Acronis

DEVELOPED BY PETRI.COM AND ACRONIS

WHITEPAPER

Protecting and Securing Your Critical Data with Acronis Cyber Backup

YOUR ORGANIZATION'S IT SECURITY IS THE FIRST LINE OF DEFENSE AGAINST INCIDENTS THAT CAN CAUSE BUSINESS INTERRUPTION AND DATA CORRUPTION.

PROTECTING AND SECURING YOUR CRITICAL DATA WITH ACRONIS CYBER BACKUP

Businesses today face far more invasive and potentially damaging threats than at any time in the past. Your organization's IT security is the first line of defense against incidents that can cause business interruption and data corruption. While backup should underpin every business' data protection strategy, it is no longer enough. To truly protect your data, you must become #CyberFit by deeply integrating security into data protection processes like backup and recovery—an approach called cyber protection.

Despite increasing attention to security, backup procedures are often neglected in IT security policies. Like the old adage says, an ounce of prevention is worth a pound of cure: stopping threats before they can cause irreversible data corruption can save your business the expense and effort of data restoration. In some cases, it can be the difference in your company's survival.

It's important to recognize that your backups contain all of your private and potentially sensitive company data. Unauthorized access or hacking into backups can result in intellectual property theft as well as information exposure that could damage your business.

> **Today's threats go beyond simple data loss and recovery from failures. Backup solutions need to integrate with security to enable better business continuity and protect critical data from threats like external hackers, insider attacks, and a broad array of malware, including ransomware.**

Securing backups is essential. Considering that many businesses today are taking advantage of the cloud to store backups off-site, it's equally important to be certain those backups have multiple layers of protection. The most critical feature of any backup solution is its ability to meet low recovery time objectives and recovery point objectives (RTOs and RPOs). RTO defines how long you can go without access to your data; RPO defines how much data loss your organization can tolerate.

> **This whitepaper explores the challenges involved in protecting and securing private business data. You'll learn how Acronis Cyber Backup delivers uniquely secure protection for critical data, increases recovery speed, and eliminates downtime caused by ransomware, one of the fastest-growing and most destructive malware strains today.**

THE GROWING DANGERS OF RANSOMWARE

Data protection plans today must address the growing threat ransomware attacks pose in order to prevent serious downtime and data corruption.

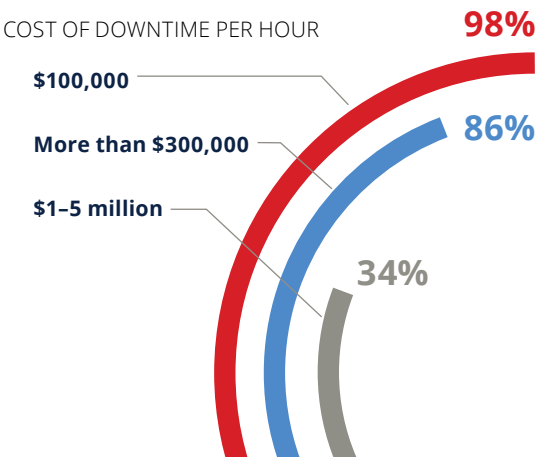
> **"Businesses today are up against a rising tide of threats. Cybersecurity threats and data espionage are more prevalent than at any other point in our history – contributing to an anticipated $2 billion loss due to ransomware this year. What's scarier is malicious attacks are no longer limited to hackers: Ransomware-as-a-service kits can be purchased for a mere $39 by anyone with low moral standards and a desire to generate a few dollars."**
> *— Eric O'Neill, former FBI counter-terrorism and counterintelligence operative*

Malware is hostile or intrusive software that invades servers, PCs, laptops, tablets, and mobile devices for malicious purposes, such as stealing, altering, or destroying data. Ransomware is a particularly virulent form of malware that encrypts the data on an infected system and attempts to extort a payment in exchange for the decryption keys that can unlock it.

Security researchers and law enforcement agencies forecast that the ransomware threats will continue to rise, making the ability to secure and recover your data from such attacks more important than ever. In fact, the damage caused by ransomware isn't limited to your production systems; it can also attack and destroy replication targets and backups.

