Enterprise Strategy Group | Getting to the bigger truth.™

ESG SHOWCASE

Zero-loss Strategy: A New Approach to Ransomware Protection

Date: August 2022 **Author:** Christophe Bertrand, Practice Director

ABSTRACT: Ransomware and cyber-attacks have become common and potentially costly occurrences for most organizations, forcing IT leaders and business executives to reconsider their data protection strategies and processes. A zero-loss strategy can help organizations plan, manage, and reduce the impact of ransomware.

Overview

Data is essential to the operations of nearly every business, and when data is corrupted or lost, the impact on operations can be devastating. Data loss can result from ransomware attacks, system failures, and other causes. Because any loss can be devastating, businesses are demanding that IT teams do everything they can to protect data and to ensure speedy resumption of business operations if data is ever lost.

Ransomware as a cause of data loss is particularly vexing, but the constant barrage of new and creative threats makes being breached nearly a given. The encryption of a company's data via ransomware can be a business-defining moment—some businesses survive relatively unscathed, but others are crippled. Often, it's the businesses that still rely heavily on legacy processes that have the most trouble because a great deal of work and resources must be devoted to identifying what data is impacted and recovering corrupted data. All of this can take days or weeks, with the disruption to the business continuing unabated. It's no wonder this issue has exceedingly high visibility among senior executives, which puts additional pressure on IT/SecOps teams to deploy an effective solution. According to ESG research, ransomware preparedness is the most important business priority for 26% of respondents and is among the top five business priorities for another 53%. Given the high levels of attention ransomware preparedness is receiving, 35% of businesses reported that they will significantly increase their spending on ransomware preparedness over the next 12 to 18 months.[1]

Such attacks are occurring constantly. According to ESG's research, 79% of organizations have experienced at least one attempted ransomware attack (successful or not) within the last 12 months. While ransomware occurs in the cyber world, its impact potentially can extend across all facets of IT operations, especially data protection. Being prepared is only a step in a series of organizational efforts and technology investments that lead to resilience.

But companies must recognize one important fact about ransomware: Ransom payments don't guarantee full data recovery. ESG research shows that 87% of organizations that have been victimized by a ransomware attack in the last 12 months failed to recover all their data after paying a ransom.

[1] Source: ESG Research Report, *The Long Road Ahead to Ransomware Preparedness*, June 2022. All ESG research references and charts in this showcase are from this research report unless otherwise noted.

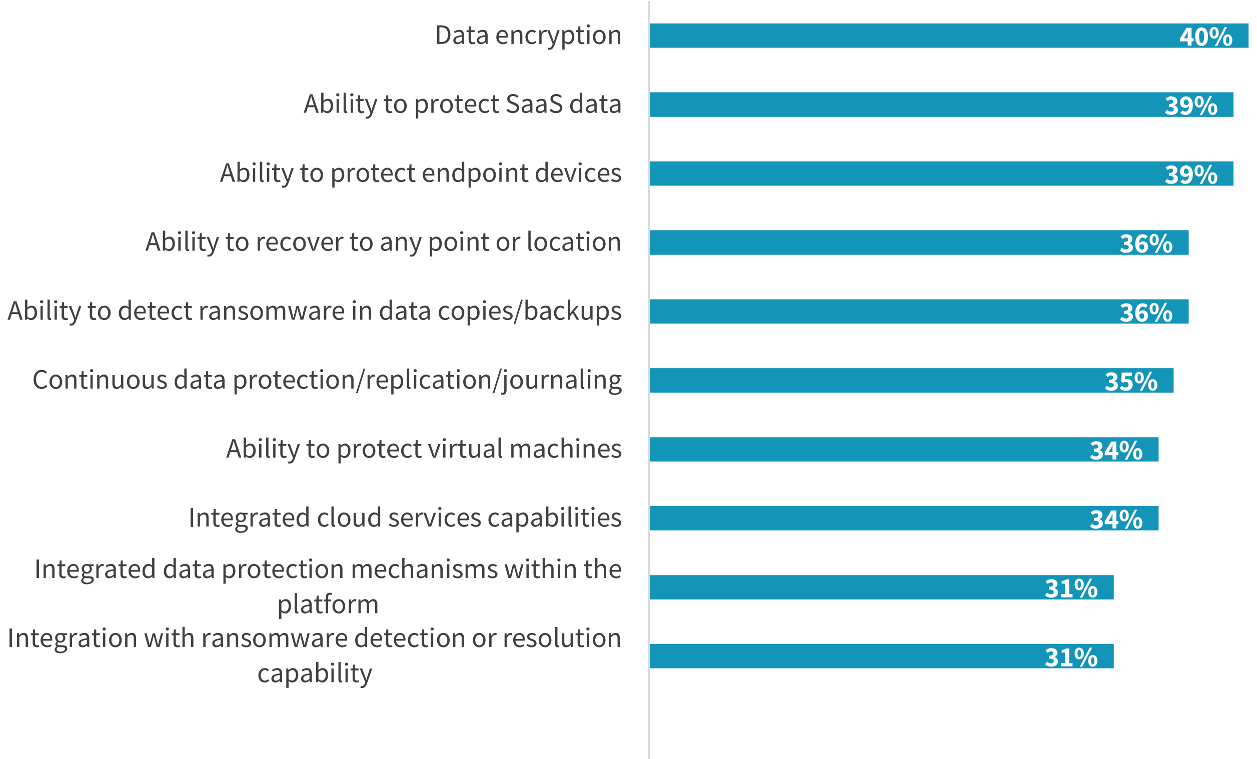
The bottom line is that management teams want an effective solution to mitigate any attack, protect data, and recover operations quickly. Upper management faces compliance demands for protecting data from regimes such as HIPAA and Sarbanes-Oxley, both of which have requirements to prepare a documented plan for protecting data.

