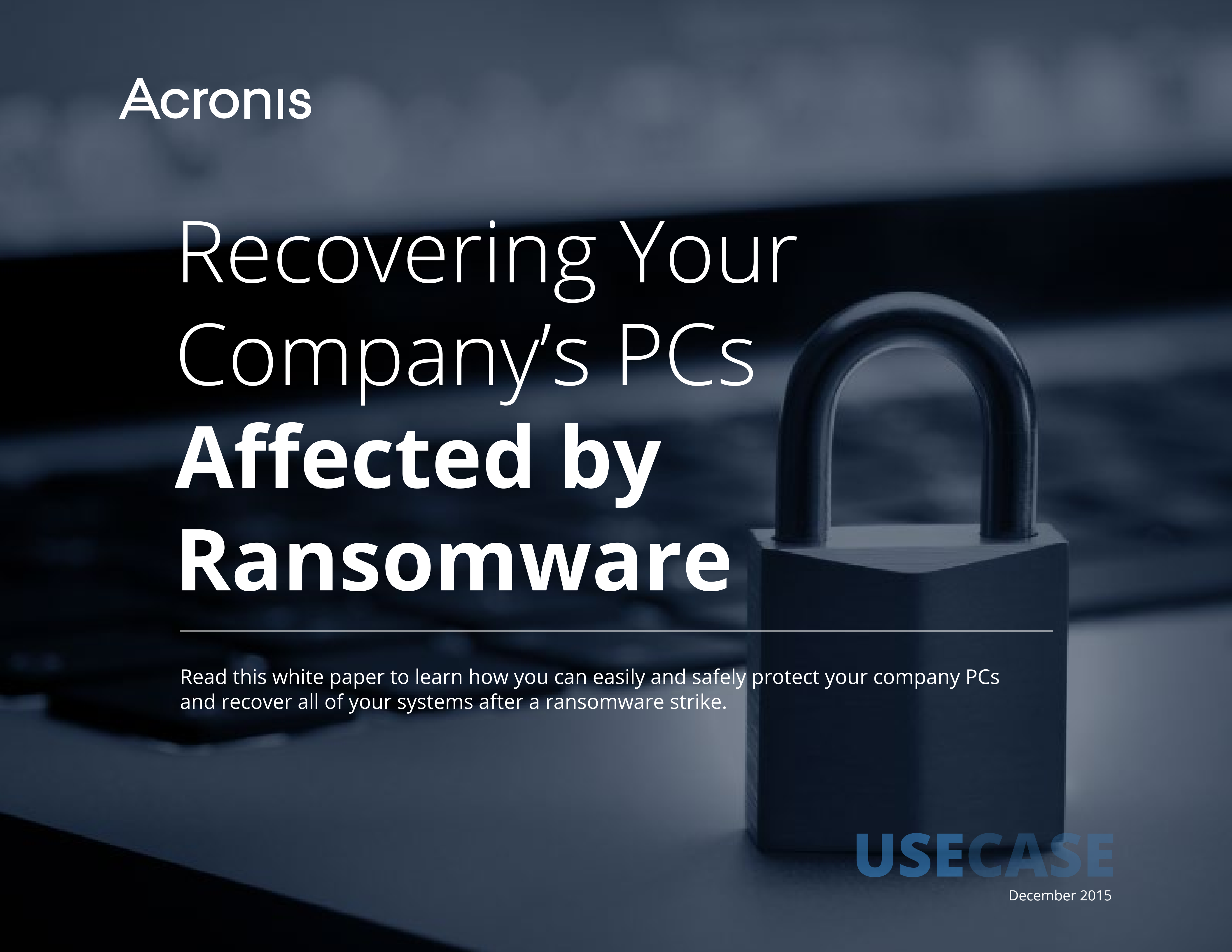

Acronis

Recovering Your Company's PCs **Affected by Ransomware**

Read this white paper to learn how you can easily and safely protect your company PCs and recover all of your systems after a ransomware strike.

USECASE

December 2015

Introduction

Data is your organization's lifeline and no matter how much you try to classify and centralize it, your users will always have critical data you do not know about. According to industry analysts, up to 80 percent of a company's critical data is located on PCs, not on servers.

TrendMicro[1] found that 56 percent of employees frequently or very frequently store sensitive data on personal devices such as laptops. It is almost a certainty that your CEO stores critical company documents on his/her PC – not copied to any company server – and probably not protected.

Now, there is a new threat — **ransomware.**

Ransomware is a type of malware that blocks access to your files and systems until you pay a ransom. The first example of ransomware happened on September 5, 2013, when **Cryptolocker** was unleashed. It quickly affected many systems with hackers requiring users to pay money for the decryption keys.

In four months of 2013 alone, the ransoms paid topped $30 million.

In 2014, Zerolocker, Cryptowall, and Sypeng were the most notable ransomware examples — and in 2015, the CTB-Locker started the trend of demanding untraceable Bitcoins as payment.

