COMMVAULT

Keeping your business safe from ransomware

How Commvault is helping organizations protect against and recover from ransomware attacks.

© 2021 Commvault Systems, Inc. All rights reserved.

When ransomware strikes, respond and recover quickly

29% reported attacks happened weekly or more frequently[2]

Ransomware attacks increased by 435% in 2020[3]

60% of organizations experience a ransomware attack over 12 months[4]

Just because your organization has not experienced a ransomware attack does not mean it never will. A ransomware attack is when a cybercriminal encrypts a victim's files and demands a ransom payment for keys to decrypt the data. Every 10 seconds, an organization becomes a victim of a ransomware attack.[1] Any organization that believes it can survive a ransomware attack without reliable data protection is sadly mistaken.

A ransomware attack should be a top concern for every organization. Having your data encrypted and held for ransom is a nightmare – and these attacks are increasing at an alarming rate.

Ransomware attacks are on the rise,[5] and it typically takes a long time to recover the data – if it is recoverable at all. Unfortunately, these types of attacks are expected to remain prevalent.

1 Phil Muncaster"One Ransomware Victim Every 10 Seconds in 2020," Infosecurity Magazine, February 25, 2021
2 Lance Whitney, "The Many Ways a Ransomware Attack Can Hurt Your Organization," TechRepublic (TechRepublic, June 16, 2021)
3 Shawn Henry, "Crowdstrike Services Cyber Frontline Report," n.d.
4 ESG Master Survey Results, 2020 Technology Spending Intentions Survey, January 2020.
5 Deep Instinct, 2020 Cyber threat Landscape Report

© 2021 Commvault Systems, Inc. All rights reserved.

The cost goes far beyond the payoff

$10 trillion spent on cybercrime by 2025[1]

Firms on average experienced 23 days of downtime following an attack[2]

The average cost of an attack was $154,000 in 2020[3]

The consequences of a ransomware attack can be devastating. With downtime and costs expected to increase year-over-year, organizations must prepare to minimize the impact and expense – including negative financial impacts and damage to their brand.

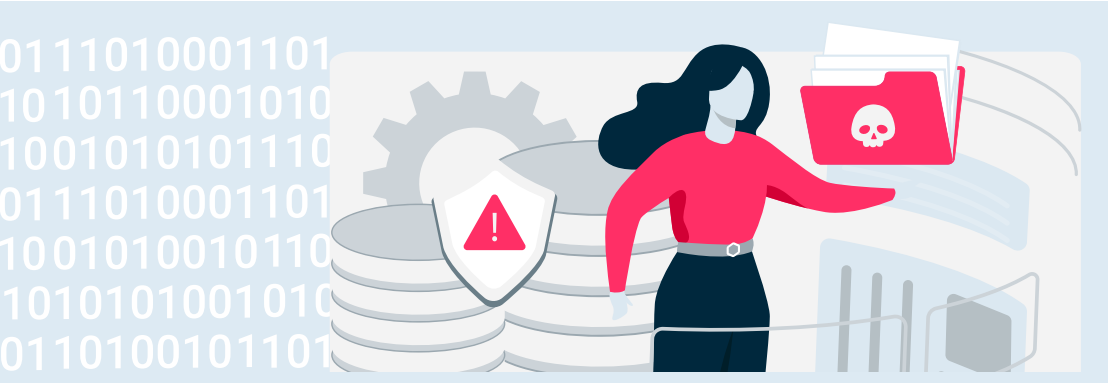
The average ransom payment is around $154,000,[3] but it can be much higher. For example, Oslo-based Norsk Hydro recently paid $71 million to attackers.[4] In addition, it typically costs 10 times the ransom payment to restore the data, $1.85M on average.[5] There's no way around it: no matter how you deal with a ransomware attack, the organization takes a hit in productivity, customer satisfaction, employee morale, and brand reputation.

