



Build a cyber-resilient organization

Achieve strong organizational security and ensure business continuity in the face of a cyberattack with Rubrik and Microsoft



Ransomware is on the rise

As business becomes more digital, the risk of ransomware increases

Ransomware remains a serious threat to organizations all over the world. With high stakes, unreasonable demands, and unprecedented costs, it is designed not just to compromise your technology, but to take down your business. Unfortunately, attacks keep rising as ransomware continues to evolve, making recovery even more difficult.

Contents

Ransomware is on the rise	2
Stay ahead of threats	4
Strengthen your cyber defense	6
Recover quickly and completely	8
Case study: Payette	10
Stop ransomware and regain control with Rubrik and Microsoft	11



25%

Ransomware attacks surged dramatically in 2022, with ransomware involved in 25% of all breaches.¹



34%

Of all cyber insurance claims, 34% were ransomware-related in the first half of 2022.²



While the average ransom payment is \$812,360, it is only part of the total cost of a ransomware attack, which IBM pegs at \$4.5 million on average.³

Achieve business resilience against cyberattacks with Rubrik and Microsoft

Fortunately, as threats evolve, so too do the cybersecurity solutions available to companies. Together, Rubrik and Microsoft deliver end-to-end Zero Trust Data Security to protect mission-critical applications and hybrid cloud environments. Defend against escalating ransomware threats everywhere, across enterprise, cloud, and SaaS using the Rubrik Integration with Microsoft Sentinel for Ransomware Protection.

Stay ahead of threats

Conduct deeper and faster investigations to help understand the scope and root cause of an attack.

Strengthen your cyber defense

Implement a modern, zero trust framework to secure your data, prevent reinfection, and ensure recoverability.

Recover quickly and completely

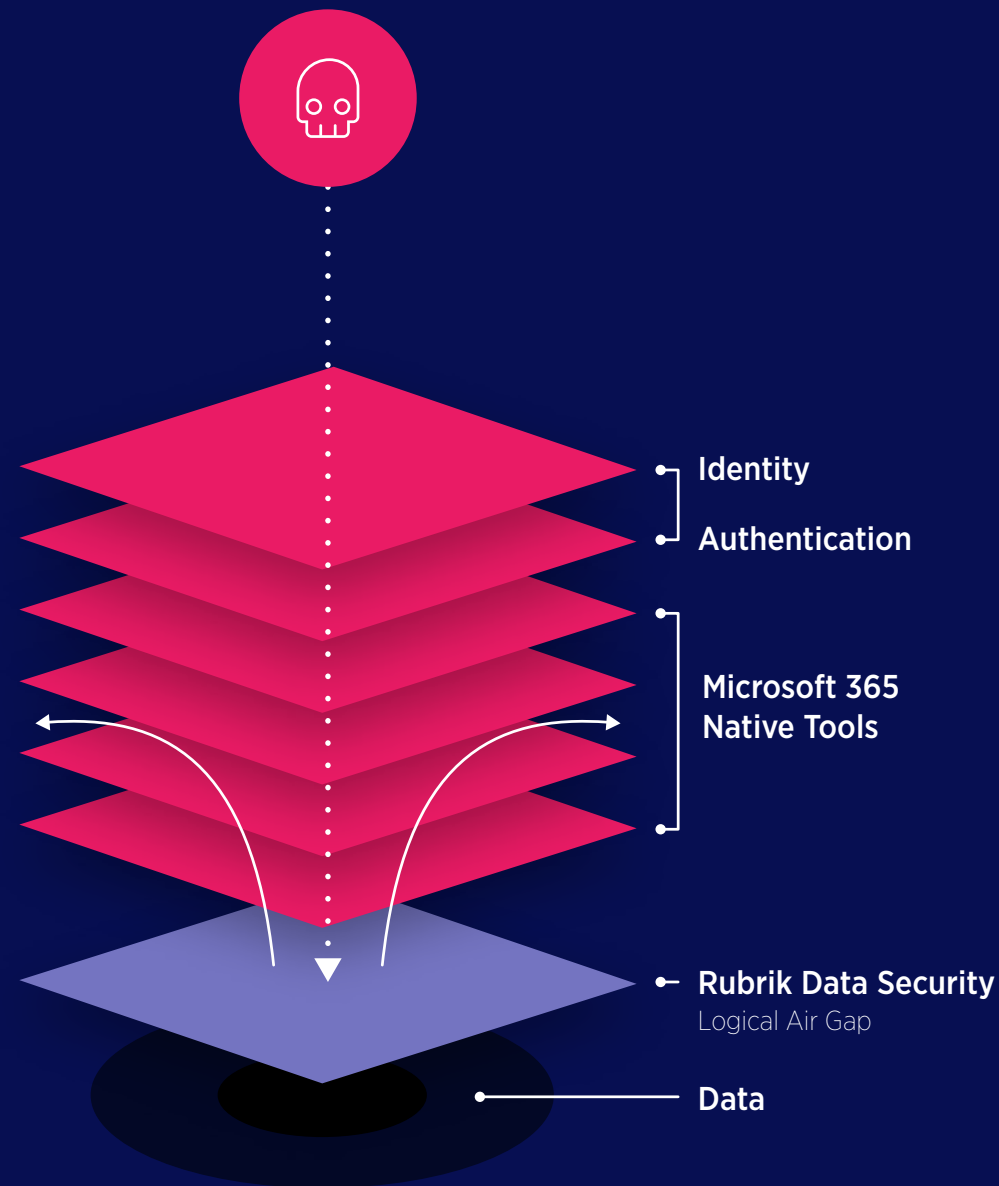
Trigger a recovery workflow directly from the Microsoft Sentinel dashboard using automated playbooks.

