COMMVAULT

WHITEPAPER

# Data protection and recovery: A foundation to a cyber readiness plan

By: Brian Brockway, Global CTO, Commvault

## Overview

The recent headlines on ransomware have been extraordinary – from Colonial Pipeline, to Honeywell, to the recent attack on Kaseya. The economic impacts of these emerging threats are now impacting business on the order of billions of dollars. We want to deep dive into these ever more sophisticated attacks with some specific and more technical recommendations on how to best position your organization to respond to malware attacks.

Our economy's fundamental dependence on the "network" and the ongoing digital transformation has driven the enormous efficiencies and effectiveness over the past three decades. However, our speed to embrace the digital transformation to gain these advantages was often done with little regard for warnings from our security and risk management teams have generated many vulnerabilities. Greater security integration is often overlooked to maintain a competitive advantage in the face of the constant wave of new startups and disruptive "never-seen-before" new business processes – think Uber or AirBnB. This race to maintain competitive advantages often creates vulnerabilities that ransomware and malware attacks target. Our new digital ecosystem demands a fundamentally new approach in terms of cybersecurity that synchronizes protecting the underlying information management systems and data that is now the lifeblood of our new economy.

The goals of a malware attack can be notably different for Federal agencies than for commercial companies. The attack on Federal agencies more often aims at embedding malware to extract data over an extended period of time. The best example of such an attack was the Office of Personnel Management (OPM) event where large amounts of data on the Federal and DoD workforce were extracted to gain an intelligence advantage. However, while the objective goals may be different – ransom versus the methods of the attacks are similar – the ransomware attacks are a subset of the malware attacks in general. What is important to remember is that both are attacking data stores.

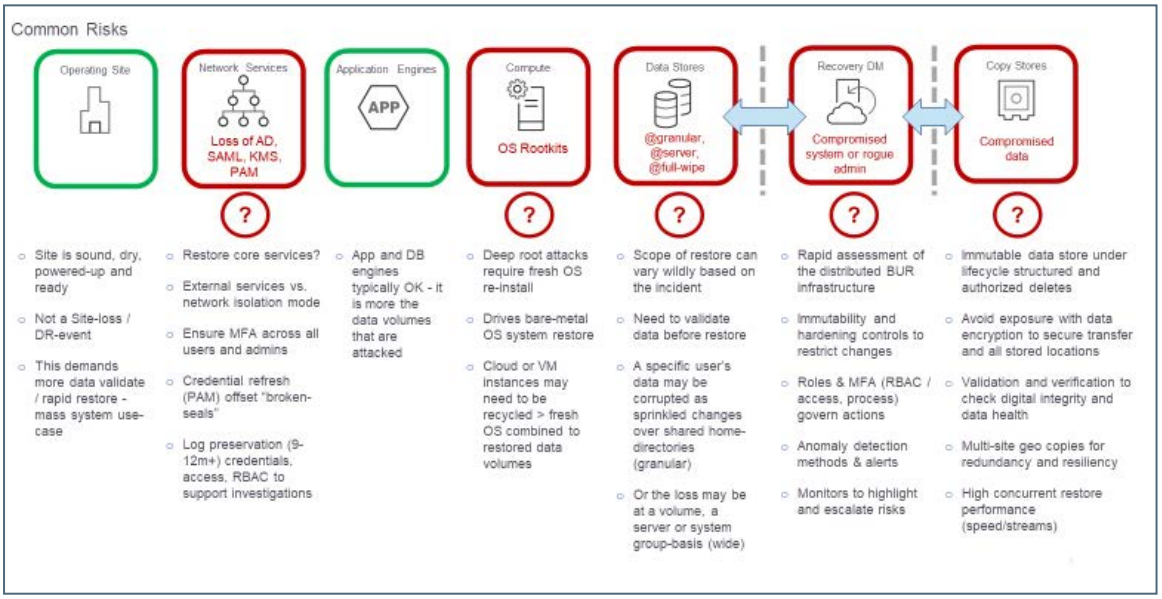
These attacks continue to take advantage of security gaps in core IT operations, and a cyber risk profile drives the need for a comprehensive approach to intelligent data management differently from just a Disaster Recovery strategy. Using a cyber risk profile helps identify key vulnerabilities, but it also helps prioritize and focus on the key operational systems that require the greatest protection and also the highest priority for restoral.

