REPORT REPRINT

This Impact Report was published by 451 Research as part of our syndicated Market Insight subscription service and subsequently licensed for commercial use by Code42.

Code42 leverages endpoint backup to leap into data management and security

HENRY BALTAZAR, LIAM ROGERS

26 MAY 2017

The company recently released version 6.0 of its data-protection platform to take on internal threats while introducing new data analytics and visibility tools, which are at the core of the latest release.

THIS REPORT, LICENSED EXCLUSIVELY TO CODE42, DEVELOPED AND AS PROVIDED BY 451 RESEARCH, LLC, SHALL BE OWNED IN ITS ENTIRETY BY 451 RESEARCH, LLC. THIS REPORT IS SOLELY INTENDED FOR USE BY THE RECIPIENT AND MAY NOT BE REPRODUCED OR RE-POSTED, IN WHOLE OR IN PART, BY THE RECIPIENT, WITHOUT EXPRESS PERMISSION FROM 451 RESEARCH.

451 Research®

©2017 451 Research, LLC | WWW.451RESEARCH.COM

Code42 got its start as an endpoint data-protection specialist and has steadily added to its product portfolio, while extending from on-premises to SaaS offerings. Enhancing backup and recovery products with additional levels of security and data management capabilities has been a trend in the market, and the company has focused its product development efforts on adding search and data analytic capabilities, which are at the core of the recently released version 6.0.

THE 451 TAKE

Players in the backup market have been gravitating toward providing additional security features to better meet the expectations of customers that are struggling with insider data threats and newer problems such as ransomware. Code42 is certainly catering to this and other customer interests with its platform update. Addressing the threat of ransomware in particular has been a recurring theme among many vendors in this space, but the company is tackling internal threats with equal zeal as external ones. It's taking a proactive approach as it aims to ramp up an enterprise's ability to maintain a higher level of visibility into user data activity and both detect and respond to insider data exfiltration. The company has built up a healthy installed base with thousands of enterprise customers, and now generates over $100m in revenue. However, based on current market activity, Code42 will likely see increasing competition from other backup providers also looking to bolster their offerings with security and compliance features as well as deeper analytics to better serve client needs beyond basic file recovery.

CONTEXT

Code42 is headquartered in Minneapolis, with additional US offices in San Francisco, Denver and Washington DC, as well as international offices in London and Munich. The company was founded in 2001 and has a current headcount of 515. It raised $85m in a recent series B round led by JMI Equity and New Enterprise Associates, bringing its total funding to date to $137.5m. Its customer count is 39,000, with a shade under 6,000 being enterprise licenses. Revenue is currently in excess of $100m, with the majority recurring.

STRATEGY

Providing security features that meet user demands and concerns is a major driving force behind v.6.0. Offering more versatile data protection that affords more holistic visibility is intended to foster a more actionable environment for clients. Maintaining data visibility presents its own unique challenges in addition to those of real-time data protection and recovery.

The latest release also introduces Code42's partnership with identity and access management provider Okta, which recently went public. By Code42's assessment, over 30% of its enterprise customers are already using Okta. While this is a logical move for the company, it plans to offer additional partner support and integrations in the future. This could be an opportunistic strategy to bolster its data-protection platform with added functionality, especially because the fragmented and complex nature of the security industry can make keeping pace with demanded features a daunting task. As it addresses more security concerns, Code42 anticipates taking more steps in the direction of machine learning and user behavior analytics (UBA). Its current machine-learning tools are its own, but Code42 plans to consider third-party tools moving forward.

PRODUCTS

Code42's data-protection platform covers endpoint backup and recovery, device migration, threat monitoring and ransomware recovery. The three components of v.6.0 are security center-based alerting, access locking and partner integrations. The focal point of the new update is proactively countering internal threats that can be difficult to detect based on the complexity of managing user privileges. The platform enables greater visibility by employing endpoint monitoring to allow users to see who is moving data, when it was moved and where it was moved to.

The security center dashboard provides alerting for departing employees and generates email notifications about suspicious activity such as the employee moving large amounts of data. Since many internal threats related to departing employees are not discovered in a timely manner, Code42 is aiming to automate this process to mitigate risk and damage.

The access lock serves to combat insider and outsider threats by providing administrators with an API that can remotely lock devices that have the Code42 client installed. This is targeted at preventing unauthorized access in situations where devices themselves might have been compromised. The final element of the update, the Okta partnership, allows customers to integrate their cloud-based Code42 security features with on-premises tools such as lightweight directory access protocols and single-sign-on authentication.

COMPETITION

Code42's backup and recovery product faces a fair amount of competition in the endpoint backup market from several players, including Carbonite, Druva and Dell EMC's Mozy – although we would note that all of these firms have expanded their offerings over the years well beyond endpoints. Given the large amounts of data being accessed and created on mobile devices and desktops, endpoint backup products from vendors such as Code42 are in a good position to deliver advanced data management and data loss-prevention capabilities since they see every file and the changes made to them during the backup process. As Code42 extends into data management and security, its offerings will compete with a broader section of the data-protection sector.

The enterprise and midrange backup market is mature and includes a large number of significant players such as IBM, Commvault, Dell EMC, Veritas, Arcserve, NetApp, Veeam, VMware, Unitrends and Acronis. All of these vendors have added or are in the process of adding advanced data analytics and reporting tools to help organizations identify sensitive data and prevent data loss. While improving backup and disaster recovery continues to be a key problem for organizations, customers want to get more value out of their data-protection dollars.

In the startup space, disruptors such as Cohesity and Rubrik are blending backup, data management and analytics into an interesting new class of secondary storage-oriented hyperconverged infrastructure. Given that these vendors and many of the aforementioned players are focused on VM and server backup, and not necessarily in a good position to capture endpoint data, there is a possibility that Code42 could be deployed in conjunction with offerings from other backup and data-protection players.

SWOT ANALYSIS

STRENGTHS

Code42 has a solid base of customers and is being attentive to their feature requests. Its products cover a broad range of clients, from consumers up to large enterprises.

WEAKNESSES

The company is still best known for its endpoint backup products and needs to boost its presence in data management and data loss prevention for enterprises and service providers.

OPPORTUNITIES

Machine learning and UBA are areas where Code42 could create differentiation in a crowded data management segment as users focus more on analytics and proactive security measures. Additional partnerships could provide a path forward in these areas.

THREATS

The backup and recovery sector will become increasingly competitive as vendors add security features to meet customer demands. Keeping up with user expectations may also prove challenging given the sheer number of security concerns that enterprises must address.