The setbacks organizations experience from ransomware attacks are profound, and full recovery can take months or often years. Therefore, organizations should ensure their data protection and management solution can help protect, detect, and recover from ransomware.

1 Steve Morgan, "Cybercrime to Cost the World $10.5 Trillion Annually by 2025," Cybercrime Magazine, April 27, 2021, https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/.
2 Danny Palmer, "Ransomware Extortion Demands Are Growing, and so Is the Downtime Caused by Attacks," ZDNet (ZDNet, April 27, 2021)
3 Bill Siegel, "Ransomware Payments Decline in q4 2020," Coveware (Coveware: Ransomware Recovery First Responders, June 9, 2021)
4 McAfee, The Hidden Costs of Cybercrime 2020, December 9, 2020
5 SOPHOS, The State of Ransomware 2021, April 2021

© 2021 Commvault Systems, Inc. All rights reserved.

Commvault ransomware solution



Commvault is a recognized leader in providing data security that helps organizations protect, detect, and recover from ransomware attacks. Our solution can reduce your attack surface with a combination of hardware-independent immutability, air gapping, and automation support.

Commvault can provide early detection of unusual behavior through artificial intelligence and honeypots, enabling you to act sooner and limit the impact on your organization.

Minimizing business disruption is an essential part of the Commvault solution. Every minute counts, and with Commvault, you can rapidly and consistently recover from incidents that threaten your data.

Our unified customer experience provides data visibility to ensure consistent policies and actions across your entire environment.

Most complete ransomware protection & broadest coverage.

Consistent, repeatable processes and the most recovery options.

Best visibility across your data to manage and identify risk.

Learn more about Commvault solutions ›

© 2021 Commvault Systems, Inc. All rights reserved.

A layered approach to protecting data

Commvault follows a protection and recovery framework that ensures your organization is prepared for all kinds of cyberattacks. Based on the NIST framework, these five key elements work to protect an organization's data and quickly recover it in the event of a ransomware attack.

With Commvault, these organizations have been able to not only survive a ransomware attack but go on to thrive. The following case studies are just a few examples of how Commvault is helping organizations worldwide.

01	Identify	Assess and migrate risk
02	Protect	Isolate, lock, and harden data from changes
03	Monitor	Find anomalous threat patterns
04	Respond	Analyze data and perform orchestrated actions
05	Recover	Recover clean data quickly meeting objectives

Learn more about Commvault approach >

© 2021 Commvault Systems, Inc. All rights reserved.

ALLIANT

Background

Alliant Credit Union is a not-for-profit financial cooperative with 450,000 members and more than 600 employees. As a digitally focused bank with only two physical locations, Alliant is keen on data protection. The organization cannot afford to put its data at risk.

Challenge

The previous data protection solution required significant effort, and the IT staff were constantly dealing with issues. With its new solution, Alliant wanted to ensure that member services were not disrupted by downtime and improve recovery times for both disaster recovery sites.

Solution

Commvault helped with snapshot management and replication using the IntelliSnap® software that simplified backup and improved recovery times. Commvault also helped in eliminating manual processes, which accelerated disaster testing. Thanks to this solution, Alliant has more reliable backups and faster recovery times.

> "Data recovery used to take an hour, but with Commvault we can restore it in minutes — and all with point and click; it has eliminated a very tedious process."

Julio Arevalo, Manager of Systems Engineering

Alliant Credit Union gets faster and more reliable backups

90% reduction in recovery times at secondary site and 75% reduction at disaster recovery site

Decreased backup times from 30 hours to four hours using snapshots

Improved confidence in its backup process with a more reliable solution

Read the case study >

COMMVAULT

© 2021 Commvault Systems, Inc. All rights reserved.

(주)엔피씨시스템

Background

NPC Systems is a Korean ERP solutions provider that experienced a ransomware attack and could not recover some backup copies. After dealing with one attack, it was vital for the organization to ensure it wouldn't happen again.

