Acronis

WHITE PAPER

MSPs can turn the rising ransomware threat into revenue

How to boost your business with cyber protection services

Cybercrime is a booming business, inflicting damage to numerous organizations. In 2021, data breach costs rose from $3.86 million to $4.24 million — the highest average total cost in 17 years.[1] Cyberattacks are a costly business, resulting in profit-sapping downtime, lost revenues, brand damage, stock price losses and regulatory fines.

The Acronis Cyber Readiness Report, which surveyed 3,600 IT managers and remote workers across 18 countries around the world in order to evaluate their cyber readiness during the second year of the pandemic, found that 30% of companies are attacked at least once a day, and that 81% of all respondents reported encountering a cyberattack at least once a week during the past year.[2] Meanwhile, various researchers concluded that downtime costs can range from $10,000 per hour[3] to as much as $260,000 per hour.[4]

Of the many malware types out there, ransomware is currently the most pervasive cyberthreat. The FBI's Internet Crime Complaint Center reported 2,084 ransomware complaints from January to July 31, 2021, which represents a 62% year-over-year increase[5]. All industries were affected by ransomware during this period. For example, based on ransomware leak site data, the professional and legal services industry was the most targeted by ransomware breaches in 2021, followed by the construction industry.[6]

It's no wonder that business and IT leaders worry that an attack could take down their company next – and their careers along with it.

Ransomware effectively compromises its targets (often simply by getting an unwary employee to click on a phishing email) and causes abrupt system shutdowns that are highly public and disruptive. Meanwhile, cryptocurrency payments hinder law enforcement actions. It's a simpler and more profitable crime than breaching an organization's defenses to steal and resell sensitive data.

Ransomware: both a threat and an opportunity

As a managed service provider (MSP), you recognize this particular cybercrime wave as both a threat and an opportunity.

Part of the threat arises from the fact that tech vendors and service providers are being used to reach business customers and government institutions in complex supply-chain attacks — the most notorious being the SolarWinds breach discovered in December, 2020.[7] By breaking into software firms and embedding malware in popular applications, cybercriminals can now compromise the service providers that use those tools — and from there, the clients whose IT infrastructures they manage.

But being a ransomware attack target is just a part of the threat: the inability to stop ransomware attacks on clients also harms an MSP's competitive position and its ability to grow. For MSPs, this challenge is growing and complex.

Statistics show that:

30%

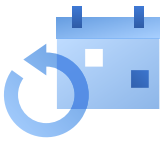
of U.S. small businesses have weak points that bad actors can exploit[8]

44%

of ransomware attacks impacted businesses with fewer than 1,000 employees in Q3 2021[9]

22 days

of business interruption time that an average business faced in Q3 2021 from a ransomware attack[10]



350%

more social engineering attacks that a small business (<100 employees) employee will suffer vs. an employee of a larger enterprise[11]

97%

of MSPs are concerned that their organization could suffer a breach that will also compromise their clients' IT systems over the next 12 months[12]

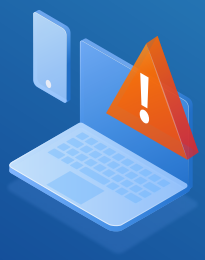
49%

of MSPs admit their clients do not completely trust the security of the services their organization provides[13]

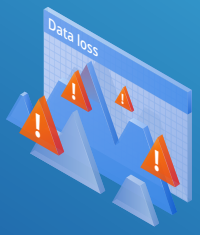
Every business challenge also presents opportunities. You must protect yourself against ransomware attacks and ensure they can't spread. But there's also an opening to build highly profitable and differentiated new offerings for your customers — by offering cyber protection services that defend against ransomware and other data loss threats. Consider:

TOP DRIVERS OF IT BUDGET INCREASES IN 2021[14]

1. Need to upgrade outdated IT infrastructure



2. Increased priority on IT projects



3. Increased security concerns

92%

Percentage of SMBs that **would consider hiring a new MSP** if offered the right cybersecurity solution[15]

34%

Increase in costs that an SMB **would pay** to get the right cybersecurity solution[16]

61%

Increase in decision makers stating that their organization **lacks the skills in house** to be able to properly deal with security issues[17]

Accordingly, the value proposition that you can present to your SMB customers is simple and compelling: "Let us take the threat of ransomware and other malware attacks off your list of worries. We'll protect you from a host of other data loss possibilities, too."