Stay ahead of threats

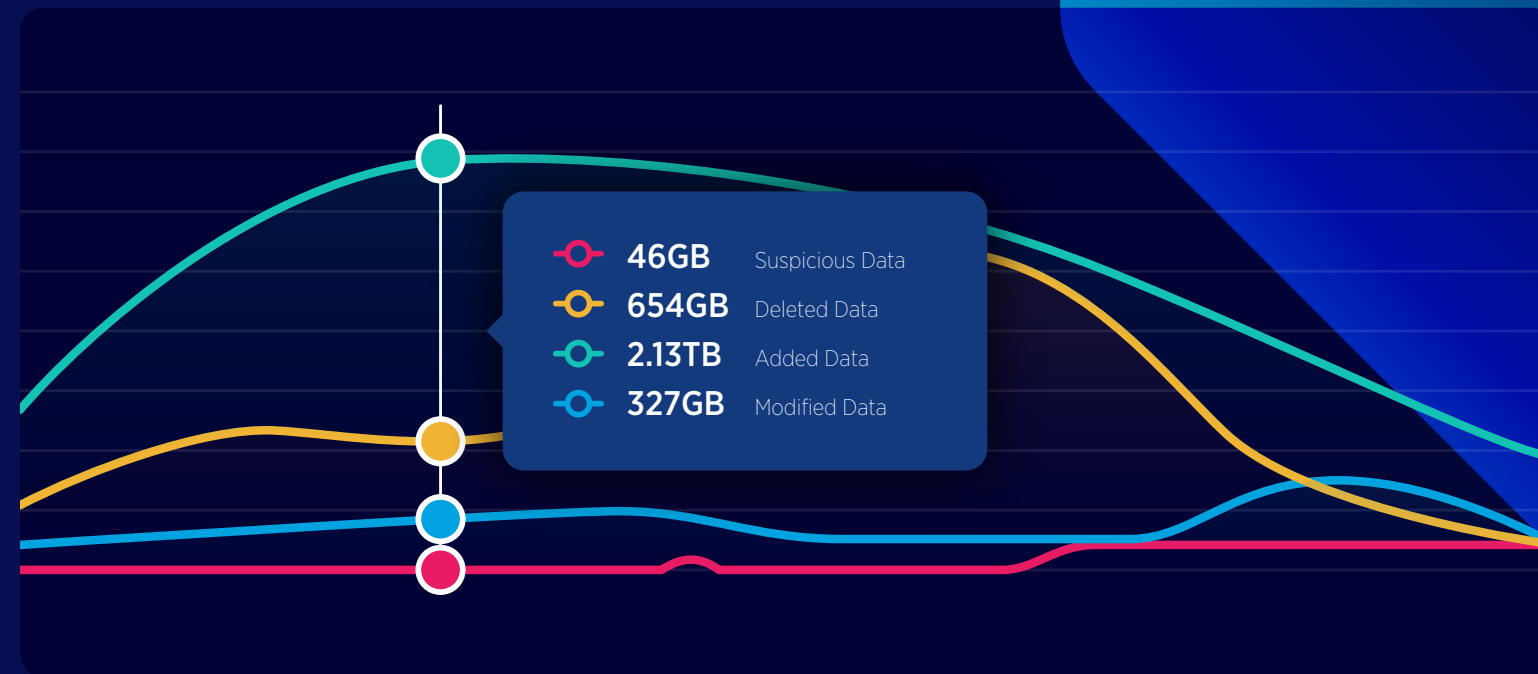
See and stop threats across the enterprise before they cause harm