According to a February 2015 McAfee Labs Threats Report, the number of ransomware types grows an average of 155 percent each quarter.

Bromium[2] research shows that ransomware can target more than 230 different types of computer files — and chances are that your CEO's files are on that list.

Antiviruses and firewalls may provide a good level of protection. However, once your PC is affected, the only way to not pay a ransom is to have a backup copy of your data stored in the cloud. Even local backups stored on USB drives, for example, may also be encrypted – rendering them useless.

The following use case describes how one company protected their company PCs and recovered all of their systems after a ransomware strike.

[1] http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/sb_5-reasons-why-small-business-lose-critical-data.pdf
[2] http://www.bromium.com/company/press-releases/bromium-research-reveals-sophisticated-crypto-ransomware-menace.html

Ransomware Use Case

The Company's PCs

The company has 150 employees, located in one central office. The staff uses a mixture of Windows®-based laptops and desktops connected to a central data center via a wired and wireless infrastructure.

While the company uses centralized storage, document management systems, and numerous business applications, up to 80 percent of the PCs contain critical company data that is not copied to the company's central repositories.

The Company's Backup Policy

The company's PC backup policy is a subset of an overall enterprise-wide disaster recovery plan, which defines the business continuity strategy and required IT equipment to support all company operations — communications, business and banking, finance, auditing and compliance, logistics, human resources, and so on.

The IT department recognized that a substantial portion of the company's data is stored on employee desktops and laptops. For this reason, the company included all personal computing devices into the scope of the company's backup policy.

The Company's Backup Products

The company uses Acronis® Backup Advanced to protect its users' PCs. It also uses Acronis Backup Advanced to support the backup and recovery of other platforms in their primary data center. Powered by the Acronis AnyData Engine, the Acronis Backup Advanced provides fast backup and recovery for Windows, Linux®, and hypervisor environments using disk-image technology that saves complete images of the systems — including the operating system, applications, configurations, and data.

The Acronis' AnyData Engine powers all Acronis products, enabling the company to capture, store, recover, control, and access data in virtual, physical, cloud, and mobile environments. Each product is optimized for a specific workload but also seamlessly blends into a total solution. The same unified console is used to configure, install, and maintain each product.

Since the company protects multiple systems with Acronis Backup Advanced, it uses the Acronis Management Server (AMS), a single pane-of-glass, to manage the backup and recovery of all data across the entire infrastructure.

With Acronis Backup Advanced, the IT team can easily back up laptops and desktops and recover files, folders, or the complete system. Since the company started using this product, it has been able to:

- Reduce downtime and improve employee productivity.
- Simplify disaster recovery and ensure business continuity using Acronis' flexible recovery options.
- Streamline IT operations with one complete solution that is easy to install, configure, and manage.

- Protect the entire data center with Acronis Backup Advanced.
- Eliminate single point of failure because if the console fails, the backup and recovery on all PCs (and all other systems) is still fully functional.

Backup Source Systems

Leveraging the power of the Acronis AnyData Engine, Acronis Backup Advanced executes full system backups, capturing approximately 8TB of uncompressed data. With the product's differential and incremental backups, the company only backs up changes, which helps optimize storage space. The company's average daily data change is about 1.5 percent. Daily incremental backups capture 120GB of data while weekly differentials capture 600GB of data.

The Backup Storage Policy

The company initially backs up all of their systems to local NAS devices and then copies the backups to the Acronis Cloud. To simplify IT administration, Acronis Backup Advanced includes backup and staging in the same backup plan. This hybrid backup approach mirrors Acronis' recommended 3-2-1 backup strategy: maintain all data in three locations (production systems, backup on NAS, and backup in Acronis Cloud), on two types of media (disk and cloud), with one copy of backup data stored offsite.

In the event that files are lost on one PC or a user only loses a handful of files, IT can recover those files from the local backup copy. In the event of a major event, IT restores backup copies from the Acronis Cloud.

The Backup Schedule

Acronis Backup Advanced supports a GFS (Grandfather-Father-Son) rotation scheme that fits the company's needs. Using this feature, the company can run full backups of all data on a monthly basis, weekly differential backups, and daily incremental backups to minimize storage requirements and reduce backup time.

IT backs up laptops during the working day since many employees take their laptops home and on business trips. The desktops' backup starts after office hours.

The IT team does not need to define the exact time to back up each individual PC. Acronis Backup Advanced automatically distributes the time of the individual PC backups randomly over a defined period.

IT does not have to define the blackout period for the backup window; Acronis uses snapshot technologies so the backup is transparent to users and does not affect business operations. Acronis's disk-imaging technology also backs up all the data consistently — even if the files are open.

To reduce the impact on users with lower-performance machines, IT can limit the backup resource usage.

Ransomware Strikes

The ransomware affects numerous machines in the company, and the company IT team invokes the recovery plan. Here is the timeline.

Day 1

10:30am **The ransomware strikes.**
IT is yet unaware of the strike.