The challenge is to make this offering sticky and profitable, which is to say: simple, manageable, high margin, and compatible with your existing infrastructure.

Three common ways MSPs fight ransomware and their pitfalls

The solutions available to help MSPs address this opportunity typically fall into one of three categories: backup, backup with limited ransomware defenses, and backup combined with third-party endpoint anti-malware software. Each has its limitations:

1. Backup by itself works by restoring compromised systems to a point in time preceding the attack. But relying on backup alone has several weaknesses. Restoring dozens or hundreds of systems from backup (especially from slower media like tape or cloud) can be time-consuming, disruptive to the business, prone to error and painfully expensive. Furthermore, the recovery point may be outdated and a lot of valuable data created between the backup and the attack will be lost.

2. Backup with limited ransomware defenses can defeat some attacks, reducing the need to rely on backup alone for recovery. But attack detection typically relies on coarse statistical measures to compare the rate of file changes against a baseline threshold. A sudden spike in the file change rate indicates a possible attack. Unfortunately, this approach is reactive and prone to both detection failures and false positives, each carrying its own significant costs.

As with backup alone, this solution cannot help if the attack manages to locate and compromise the backups (a capability of many ransomware variants), thwarting recovery entirely.

3. Backup combined with third-party anti-malware software seeks to use more sophisticated endpoint defenses against ransomware. A lack of integration between the two components and their agents, however, frequently leads to system performance issues, process conflicts that can disrupt backups, and deployment and management challenges for the MSP.

A more advanced and efficient option for MSPs

A fourth alternative offers MSPs a simpler, more effective and more efficient option: Acronis Cyber Protect Cloud with Acronis Active Protection technology. This solution, used by more than 10,000 MSPs, enables the delivery of cyber protection services that combine backup as a service with integrated AI-enhanced cybersecurity capabilities (including antivirus, anti-malware, and anti-cryptojacking) and automatic remediation features:

- Acronis Active Protection uses artificial intelligence (AI) and machine learning (ML) to detect and disarm cyberattacks. Continuous training of the advanced behavioral detection engine in the Acronis Cloud AI infrastructure produces the industry's lowest false-positive rate for malware detection, including zero day (i.e., previously unknown) attacks.
- Integrated self-defense mechanisms prevent ransomware attacks from compromising Acronis backup processes, agents and archives.
- Automatic remediation uses a local cache to instantly restore any files damaged prior to attack detection, ensuring immediate resumption of business operations without requiring a full recovery from backup.
- Vulnerability assessments and automated patch management close the security gaps that let ransomware into your system, while URL filtering blocks websites that spread malware.
- The same advanced behavioral detection engine also identifies and terminates cryptojacking attacks, which covertly consume system resources to illicitly mine cryptocurrency — a costly drain on system performance, power and cooling resources. So far in 2022, there have been 15.02 million cryptojacking incidents per month, an increase of 86% over 2020.[18]

In short, Acronis Cyber Protect Cloud's unique integration of backup, cybersecurity, and endpoint management enables you to instantly reduce your clients' exposure to ransomware. Installing one agent is all you need to deliver complete cyber protection, while avoiding process conflicts and performance issues.

> **"Acronis provided excellent performance, is easy to use and has a rich feature set. On top of that, it is the only solution in the test to provide dedicated protection from ransomware attacks. This earned Acronis the first ever approved backup and data security certificate of AV-TEST."**
>
> **David Walkiewicz**
> Director Test Research,
> av-test.org

Delivering cyber protection services with Acronis

But there's much more for service providers than just advanced ransomware protection capabilities. Acronis Cyber Protect Cloud is a part of Acronis Cyber Cloud, a multiservice cyber protection platform built specifically for service providers. It's your **Swiss Army knife for delivering cyber protection services that offers both:**

1. An integrated set of solutions that includes **best-of-breed backup, disaster recovery, cybersecurity (including antivirus, anti-malware, anti-ransomware, and anti-cryptojacking), file sync-and-share, file notarization, software-defined storage, and endpoint management.**
2. A **platform** for unified service provisioning, accounts management, monitoring, integrations, whitelabeling, and beyond.

