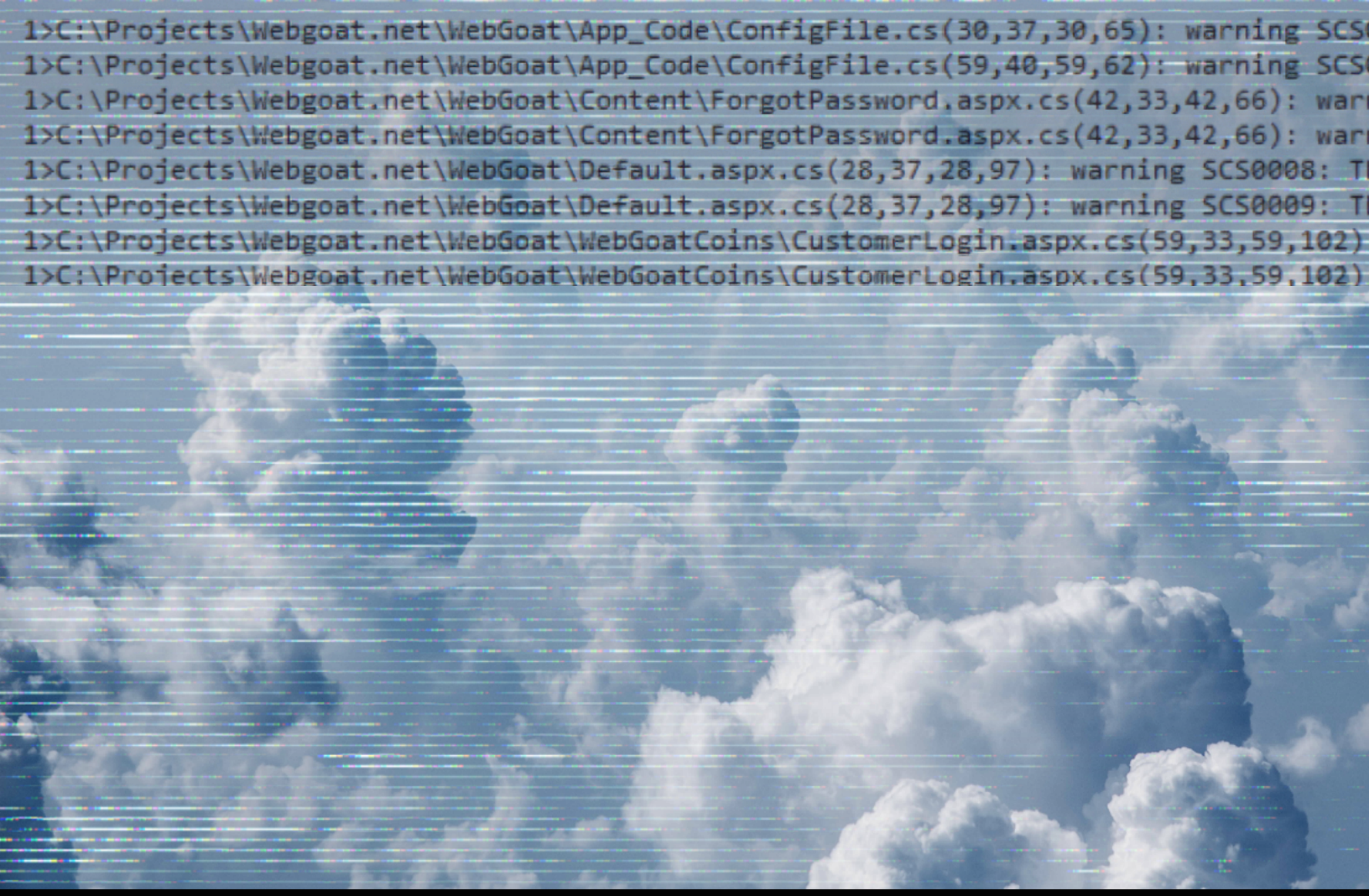


Guide

Commvault®

The Ransomware Solution Your CISO Will Love

THE NEW THREAT LANDSCAPE

In today's ever-evolving threat landscape, cyber attacks have become more widespread and costly than ever. For security and technology leaders, developing a robust strategy for cyber resilience and recovery is not just essential, it's a matter of urgency. Breaches **will** happen. Do you have the means and resources to detect a breach—and a plan for how you'll respond?