THE VALUE OF DATA AND THE COSTS OF DOWNTIME

There's no doubt that downtime is very expensive. Gartner reports that the average cost of downtime for all types of businesses is $5,600 per minute, which equates to roughly $300,000 per hour.[1] Information Technology Intelligence Consulting (ITIC) did a somewhat more granular study that showed that for 98% of businesses, a single hour of downtime costs more than $100,000. For 86% of businesses that hour of downtime costs more than $300,000, and for 34% of larger businesses an hour of downtime costs $1 million to over $5 million.[2]



! Downtime has more than just financial consequences as well. It can also have a major impact on your business. National Archives and Records Administration reported that 93% of companies that lost their data for 10 days or more during a disaster filed for bankruptcy within one year.[3] According to the University of Texas, 43% of companies that suffer catastrophic data loss never reopen and 51% close within two years.[4] Similarly, the Boston Computing Network's Data Loss Statistics showed that 30% of all businesses that have a major fire go out of business within a year and 70% fail within five years.[5]

THREATS TO YOUR CRITICAL DATA BACKUPS

Traditional backup is dead as a result of all of these factors. In fact, the traditional backup process: producing a copy of your data to recover from, can create a false sense of security—without proper protection, your backups may become infected or corrupted.

Some of the biggest risks to your critical data include:

- Modern threats that can bypass traditional signature-based anti-viruses
- Malware strains that intentionally search for and destroy backup files
- Threats that corrupt backup software executables
- Obsolete backup applications that lack secure design, offering weak or no encryption, or use an outdated architecture with multiple points of vulnerability and failure
- Vendor backup applications that are limited to software and do not protect data end-to-end

The threats to your company's data are continually evolving, including a new generation of threats that target backups as well as system data. For instance, the ransomware Zenis encrypts your files and purposely deletes backups. Likewise, Locky and Crypto ransomware destroy data shadow copies, as well as data restore points.

To ensure a truly secure backup, you need security-rich cyber protection for your entire IT infrastructure and data: physical systems, virtual systems, cloud services, and mobile devices, plus the corresponding backups for these devices. By layering security on top of backups, you can proactively prevent downtime and data exposure as well as detect and correct data corruption.

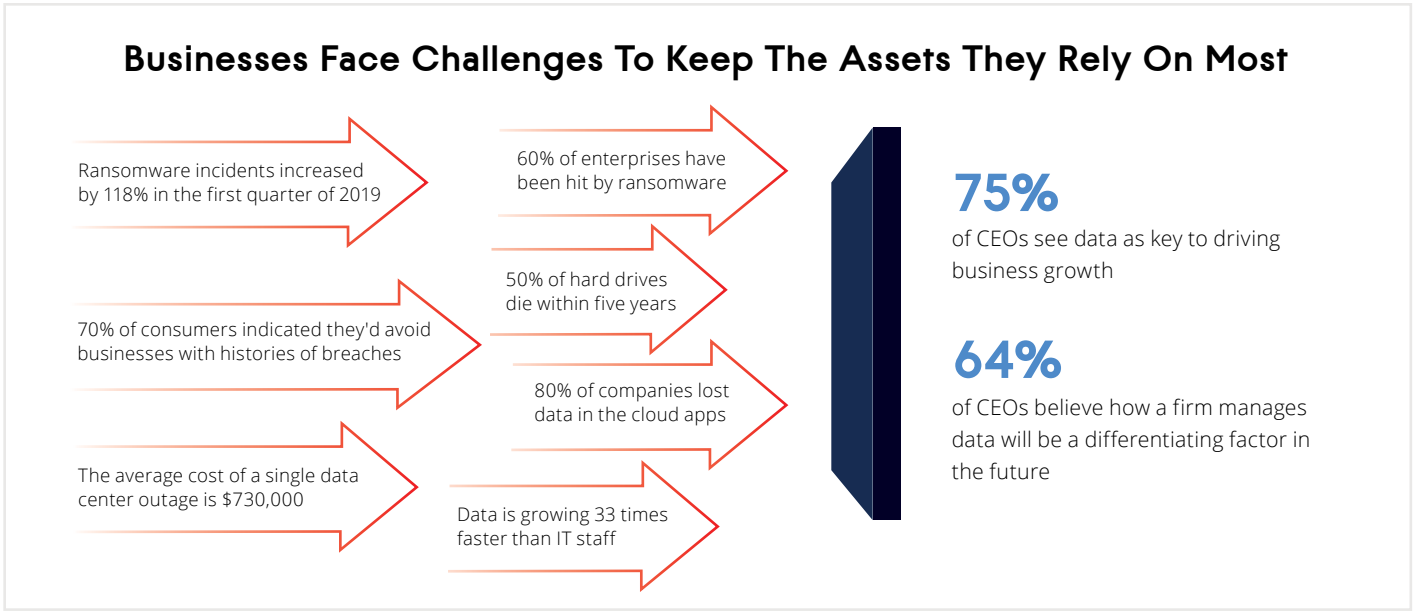
You need to ensure that you can restore your backup by securing your backup process at every stage and securely storing your backup files. Your cyber protection solution needs to protect you from downtime by proactively blocking ransomware and automatically restoring data in case of an attack.