Key Requirements from IT Professionals

Data protection and ransomware prevention are technical problems that come under the purview of the IT team. An ESG research survey asked respondents what capabilities part of a ransomware-recovery request for proposal should have. The strong demand for encryption that was reported is not surprising, but protection for SaaS data and protection for endpoints are capabilities that have emerged recently. Yet, the most important finding is that the top eight features are separated by just six percentage points. In other words, all the capabilities matter.

Figure 1. Ransomware Recovery

If your organization were to be the victim of a successful ransomware attack, what is its planned method of recovery for the impacted applications and data? (Percent of respondents, N=620, multiple responses accepted)



Source: ESG, a division of TechTarget, Inc.

Zero-loss Strategy: Meeting the Challenge of Ransomware Attacks

A new approach to ransomware and data protection, the zero-loss strategy, is well suited to current and future needs. A zero-loss strategy provides a comprehensive solution and is implemented using a multilayered security framework, helping to mitigate the impact of ransomware and ensure data integrity. It also minimizes operational complexity and brings certainty to recovery.

Ransomware puts a tremendous amount of pressure on organizations. They must remain vigilant and on top of their game. A zero-loss strategy helps them continuously plan, identify, and monitor data across any workload, with a faster response time and flexible restore options. One important new element of this approach is that it combines attack identification and remediation while ensuring data protection.

Zero loss uses a comprehensive approach with several layers of capabilities that all work together to provide more protection than individual solutions and that are focused on only one aspect of the problem. The concept is designed to protect against the entire ransomware lifecycle. With a cohesive process, it is now possible to simplify and speed up recovery in the event of any successful incursion. This “time to resuming operations” is the real measure of how valuable a ransomware-protection solution is. The only thing the business cares about is getting back to normal operations.

The Characteristics of a Modern Zero-loss Strategy for Data Protection

Zero loss demands an underlying technology platform that has the comprehensive functionality necessary to support it. Simply rebranding legacy data protection solutions does not solve the problem or deliver the key benefits.

The starting point is the combination of modern management and protection capabilities, with a focus on management functionality. The foundation for zero loss is visibility of all the data that needs protection across the IT estate. Comprehensive visibility lets SecOps/IT teams identify any malicious or potentially malicious activities in both production data and backups. With this broad visibility, the system will deliver key information from reporting/management tools that quickly identify and alert to any potential incursions or issues. To ensure protection, constant monitoring of data—both live and backups—is required to ensure any ransomware infection doesn’t get a head start.

To enable zero loss, it is essential to have coverage for all workloads and to eliminate gaps in data protection and monitoring. This visibility must work across SaaS, cloud-native, and on-premises infrastructure with consistent management tools and reporting to enable the IT or SecOps team to respond at speed. This includes the ability to support cloud integration. A scalable, single management console provides ops teams with one complete and comprehensive source to simplify their work and speed response.

However, the most important functionality is the ability to get the business back to the state of operations that existed before the event. The new platform must make the recovery process seamless and faster. “Speed to normal” is the most important metric and must permeate the solution. Recovery requires the ability to isolate any files that might be corrupt at a very granular level and stop them from spreading corruption to production or backup data. This process must be automated where possible and use intelligence to reduce the time necessary to regain operational stability. The solution must support the ability to restore to any target, as, during an event, some infrastructure may be compromised or unavailable, making “restore to anywhere” an essential capability.

