White Paper

Mitigating Ransomware Risks with SimpliVity Hyperconverged Infrastructure

Executive Summary

Ransomware has quickly become one of the most pervasive and dangerous cyberthreats. 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 a pristine 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 SimpliVity hyperconverged infrastructure accelerates data backup and recovery functions, mitigating ransomware risks.

> "Ransomware has quickly emerged as one of the most dangerous cyberthreats facing both organizations and consumers, with global losses now likely running to hundreds of millions of dollars."
>
> – Symantec ISTR Special Report: Ransomware and Businesses 2016

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. Ransomware 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.

The latest ransomware attacks are difficult to prevent or remediate. All are specifically designed to avoid detection by security applications - using techniques like polymorphism and throw-away command and control servers - and to impair recovery efforts. Some encrypt native Windows backup files, prohibiting restoration without a decryption key. Others use deleteware to delete native backup files altogether, making recovery impossible.

Ransomware is also becoming more pervasive. 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.[1] But law enforcement agencies like the FBI strongly encourage organizations not to pay ransom.[2]

According to the FBI:

- Paying a ransom does not guarantee an organization will regain access to their data; in fact, some were never provided with decryption keys after having paid 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.[3] 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.

SimpliVity Accelerates Data Recovery and Mitigates Ransomware Risks

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. SimpliVity's 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 special-purpose data backup and recovery tools, data deduplication solutions, and WAN optimization appliances.

SimpliVity's inherent data efficiencies enable more frequent backups for near-continuous data protection, longer retention periods and faster recovery. With SimpliVity, terabyte-sized VMs can be backed up and restored in minutes or seconds—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.

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

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

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

SimpliVity's solution performs inline deduplication, compression and optimization on all data at inception across all phases of the data lifecycle (production, backup, offsite, archive, and in the cloud), across all storage tiers within a system (DRAM, Flash/SSD, and HDD). By driving efficiencies at the point of origin the solution conserves storage capacity and minimizes 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.

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 offsite replication. Reduce bandwidth costs by transferring only unique data between sites.
- Rapid recovery. Restore a 1TB VM in just 60 seconds, backed by SimpliVity's HyperGuarantee.

SimpliVity customers report a 70% improvement in backup and disaster recovery in a recent independent survey[4], while 63% of SimpliVity customers reduced their recovery times from days or weeks to hours or minutes.[5]

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. SimpliVity's 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.

> "When our 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."
>
> – Woody Muth, CIO, Worth & Company, SimpliVity Customer

[4] IDC White Paper, sponsored by SimpliVity, "SimpliVity Hyperconvergence Drives Operational Efficiency and Customers are Benefitting," April 2016

[5] TechValidate, TVID: AB9-336-72D

Recovering from Cryptolocker with SimpliVity

SimpliVity customer Central One Federal Credit Union understands the implications of a ransomware attack firsthand. The problem started a little after three o’clock on a July afternoon when a critical financial file couldn’t be processed by an employee. “It took a long while for the team to figure out exactly what was going on,” recalls Neal Reardon, assistant vice president of information systems and technology at Central One. “We thought it was a problem with our core application. So we called the application vendor, and they couldn’t figure it out, so we just kind of were waiting on it.” Eventually around 8:00PM a ransom demand was discovered.

The operations team realized it needed to restore from a previous backup as quickly as possible. A 500GB VM was restored in just seconds and the associated database was up and running in a matter of minutes. The entire recovery process took only about 15 minutes.

Bottom line: No data lost. No ransom paid. Rapid remediation.

> “When one of our customers was infected by ransomware we restored their business-critical applications and files in minutes. If we had relied on a traditional data protection solution the customer could have been down for a full day.”
>
> – Lars G. With, Managing Director, Iterum, Norwegian ASP and SimpliVity Customer

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. SimpliVity hyperconverged infrastructure with built-in data protection accelerates backup and recovery functions and mitigates ransomware risks. With SimpliVity, organizations can restore critical applications quickly and easily, minimizing business disruptions and revenue loss.

For more information, visit:
www.simplivity.com