TAG

ANALYST REPORT: INSIGHTS AND RECOMMENDATIONS FOR IMPROVED CYBER RESILIENCE USING CRASHPLAN

DR. EDWARD AMOROSO
CHIEF EXECUTIVE OFFICER, TAG

CrashPlan™

ANALYST REPORT: INSIGHTS AND RECOMMENDATIONS FOR IMPROVED CYBER RESILIENCE USING CRASHPLAN

DR. EDWARD AMOROSO, CHIEF EXECUTIVE OFFICER, TAG

The research reported here shows that enterprise teams will benefit from deployment of purpose-built backup solutions to improve the resiliency of the data that resides on the endpoint. Commercial vendor CrashPlan is shown to effectively implement data backup for enterprise devices resulting in improved security and ability to withstand ransomware attacks.

INTRODUCTION

The analyst team from TAG Infosphere[1] recently engaged with the CISO and industry experts of commercial vendor CrashPlan to engage in a joint investigation into the benefits of endpoint backup solutions for enterprise teams. The work involved active discussions with Chief Information Security Officers (CISOs), a mini survey with security practitioners, and a thorough investigation by TAG analysts into the data protection and resilience platform CrashPlan.

The results of the TAG analysis revealed a protection gap for most businesses in how they maintain cyber resiliency for their endpoint data devices such as computers (PCs) and laptops. This protection gap can leave an organization's important data vulnerable to ransomware attacks and malicious actors. This can also lead to significant financial, legal, compliance and reputational costs to organizations that experience a data breach.

This report explains and illustrates the data protection gap identified during the research study and proposes an improved enterprise data protection scheme that will reduce the associated risk, especially with respect to the ever-growing potential for ransomware attacks. CrashPlan is shown to be an excellent commercial partner option to achieve the cyber resilience inherent in the proposed scheme.

OVERVIEW OF THE RESEARCH

Our objective in the work reported here was to determine the degree to which organizations data is at risk due to lack of a strong endpoint data protection capabilities and data resilience gaps and whether these are understood by security practitioners. At TAG, we have the great advantage to work on a day-to-day basis with nearly 120 major enterprise security teams and this provides us an accurate proxy for the posture and sentiment across the industry.[2]

The main question addresses the issue of how companies protect the data that resides on their endpoints. Obviously, enterprise security teams understand the challenge posed by ransomware attacks, but we suspected that many of the organizations queried were mis-using cloud collaboration tools for endpoint data resilience, and that many were relying on internal policies for endpoint data protection that rely on human interaction and may not always be followed or enforced.

The research was conducted in partnership with CrashPlan, who has been an industry leader in endpoint data protection and resilience over 20 years. CrashPlan assisted in developing the questions and in analyzing the results, leveraging their experience in data protection and resilience as well as insights derived from customer interactions.[3]

RESEARCH INSIGHTS

Our survey and research analysis with CISOs produced a series of useful results, the most consequential of which involves the broad observation that a *majority of enterprise security teams today have insufficient security policy enforcement and have not deployed effective endpoint data protection controls to ensure the resilience of data stored in a distributed manner across their endpoints.*

This is a surprising result given the awareness and proliferation of ransomware as well as both malicious and inadvertent insider threats as common enterprise security threats today. Accordingly, three specific insights emerged as a result of the research investigation – and all insights point to weaknesses in current enterprise security configurations. Obviously, we offer these insights in the hope that practitioners will take steps to address the challenges:

Insight 1: Manual policy enforcement is not viewed as a dependable control for tasks such as endpoint data resilience.
It was clear from our discussions with CISOs that policy is a major component of their strategy to protect endpoint data. Most of the security professionals surveyed agreed that some policy was in place, usually with the objective to drive manual or automated compliance, but almost all of these practitioners expressed great doubt that the policy was being effectively enforced or even noticed.