Since it is likely a matter of when, not if, hackers will strike, taking a proactive approach to protect your data is key. Rubrik helps you analyze backup data for unusual behavior with Ransomware Investigation, part of the Data Observability capability of the Rubrik Security Cloud.

The Rubrik Data Observability engine constantly monitors and remediates data risks with pre-built scanners for blast radius identification, sensitive data recovery, and threat hunting. In short, it turns a passive backup system into an active defense system with machine learning that identifies when, where, and how cyberthreats have impacted data to enable rapid recovery. Further, Rubrik proactively analyzes behavioral patterns and detects anomalies as a last line of defense – all without impacting your production system.



Investigate threats to data



Ransomware monitoring and investigation powered by machine learning to detect data anomalies, encryptions, deletions, and modifications.

Sensitive data monitoring to find and classify the most sensitive data and assess exfiltration risk.

Threat monitoring and hunting to identify indicators of compromise and find the last known clean copy of data.

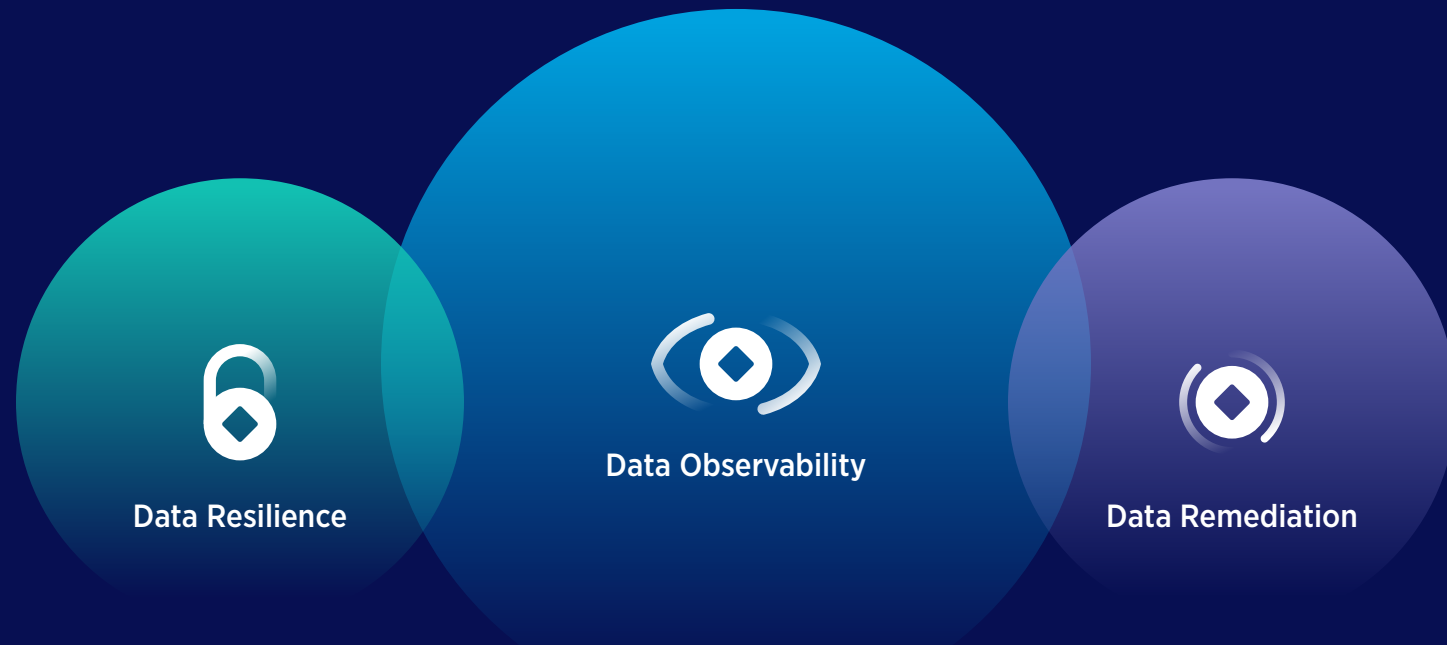
Strengthen your cyber defense

Enable comprehensive security that safeguards data and ensures recovery in the case of an attack

Organizations are destined to pay a ransom if they can't recover encrypted files quickly – not to mention experience significant revenue and brand damage. Together, Microsoft and Rubrik strengthen your defense in depth to give you complete data protection.

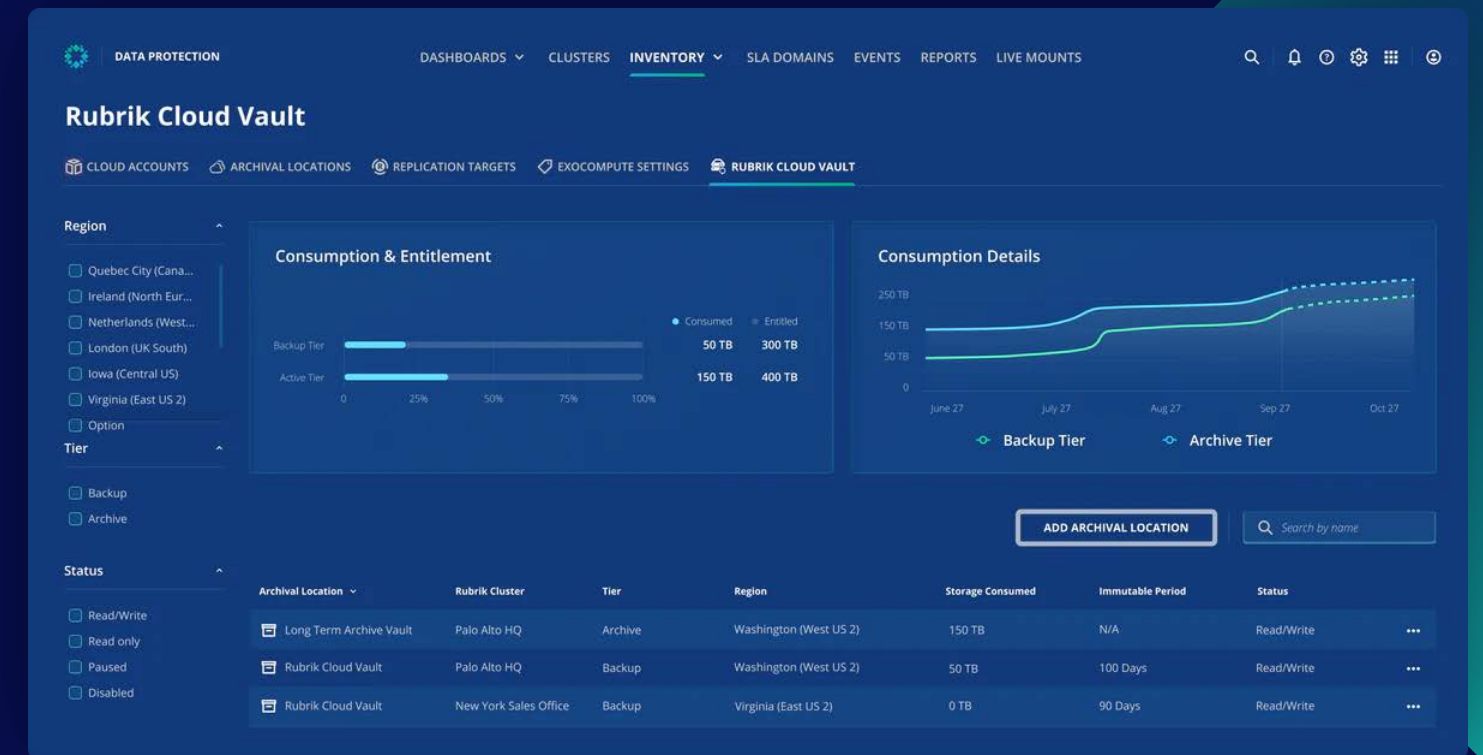
The integration with Microsoft Sentinel helps bridge the gap between Security and IT Operations to provide both groups a common view of data risks and threats. This gives businesses the timely insights