Meanwhile, quick restoration requires a solution that lets you select multiple different recovery points.

> **"The shift to detection and response approaches spans people, process, and technology elements and will drive a majority of security market growth over the next five years. While this does not mean that prevention is unimportant or that chief information security officers (CISOs) are giving up on preventing security incidents, it sends a clear message that prevention is futile unless it is tied into a detection and response capability."**
> *— Sid Deshpande, Principal Research Analyst at Gartner*

Let's look at the core backup and recovery features built into Acronis cyber protection products, then dive into their advanced security capabilities.

Figure 1—Data Protection Challenges [6–10]



ADVANCED CYBER PROTECTION CAPABILITIES IN ACRONIS CYBER BACKUP

Acronis Cyber Backup addresses all five vectors of cyber protection—safety, accessibility, privacy, authenticity, and security (SAPAS). It provides a complete cyber protection solution for hybrid IT environments: backing up and recovering physical, virtual, cloud, and mobile device data, while proactively detecting and defeating malware and ransomware attacks.

> **Acronis Cyber Backup supports 21 of today's popular platforms, including Windows Server 2016 back to Windows Server 2003 and Windows 10 back to Windows XP SP3.**
>
> **It supports all of the current Linux distributions, including Red Hat Enterprise Linux 4.x–7.4, Ubuntu 9.10–17.04, Fedora 11–24, SUSE Linux Enterprise Server 10–12, Debian 4–9.2, and CentOS 5.x–7.4.**
>
> **It also supports Apple OS X 10.11 and later, macOS 10.13, iOS 8 and later, and Android 4.1 and later. Acronis Cyber Backup also supports all of the most popular hypervisors, including VMware vSphere, Microsoft Hyper-V, and Citrix XenServer.**

Acronis Cyber Backup provides several advanced cyber protection and recovery features that enable you to secure your backups as well as lower your RTOs and RPOs.

ACRONIS INSTANT RESTORE REDUCES RTOS BY RUNNING VMS DIRECTLY FROM BACKUPS

Acronis Instant Restore enables you to vastly reduce your recovery times by using your backup to immediately start a Windows or Linux virtual machine directly from storage. As no data is moved, you can start your backup VM and get it up and running in seconds. The Acronis agent on the host creates a virtual data store that allows the host to read directly from the backup and start the VM. Changes to the VM are written to a temporary file on the host—all in a manner that is completely transparent to the virtualization host.

REMOTE AND BARE-METAL RECOVERY REDUCE RTO WITH DIRECT RESTORE CAPABILITIES

Bare-metal restore accelerates recovery by restoring a full system backup on a computer that has an empty system drive. This avoids a lengthy OS installation before running restore processes. There's no need to reinstall backup or other applications. You can immediately restore from a complete system image. The built-in smart-boot technology automatically detects the system's startup requirements. If your computer has been infected by a virus or ransomware then recovery from the bare-metal image eliminates any malware that may have been present. You can also perform remote recoveries by connecting to the Linux-based Acronis Bootable Agent from a networked system using the Acronis Management Console.

ACRONIS UNIVERSAL RESTORE ENABLES BACKUPS TO BE RESTORED TO DISSIMILAR SYSTEMS

Sometimes recovery fails when using an entire disk image to recover to a new system with hardware that is not identical to the original machine. The system typically cannot boot because the boot drivers in the backup image do not match the new hardware requirements.

Acronis Universal Restore solves this problem by reconfiguring the target operating system before booting, first by analyzing the target system, then changing any relevant OS settings and injecting any new drivers required to successfully boot the system. Acronis Universal Restore can also be used to migrate data between physical and virtual machines.

