COMMVAULT

WHITEPAPER

Be Ready — Cybersecurity issues in today's digital ecosystem

In a recent article, we focused on the critical need for intelligent data management to improve organizational effectiveness, efficiency, and operational readiness. Let's expand that conversation and help organizations and leaders build an intuitive context around critical cybersecurity issues in today's digital ecosystem. We're using the word 'ecosystem' as the data environment has many of the same traits of how we describe our natural world of living things. Whatever solutions your organization looks to implement, they must respond to the ever-changing digital landscape.

Are you tracking all the new guidance on cyber coming from the Executive Branch and Department of Defense (DoD) models?

- President Biden's Executive Order on Improving the Nation's Cybersecurity
- Cybersecurity Maturity Model Certification
- NSA issues guidance on zero trust security model

The recent large-scale attacks on industry leaders like SolarWinds and the attacks on Honeywell and the Colonial Pipeline continue to raise concerns and generate new focus and new programs to respond to these cybersecurity threats.

We thought a quick cyber guide to how the landscape is changing and that provides further insight into how to best prepare your organization to respond would be of great value to you and your organization.

Understanding the nature of cyber attacks and where the most significant vulnerabilities lay is the priority. All organizations build their capabilities around People, Processes, and Technology to deliver their goods and services, and each of these aspects is vulnerable to cyber attack.

People

As with many new technologies, it isn't always the flawed automation, but often how we as individuals bring less than optimal behavior to using that new technology – think Cyber Hygiene. As an easy-to-understand analogy, think about car safety technology and the individual. First, there was the enormous resistance to safety belts, but then even when implemented, the next most challenging step was to get individuals to use them as a normal practice. We alarmed the car, we made them work automatically, and then the industry moved to airbags where the individual is out of the safety cycle. And the next step to that is self-driving cars. The point of this analogy is that humans often take shortcuts that undermine the safety or security features that have been set up in systems.

At the administrator level, the number of behaviors that leave backdoors in place or keep access up and running for days at a time rather than shutting them down at the end of the day are additional examples. Trivial passwords are another example. Automation is being brought to bear to prevent simplistic passwords forcing more difficult ones and reducing 'lazy' behaviors by automatically ending sessions after so much time of inactivity. And in response, the hackers and adversaries of the world have begun even more sophisticated attacks for which additional measures must be taken.

What is the key lesson learned for organizations? Security must be integrated from the outset and must be implemented with the understanding that individuals will often view these added security features as a burden. How to do that – lots of focus on training for sure, but business leaders should be pressing their IT and security subject matter experts to research better solutions from the outset. They should encourage the IT staff to spend time in the operations of the people that they support to understand their challenges and look for solutions that minimize extraneous procedures. To be most effective individuals must be included at the outset to develop buy-in.

Process

As summarized by the National Institute of Standards and Technology (NIST), Zero Trust is an "evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources."

Said more blatantly, Zero Trust means "Trust Nothing, Verify Everything" according to a recent article in Forbes.

- **Offers identity management suitable for complicated IT ecosystems.** A Zero Trust model moves organizations away from a binary access system — access granted or denied — to a system of authenticating and granting access based on a number of identity variables. This process includes verifying that the user is who they claim to be and that, in real-time, they have the correct permissions to access what they're trying to access and work on secure devices and networks.
- **Provides conditional access.** Conditional access based on Zero Trust allows for security to be tightened or relaxed according to each team, department, or organization's unique needs. By assuming least privileged access, the Zero Trust model can deliver robust security that's both automatic and adaptive.
- **Automatically integrates multifactor authentication (MFA)**. Augmenting conditional access is the automated integration of multifactor authentication (MFA), allowing for a robust and holistic virtual identity reconciliation rather than static username and password.

The same is occurring as we transform our world digitally. The speed of moving data is at the speed of light. When attacks occur in our digital world, they occur at that speed and the attacks are now no longer just one physical target, instead targeting a vast array of IT infrastructure simultaneously.

Technology

The cyber threat landscape including ransomware, has transitioned to a case of when, not if. To ensure you can recover your data and not pay the ransom, you need to trust that your data protection vendor shares your level of vigilance. The right solution requires the best technology, the right people, and processes.

