickly and easily, minimizing system downtime, business disruptions, and revenue loss.



The HPE SimpliVity solution performs inline deduplication, compression, and optimization on all data at inception across all phases of the data lifecycle (production, backup, off-site, and archive). By driving efficiencies at the point of origin, the solution conserves storage capacity and drastically reduces disk I/O and network traffic, accelerating data replication and workload mobility. Processor-intensive functions are offloaded onto purpose-built hardware, freeing up compute cycles for business-critical applications.

HPE SimpliVity's built-in data protection capabilities deliver:

- Full logical backups every time: Take full logical backups with no incremental chains or dependencies on parent VMs.
- Near-zero overhead: Back up VMs every few minutes with virtually no impact on running applications.
- WAN-efficient off-site replication: Reduce bandwidth costs by transferring only unique data between sites.
- Rapid recovery: Restore a 1 TB VM in less than 60 seconds, backed by the HPE SimpliVity HyperGuarantee.

HPE SimpliVity customers report a 70% improvement in backup and disaster recovery in an independent survey,[5] while 57% of customers reduced their recovery times from days or weeks to hours or minutes.[6]

HPE SimpliVity's global unified management capabilities simplify routine data backup and recovery tasks. IT generalists can configure backup policies and restore VMs in seconds with just two or three mouse clicks using familiar tools like **VMware® vCenter™**. The optional RapidDR solution simplifies and accelerates disaster recovery efforts through automation. Administrators can automatically power on and reconfigure VMs with a single mouse click, based on pre-configured workflows.

Real-world customers recover from CryptoLocker with HPE SimpliVity

HPE SimpliVity customers like **Carolina Sunrock** understand the implications of a ransomware attack firsthand. According to the systems administrator who deployed the HPE SimpliVity hyperconverged system, disaster recovery is no longer a concern. "About 2 months ago, we were hit with a CryptoLocker virus, and with HPE SimpliVity's DR, I was able to restore our data and have our Citrix® server back online in 45 seconds. With our old vendor, it would've taken me days."

When **Worth & Company's** production systems were hit with the CryptoWall virus, "we were able to restore all of our critical applications to a known working state within a matter of hours, minimizing the impact on the business. With our previous implementation some of our apps would have been out of commission for days."

Guelph Hydro Electrical Systems experienced similar results with HPE SimpliVity. Fast recovery was a critical factor when they were evaluating hyperconvergence vendors. The operations team needed to restore from a previous backup as quickly as possible, and the HPE SimpliVity infrastructure delivered on that promise. "With the backups, it's as simple as going back to earlier in the morning and right-clicking Restore from Backup. And within five minutes, the user is up and running." Guelph Hydro restored their database quickly after they discovered a CryptoLocker attack. "For other companies, this could have been a disaster. For us, it was an inconvenience."

5, 6 **IDC White Paper**, sponsored by HPE, "HPE SimpliVity Hyperconvergence Drives Operational Efficiency and Customers are Benefitting," June 2017

Conclusion

Contemporary ransomware programs can evade enterprise security systems, paralyze IT infrastructure, and disrupt mission-critical applications. A comprehensive offline backup and recovery solution is essential for remediating ransomware infections and limiting exposure. HPE SimpliVity hyperconverged infrastructure with built-in data protection has been proven to accelerate backup and recovery functions and mitigate ransomware risks. With HPE SimpliVity, organizations can restore critical applications quickly and easily, reducing business disruption and revenue loss.

Learn more at
hpe.com/info/simplivity

Make the right purchase decision. Click here to chat with our presales specialists.

Sign up for updates

© Copyright 2018 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

Windows is either a registered trademark or trademark of Microsoft Corporation in the United States and/or other countries. Citrix is a registered trademark of Citrix Systems, Inc. and/or one more of its subsidiaries, and may be registered in the United States Patent and Trademark Office and in other countries. Linux is the registered trademark of Linus Torvalds in the U.S. and other countries. VMware vCenter is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other third-party trademark(s) is/are property of their respective owner(s).

a00038991ENN, January 2018