GRANULAR RECOVERY OF INDIVIDUAL FILES AND EMAILS

Users often look to restore accidentally deleted, individual items. Acronis Cyber Backup enables granular recovery by powering searches for specific documents, like files and emails, then restoring them individually without having to recover the entire backup. This significantly reduces RTOs and operational efforts.

RAPID VSPHERE RESTORES WITH VMFLASHBACK

Acronis vmFlashback enables fast VMware vSphere VM recovery by selectively restoring only the virtual hard disk data blocks that have been changed since the last backup, foregoing the need to restore the entire VM. Acronis vmFlashback uses VMware's Changed Block Tracking (CBT) technology to track and save only those blocks of information in a VM backup that have changed since it was created. CBT identifies the disk sectors that have been changed by comparing special change set IDs. When a restore is required, CBT provides a list of changed disk blocks by comparing the disk IDs from the backup to the current virtual disk set IDs, then restoring only the changed disk blocks.

ACRONIS DELIVERS EASY, EFFICIENT, AND SECURE CYBER PROTECTION FOR ALL DATA, APPLICATIONS, AND SYSTEMS

Acronis Cyber Backup provides a unique backup security solution that goes beyond simple protection of your backup files. Acronis' team of security experts developed a unique approach to cyber protection by integrating key technologies into the fundamental core of Acronis Cyber Backup, which addresses all five vectors of SAPAS.

Acronis Cyber Backup now utilizes microservices, the Go programming language, and new engineering practices in the product's development lifecycle. Using a team of ten dedicated security experts, Acronis has implemented a Secure Development Life Cycle (SDLC) that utilizes security-focused code and design review processes. Each version of Acronis Cyber Backup is built in our lab in Schaffhausen, Switzerland, and signed as it is released.

Acronis Cyber Backup is fully TAA compliant and features more than 100 patents in cyber protection and security. Acronis Cyber Backup provides a number of tightly integrated security features that enhance enterprise data protection capabilities.

! Acronis Cyber Backup addresses all five vectors of cyber protection—safety, accessibility, privacy, authenticity, and security (SAPAS).

ACRONIS ACTIVE PROTECTION PROTECTS EXECUTABLES AND DATA FROM RANSOMWARE

Unlike most other backup software solutions, Acronis Cyber Backup is built on a secure architecture called Acronis Active Protection that prevents it from becoming compromised by malware and ransomware. Acronis installs a special protected driver on the system that monitors systems files, executables, and data.

Acronis Active Protection detects unexpected malware activity and prevents any possible corruption of the Acronis Cyber Backup executable programs. Acronis can detect and halt a ransomware attack, and any data that was corrupted by the attack can be recovered and restored from a protected Acronis Cyber Backup archive.

BACKUP ENCRYPTION PREVENTS UNAUTHORIZED ACCESS

To provide better protection from brute-force attacks, Acronis has strengthened its backup encryption and traffic encryption.

> **Acronis Cyber Backup supports industrial-grade AES-128, AES-192, AES-256, and GOST encryption algorithms, and uses machine-based encryption with a different key for each individual machine. Backup users can select the algorithm and set the password used for encryption. The Acronis agent handles key creation.**

Users also have the option to avoid storing encryption keys in the Acronis Management Server (AMS) or the cloud. The password you assign to the backup is not stored as a part of the backup and cannot be retrieved. This provides an extra level of protection from targeted malware attacks by ensuring that passwords cannot be found in the Acronis agent, program files, or backups.

This protects your critical backup data and prevents it from being compromised even if a hacker somehow gains unauthorized access to it.

SECURE MODERN STORAGE FORMAT AND ACRONIS NOTARY BLOCKCHAIN AUTHENTICATION

In addition, Acronis Cyber Backup uses the new and improved Archive 3 storage format to strengthen backup storage security. Archive 3 is a modern format designed for both block and file-level environments. It supports up to a billion files, 100,000 slices, and a 50 TB archive size. The Archive 3 format supports asynchronous data access, fast browsing, and paging. It also provides built-in block-level deduplication and adaptive compression using the ZSTD/LZ4 algorithms.

Data encryption support separates encryption keys and passwords enabling you to change passwords without requiring re-encryption. Secure storage provides the first line of defense for your critical backup data.