Challenge

NPC System needed to cut time for administrators to verify backup results and identify the reason for backup failures. Moreover, the company was experiencing very high licensing costs, which prevented future growth in system development.

Solution

NPC Systems deployed Commvault Complete™ Backup and Recovery to accelerate data backups and protect data across their database, applications, and operating systems. Reducing manual backup and recovery tasks is a bonus.

> "By using Commvault Complete Backup & Recovery for secondary backup, we are confident that our data is secure and that we've eliminated the risk of data loss in the event of disasters and cyberattack."

Jeon Hyeon Seo, Team Leader | System Operation Unit

NPC System ensures data readiness

10x acceleration of backup speed

50% reduction in backup and recovery tasks for administrators

Ensured the business is prepared in the event of cyberattacks or natural disasters

Read the case study >

© 2021 Commvault Systems, Inc. All rights reserved.

Hyosan Medical Foundation
SAM Medical Center SAM Hospital

SAM Medical Center gets support for critical hospital operations

Background

SAM Medical Center operates two hospitals in South Korea and has relationships with missionary hospitals in seven other countries. Due to the increasing numbers of ransomware attacks across the healthcare industry, SAM decision-makers made upgrading the institution's data security a key priority.

Challenge

SAM Medical Center was manually cloning their data from the main storage system and needed to ensure sufficient storage devices. They also lacked an efficient and reliable disaster recovery system to avoid data loss and disruption to hospital operations. There was a high risk of human error while they were using manual backup procedures. The possible loss of patient records was a risk SAM leaders were unwilling to take.

Solution

SAM Medical Center implemented Commvault Complete™ Data Protection across the two hospitals to help with their backup and disaster recovery. This reduced licensing costs enabled faster recovery, minimized hospital operations disruptions, and improved the overall data management efficiency using the solution's intuitive dashboard.

> "It is not the best to have a situation where disaster recovery is needed. But Commvault gives us the confidence that we can respond immediately to unexpected events, such as a ransomware attack or data loss caused by user mistakes."

Sang-seok Park, Department Head of Information Strategy

10X increase in backup speed

Gained integrated, reliable, and cost-effective solution to protect entire environment

40% data compression ratio through deduplication

Read the case study >

© 2021 Commvault Systems, Inc. All rights reserved.

Background

Emirates Steel is a producer of finished steel products that was looking to move to the cloud for greater efficiency and security while complying with the UAE's strict National Electronic Security Authority regulations.

Challenge

The current day-to-day operations were inefficient and time-consuming. Emirates Steel was using multiple backup systems, which limited IT staff productivity and complicated backup and recovery functionality.

Solution

Emirates Steel implemented Commvault Complete™ Backup and Recovery for its entire ERP backup and all the unstructured data from their departments. This drastically simplified the recovery process, maximized data space, and eased the adoption of new technologies.

> "Commvault gives us confidence that we can recover rapidly from any scenario, including potential ransomware attacks."

Mohammed Azam, I.T. Infrastructure Head

Emirates Steel streamlines recovery process

Responsive, 24/7 support services

Simplified self-service recovery of the ERP system

Maximum data space made available through deduplication

Read the case study >

© 2021 Commvault Systems, Inc. All rights reserved.

Increase data availability with Commvault ransomware protection and recovery

These are dangerous times. Now more than ever, keeping your data safe must be a top priority. Do not wait for a ransomware attack before you act. **Be ready with Commvault.**

Learn more about how you can better protect and recover from ransomware at **commvault.com/ransomware ›**

COMMVAULT

commvault.com | 888.746.3849 | get-info@commvault.com

© 2021 Commvault Systems, Inc. All rights reserved. This document is confidential and is not to be shared. Please note that the information about competitors' products is based on current, publicly available information. The accuracy of this information is solely based on statements that a competitor has made, any misrepresentation or inaccurate information is due to our reliance on their statements.