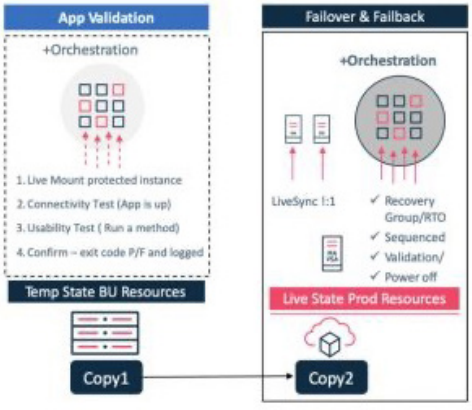
Recovery readiness is a key strategic goal for Commvault. Organizations require tools to constantly measure their recovery readiness state so they can expose and remediate problems, validate the recoverability of their data and business applications through automated testing, and continually harden their environment to improve their security and reduce their risk profile.

Cybersecurity recommendations

Commvault knows that when it comes to data security, it is paramount to have a multi-layer security strategy and keep in mind that recovery readiness is key. This includes ensuring that your mission-critical data can withstand a targeted attack designed to destroy primary and backup copies of your data, and that complexity has been removed with a recovery that is as automated and orchestrated as possible.

Any plan you develop must work broadly and deeply enough to reach valuable data wherever it resides. Your plan should extend beyond central servers and organization-wide applications to cover laptops, files in a wide range of media formats and function-specific applications.

Recovery readiness



Recovery readiness means that recovery stages are documented, automated, and predictable. Commvault capabilities to support recovery readiness include:

- **Highly available data protection architecture** – Commvault architecture can be protected using Live Sync replication of the database to one or more standby nodes. The database can be protected natively in any public cloud and is a free protection service offered by Commvault.
- **Recovery orchestration** – the Commvault control plane manages, operates, and maintains records for all managed data. It can be fully recovered with a single click, which can be tested ahead of time by a fully orchestrated test failover to provide restore validation without disrupting production.
- **Data integrity validation** – Commvault provides multiple methods of data integrity validation. Data signatures are used to confirm the integrity of any data transferred, received, and written to storage media. In addition, automated tasks for regularly validating the data on storage are provided.
- **Application recoverability validation** – a fully orchestrated application recovery validation task can 1) provide access directly to the data protection copy from the backup infrastructure, 2) start the application, and 3) connect and run a test method to validate both the data and application recoverability.
- **Easily identify data to recover** – data can be searched across any time period, and options include show/hide deleted items, latest, specific point in time and time range. These options provide a simple way to select the correct data to recover.

Backup target immutability

Ensuring backup copies are immutable and cannot be altered or encrypted by ransomware is critical. It must be cost-effective for all data within your environment and can be turned on for the storage of your choice: on-premises or in the cloud solutions. The backup store immutability feature employs proven methods to restrict write and delete operations, which prevent bad actors or malware from modifying files in the protected path.

With a multi-layer strategy recommendation, some customers choose to implement additional strategies for greater protection. For specific data, organizations may utilize write once, read many (WORM) copies on premises or in the cloud, and implement air gap isolation strategies. These are simple to implement in Commvault solutions through policies, including network segmentation, encrypted network topologies, gateways, and firewalls. Also, our products support automation to orchestrate network and server disconnection.

Foundational hardening

The principal of foundational hardening is important for all software environments. The core components of the Commvault solution rely on the underlying operating system, database, application, and web server technology. Therefore, all security vulnerabilities within the underlying technologies need to be closed so that they do not become entry points for cyber threats.

- Apply hardening recommendations – Automatic enablement of hardening recommendations based on National Institute of Standards and Technology (NIST) Standards.
- Binary signing including third party – A Commvault framework to digitally sign binaries and ensure they have not been modified by a malicious actor. Any third-party libraries are updated regularly and in response to reported vulnerabilities.
- CIS Level 1 hardening – Commvault software has been tested and confirmed as capable of Center for Internet Security (CIS) Level 1 hardening.

