Acronis

WHITEPAPER

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 businesses estimated at $3 trillion per year and growing to $5 trillion by 2024, according to a recent report by Juniper Research.[1] Cyberattacks are a costly business nightmare, resulting in profit-sapping downtime, lost revenues, brand damage, stock price losses and regulatory fines.

Tech research firm IDC reports that 93% of organizations have been attacked within the past three years, and nearly half suffered at least one unrecoverable data loss event within the same period. Meanwhile, various researchers concluded that downtime costs can range from $10,000 per hour[2] to as much as $260,000 per hour[3].

Of the many malware types out there, ransomware is currently the most notorious cyber threat, growing by 195% in Q1 2019.[4] It has dominated headlines with high-profile, costly attacks, most notably on the manufacturing, healthcare, local government and education sectors.

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 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 increasingly MSPs fall victim to the same attacks as their customers. Evidence includes a multi-MSP breach that infected 2,000 customer systems with ransomware,[5] and another attack that forced the MSP to pay a $150,000 ransom[6] to unlock their own systems.

But being a ransomware attack target is just a part of the threat: the inability to stop ransomware attacks on customers is harmful for an MSP's competitiveness and ability to grow. For MSPs, this challenge is growing and complex. Statistics show that:

71%

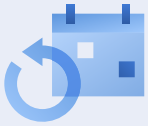
of ransomware attacks target **small to medium businesses (SMBs)**[7]

4 OUT OF 5

MSPs **had to deal** with a ransomware attack on their customers in the last year[8]

24%

of SMBs **have already changed** MSPs in the aftermath of a cyberattack[9]



61%

of MSPs **in the past 12 months were forced** to spend a day or more helping a customer recover from an attack[10]

ONLY 31%

of MSPs are **very confident** of their ability to secure their clients against future ransomware attacks[11]

74%

of SMBs using an MSP said they would take **legal action against their provider** if they suffered a cyberattack[12]

Every business challenge also presents opportunities. You must protect yourself against ransomware attacks and ensure they can't spread. 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 PRIORITY OF IT PROFESSIONALS IN 2019[13]

1. Improving security

2. Reducing IT costs

3. Delivering higher service levels

89%

Percentage of SMBs that **would consider hiring a new MSP** if offered the right cybersecurity solution[14]

25%

Increase in annual costs that businesses already using an MSP **would be willing to pay** to get "the right cybersecurity solution" from a new provider[15]

89%

Percentage of SMBs not currently using an MSP that **would consider hiring one** if it offered "the right cybersecurity solution"[16]

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 possible data losses, 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 ITS 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. This approach 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 and painfully expensive.[17] Further, the recovery point may be sufficiently old that 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, 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 Backup Cloud with Acronis Active Protection technology. This solution, used by over 10,000 MSPs, enables the delivery of cyber protection services that combine backup as a service with integrated anti-malware and automatic remediation features:

- Acronis Active Protection uses artificial intelligence (AI) and machine learning (ML) to detect and disarm ransomware attacks. Continuous training of the AI/ML engine in the Acronis Cloud AI infrastructure produces the industry's lowest false-positive rate for ransomware detection, including for 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.
- The same Acronis Active Protection engine also detects and terminates cryptojacking attacks, another pervasive malware threat that grew by over 4,000% in 2018.[18] Cryptojacking covertly consumes system resources to illicitly mine cryptocurrency, a costly drain on system performance, power and cooling resources.

In short, Acronis Active Protection is a one of a kind technology that enables you to instantly reduce yours and your customers' exposure to ransomware – and you don't have to install anything else on top of your backup agents because it is already integrated into Acronis Backup Cloud.

> "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 Backup Cloud is a part of Acronis Cyber Cloud, a multi-service 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 suite of solutions that includes **secure backup, disaster recovery, malware and ransomware protection, secure file sync-and-share, file notarization and software-defined storage for backups.**
2. A **platform** for unified service provisioning, accounts management, monitoring, integrations, white-labeling, and beyond.