> **Acronis Cyber Backup storage is European Union (EU) General Data Protection Regulation (GDPR), ISO 27-001, and HIPAA compliant. Acronis Cyber Backup replication can be used to copy your backups to a secondary location.**

Acronis has pioneered the use of blockchain for data protection. The Acronis Notary features use blockchain to provide notarization and electronic signatures of backup files. Blockchain enables the integrity of your backup files to be verified, ensuring that they have not been altered. To verify and protect data backups, Acronis Notary computes a cryptographic hash that is unique for each file.

The algorithm that creates this hash will always produce the same output for a given input file, enabling it to verify the file's authenticity. This ensures that the backups you have archived have not been altered or corrupted by malware and that they can be used to restore your critical data with confidence.

ROLE-BASED ACCESS PROVIDES ADMINISTRATIVE DELEGATION AND REMOTE ACCESS

To provide flexible administrative functionality, Acronis Cyber Backup uses a role-based access model. Role-based access enables you to simplify data protection for your remote offices, branch offices, and individual departments by establishing different roles for multiple administrators and delegating different backup tasks to local personnel.

Acronis uses two types of roles:

- **Regular users**—Regular users can perform file-level backup and recovery of any files that they have permissions for. They can create and manage backup plans and tasks, and view backup plans and tasks created by other users.
- **Administrative users**—Administrative users can perform file-level backup and recovery of all data on a system and can back up and recover the entire machine. They can create and manage backup plans and tasks for different users.

Acronis Cyber Backup provides centralized and remote management of backups to make it easier to protect data that resides in remote locations, private clouds, public clouds, and mobile devices. Remote backup administration via the internet can help reduce RTOs with easy access to bootable media and the ability to restore bare-metal servers.

SECURE CLOUD DATA PROTECTION

Acronis Cyber Backup includes 5 GB of free cloud storage, enabling all active customers to start storing their most critical data in the cloud. Acronis Cloud Storage is fully integrated into Acronis Cyber Backup. Users have the option to store encrypted data in the Acronis Cloud.

The purpose-built, highly reliable, and secure Acronis Cloud Storage uses the scalable and secure Archive 3 data storage format. By leveraging the cloud, you can create hybrid cloud backup plans that implement the 3-2-1 data protection strategy, i.e. keeping at least three copies of your data on at least two different media with at least one off-site storage location.

The Acronis Cloud can be used to store an additional backup copy on cloud storage media in an off-site location. Acronis Cyber Backup can also replicate archives to Amazon Web Services (AWS), Microsoft Azure, or another remote data center for added backup protection.

ACRONIS CYBER BACKUP INTEGRATES WITH POPULAR ENDPOINT SECURITY SOLUTIONS

Malware variants like ransomware can disrupt business operations, destroy critical data, reduce cash flow, dilute customer and partner trust, and reduce profit margins, as when frightened customers and partners begin returning products or asking for discounts. Acronis Cyber Backup is designed to integrate with other endpoint security solutions, increasing cyber protection across your organization's environment and helping you to become #CyberFit.

To protect against malware like ransomware, Acronis Cyber Backup is integrated with most anti-virus solutions, providing deep kernel-level protection for all major computing platforms. Acronis' security strategy focuses on leveraging and integrating with existing protection technologies—not replacing them. It uses a single agent that shares low-level interceptions for both backup self-protection and defense against malware attacks.

Acronis Active Protection proactively detects attacks before they occur and provides an active defense of endpoints and backups to terminate attacks in progress. Acronis Cyber Backup can restore all files after an attack.

> This unique, proactive technology prevents system downtime caused by 99.99% of ransomware attacks. Any files impacted by an attack are quickly, automatically restored.

Acronis combines its expertise in malware protection, backup, artificial intelligence (AI), and machine learning (ML) to provide total control of the executable lifecycle on protected systems. Acronis has been thoroughly tested and proved in many real-world production environments, successfully defeating over 460,000 ransomware attacks in the past 12 months, protecting over 5,000 petabytes (PBs) of customer data for more than 500,000 customers.

! Acronis Active Protection technology prevents system downtime caused by 99.99% of ransomware attacks.