Related studies, including from Harvard Business Review, suggest a similar challenge with a study showing that roughly two-thirds of employees admit to violating business policies. The implication, obviously, is that administrative control using manual procedures is inferior to technical controls based on automation. This appears to be true not only for endpoint data protection but for more general policy enforcement as well.

Insight 2: Cloud collaboration tools are insufficient to support the functional requirements for endpoint data resilience.
During discussions with CISOs, security practitioners and CrashPlan, it also became clear that cloud collaboration tools are mis-used and relied upon for data backup and resiliency. There was an increase in use of such platforms during the COVID-19 pandemic as companies went to a remote work model and that trend has continued to a degree post-pandemic. Cloud collaboration solutions are typically implemented by IT teams to enable user collaboration within the organization and as the pandemic evolved and employees were working from home, collaboration tools were an easy way to address efficiency and collaboration but are often mis-used to address backup needs as they had already been purchased for collaboration.

While such solutions are obviously wonderful means for driving sharing, collaboration, and virtual operation of teams, they were not designed for backup. This implies that teams reusing such capability to address ransomware risk, execute recovery at scale across the organization, data backup and improve data resilience are seeing gaps and challenges in this approach, including missing files, file versions, short durations for retention, scaling issues for recovery.

Insight 3: Many enterprise teams possess a false sense of security for endpoint data resilience and restoration post-incident.
Any reference to "false sense of security" is more sentiment-based than scientific, but the effect is clearly present among modern working CISOs. The challenge is evident in the various ransomware, malicious, or inadvertent insider threat cases that appear so frequently in the community, including ones that reach the mainstream media. In each case, the likelihood that cloud collaboration tools are being used is high, but the deployment obviously had little impact on ransomware protection.

Virtually none of the CISOs included in our research survey reported having strong validation and test methods for the restoration processes in place post-incident. This also drives our observation that any confidence that exists in post-breach restoration of endpoint data is based more on general sentiment than on well-tested and validated infrastructure that was designed and deployed specifically to address endpoint data risk.

PROPOSED IMPROVED CYBER RESILIENCE

Given the results of our survey, we determined that a new security protection model was needed to help enterprise practitioners address this aggregate cyber risk to the data stored on their endpoints. The model that resulted, which we refer to as MEAD (Malware, EDR, Analytics, and Data) integrates existing endpoint security controls with attention to this newly recognized aggregate stored data risk.

The MEAD model is based on the reasonable presumption that modern endpoints are well-covered in the areas of malware avoidance, using next generation antivirus solutions, endpoint security coverage with modern endpoint detection and response (EDR) solutions, and analytics with a range of endpoint security solutions that support tracking, review, and updates to endpoint systems.

The newest protection component – designated by the D in the MEAD model, involves data protection and resilience, and this demands a new cybersecurity control that supports the types of enterprise risk issues addressed in our survey of CISOs described above. That is, a new data control is required that can carefully manage and mitigate the aggregate data risk for endpoint data storage (see Figure 1).

