IDC LINK
Real-time IDC Research® opinion on industry news, trends and events

Acronis Announces Acronis Cyber Protect and Cyber Protect Cloud

April 28, 2020

By: Phil Goodwin, Robyn Westervelt

IDC's Quick Take

Data protection and data security are no longer separate disciplines or tasks for IT organizations. IT leaders are now approaching data protection and security in a holistic manner and vendors are responding with integrated platforms to offer both better cyber attack prevention and faster recovery in the event of a successful attack. These solutions must be equally adaptable to the cloud and on-premise infrastructure.

Product Announcement Highlights

Acronis today announced Acronis Cyber Protect Cloud, a platform for cloud service providers designed to prevent malware intrusion, perform malware detection and backup data continuously with an immutable copy for assured recovery. Acronis Cyber Protect Cloud includes Acronis's AI capability for detecting ransomware in the pre-attack phase as well as an interesting implementation of blockchain technology to assure the validity of data contained in files. Acronis Cyber Protect Cloud is available immediately and a version of the product that will be sold directly to enterprises and SMBs, named Acronis Cyber Protect, is expected to be released for general availability in the summer of 2020.

Acronis has been delivering capabilities for data protection (e.g., backup/recovery, disaster recovery) and cyber recovery (e.g., blockchain, Acronis Notary) for several years. Acronis Cyber Protect is the next level of this implementation to now protect primary storage, backup storage and end point devices and data. Many of the new cyber protection features will be added to the company's consumer product, Acronis True Image, later this year. It applies to both on-premise and cloud workloads, although the initial roll-out (dubbed Phase 1) will be only available as a service from qualified cloud service providers (CSPs). In Phase 2, the platform will be sold directly to SMB and enterprise organizations via Acronis's channel partners.

Acronis Cyber Protect has eight key elements:

- Continuous data protection – critical workloads can be designated for continuous protection, resulting in near-zero RPO and RTO recoveries
- Protection from re-infection – restore OS images (including VMs) with the latest update patches, security patches and update anti-malware prior to data restoration to help protect from re-infection
- Malware scans from centralized locations – full disk backup scanning from a central location helps reduce the risk from rootkit and bootkit infections and reduces the load on endpoint devices
- Smart protection plans – Acronis's cyber protection operations center (CPOCs) monitors threats and alerts and automatically adjusts protections plans accordingly. The change in plans can

increase the frequency of backups or perform deeper anti-virus scans; plans return to normal after the threat abates

- Fail-safe patching – provides full image endpoint backup priority patching, so that the original configuration can be restored quickly if the patch effort fails for any reason
- Forensic data capture – by activating the forensic data capture mode, memory dumps, full images and HDD sector-level information is captured for future analysis
- Data compliance reporting – assure data compliance and auditing of important files by tracking their backup status and alerting if files are not backed up
- Global and local white lists - scan backups with anti-malware technologies (AI, behavioral heuristics, etc.) to whitelist organizational unique apps and avoid "false positives" in the future

Common use-cases for Acronis Cyber Protect, in addition to normal backup and recovery, include auto-response to emerging threats, real-time (CDP) protection of important documents, 0-day malware and ransomware protection and recovery, and compliance and forensic analysis.

IDC's Point of View

Acronis is among the companies on the forefront for integrated data protection and cyber protection. We believe that Acronis Cyber Protect is among the most comprehensive attempts to provide data protection and cyber security to date. Disconnected point-product deployments put the burden on the IT staff to assure that gaps between anti-malware software, backup software, analytic software and so on cannot be exploited. We believe that integrated data protection and data security platforms, augmented with AI and ML technology, will continue to evolve to address increasingly sophisticated attacks. While preventing these attacks is the goal, organizations must also have the tools for rapid, certain data recovery.

Acronis shows potential to disrupt traditional IT security vendors by delivering integrated components for backup/recovery and malware detection and protection. This level of integration is attractive to enterprise buyers that frequently site the need for security solutions that are less complex to manage. IDC's Data Security Survey 2020 found that while a quarter of sensitive data still resides in on-premises datacenters, the sensitive data making up the other three quarters is spread evenly across desktops and laptops, smartphones, and public and private cloud environments. The more than 600 IT and IT security survey respondents told IDC that the most sensitive data resides at the endpoint. More than 64% of those surveyed called endpoint data either very sensitive or extremely sensitive.

Acronis's backup-as-a-service (BaaS) and on-premise backup are attractive to buyers seeking a modern approach to cover traditional applications, cloud-native applications, edge devices or any combination. Its multi-tenant cyber-protection is designed for both private cloud and managed service provider (MSP) deployments. Acronis product strategy is consistent and in-line with enterprise requirements for cyber resiliency technologies. Senior management have been successful executing on that strategy, making Acronis cyber protection a more cohesive and tightly integrated than competitive offerings.

Ransomware protection continues to be in great demand. In a recent engagement with IDC, a consumer goods manufacturer failed to have modern backup and recovery systems resulting in intellectual property loss and costly downtime at its production facility. The company struggled to recover data from an old tape backup. The information was so critical that senior management were forced to phone retirees to retrieve lost product formulas. If that manufacturer had Acronis' modern backup and recovery software combined with its active protection, not only would it have potentially avoided the

data loss, but it may have avoided the security incident altogether using Acronis ransomware protection technology for data processing environments.

In addition, Acronis' core technologies consisting of modern backup and recovery and antimalware detection and containment as well as forensic data capture and data compliance reporting capabilities are in-line with the emergence of converging security technologies that were once perimeter-centric. Pervasive Data Defense platforms are a novel way to provide perimeter-free protection over critical data assets across hybrid and multi-cloud environments. These platforms represent the convergence of cloud security gateways, data loss prevention platforms, and secure web gateway functionality. They are also incorporating other technologies that provide visibility and control over corporate endpoints such as backup and recovery software and services DNS filtering, browser isolation, and integrated endpoint protection. This security market convergence enables enterprise security teams to leverage a single unified policy engine, a single management console, centralized analytics, and a consolidated reporting framework.

Acronis's biggest challenge will be to establish market dominance in the early stages of cyber protection and recovery market development before much larger competitors can enter and gain attention. Even with advanced, differentiated technology, Acronis has yet to experience a "break out" moment to emerge as a market share leader in the data replication and protection market according to IDC data. However, the company recently received a significant equity investment from Goldman Sachs which will give it added resources to embark on the large-scale marketing and development needed to compete with much larger organizations.

Subscriptions Covered:
Data Security, Multicloud Data Management and Protection