**To organize the discussion, we look at the following key points:**

- Securing the data stores at the foundation (immutable copies, air-gaps, MFA, RBAC)
- Automated detection with anomaly intelligence
- Preparing for the worst - planning and automating for a cyber recovery site

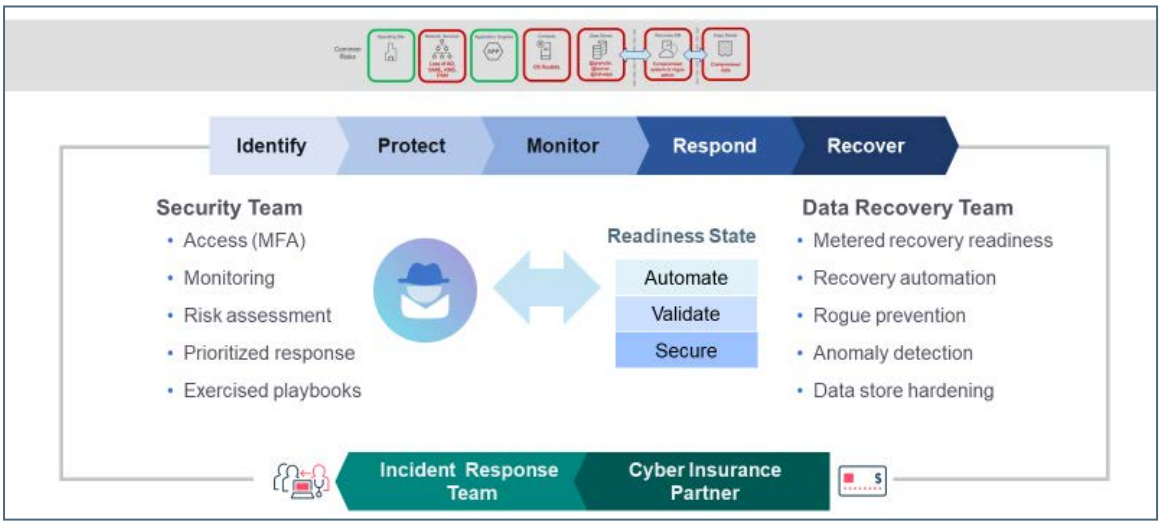
The diagram below shows the key risk areas for creating a cyber risk profile. The green areas are often where most organizational efforts are focused, while the areas in red are often overlooked as part of a complete assessment. Under each of these categories is a list of key impacts that should be addressed from having key procedures in place when an attack is underway.

**The 'data' cyber risk profile is different from traditional DR case**




Our previous articles (Be Ready - Cybersecurity in today's digital ecosystem and Are you ready? Intelligent Data Management as a foundation to operational readiness) presented the NIST model for cyber readiness and here is a diagram that better illustrates the approach to have a proactive plan. The diagram not only highlights the key aspects of the NIST guidelines of Identify, Protect, Monitor, Respond, and Recover, but extends that framework to delineate the different role and focus for the IT security team versus the data recovery team and their tasks to ensure a holistic plan.

**Cyber security demands a proactive protection and response plan**

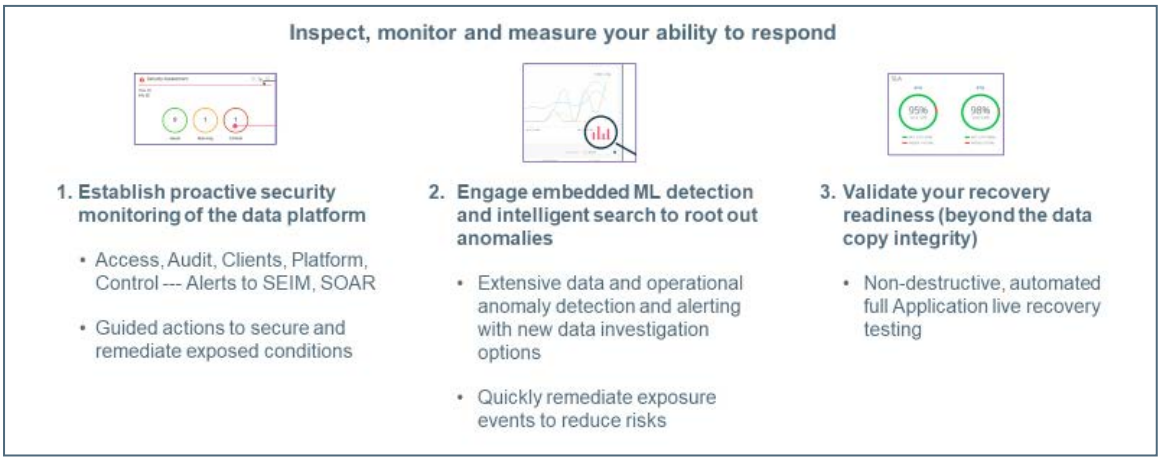



Notice also that features of automation, validation and secure management of the recovery process must not only be planned but also exercised for managing the data recovery process. For automation, the goal is to reduce downtime and impact business operations and align resources to respond to an incident. Location of key data stores for recovery should be known and how to reach them when the network is potentially in a degraded state. Before recovery procedures can begin, it is critical first to evaluate and 'Validate' the data with an eye for anomalies, alerts, and determine if the action is to isolate potential malware and then further evaluate for removal. The goal is to ensure that the recovery process does not reintroduce