they need to recover quickly and confidently with malware-free backups to restore critical operations and avoid business disruption. Rubrik's comprehensive data security complements Microsoft's perimeter security, cloud security, and threat detection tools to further strengthen your data defenses and protect from threats. And in the case of a breach, the Rubrik Integration with Microsoft Sentinel for Ransomware Protection helps recover your data quickly so you can put attacks behind you and resume business as usual sooner.



Stack the odds in your favor with Rubrik Cloud Vault

Rubrik Cloud Vault (part of Rubrik Security Cloud's Data Resilience capability) delivers a fully managed, secure, and isolated cloud vault service built on Microsoft Azure. Simplify air-gapping of critical data and provide end-to-end data immutability to ensure data is not compromised, corrupted, or maliciously deleted.



Recover quickly and completely

Speed up recovery time with automated responses right within Microsoft Sentinel

Attackers know that if they can take down your data, they can take down your business. That's why organizations need a smarter way to keep their data safe with options to quickly recover sensitive information when defenses are compromised.

Rubrik's integration with Microsoft Sentinel makes threat detection and response efforts smarter and faster. Rubrik helps you secure your data in

Microsoft Azure and ensure data protection and recoverability across your Microsoft applications including Azure VMs and Managed Disks, Azure SQL, Microsoft 365, Azure NetApp Files, SQL Server, and physical or virtualized Windows. And while shared responsibility means you are responsible for protecting your data, Rubrik secures against data loss with logical air gap and tight API integrations with Azure.

Blueprint Name	Source Cluster	Target Cluster	VMs	RPO Lag	Status
Payroll App	Rubrik Site-A	Rubrik Site-B	2	Low	Ready
Payroll App	Rubrik Site-A	Rubrik Site-B	2	Low	Ready
Website	Rubrik Site-A	Rubrik Site-B	12	Low	Ready
Legal App	Rubrik Site-C	Rubrik Site-B	3	Low	Ready
Identity Services	Rubrik Site-D	Rubrik Site-B	4	High	Ready

Take a zero trust approach

With Rubrik's Zero Trust Data Security, you can count on the power of analytics and automation to recover within hours, and:

- Mitigate attack vectors that cyber criminals commonly exploit.
- Utilize true immutability, anomaly detection, sensitive data discovery, retention lock, and multi-factor authentication.
- Ensure rapid recovery during an incident.

Snapshot	Estimated Size Change	Estimated File Difference
May 13, 2022 11:00AM	14.7 kB	424 files
May 12, 2022 11:00AM	164 kB	318 files
May 11, 2022 11:00AM	96 kB	174 files

Enjoy a simple solution that will help you take your security posture to the next level.

Case study: Payette

Situation

Payette is an award-winning architecture firm with the mission to create buildings of purpose – from cutting-edge 5.5M square foot science centers to world-changing hospitals across the globe. Payette’s largest data sets are unstructured NAS data, and the ability to retrieve and access previous project files is critical to the business’s efficiency and success. And, with finance, HR, payroll, and all fiscal transactions running on NAS, data security is a top priority.