JOHNSON ELECTRIC BLOCKS RANSOMWARE ATTACKS WITH ACRONIS CYBER BACKUP

Johnson Electric, one of the world's largest providers of motors, solenoids, micro-switches, flexible printed circuits, and micro-electronics, adopted Acronis Cyber Backup to better protect their critical data and to block ransomware attacks. Before implementing Acronis, Johnson's Ohio office suffered a series of four ransomware attacks that their existing anti-virus protection failed to detect. The total downtime from the four malware attacks was more than 30 hours. After the attacks, Johnson Electric adopted Acronis because it was the only backup solution with cyber protection that could address both data protection and cybersecurity. Since adopting Acronis Cyber Backup, Johnson Electric has not suffered any further ransomware attacks.

> **"Ransomware was a major point of concern for us. With the innovative features such as Acronis Active Protection against ransomware, we are implementing the strongest defense on the market today. And the Acronis Notary technology available in 12.5 is strategically important to us for the future."**
> *— Joel Stuart, Johnson Electric Network Administrator*

460,000 RANSOMWARE ATTACKS

stopped by Acronis Active Protection in the past 12 months

! Acronis has been thoroughly proven and tested in many real-world production environments, successfully defeating over 460,000 ransomware attacks in the past 12 months, protecting over 5,000 petabytes (PBs) of customer data for more than 500,000 customers.

ACRONIS JOINS AMTSO STRENGTHENING ITS MALWARE PROTECTION

In April 2018, Acronis joined the Anti-Malware Testing Standards Organization (AMTSO) to make its cyber protection solutions even more secure. The AMTSO is an international non-profit association focused on addressing the global need for improvement in the objectivity, quality, and relevance of anti-malware testing methodologies. As a part of the AMTSO, Acronis adheres to evaluation standards for cyber protection products and takes part in establishing protocols and procedures for future technologies, thereby improving security testing practices within the industry.

The new partnership enables Acronis to leverage objective and statistically significant testing methodologies to provide modern protection, as well as tapping into the AMTSO's Real Time Threat List (RTTL) database.

ACRONIS CYBER BACKUP DELIVERS COMPLETE CYBER PROTECTION FOR YOUR BUSINESS

Acronis Cyber Backup provides an easy, efficient, and secure cyber protection for your business-critical data and backups. It offers a number of fast recovery options that will lower your RTOs and RPOs. In addition, it provides many advanced and unique security capabilities to protect your critical data from unauthorized access, insider attack, and malware variants including ransomware.

Acronis Cyber Backup uses strong encryption and built-in Acronis Active Protection anti-malware technology, with deep kernel-level support of all major computing platforms that makes them highly resistant to ransomware. Its unique integration with leading anti-virus products adds an extra level of defense against fast-growing security threats like ransomware.

ACRONIS CYBER BACKUP COMES IN BOTH A STANDARD EDITION AND ADVANCED EDITION

Designed for small and medium businesses, **the Standard Edition** provides essential advanced data recovery capabilities and integrated malware protection.

The Advanced Edition is designed for mid-market businesses and enterprises, offering extended functionality to support larger organizations, including centralized storage with deduplication, role-based administration, blockchain-based data protection, Acronis Instant Restore, and automated bare-metal recovery.

Learn more about Acronis Cyber Backup here: Acronis Cyber Backup Key Features.

Acronis Cyber Backup

! The secure cyber protection capabilities in Acronis Cyber Backup are designed specifically to defend your organization's critical data from these fast-growing and potentially lethal threats.

LIST OF REFERENCES

1. The Cost of Downtime. Gartner blog. Andrew Lerner, 2014
2. Hourly Downtime Costs Rise: 86% of Firms Say One Hour of Downtime Costs $300,000+; 34% of Companies Say One Hour of Downtime Tops $1 Million. Information Technology Intelligence Consulting (ITIC), 2019
3. Business continuity statistics: Where myth meets fact. The U.S. National Archives and Records Administration, 2009
4. Data Loss Can be Catastrophic; Plan For Disaster Recovery Today! The University of Texas, 2007
5. Data Loss Statistics. Home Office Computing Magazine, 2011
6. Ransomware Attacks Double in 2019, Brute-Force Attempts Increase. Health IT Security, 2019
7. Understanding the Depth of the Global Ransomware Problem. Osterman Research, 2016
8. Hosting and Cloud Study, 2017. 451 Research, 2017
9. Emerson Network Power-sponsored study by the Ponemon Institute, 2016
10. PWC 2016 US CEO Survey

Acronis