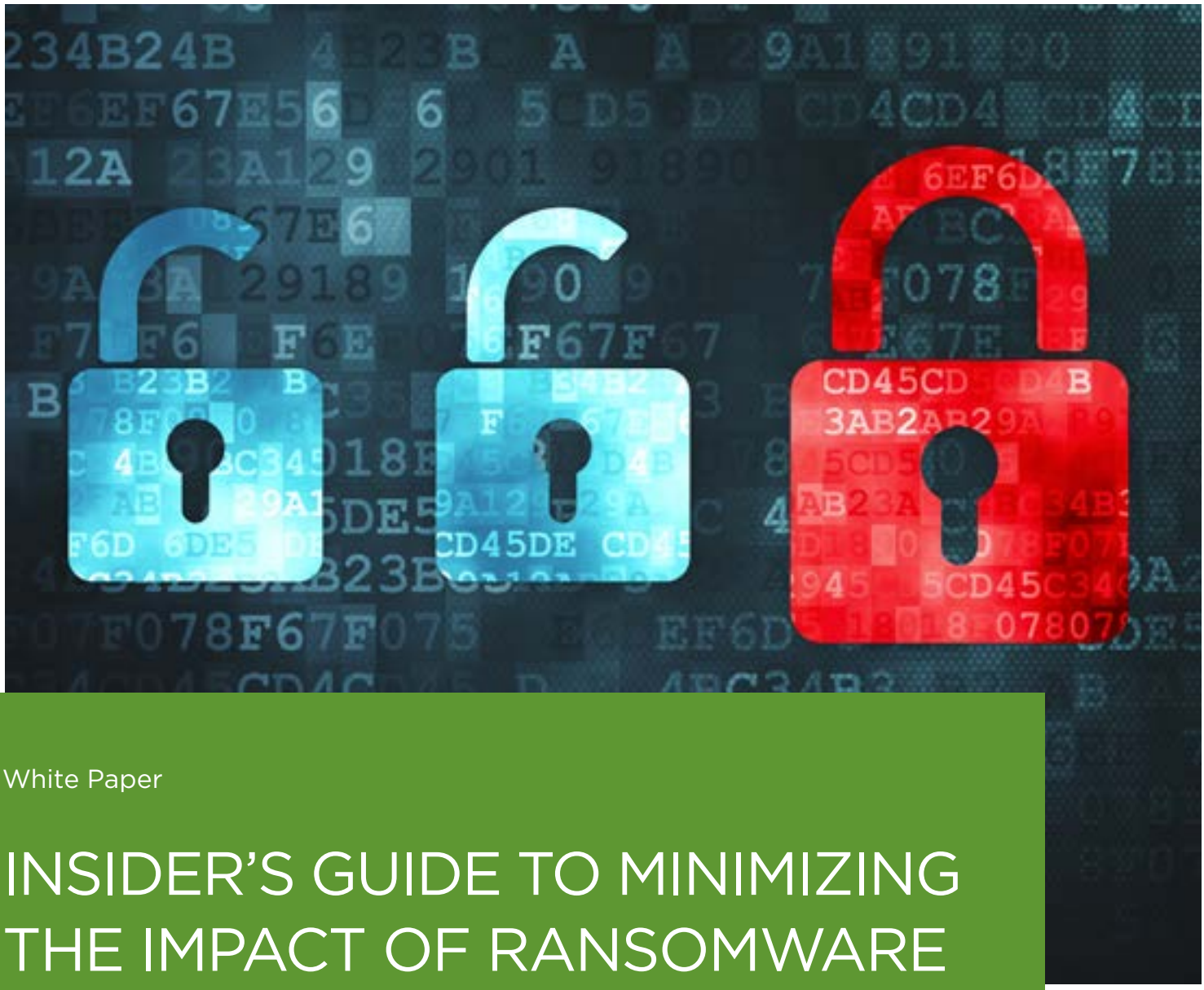
druva



White Paper

INSIDER'S GUIDE TO MINIMIZING THE IMPACT OF RANSOMWARE

Six Step Plan for Comprehensive Data Protection

Q319-CON-10938

Your Data Held Hostage

Ransomware attacks have become the cybercrime du jour, affecting a growing number of organizations nationwide. An easy, low-risk way for criminals to exploit almost any network intrusion, ransomware is a type of malware attack that prevents organizations from accessing their own data or computer system until they pay a ransom to obtain a decryption key.