You might be relying on traditional data security solutions that use a patchwork of poorly integrated security solutions. In that case, your security teams will be at a disadvantage out of the gate as they try to see the full scope of the attack.

And any lack of collaboration between IT and security during an incident will cause your organization to fall even further behind an adversary that's moving fast.

The price for a poorly implemented response plan is a lot of expensive downtime, compliance fines, security breaches, and, ultimately, damage to your organization's reputation.

$365K

is the cost of downtime each hour.[1]

CHAOS DEMANDS A UNIFIED APPROACH

Unfortunately, the chaos and hours of work that follow a security breach can make it difficult to decide who should respond and how. There's no time for internal conflict. Security and IT teams must work hand-in-hand, strategically and tactically. This collaboration is vital for efficient and effective risk management.

Yet only 30% of SecOps teams fully understand the role of ITOps.

And only 29% of ITOps teams fully understand SecOps.[2]

Cyber resilience can serve as the bridge between IT and Security, enhancing your organization's overall security posture. Security and technology leaders must equip their teams with the right tools and strategies to mitigate risks and protect data and reputation. These tools need to be integrated to provide context and a comprehensive understanding of attacks, incidents or breaches.

61%

of CISOs agree that their organization is unprepared to cope with a targeted cyber attack.[3]

Start building a more cyber-resilient organization today by bridging the gap between ITOps and SecOps. Be prepared for any threat, including ransomware, with a unified solution that offers early warnings, continuous recovery readiness, and self-scaling cyber recovery. Take an approach that safeguards data across your entire hybrid cloud infrastructure and makes recovery in both cloud and on-premises environments easier.

Of course, ransomware is always a symptom of a larger breach, and it's shortsighted to address only the ransomware delivery mechanism without addressing the underlying problems of securing the breach and eradicating the attacker's access. The fact is that 80% of companies experiencing a ransomware attack had second or third attacks. Are you prepared?

1 Splunk, "**Digital Resilience Pays Off Report**," February 2023.
2 IDC, "**The Cyber-Resilient Organization: Maximum Preparedness with Bulletproof Recovery**," September 2023.
3 Proofpoint, "**2023 Voice of the CISO Report**" May 2023.

EVERYONE'S IN IT TOGETHER

While the goal of everyone involved in cyber resilience is to protect the business from harm, IT and SecOps can go about it in different ways that may leave potential exposure to outside threats. The key is to establish common ground. Here are a few examples:

1. **Shared goals**: Both IT and security teams aim to protect the organization's assets, systems, and data. They work towards maintaining the confidentiality, integrity, and availability of information.

2. **Collaboration**: IT and security teams often collaborate closely to implement and maintain security measures. They work together to identify vulnerabilities, implement security controls, and respond to incidents.

3. **Risk management**: Both teams are involved in assessing and managing risks. IT teams focus on operational risks related to system availability and performance, while security teams focus on mitigating risks associated with unauthorized access, data breaches, and other security incidents.

4. **Compliance**: IT and security teams work together to ensure compliance with relevant regulations and standards. They collaborate to implement controls and processes that meet legal and industry requirements.

5. **Incident response**: In the event of a security incident, IT and security teams collaborate to investigate, contain, and remediate the issue. They work together to minimize the impact and restore normal operations.

6. **Awareness and training**: Both teams play a role in promoting security awareness and providing training to employees. IT teams educate users on safe computing practices, while security teams provide guidance on identifying and reporting potential security threats.