Challenge

Dan Gallivan, Director of IT, dropped what he was doing early one Saturday morning when he received an urgent call alerting him that systems were going down – they were under attack. As Gallivan realized the PC LAN and network services had been exploited, he immediately called in his security team. 50TB of Dell EMC Isilon data was suspected to be encrypted and corrupted, and a server had been compromised.

Result

Thanks to Rubrik Security Cloud, critical systems were back online in less than 24 hours and achieved 100% recovery within one week, meaning zero business impact. Due to Payette’s quick recovery efforts, the hacker never even had the opportunity to deliver a ransom note. Without Rubrik, Payette would have had to resort to a full wipe-and-replace, losing multi-million-dollar projects, designs 3.5 years in the making, payroll, and financial data.

Solution

It is simpler than ever to secure your Azure data with Rubrik. Payette noticed this firsthand when adopting Rubrik Cloud Data Protection.

- In less than 24 hours, critical systems were back online.
- 100% recovery within 1 week and zero data lost.
- Azure and Microsoft 365 data resilience against cyberthreats.

“Our clients want to know they are partnering with a trustworthy and secure firm. Rubrik is our insurance policy for our data. How do you quantify that peace of mind? It is priceless.”

– Dan Gallivan, Director of IT

“We used CloudOn to migrate VMs to Azure and CloudOut to deploy and build our Azure infrastructure. It’s Incredible being able to move these workloads into Azure, and then have Rubrik protect them.”

– Dan Gallivan, Director of IT

[Read the full case study](#)

Stop ransomware and regain control with Rubrik and Microsoft

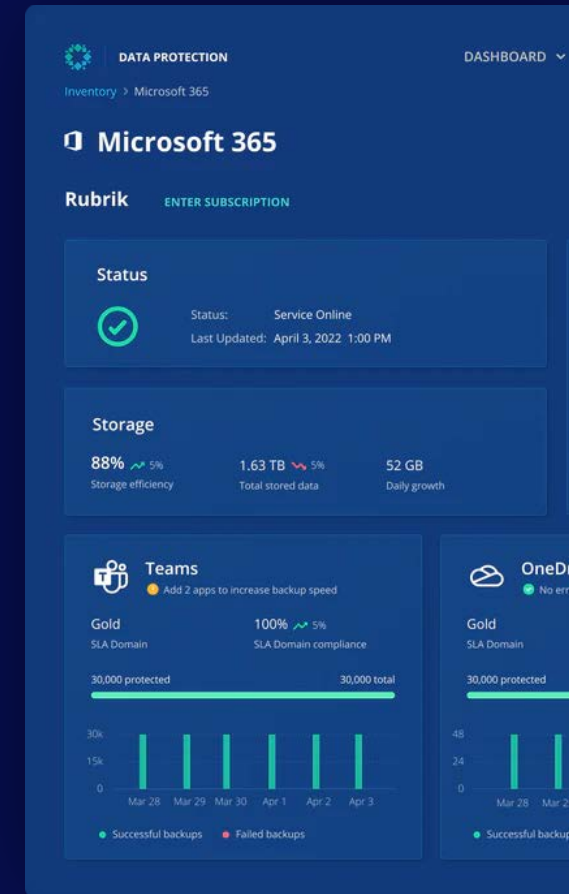
Ransomware attacks can be devastating, but they are possible to survive. Together, Rubrik and Microsoft make it easy to protect your mission-critical applications on-premises, in the cloud, and everywhere in between – so your data is always secure and available. Keep your data safe and recoverable in the face of ransomware attacks with the Rubrik Integration with Microsoft Sentinel for Ransomware Protection.

[Learn more](#)

[Learn more](#) about Rubrik and Microsoft.

[Get it now](#)

Find us on [Microsoft Commercial Marketplace](#)



¹ 2022 Data Breach Investigation Report | Verizon

² Corvus Risk Insights Index, 2022 | Corvus

³ Cost of a Data Breach 2022 Report | IBM

