rubrik | Microsoft

Take the Fear Out of Ransomware with Zero Trust Data Security

Introduction

Ransomware continues to spawn dramatic headlines in the media, from the Dark Web to *The New York Times*. IT administrators and security professionals, right through to the C-suite and the board, fear the business disruption, damage to reputation, and escalating costs that come with malware. Facing pressure from boards and governing bodies, organizations are scrambling to protect themselves from this escalating threat.

Ransomware has been declared a clear and present danger by the U.S. Department of Justice.[1] Cyber insurance premiums are soaring. There's been a 116% increase in ransomware attacks this year.[2] The emergence of ransomware-as-as-service (RaaS) has meant an onslaught of attacks. The most sophisticated ransomware groups have a side hustle, selling their tools to aspiring threat actors as a bundle, providing the malware and the phishing operation, payment platform, and premade data leak site.[3] The FBI has warned that there are now 100 different ransomware strains circulating[4].

There's a widespread feeling of helplessness among those tasked with protecting data. And it's no wonder when the odds are stacked so unequivocally against them.

Human error, a dispersed workforce, legacy applications, complex networks, and a lack of visibility combine to make front-line defense almost impossible and an attack inevitable. How do you protect your organization? How do you ensure business-critical data stays safe so you maintain business continuity? Where is all that data located, and is it protected?

Organizations need to shift their defense strategy from solely focusing on the front end to strengthening their backend. You can't stop every malware attempt—after all, they only need to be right once, whereas your defenses must be insurmountable every time. You need to ensure you can recover as quickly, easily, and efficiently as possible.

That's where Zero Trust data security comes in.

This eBook walks you through the various challenges organizations face while trying to protect their data from ransomware, offers steps to overcome the most significant hurdles, and demonstrates how to recover data after an attack and avoid paying the ransom using Zero Trust data security.

Microsoft and Rubrik bring best-in-class offerings and capabilities that unify management and offer a holistic approach to Zero Trust data security for your hybrid cloud. Together, Rubrik and Microsoft help organizations manage hybrid and multicloud data security and defend against escalating ransomware threats.

Chapter One

The Relentless Reality of Ransomware

For threat actors, ransomware is a big, dirty business with big costs incurred by the victims. The average ransomware recovery costs are now $1.85 million, more than double what they were one year ago.[6] And you can't depend on cyber insurance to foot that bill. Forty-two percent of companies with cyber insurance policies in place indicated that insurance only covered a small part of damages resulting from a ransomware attack.[7]

In the first half of 2021, the ransomware scourge hit a staggering 304.7 million attempted attacks within SonicWall Capture Labs' telemetry (for perspective, the firm logged 304.6 million ransomware attempts for the entirety of 2020)—a 151% year-to-date increase.[8]

According to a recent study, the number of organizations deciding to pay an encryption ransom has risen to 32% compared to 26% the year prior. The sore spot, though, is that the same global survey discovered only 8% of those organizations got all their data back despite outlaying the requested funds, and nearly one-third (29%) of organizations couldn't recover more than half of the encrypted data[9].

A different study found that 80% of organizations that paid the ransom experienced a second breach, 46% believing it to be caused by the same threat actors, while 46% of those who paid said at least some of their data was corrupted.[10]

It seems you just can't win.

> "Ransomware attacks are only going to get worse and more pervasive in people's lives, and they're not disappearing anytime soon. There's a line of cybercriminals waiting to conduct these ransomware attacks. Anytime one goes down, you just see another group pop up."
>
> **Allan Liska**
> Intelligence Analyst, Recorded Future[5]

$1.85 million

is the average bill for rectifying a ransomware attack, considering downtime, people time, device cost, network cost, lost opportunity, ransom paid, etc. [11]

92%

of organizations don't get all their data back [12]

53%

of ransomware victims report suffering brand and reputation damage as a result of an attack [13]

Threat actors are unrelenting in their attempts to breach defenses. While some approaches—such as poorly-written phishing emails from a distant beneficiary you've never heard of—are apparent, the exploitation of software vulnerabilities is not. If at first a threat actor doesn't succeed, you can be sure they will try, try again.