7. **Stress testing**: A team that trains together builds bonds and achieves more. Stress testing your plans, policies, and ability to interact finds areas for potential improvement. Better to have it all worked out under ideal conditions, without the stress of an attack.

Overall, effective collaboration and communication between IT and security teams are crucial for maintaining a secure and resilient IT infrastructure.

ATTACKS HAPPEN. ENSURE YOUR SECURITY AND IT TEAMS ARE READY.

C-level security and IT executives need advanced data security capabilities to address cyber risks effectively, minimize threats, and enhance recovery outcomes.

Remember, it is not a matter of **IF** you have a breach but **WHEN** you **DETECT** the breach, **WHAT** you did to prepare, and **HOW** you respond to the breach.

Starting the Conversation

To spur better collaboration and find common ground here are some questions to consider:

- How well-prepared is your organization to respond to cyber threats and ensure business continuity in the event of an incident?
- What are the critical assets and what is the expected business down time?
- What are the assumptions made on being available – has the exercise taken into account, AD outage, Vmware outage, cloud region outage?
- Do your teams understand their roles and responsibilities during an attack?
- Who has access and visibility to what? Do you have out of band conversation mechanisms?
- How do you secure and manage data as you adopt hybrid cloud environments?
- What would it cost the business and reputation if there was a breach and ransomware to follow?

COMMVAULT CLOUD: CYBER RESILIENCE FOR THE HYBRID WORLD

Having the right technology to serve those common goals is also a must. Commvault Cloud®, powered by Metallic AI, is the only cyber resilience platform built to meet the demands of the hybrid enterprise and equip SecOps and ITOps teams with the data security and recovery capabilities they need in the face of evolving AI-driven threats.

In the ever-expanding and ultra-complex hybrid world, there are inherent risks to solve, mitigate, and accept. Can you quickly identify assets created with little or no warning? Are you aware of software, hardware, and external services that could expose your data to cyber threats? All of this forces CISOs to make tough choices on how to prioritize and align finite resources, ever-expanding risks and business needs most effectively.

For many reasons, organizations are looking for single-vendor solutions. Regulations, compliance, and policy have all pushed organizations to want to know more about the cybersecurity that a service provider is delivering in their respective place. IT and security leaders ask vendors for details about their pen testing, software development lifecycle (SDLC), software bill of materials (SBOM), and other documentation to prove they won't inherit a vendor's poor cybersecurity.

Commvault Cloud is purpose-built to protect, monitor, report, manage, and recover data from any workload — from any location — all from a **single pane of glass**. Eliminating the need to pay extra for bolt-on tools that ultimately create gaps and vulnerabilities. Powered by an engine with always-on AI, Commvault Cloud offers a unified platform that protects all your workloads against evolving threats, while ensuring a rapid, and, most importantly, clean recovery.

83%

of organizations believe consolidating systems to a single vendor would be desirable.[4]

5x Lower TCO

Commvault boasts 5x lower TCO compared to other cloud-native protection tools.[5]

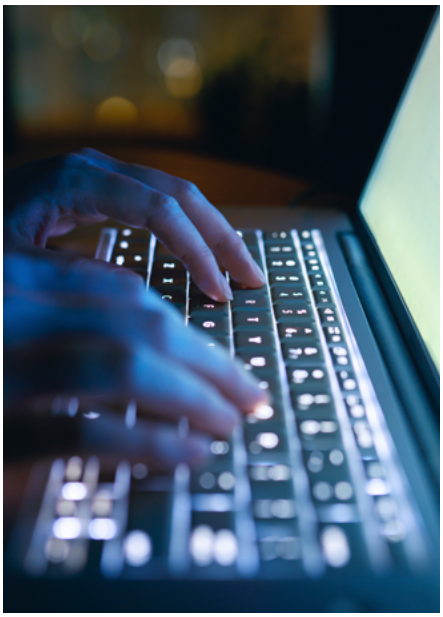
4 Forta, Digital Guardian Data Protection, "**Top Considerations for CISOs When Consolidating Information Security Solutions**," April 2023.
5 Commvault customer TCO analysis.

