Publication date:
14 Dec 2021
Author:
Rik Turner, Principal Analyst, Emerging Technologies

Acronis taps Perception Point for email security as part of its Cyber Protect Cloud

Omdia view

Summary

Data protection and security vendor Acronis has launched an email security service as part of its broader offering, which combines its flagship backup and restore capabilities with security technology. Omdia sees a market opportunity for the vendor in the fact that the continued rise of ransomware makes a portfolio that brings these two areas together increasingly relevant.

The latest addition to the Acronis portfolio, Advanced Email Security, is the result of a partnership the vendor has struck with Perception Point, a developer of security for cloud-based business email services, which, in practice, means Microsoft 365 and Gmail.

Ransomware drives security and data protection together

The idea of bringing data protection technology and cybersecurity together under one roof is not a new one. The argument goes: why not get protection from attacks from the same vendor that provides you with the backup copy of your data, so if an attack gets through and defaces, corrupts, or otherwise renders unusable your production data, you'll still have a fallback? Indeed, this was a major part of the rationale behind then-security market leader Symantec's December 2004 acquisition of its counterpart in backup and restore, Veritas.

The two vendors in that case were huge entities, and while the merged company continued to be a major player for the next decade, they never really delivered on the acquisition's early promise, such that the marriage was dissolved in 2016. Now, however, the argument for cybersecurity plus data protection has gained new currency, due to the surge in the number and severity of ransomware attacks.

One vendor estimates that 2021 as a whole will see a staggering 714 million ransomware attacks against its customers, representing a 134% increase on 2020, according to information-age.com. And while Verizon's authoritative *Data Breach Investigations Report* (DBIR) for 2021 states that 90% of all attacks resulted in no actual financial loss to the victim because no ransom was paid, the US Treasury's Financial Crimes Enforcement Network (FinCEN) also reports $590m in ransomware-related activity in the first six months of the year, up from $416m for all of 2020. In other words, not everyone is paying, but those who are paying out increasingly large sums.

A backup held offline can foil ransom attempts

The cornerstone of a ransomware attack is, of course, that it encrypts a victim's data stores so as to charge a ransom for the key to decrypt. To guarantee the efficacy of its attack, this also means encrypting backed-up copies of the data, making it imperative for at least one copy to be held offline if the victim is to avoid the extortion attempt.

Thus an appropriate data protection system needs to be in place to create backups, ideally with one of them kept offline for the eventuality of a ransomware attack, while others may be held on- or nearline for production systems to access as required. This is, in essence, the market opportunity presented by ransomware for vendors of backup and restore technology.

Acronis, which made its name in the data protection market (i.e., backup and restore technology), has been expanding into cybersecurity over the last couple of years, branding its offering, which combines the two capabilities, as "cloud protection." Its cloud-delivered services are marketed under the Acronis Cyber Protect Cloud banner, delivered via a single agent deployed on the workload to be protected, and managed through a single console.

As for its route to market, Acronis delivers Cyber Protect Cloud through various types of service providers: managed service providers (MSPs) are its primary route, in keeping with its midmarket and SMB target audience, followed by telcos, cloud distributors, and traditional value-added resellers (VARs).

Acronis has been quite an acquisitive company in recent years, with some of its expansion into cybersecurity coming through M&A activity. For example:

- In March 2021 it acquired Nyotron, a last-mile detection and response provider.
- In November 2020 it bought penetration testing provider CyberLynx.
- In July 2020 it acquired DeviceLock, a developer of endpoint device/port control and data leak prevention technology.
- In December 2019 it bought 5nine Software, a provider of cloud management and security tools.

Acronis Cyber Protect Cloud: core features and Advanced Packs

Acronis Cyber Protect Cloud consists of a set of core functionality, charged on a pay-as-you-go basis:

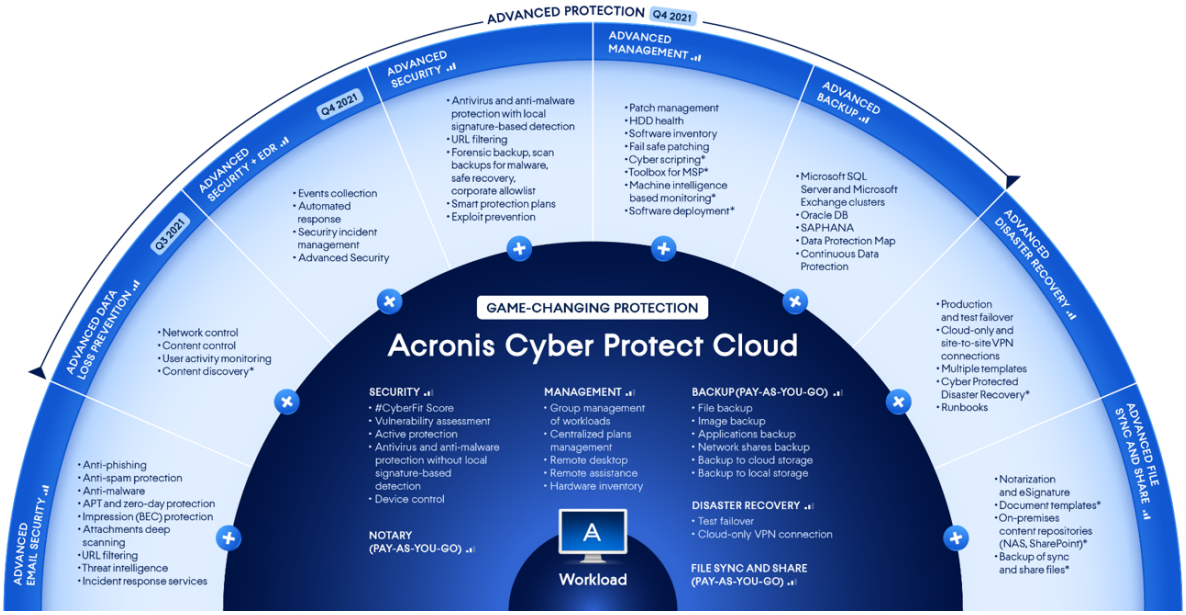
- Backup for files, images, applications, and network shares, with the backed-up data going to either cloud or on-premises storage. Acronis combines traditional backup and restore capabilities with AI to detect and block ransomware, blockchain-based verification of data authenticity, and end-to-end encryption.