Ransomware is on track to become a $11B industry

According to CyberSecurity Ventures, global damage costs from ransomware are estimated to be more than $8B in 2018 and up to $11.5B in 2019. By the end of 2019, they expect there to be a ransomware attack every 14 seconds (up from every 40 seconds in 2016).

No industry is immune from ransomware attacks, although some industries, like healthcare, have been hit harder than others. For instance, the NotPetya attack costed Merck more than $670M in 2017. As mentioned by Healthcare IT News, ransomware attacks on healthcare organizations are expected to quadruple by 2020. Similar to NotPetya, BBC reported that WannaCry, another significant attack, hit the British National Health Service in May 2017. It disrupted more than one-third of organizations—cancelling at least 6,900 patient appointments and surgeries (that number may be as high as 19,000 appointments in total).

With ransomware attacks on the rise, organizations of all sizes have found themselves vulnerable and struggling to reduce risk and respond to attacks.

Computing Conditions and Practices Open Door to Attacks

There are a number of security vulnerabilities that leave computing networks open to ransomware. Most incidents get through even the most elaborate perimeter defenses by phishing with a tainted link or e-mail attachment, luring an unsuspecting user. Systems with out-of-date or misconfigured software can also be compromised to help spread ransomware. While Windows computers have been a big target, Android and Mac systems have been targeted as well, meaning that no computing platform is safe. Dave Packer, Druva's VP of Product Marketing, put it this way: "The big issue at the end of the day is if there is any security hole, someone out there knows about it and is going to try to exploit it, and it's always going to be the people you don't want."

The widespread use of mobile devices by today's workforce has also escalated the risk of malware attacks. While many companies are protected by a corporate firewall, employees are now connecting to enterprise data and services using their own weakly protected mobile devices. Likewise, the deployment of unsecured mobile applications for employees and customers has created new opportunities for attacks.

> ***"The widespread use of mobile devices by today's workforce has also escalated the risk of malware attacks."***
>
> *— Dave Packer, VP of Product Marketing, Druva*

The Cost of Inaction

Organizations may be tempted to cross their fingers and hope they won't be targeted. Unfortunately, the chances of ransomware or other malware attacks are very high, with serious consequences for organizations that fail to take preventive action. In addition to paying a stiff ransom, victims may suffer costly business downtime and, in some industries, fines and penalties for data breaches, not to mention a loss in reputation as well. All of these can be very expensive in their own way. It likewise takes time and money to respond reactively to incidents

when there's no viable plan in place. Companies that pay the ransom to recover their data still face the threat of significant data loss if their files are altered during the decryption process, especially if an organization is under litigation as it poses the risk for data spoliation. And don't forget that many victims of ransomware never recover their data even if they do pay the ransom.

Before Ransomware Strikes

75 percent of organizations infected with ransomware were running up-to-date endpoint protection (Sophos News). In order to prevent these attacks and get ahead of the damage that can be caused, more organizations are now seeking proactive approaches to solving major issues involving data loss and intrusion. Traditional security solutions like firewalls, intrusion detection/prevention systems (IDS/IPS), and data loss prevention (DLP) solutions, while preventing some attacks, are always constrained by their inability to fully prevent and recover from newly emerging threats.

Organizations need to be empowered with a solution that can provide intelligence around their data points, events, and actions that are outside of the expected data behavior patterns of a given set of users. The end result is a highlighting of potentially malicious activity. These early anomaly insights could be significant indicators of cyber intrusions, employee fraud, or rogue behavior. Such a solution—commonly referred to as an unusual data detection system that serves as an early, proactive indicator into infrequent but anomalous activities—can successfully complement legacy security products to address these issues.