the malware. The 'Secure' foundation begins at the data protection architecture (policy, controls, copy, stores) deployed with zero-trust and immutability principles to fortify the data environment against a broad spectrum of threats and risks. For both IT security and the data recovery team, the alerts to an attack must also include an assessment of where the attack has originated to ensure that the insider threat – a credentialed user that is creating the exploit - can also be identified.

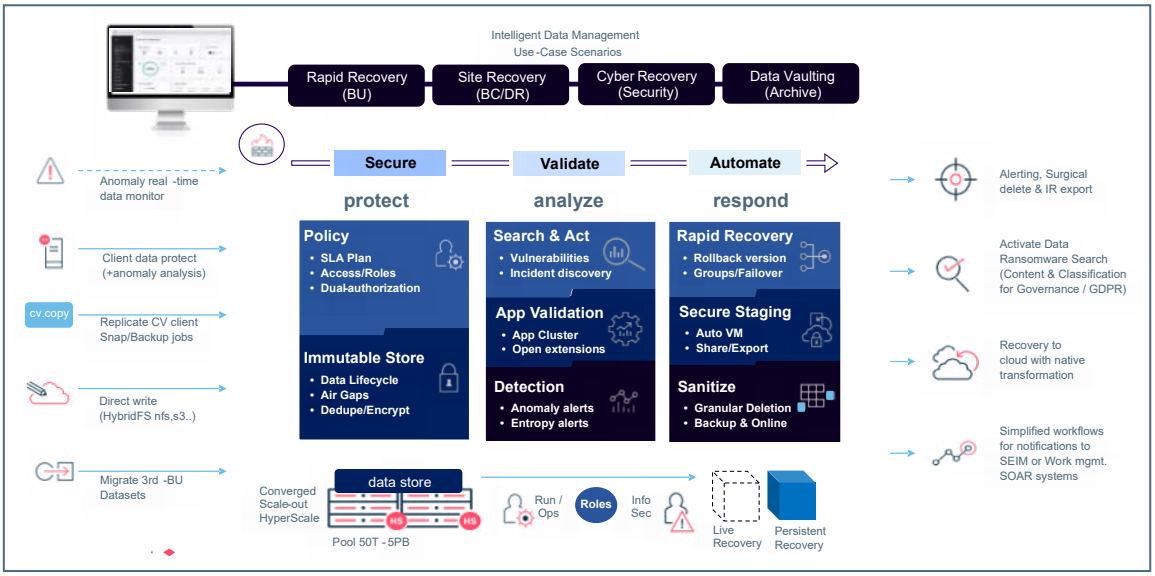
Throughout this cyber risk assessment process from the perspective of protecting an organization's key data, there should be an effort to create metrics to measure your readiness state. The data administration team should constantly be evaluating the alerts and performance statistics of the backup and recovery system to identify incidents and ways to embed machine learning (ML) that can create response rules from automated alerts to prevent an attack from escalating. An easy-to-use dashboard is critical to an effective monitoring capability. Lastly, continual data testing, audits of data validating recovery procedures are critical readiness elements.

### Validate and continuously measure your readiness level




Below is an operational view of a cyber data readiness solution as an example that synthesizes a holistic operational view on one page the key elements that we have outlined above and throughout our articles on maintaining readiness and recovering after a malware or a ransomware attack. It represents integrating a key intelligent data management platform as central to implementing a successful solution.

### Data protection and recovery: A foundation to a cyber readiness plan




By having this operational view as your guide, you will effectively guide your organization to a comprehensive Cyber Data Readiness solution and be ready for the "when" and not "if" scenario and be able to sleep comfortably at night.

## About Commvault

Commvault liberates business and IT professionals to do amazing things with their data by ensuring the fundamental integrity of their business. Its industry-leading Intelligent Data Services platform empowers these professionals to store, protect, optimize, and use their data, wherever it lives. Delivering the ultimate in simplicity and flexibility to customers, its Intelligent Data Services platform is available as a software subscription; integrated appliance; partner-managed, and software-as-a-service — a critical differentiator in the market. For 25 years, more than 100,000 organizations have relied on Commvault, and today, every quarter, Metallic is adding customers who leverage it to modernize their environments as they look to SaaS for the future.

To learn more, visit commvault.com/ransomware >