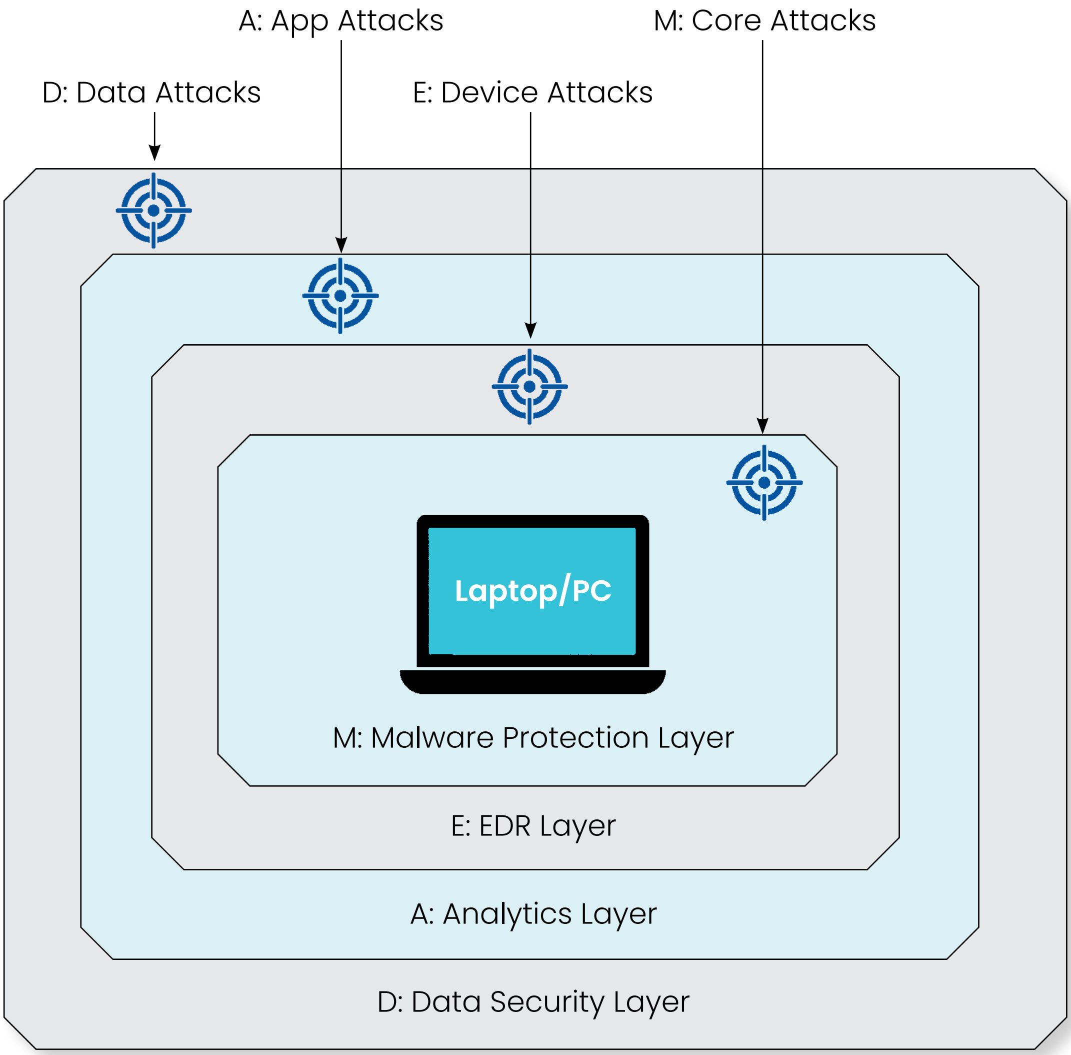

Figure 1. MEAD Model for Endpoint PCs and Laptops

As suggested above, the MEAD model specifies that existing endpoint protections become more tightly integrated with aggregate data security solutions for endpoints. Thus, an anti-malware solution (e.g., MalwareBytes), EDR solution (e.g., CrowdStrike), and endpoint analytics solution (e.g., Tanium), could be easily integrated into a comprehensive endpoint solution using a purpose-built endpoint backup and data protection solution (e.g., CrashPlan).

OVERVIEW OF CRASHPLAN

CrashPlan offers a cloud-native platform designed to address the aggregate risk associated with data stored on endpoints within organizations. It offers a comprehensive backup and data protection system that safeguards valuable business data from loss, theft, or accidental deletion. Businesses of all sizes, across all different business sectors, use CrashPlan today to ensure a more robust data protection and resilience approach.

CrashPlan operates by continuously and securely backing up data on individual endpoint devices to a centralized cloud-based repository. This approach ensures that data is protected in real-time, eliminating the risk of data loss due to hardware failures, user errors, or cyber threats. Additionally, CrashPlan employs strong encryption measures to safeguard data during transmission and storage, ensuring compliance with various data security regulations.