IT administrators often collaborate with their peers on information security teams to ingest such information within a centralized security event and information management (SIEM) platform, derive unique insights, and proactively take remediation measures to prevent security breaches and data loss. These insights also help IT departments evaluate the potential business impact of such problems and adjust their recovery time objectives (RTOs) and recovery point objectives (RPOs) to better protect end-user data on endpoints and cloud applications.

Data Backup Thwarts Ransomware, Provides Other Benefits

Instead of playing a game of catch up, the best defense is a dual-pronged approach that combines advanced malware detection with backup to minimize the chances of data loss. Experts agree that a crucial part of thwarting ransomware and other incidents of malware is through regular time-indexed backups. Indexed snapshot backups of data across servers, laptops, and cloud apps enable the restoration of information back to its original state. As a result, organizations can access their data from any point in time prior to the attack.

It's easy to see how a solid backup plan improves an organization's security and negotiation stance when confronted with an attack. Enterprise-grade data backup also provides several major benefits unrelated to ransomware, whether the data loss stems from malware, system failures or human error. The right data backup solution facilitates better information governance and gives organizations the ability to view audit trails and protect data for compliance purposes. A cloud-based backup solution also provides critical off-site storage when on-premises data is at risk.

A 6-Step Plan for Data Backup

Druva's data protection experts have outlined six proactive steps that IT can use to keep data safe. These steps provide the foundation of a backup plan that is highly efficient, seamlessly executed, and unnoticeable to the end user.

1. **Protect Distributed Data: "How"**
   An enterprise-grade automated backup solution that performs regular backups across devices, desktops and cloud apps, such as Office 365, will protect distributed data and act as an insurance policy in case of a ransomware strike or other intrusion. Make sure to select a cloud-based backup solution, as it provides off-site storage. Off-site storage that leverages any of the AWS storage regions not only provides off-site capabilities, but also complies with local data residency laws by storing it in

the same region. Importantly, off-site storage is, by its very nature, safer: data is isolated from the enterprise network where day-to-day business requires constantly opening email and running executables.

2. **Backup Distributed Data: "Who"**
   Does your current backup plan cover 100 percent of your user base, including geographically distributed teams? To reduce your exposure to potential data loss, review and validate the deployment scope of your backup plan to ensure that your backup solution deploys automatically to all end users needing protection. At a minimum, you should ensure that key users are covered by your data protection policy.
3. **Review the Scope of Your Data Backup: "What"**
   What are you backing up? You're probably protecting desktops and email, but what about other user-specific data sets such as profiles, system and app settings, or folders? We highly recommend that you review, validate, and, as needed, modify backup content to ensure that all important data for protected users is backed up. If you need a more comprehensive plan, you should consider creating custom folders where users can store data for backup and further reduce data loss.
4. **Check Backup Frequency Across Distributed Teams: "When"**
   How often are you backing up? Every two days? Eight hours? Four hours? Do you need an even more aggressive schedule for executives? Review, validate and, if needed, modify backup frequency to ensure automated, periodic backup of mission-critical data for all protected users. As a general rule, we recommend that you backup data, at minimum, once every four hours, and every two hours for key users. You may also want to select a different backup frequency depending on the requirements of specific users and teams.
5. **Validate Your Retention Policy: "How Long?**
   How long are you keeping your backups? 14 days? Seven weeks? Six months? Review, validate and, if needed, adopt a longer retention policy to meet internal objectives and ensure a sufficient Recovery Point Objective (RPO), especially for key people and departments. Your data retention policy may vary depending on your industry, regulations, and internal IT policies. IT, Legal, and Compliance teams may need to weigh in on data retention needs.
6. **Re-Assess Policies Periodically: "Looking Ahead"**
   While the preceding measures might provide sufficient protection for the foreseeable future, we highly recommend that you revisit your backup policies approximately every six months to ensure that they meet your organization's needs. IT often has the primary responsibility for this routine and, in some cases, acts in coordination with the Legal team.
7. **Monitor for Ransomware Attacks: "Be Aware"**
   Keeping track of unusual file deletions, modifications, encryptions, and header changes can minimize damage by enabling fast responses such as isolating infected hardware before malware has the chance to spread. The earlier you isolate a problem, the more-recent a backup you'll be able to restore, minimizing lost productivity.