10:42am **First report reaches the IT team and the Help Desk responds.**
IT disconnects the infected PC from the network.

10:51am **Users report seven more ransomware infections.**
The IT team realizes the scale of infection, shuts down the company network, and starts a company-wide check.

12:07pm **Company-wide checks are complete.**
IT identifies that 23 machines are affected.

12:18pm **IT restarts the network.**
IT shuts down all affected PCs and keeps them disconnected from the LAN.

12:27pm **IT contacts the Acronis support team.**
IT requests Acronis to send a Large Scale Recovery hard disk drive (HDD) that contains the backed up data (stored in the Acronis Cloud) for the 23 PCs.

3:45pm **Acronis sends the HDD by courier.**
The Acronis support team finishes copying 23 backups (923GB) to the external HDD and sends it to the company via an overnight courier.

Day 2

8:33am **The HDD arrives at the company.**

8:51am **IT copies the HDD to central storage.**
The IT team copies the backups to higher-performance central storage to facilitate the parallel recovery.

9:05am **The first backup is copied to storage; the first PC's recovery can start.**
The IT team boots the affected PC from Acronis Bootable Media with the network still disconnected.

9:07am **First boot is complete.**
Acronis Backup Advanced has been loaded on the PC. The IT team connects the network and launches the recovery process.

9:53am **First recovery is complete.**
The machine is restored and is rebooted.

10:02am **The first machine is restored.**
The copying of backups to central storage continues.

12:37pm **All backups are copied to central storage.**
15 machines are now recovered.

2:29pm **The final affected machine is restored.**
All 23 machines are recovered. No ransomware is detected.

Summary

Ransomware affected a significant number of employees' PCs but the company is prepared. The IT team developed a PC recovery plan that included the details about the backup source systems, backup storage policy, backup schedules, and backup duration. The management team approved the PC recovery plan and the IT team exercises the plan on a regular basis using different scenarios.

The timeline of actions clearly lays out the steps the IT engineers took to recover the PCs and restore the users back to a productive state.

Using Acronis Backup Advanced, the IT team achieved all of the business objectives set forth in the PC recovery plan and restored productivity to all users in 28 hours.

Along with PCs, the IT team also uses the Acronis Backup Advanced to support the backup and recovery of their primary data center:

- **Windows Servers:** Image- and/or file-based backups protect entire machines running a Windows Server Operating System
- **VMware and Hyper-V virtual hosts:** Agentless backup protects VMware® and Hyper-V® virtual machines, including virtual Microsoft® Exchange, SQL Server®, SharePoint®, and Active Directory®
- **Microsoft Exchange servers:** Application-level backup of databases and mailboxes protects critical e-mail and collaboration system
- **Microsoft SQL Servers:** Single-pass backup protects Microsoft SQL Server with application-aware restore from a single database/content database to the entire server
- **Microsoft SharePoint farm:** Single-pass backup protects all server roles in a SharePoint farm with application-aware restore from a single database/content database to the entire server
- **Active Directory Domain Controllers:** Consistent single-pass backup and recovery protects Domain Controllers, Active Directory databases, system volumes, and logs
- **Cloud Backup add-on:** The entire data center is protected with secure, scalable offsite cloud backup, available through flexible subscriptions; initial seeding and large-scale recovery programs make it easier to move large amounts of data and avoid network bottlenecks.

Acronis Backup Advanced is powered by the Acronis AnyData Engine, which combines backup, bare metal restore, and system recovery to protect data whether it resides on premise, in the cloud, or in remote offices. With Acronis Backup Advanced, the company simplified backup and disaster recovery, significantly reducing the IT time and effort to recover their systems and get the business back up and running.

Top 5 Reasons to Choose Acronis Backup Advanced

1. **Quickly capture** everything on your PCs using patented, image-based backups.
2. **Restore** entire systems quickly when massive attacks or disasters happen.
3. **Recover** individual files, folders, applications, or your complete system to any hardware or virtual machine (VM).
4. **Ensure** business continuity and disaster recovery protection with Acronis' rich functionality.
5. **Simplify** IT administration with centralized management of data protection.

Recommended links

Acronis Backup Advanced

About Acronis

Acronis sets the standard for new generation data protection through its backup, disaster recovery, and secure access solutions. Powered by the AnyData Engine and set apart by its image technology, Acronis delivers easy, complete and safe backups of all files, applications and OSs across any environment—virtual, physical, cloud and mobile.

Founded in 2002, Acronis protects the data of over 5 million consumers and 300,000 businesses in over 130 countries. With its more than 100 patents, Acronis products were named best product of the year by Network Computing, TechTarget and IT Professional and cover a range of features, including migration, cloning and replication.

For additional information, please visit **www.acronis.com**. Follow Acronis on Twitter: **http://twitter.com/acronis**.

Acronis

For additional information, please visit http://www.acronis.com

To purchase products, please visit http://www.acronis.com or search online for an authorised reseller.
Acronis office details can be found at http://www.acronis.com/company/worldwide.html