A strength of CrashPlan is its scalability, making it suitable to efficiently manage the backup needs of a large number of endpoints, providing administrators with centralized control and monitoring capabilities. CrashPlan's solution mitigates the aggregate risk associated with data stored on endpoints by providing continuous, secure, and scalable backup and data protection services, thereby ensuring business continuity and data resilience.

The integration features of CrashPlan make it a perfect candidate for inclusion in a protection architecture driven by the issues raised throughout this report – including support for the MEAD model. Any organization concerned with the aggregate data risk referenced above would be wise to review how CrashPlan can be deployed in their environment to drive a security scheme that directly addresses the risks explained in detail in the narrative above.

CONCLUDING REMARKS

The implication of our work is that organizations clearly will benefit from a purpose-built endpoint data protection and resilience platform. The gap that emerges with use of cloud collaboration tools is also something that can be addressed by focusing in this area. To that end, we recommend the following action plan:

1. **Inventory** – Enterprise security teams should review their existing solutions for endpoint data protection, including policies (as discussed in the survey).
2. **Requirements** – Based on existing policies and controls, a threat-based assessment should be used to develop functional requirements to improve endpoint data resilience.
3. **Vendor Selection** – Source selection of a suitable vendor partner – and we recommend that CrashPlan be included in such review – will be the next step toward implementing a program of improved endpoint data resilience.

Certainly, each organization will need to tailor any management action plan to local conditions, budget, and related initiatives. As always, TAG analysts are available to provide expert assistance to enterprise teams undertaking such work.

APPENDIX: SURVEY SUMMARY

Our research process started with a survey posed to two dozen CISOs connected to TAG Infosphere's Research as a Service (RaaS) offering as customers. The survey involved three simple questions designed to gain insight into how the participants addressed the aggregate risk to the data stored on their PCs and laptops. Answers were collected in a non-attributable form to maintain anonymity. The results are provided below:

Question 1: Do you have a policy and associated control in place to protect the confidentiality, integrity, and availability of stored data on your employee PCs and laptops? If so, do you think it is working? This question specifically referenced a policy, because we were interested in understanding the degree to which the aggregate threat was being addressed. Our presumption was that certainly some protection would be in place, often based on ad hoc local decisions by endpoint owners or local business units and teams. A policy, however, would demonstrate focus across the entire organizations.

Based on the survey, we found that 93% do, in fact, have a policy in place, and that some type of associated control had been deployed for employee PCs and laptops. This was a promising result, even though one wonders about the 7% who claimed no policy (the CISOs queried were from mostly large businesses). Of the 93% with a policy in place, only 7% claimed confidence that their policy was definitely working. This is not a large percentage obviously.

Interestingly, when asked about the effectiveness of their policy, 36% were certain their policy was not working, and an additional 57% suspected that it might only be partially working. This results, if you do the math, in 93% of those with policies in place, not thinking they were working. This does not count, by the way, the 7% with no policy. This is not a good result for enterprise attention to the aggregate risk for data on PCs and laptops.

Question 2: Would you be surprised if a data breach were to occur involving data stored on your PCs and laptops?
This question was intended to identify whether the CISO or their enterprise security team would be honestly surprised if a serious breach were to occur in this area of aggregate data stored on PCs and laptops. This type of softer question, we have found, is an effective means for determining the sentiment of team members directly responsible for such protection. Asking experts to offer sentiment really does expose their honest views regarding risk.

We were surprised to learn that a whopping 71% of those asked responded that they would not be surprised if they had a serious data breach on their PCs and laptops. If the question was extended to include that they might be surprised, the number grew to 86%. This seems an important result because such sentiment implies that serious risk must exist in this area. If that many CISOs would not be surprised if something bad happened, then a problem exists.