How the Druva Cloud Platform Can Help

Druva can help IT teams proactively detect and recover from ransomware attacks by monitoring for suspicious activity on end-user devices (Druva inSync) and ensuring thorough backups before an event (Druva inSync and Druva Phoenix). Designed for endpoints (e.g. laptops, desktops, smartphones, tablets) and cloud applications as well as servers, Druva solutions provide automated, enterprise-grade backups—enabling quick data restores in case servers or end users are compromised—even if hardware is locked forever. Specifically, Druva offers:

Data Protection for Ransomware: Enables automatic, scheduled backups, and provides complete control, configurability, and accessibility to backup content.

Monitor for Ransomware Attacks: Druva inSync allows you to gain an edge on ransomware threats by continuously monitoring snapshots for anomalies such as modified or deleted files, MIME type changes, and file encryptions.

Immediate Data Access: Druva provides customers with immediate access to data from anywhere, so that users are never impacted by ransomware or other malware.

Frequent Backups: inSync enables organizations to backup data as often as every five minutes.

Multi-Zone Redundancy: Each data region has multi-data center redundancy, providing the highest level of data reliability and guaranteed availability to ensure business continuity.

Greater Storage Options: To best meet their data storage, privacy and security needs, Druva leverages AWS to provide customers with a greater choice in global storage options.

Covers Mobile Devices: Mobile devices outside the firewall are a target for introducing malware. Backing up data on endpoints is a must, and Druva inSync provides coverage by backing up data on mobile devices as well.

Granular Restore: Druva provides file-level restore capabilities for endpoints, servers, and cloud applications to ensure information is never lost and always accessible.

User-Added Folders: To ensure that all key data is protected, inSync allows end users to add folders and self-select the data for backup. End users can also self-restore their data, along with personal and application settings from any new device.

Simply Press Rewind: With federated search and audit trails, IT can easily zero-in on infected files and easily take remediation steps.

Conclusion

By following the steps outlined in this IT Guide and selecting Druva as its enterprise solution, IT can ensure that it has a rock-solid backup routine in place to reduce the impact of ransomware or other malware attacks. Armed with the ability to quickly restore data from time-indexed copies, organizations will be far less vulnerable to costly and debilitating ransom demands. Who needs weeks of drama and negative headlines when industry-leading cloud backup is available?

Discover how your organization can better prepare for a ransomware attack. Read this checklist, "You've Got Ransomware. Now What?" to learn more.

About Druva

Druva is the global leader in Cloud Data Protection and Management, delivering the industry's first data management-as-a-service solution that aggregates data from endpoints, servers and cloud applications and leverages the public cloud to offer a single pane of glass to enable data protection, governance and intelligence—dramatically increasing the availability and visibility of business critical information, while reducing the risk, cost and complexity of managing and protecting it.

Druva's award-winning solutions intelligently collect data, and unify backup, disaster recovery, archival and governance capabilities onto a single, optimized data set. As the industry's fastest growing data protection provider, Druva is trusted by over 4,000 global organizations, and protects over 100 petabytes of data. Learn more at www.druva.com and join the conversation at twitter.com/druvainc.

druva

Druva, Inc.
Americas: +1 888-248-4976
Europe: +44 (0) 203-7509440
India: +91 (0) 20 6726-3300
Japan: +81-3-6890-8667
Singapore: +65 3158-4985
Australia: +61 1300-312-729
sales@druva.com
www.druva.com