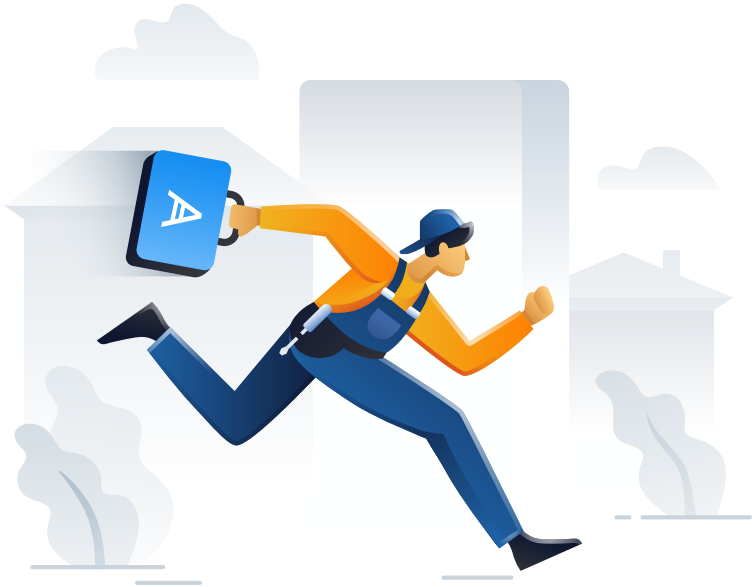
With Acronis Cyber Protect Cloud, service providers can deliver profitable, low-churn cyber protection services that will let customers fearlessly conduct business in an increasingly cybercrime-laden world. And service providers can do it with superior efficiency — from initial system deployment to unified service provisioning and customer management. The Acronis Cyber Cloud platform includes:

- Multitenancy to support an unlimited number of customers
- A multiservice management portal
- Whitelabel capabilities for easy branding
- Service usage quotas and reporting
- Integration with the most popular PSA and RMM tools
- Custom integrations of additional services via an open API

Learn how Acronis empowers you to deliver cyber protection — easily, efficiently and securely:

Contact Acronis sales for a live product demo tuned to your usecase. CONTACT SALES

Start your complimentary 30-day trial today. TRY NOW



References

[1] https://www.ibm.com/security/data-breach

[2] https://www.acronis.com/en-us/blog/posts/acronis-cyber-readiness-report-2021-reveals-critical-security-gaps/

[3] https://www.cloudradar.io/cost-of-downtime

[4] https://www.stratus.com/assets/aberdeen-maintaining-virtual-systems-uptime.pdf

[5] https://www.cisa.gov/uscert/ncas/alerts/aa21-243a

[6] https://start.paloaltonetworks.com/unit-42-ransomware-threat-report.html?utm_source=google-rapp-amer-rapp&utm_medium=paid-search&utm_campaign=Unit_42-Americas-EN-Search-Lead_Gen-US/CA_Q4&utm_content=gs-{16992445439}-{135418592603}-{593884840443}&utm_term=ransomware&sfdcid=7014u000001hKM8AAM&_bt=593884840443&_bm=p&_bn=g&gclid=Cj0KCQjwz96WBhC8ARIsAATR252kVW2uoMmVZ0db3W8lONQy7qL2NJyO2wW6_f5By5aEtVAIMMpXO44aAhFaEALw_wcB

[7] https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises- with-sunburst-backdoor.html

[8] https://www.inc.com/melissa-angell/small-business-cyber-threats-data-protection.html

[9] https://www.coveware.com/blog/2021/10/20/ransomware-attacks-continue-as-pressure-mounts#companies

[10] Ibid.

[11] https://www.barracuda.com/spearphishing-vol7

[12] https://www.acronis.com/en-us/resource-center/resource/648/

[13] Ibid.

[14] https://swzd.com/resources/state-of-it/#chapter-2

[15] https://www.globenewswire.com/news-release/2021/06/22/2251268/27043/en/SMBs-would-pay-on-average-34-more-for-an-IT-service-provider-who-could-provide-the-right-solution-a-rise-from-25-in-2019.html

[16] Ibid.

[17] Ibid.

[18] https://www.top10vpn.com/research/cybercrime-statistics/