Advanced AI, Enabling Next-Gen Capabilities

As a C-level executive responsible for your organization's data security, you need to fight fire with fire. Today's AI-driven threats require you to move fast, begin data security measures sooner, and be ready to recover at scale.

"Speed of detection is clearly key to mitigating intrusion impact, and detection, in particular, requires automation to be effective. However, most organizations are still on the journey to fully automated detection and reporting[2]."
IDC: *The Cyber-resilient Organization: Maximum Preparedness with Bullet-proof Recovery*

Commvault Cloud, powered by Metallic AI, uses artificial intelligence, machine learning (ML), and automation to deliver the industry's most advanced data protection intelligence. It predicts threats faster, ensures cleaner recoveries, and accelerates response times.



Innovative Platform Services

Commvault Cloud platform empowers SecOps and IT teams to manage processes more efficiently and cost-effectively.

We have revolutionized data security and cyber recovery by providing a layered defense delivered through a simple, unified, SaaS-like experience. Our proven capabilities are delivered through our Platform Services, which provide everything from early warning to rapid recovery of all your data, any workload, anywhere.

92%

of organizations plan to use AI and machine learning to bolster their cybersecurity.[6]

Early Warning	Risk Governance
Detect threats faster, minimize the blast radius, and lower your risk exposure.	Improve your data security posture by proactively locating and remediating risks across production and backup data.
Readiness & Response	**Cyber Recovery**
Ensure resilience with advanced preparedness, automated validation, and continual recovery testing.	Ensure rapid recovery, with the flexibility to recover from anywhere to anywhere — at scale.

6 Synchro Works Consulting, "**The Value of Danger of AI in Cybersecurity**," August 2023.

Commvault delivers the right breadth of detection, security, and recovery capabilities to reduce risk, minimize the impact of attacks, and deliver unwavering business continuity in the face of threats. Quickly and easily protect your data environment with these features:

- **Air Gap and Immutability**: Safeguards backup data in secure, air-gapped storage with strict access controls to prevent tampering.
- **Clean Restore Point Validation**: AI-driven automation verifies and ensures clean recovery points, prevents reinfection, and provides pristine datasets.
- **Data Security Posture Management**: Identify, analyze, and secure sensitive files to reduce exfiltration risks across all your production and backup datasets.
- **Early Warning**: Detect threats before encryption, exfiltration, or damage with patented early warning technology that uncovers and diverts zero-day and advanced threats before they reach your data. And masks assets and backup environments from malicious bad actors.
- **Resilienceof and Recovery**: Eliminate malware risks, prevent reinfection, and orchestrate restores at scale with reliable, rapid recovery.
- **Security Insights**: Get end-to-end observability and manage data risks efficiently. React sooner, and limit exposure through a single pane of glass.
- **Zero Trust Architecture**: Go deeper with multifactor and multiperson authentication; privileged access management (PAM); and identity and access management (IAM) tools like CyberArk, YubiKey, and biometrics (such as AAL3).

COMMVAULT CLOUD BRIDGES IT AND SECOPS:

By implementing Commvault Cloud, your organization can benefit from true data security and recovery in the hybrid cloud, enabling you to see, manage, and recover data wherever it lives.

Commvault offers our customers an advantage in ensuring resilience in the face of a cyber attack. We provide this through years of industry-leading innovation and more than 1,500 patents. One of the most powerful advantages Commvault Cloud offers is a unique architecture built for the hybrid world. It delivers the market's most predictable, fastest, and cost-optimized mass recovery.

Unleash the Power of Comprehensive Cyber Resilience

To learn more, visit **www.commvault.com** or **request a demo**.