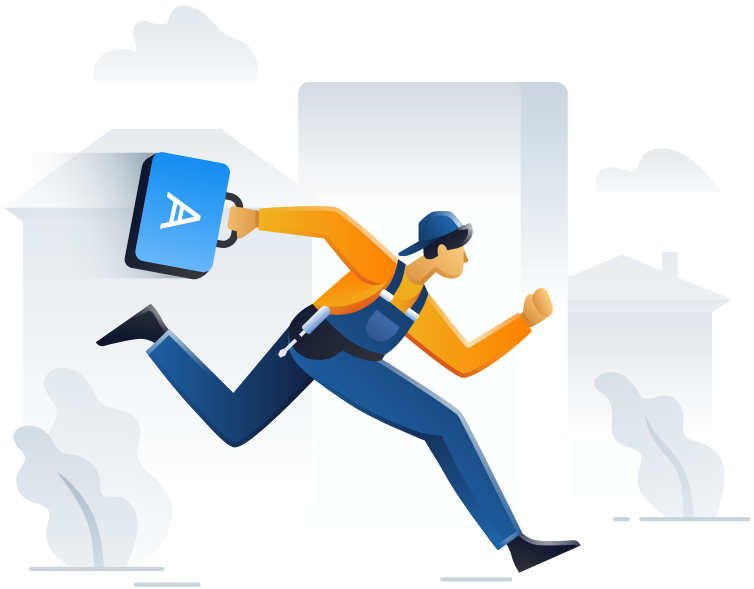
With Acronis Cyber Cloud, service providers can deliver profitable, low-churn cyber protection services that will let customers conduct business fearlessly in an increasingly cybercrime-laden world. And service providers can do it with superior efficiency – from initial system deployment to unified service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

- Multi-tenancy to support an unlimited number of customers
- A multi-service management portal
- White-label 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 lets you deliver cyber protection easily, efficiently and securely:

Contact Acronis Sales for a live product demo tuned to your use-case. CONTACT SALES

Start your complimentary 30-day trial today. TRY NOW



References

[1] https://www.juniperresearch.com/researchstore/innovation-disruption/cybercrime-security

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

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

[4] https://healthitsecurity.com/news/ransomware-attacks-on-business-targets-increase-by-195-in-q1

[5] https://www.darkreading.com/attacks-breaches/customers-of-3-msps-hit-in-ransomware-attacks/d/d-id/1335025

[6] https://www.msspalert.com/cybersecurity-breaches-and-attacks/ransomware/msp-pays-150000-to-recover-data/

[7] https://www.ncsc.govt.nz/assets/NCSC-Documents/beazley-breach-briefing-2019.pdf

[8] https://www.kaseya.com/resource/ransomware-and-your-msp-are-you-ready/

[9] http://info.continuum.net/rs/011-QRO-092/images/Underserved%20and%20Unprepared_%20The%20State%20of%20SMB%20Cyber%20Security%20in%202019.pdf

[10] https://www.channele2e.com/influencers/msp-survey-shows-ongoing-ransomware-malware-challenges/

[11] https://www.channele2e.com/influencers/msp-survey-shows-ongoing-ransomware-malware-challenges/

[12] http://info.continuum.net/rs/011-QRO-092/images/Underserved%20and%20Unprepared_%20The%20State%20of%20SMB%20Cyber%20Security%20in%202019.pdf

[13] https://www.kaseya.com/resource/2019-it-operations-survey-report/

[14] http://info.continuum.net/rs/011-QRO-092/images/Underserved%20and%20Unprepared_%20The%20State%20of%20SMB%20Cyber%20Security%20in%202019.pdf

[15] http://info.continuum.net/rs/011-QRO-092/images/Underserved%20and%20Unprepared_%20The%20State%20of%20SMB%20Cyber%20Security%20in%202019.pdf

[16] http://info.continuum.net/rs/011-QRO-092/images/Underserved%20and%20Unprepared_%20The%20State%20of%20SMB%20Cyber%20Security%20in%202019.pdf

[17] https://www.wsj.com/articles/one-year-after-notpetya-companies-still-wrestle-with-financial-impacts-1530095906

[18] https://www.coindesk.com/mcafee-crypto-mining-malware-grew-by-over-4000-percent-in-2018