Question 3: Would you be open to deploying a functional backup control in the form of a commercial platform to address this aggregate risk of data on PCs and laptops?
This third question attempted to gauge interest in CISOs and their teams reviewing, deploying, and maintaining a new system that would mitigate the risk of sensitive critical data from being targeted on PC and laptop endpoints. The question is notional in that it does not discuss specifics such as cost, but it helped to determine whether the security portfolio had a gap in coverage for PCs and laptops.

Despite the fact that every CISO queried was spending money on endpoint detection and response (EDR) and related anti-malware solutions, a high 79% replied that they would be open to deploying a new function control for PCs and laptops. (By "open to deploying," we mean that they answered that they would or might consider deployment of such a solution.) This was heartening, given the EDR coverage for those queried that when engaged on the subject they recognized the need for further data resilience at the endpoint.

[1] TAG Infosphere is a trusted next-generation research and advisory firm founded in 2016 by experienced industry executives and headquartered in New York City. TAG utilizes an AI-powered SaaS-platform to provide on-demand insights, analysis, research, and advisory to executives and practitioners in cybersecurity, artificial intelligence, climate/sustainability, telecommunications, and other major areas of business interest.

[2] Enterprise cybersecurity teams of many different sizes and across a variety of different industry sectors and countries subscribe on a monthly basis to TAG's next generation, on-demand SaaS research offering, often as a replacement for traditional industry analyst relationships. These teams, roughly 120 companies as of this writing, provide excellent support for surveys and analyses on topics related to cybersecurity, IT operations, networking, artificial intelligence deployment, and much more. They generally share openly, but under the agreement that their comments never be attributed publicly or included in aggregations that are so obvious as to expose organizational identities,

[3] The questions provided to our select enterprise participants along with the answers they shared back are listed in Appendix A. Summaries and percentage findings are also included in the Appendix.

ABOUT CRASHPLAN

CrashPlan® enables organizational resilience through secure, scalable, and straightforward endpoint data backup. With automatic backup and customizable file version retention, you can bounce back from any data calamity. What starts as endpoint backup and recovery becomes a solution for ransomware recovery, breaches, migrations, and legal holds. So you can work fearlessly and grow confidently.

ABOUT TAG

TAG is a trusted research and advisory company that provides insights and recommendations in cybersecurity, artificial intelligence, and climate science to thousands of commercial solution providers and Fortune 500 enterprises. Founded in 2016 and headquartered in New York City, TAG bucks the trend of pay-for-play research by offering unbiased and in-depth guidance, market analysis, project consulting, and personalized content—all from a practitioner perspective.

IMPORTANT INFORMATION ABOUT THIS DOCUMENT

Contributors: Dr. Edward Amoroso

Publisher: TAG Infosphere Inc., 45 Broadway, Suite 1250, New York, NY 10006.

Inquiries: Please contact Lester Goodman at lgoodman@tag-cyber.com to discuss this report. You will receive a prompt response.

Citations: Accredited press and analysts may cite this book in context, including the author's name, author's title, and "TAG Infosphere, Inc.." Non-press and non-analysts require TAG's prior written permission for citations.

Disclaimer: This book is for informational purposes only and may contain technical inaccuracies, omissions, and/or typographical errors. The opinions of TAG's analysts are subject to change without notice and should not be construed as statements of fact. TAG Infosphere, Inc. disclaims all warranties regarding accuracy, completeness, or adequacy and shall not be liable for errors, omissions, or inadequacies.

Disclosures: CrashPlan commissioned this book. TAG Infosphere, Inc. provides research, analysis, and advisory services to several cybersecurity firms that may be noted in this paper. No employees at the firm hold any equity positions with the cited companies.

TAG's forecasts and forward-looking statements serve as directional indicators, not precise predictions of future events. Please exercise caution when considering these statements, as they are subject to risks and uncertainties that can affect actual results. Opinions in this book represent our current judgment on the document's publication date only. We have no obligation to revise or publicly update the document in response to new information or future events.