Application hardening with authentication, authorization, and accounting

AAA security framework for controlling access

Authentication	Authorization	Accounting
Proving and granting access	Control what level of access is required	Tracking and auditing access and capabilities

Authentication

The process of authentication is based on each user having a unique set of criteria for gaining access. Commvault enables multifactor authentication methods to make it highly unlikely that a valid user account can be impersonated.

- Secure Lightweight Directory Access Protocol (LDAP) – supports Activate Directory and generic LDAP identity servers.
- External identity providers – are supported using secure protocols such as OAuth and SAML.
- Two-factor authentication – with logins using authenticator application.
- Certification authentication – for Commvault infrastructure to protect against spoofing.
- Credential manager – a secure container for account credentials for shared resources in the environment.

Authorization

Following authentication, authorization must be granted to the user to allow certain tasks. Commvault provides a rich and complete set of capabilities. Here's a sampling of the capabilities:

- Role-based security – manage capabilities by assigned roles to users and groups, including support for multi-tenant environments, and limited in function and scope of servers, applications, and data sets that can be accessed and managed.
- Authorization approval workflow – supporting the four-eyes principle for administrative tasks such as deleting data sets, clients, restores, targets, jobs, and policies.
- Passkey and privacy lock – supporting the principle that administrators manage the data but should not be able to view or restore the data they do not own. Used together, only the owner of the dataset at the individual, department, or company level can restore data with the required passkey.
- Data encryption – Federal Information Processing Standards (FIPS) certified encryption, 6-plus ciphers including AES 256, to encrypt data from the first touch and throughout the full data management lifecycle.
- Encryption key management – use a built-in Key Management System (KMS) or use an external system including Key Management Interoperability Protocol (KMIP), including AWS KMS, Azure Key Vault, and passphrase KMS support.

Whitepaper: Secure your data, your recovery and your mission. **Read >**

Accounting

Lastly, Commvault enforces accountability by auditing events and actions within the CommCell and providing a rich customizable interface to view this information. Hundreds of reports are readily available in the Commvault software store providing deep information on the operations, events, and actions of the CommCell. Information within reports and dashboards are only visible to users who have been given access. This allows owners to view the same audit reports and dashboards as Administrators without seeing resources they do not have permission to see.

Data isolation and air gap

The "Air Gap" control concept is a data protection architecture that limits exposure to an attack and allows for the restoration of data to a point-in-time before the attack began. Commvault can effectively address the risk of encrypted data being replicated in the data backup architecture with immutable backup targets, periodically applying a write once, read many (WORM) security policy to data copies and removing deletion capability until the retention policy is met. Commvault has improved upon physical access controls, enhanced security, simplified the process, and reduced cost. To learn more about air gap concepts, click here to read more.

Monitoring and detection

It is recommended by many experts to have a layered anti-malware and ransomware strategy. Commvault has built these capabilities into existing security software and policies for greater benefits and without incremental management overhead.

- **Monitor file system activity** – utilizes historical data and a machine-learning algorithms to detect statistically variant file system behavior.
- **Monitor honeypot files** – hidden files common and attractive to ransomware attacks are monitored for signature changes.
- **Certificate authentication lockdown** – when certification lockdown is enabled, clients cannot be added to the data protection architecture without additional administrative steps and privileges.
- **Actionable alerting** – automatically act and alert for awareness or embed a recommended action workflow into the alert for administrator execution.

Simplifying recovery readiness

True peace of mind comes from having a comprehensive, continuous recovery readiness plan. The last thing you want to do when contending with a high-pressure attack is to stop to figure out which data needs to be recovered in what order.

Recovery readiness means that recovery stages are documented, automated, and predictable.

The risks and rewards of defending cyberattacks are significant to your organization. Done poorly, it results in lost data, mission compromise, and lost credibility. Done correctly, it can lead to operations being successfully restored in a timely manner and greater recognition for a job well done. The choice is yours, the choice is simple. Be ready! And enjoy some peace of mind!

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. Driven by its values—Connect, Inspire, Care, and Deliver—Commvault (NASDAQ: CVLT) employs more than 2,700 highly-skilled individuals around the world.