- Acronis Cyber Disaster Recovery, which protects workloads in the event of an outage by spinning up systems with cloud-based recovery and restoring them to wherever the customer prefers.
- File sync and share, enabling collaboration via a cloud-based platform where documents can be uploaded, viewed, edited, and downloaded by permitted groups of people.
- Security, which includes regular vulnerability assessments, antivirus and antimalware protection without relying on locally held signatures, and device control.
- Management, which enables the group management of workloads, centralized plans management, remote desktop, remote assistance, and hardware inventory.
- Notary, a blockchain-based service for file notarization, e-signing and verification.

To this core platform, the customer can add any of a number of what it calls Advanced Packs, which are:

- Advanced Data Loss Prevention, which is based on the DeviceLock DLP technology and includes network control, content discovery and control, user activity monitoring.
- Advanced Security - Endpoint Detection and Response (EDR), which includes event collection, automated response, and security incident management.
- Advanced Security, which comprises AV and anti-malware protection based on locally-held signatures, URL filtering, forensic backup, and exploit prevention.
- Advanced Management, with features such as patch management, nard drive health scans, software inventory, and AI-based monitoring.
- Advanced Backup, featuring backup for SQL Server and Exchange clusters, Oracle databases, and SAP HANA.
- Advanced Disaster Recovery, which includes cloud-only and site-to-site VPNs, as well as runbooks.
- Advanced File Sync and Share, with notarization and e-signatures and support for on-premises repositories such as NAS filers and SharePoint.
- The new addition to this second list is Advanced Email Security.

1. Figure 1: Acronis Cyber Protect Cloud



Source: Acronis

Perception Point enables the new Advanced Pack

Email security has been in transition over the last decade ever since Microsoft took its Exchange server off customers' premises and into the cloud, delivering the technology as a service and renaming it Office 365 in the process. Since then, vendors of the dominant email security platforms, namely secure email gateways (SEGs), have all added a cloud-based version of their product.

More seriously, however, they have encountered a new competitor in the form of Microsoft itself, which now has two email security platforms called Exchange Online Protection (EOP) and Defender Advanced Threat Protection (ATP), the first of which covers most of the functionality of SEGs, i.e. antimalware, antispam, and antispyware.

Since Microsoft bundles its two security products into different SKUs of Office 365 (now renamed Microsoft 365, but still widely referred to under its old name), the challenge the SEG vendors face is that they must justify customers' ongoing spend on their products, given that they are all getting EOP and many of them may also be benefitting from ATP as well (ATP is part of the E5 SKU).

A further complicating factor is that email-based attacks have also evolved beyond the traditional adversaries countered by SEGs, namely phishing, spear phishing, and business email compromise. These new types require a different approach for detection and response, and a new category of security vendors has arisen, which Omdia refers to generically as the "non-SEGs."

Unlike SEGs, their products do not sit inline in front of the email server but rather connect to the users' inboxes via an API that enables them to avoid the one-time-only look at email traffic. And since Microsoft's own email security is widely considered to be good but not great, they tend to position their products as "catching the things that a traditional SEG or Office 365 miss." Perception Point fits into this group.

Bringing email security into the fold

Advanced Email Security comes with a range of capabilities, namely:

- Antiphishing
- Antispam
- Antimalware
- Protection from advanced persistent threats (APTs) and zero-day attacks
- URL filtering
- Threat intelligence
- An incident response service provided by a team of experts

For Acronis, the partnership expands its Cyber Protection Cloud offering into an essential area, namely email, which remains the most widely exploited vector for attacks. For Perception Point, it expands its offering beyond the enterprise customer segment, bringing MSPs and other service providers into play to broaden its addressable market without the need for the vendor itself to grow its employee headcount.

Acronis was founded as a spinout from virtualization vendor Parallels in 2003 by Serguei Beloussov, formerly CEO, and now chief research officer and president of technology Stanislav Protassov.

The vendor was founded in Singapore and incorporated in Switzerland in 2008 and retains joint headquarters in Singapore and Schaffhausen, Switzerland. It has raised a total of $408m in funding, most recently announcing a $250m private equity round, in May 2021, from CVC Capital Partners. Since July 2021, Acronis's CEO is Patrick Pulvermueller, whose previous role was as President of the Partner Business at GoDaddy, and before that he was CEO of Host Europe GmbH.

Appendix

Further reading

Omdia Universe: Selecting an Inbound Email Security Platform, 2021–22 (September 2021)

Fundamentals of Inbound Email Security (September 2021)

Author

Rik Turner, Principal Analyst, Cybersecurity

askananalyst@omdia.com

Citation policy

Request external citation and usage of Omdia research and data via citations@omdia.com.

Omdia consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help you. For more information about Omdia's consulting capabilities, please contact us directly at consulting@omdia.com.

Copyright notice and disclaimer

CONTACT US

omdia.com

askananalyst@omdia.com