To enable the zero-loss strategy, the solution must leverage the zero trust security framework to increase protection and defense. This includes continual credentials verification even inside the firewall to stop lateral spread and cross-workload corruption. It is essential to leverage the integration of data protection/monitoring solutions with other security tools to provide a layered defense and reduce vulnerabilities. This new approach integrates and coordinates disparate tools/solutions for security to provide defense in depth and leverage capabilities found in different options. This eliminates gaps in reporting and visibility that may give an attacker a head start.

Zero loss provides better protection and lowers the impact of any successful attack, minimizing the impact on the business. Recovery is the single most important objective. A modern zero-loss solution will reduce the time necessary to recover and ensure that the data used for recovery is not corrupt. Improving defenses is mandatory. Businesses must constantly improve defenses as attackers innovate and change their tactics. Zero loss is a framework that does just that. Defenders need a framework that is agile and can respond to new threat types, a strength of zero trust.

The data-protection strategy cannot limit agility or force infrastructure decisions onto the business. With the ability to protect more data and workloads (cloud, SaaS, etc.) across the infrastructure, the business retains the agility to use the most appropriate infrastructure for the workload.

Another important business benefit is that the zero-loss approach improves integration and collaboration among the different groups that are involved in protecting corporate data. With a zero-loss approach, a common set of metrics and operating approaches serves as the foundation for effective teamwork among all the groups involved in data protection and security.

Commvault Delivers an Optimal Zero-loss Strategy Solution to Protect Businesses Against Ransomware

The innovative zero-loss strategy approach from Commvault is designed to meet current and future challenges that organizations face. A zero-loss strategy provides a comprehensive solution and is implemented through a multilayered security framework, helping to mitigate the impact of ransomware. It provides the benefits organizations need.

Commvault's platform easily delivers this new strategy by providing several compelling capabilities that support better data protection and, more importantly, rapid recovery. The starting point is broad visibility to ensure that important data is actively managed and protected. This monitoring enables the identification of any abnormal activity, generally a strong indication of a ransomware event. The solution uses a single console for protecting data and workloads that are running on different infrastructure instances—IT/SecOps teams need only one management tool across the IT estate. With improved visibility, it is possible to clearly understand both the time of the event and what files may have been impacted. With this information, it is simpler to identify the last known good backup. The Commvault solution does not overwrite data, making recovery from backups simpler. This information also makes it possible to quickly identify files/datasets that may have been compromised.

Commvault also provides very broad workload protection. This service can be used across legacy workloads, cloud, and SaaS services, with native cloud integration. And it has the agility to restore to any infrastructure, providing more options to IT for returning to normal operations quickly.

Of the many features and capabilities, possibly the most important is fast and accurate recovery. It starts with a single console to manage the entire process, using the intelligence of when the attack occurred, ensuring only a clean backup is used. The recovery process is highly automated to reduce the time needed to get up and running. The automated tools also delete any files that are suspected of being infected. Further, Commvault provides on-call services that both ensure a successful ransomware protection and design plan and offer support during an event if the technical teams need additional bandwidth or expertise.

Finally, this solution reduces operational complexity. The service itself is aligned with zero trust principles, making it intuitive for IT professionals. As mentioned above, the single console used across the IT estate simplifies daily operations. In addition, the integration with key enterprise platforms such as ServiceNow, Splunk, and CyberArc make it much easier to leverage the Commvault solution.

The Bigger Truth

Data loss from ransomware attacks has the potential to disrupt business operations and has caused some firms to go out of business. Losing data makes it very difficult to get back to business as usual. For this reason, Commvault is now delivering an enhanced data loss protection strategy that is built on the concept of zero loss. With more capable technology and new features, businesses can move past a ransomware attack with reduced risk to their data and with faster resumption of normal operations.

The Commvault offering provides a single console for protecting and recovering data from all workloads. This reduces operational complexity and simplifies the process, making accurate backups simpler to create. The most important benefit of Commvault's solution is that, in the event of a successful attack, an organization can recover quickly and go back to business as usual.

Determine how prepared your organization is for a ransomware attack. Take the Commvault risk assessment to find out: https://www.commvault.com/ransomware/risk-assessment.

All product names, logos, brands, and trademarks are the property of their respective owners. Information contained in this publication has been obtained by sources TechTarget, Inc. considers to be reliable but is not warranted by TechTarget, Inc. This publication may contain opinions of TechTarget, Inc., which are subject to change. This publication may include forecasts, projections, and other predictive statements that represent TechTarget, Inc.'s assumptions and expectations in light of currently available information. These forecasts are based on industry trends and involve variables and uncertainties. Consequently, TechTarget, Inc. makes no warranty as to the accuracy of specific forecasts, projections or predictive statements contained herein.

a division of TechTarget

Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm that provides market intelligence, actionable insight, and go-to-market content services to the global IT community.

www.esg-global.com contact@esg-global.com 508.482.0188