The most common tactics to carry out ransomware attacks are email phishing campaigns, RDP vulnerabilities, and software vulnerabilities [14]

Fifty percent of 582 information security professionals surveyed do not believe their organization is prepared to repel a ransomware attack[15]. **This is because of the challenges companies face in protecting themselves, such as:**

- Human error
- Dispersed workforce
- Escalating endpoints
- Complex networks
- Legacy data storage
- Lack of visibility into where data is stored
- Inadequate firewalls and defenses

40% of CIOs say siloed data makes it challenging to identify the severity of an issue and minimize business impact[16]

Many organizations don't understand the extent to which their data backups are vulnerable. They think they have a technology stack that will prevent ransomware. They falsely believe that they are protected. But you need to have a system in place that allows you to recover when your security fails.

Chapter Two

It Doesn’t Pay to Pay (So Best to be Prepared)

Adam Wandt, a cybercrime researcher and professor at John Jay College of Criminal Justice, says that “the security blanket of cyber insurance has convinced some organizations they don’t need to implement the human and technical changes necessary to stop ransomware attacks, and that the only real long-term answer is for governments to pass laws banning organizations from paying ransoms for certain kinds of data.”

“Ransoms should never be paid and those that do should understand the damage they’re causing to our society for their own benefit and gain. Paying the ransom will lead to nothing more than more attacks on our critical infrastructure.[17]” Criminals follow the money. The less ransomware pays off, the fewer attacks there will be.

The average downtimea company experiences after a ransomware attack is 21 days[18]

The Boy Scout motto, “Always be prepared,” should be part of your ransomware protection strategy—always be prepared for ransomware.

To do that, organizations need to ready themselves for the inevitable by:

- Positioning themselves to recover quickly, limiting downtime, without paying the ransom
- Making sure their systems are hardened with the latest security best practices
- Ensuring the best and last hope of recovery—the backup data—cannot be compromised

The problem in many instances is old data protection systems. Data protection, otherwise known as backing up your data, has been around for decades. It’s fundamental to IT.

Attackers target backup systems, and they understand that the victim will not pay the ransom if they can recover their data from backups with minimal loss. So, threat actors encrypt both the primary data and the backup data.

Unfortunately for many organizations, legacy systems leave their backups vulnerable to compromise and encryption. Once malware compromises both primary and backup data, the companies wind up in an unrecoverable state and must pay the ransom. Even after that, the recovery can be quite painful and lengthy.

The FBI already urges organizations not to pay, but in some cases, not paying means going out of business.

It doesn’t have to be that way.

Cybersecurity reporter Nicole Perlroth chronicles the proliferation of cyberattacks, including ransomware. She says: “It would also help if organizations were required to have copies of their digital records and to back them up regularly. Victims wouldn’t be in the position to have to pay to recover their own data.[19]

The Zero Trust Data Security Defense

Cybercriminals are after the money. If every organization made it so they could recover without paying the ransom, the threat of ransomware would diminish.

> "Rubrik is not just about recovering from ransomware. Rubrik is the difference between survival and non-survival in this new digital age."
>
> **Matthew Day**
> CIO, Langs Building Supplies

Langs Building Supplies: The tale of a typical ransomware attack (with a Rubrik-enabled happy ending)

It was 4:00 in the morning, May 20, 2021. Matthew Day, CIO of Langs Building Supplies (Langs) woke up to every CIO's worst nightmare: the dreaded phone call, "We've been hacked."

Upon arrival at his office, he tried to bring up the system. Nothing. Instead, what came up was a ransom note: "You've been hacked." He realized, "This is not just an unplanned outage. This is a targeted attack." "We were profiled," said Day. "They looked at our business, and they took their time. They found a source that we trusted implicitly."

The attack vector was a legitimate-looking email coming from a proper email address, from the right account, in the correct format.

Two weeks later, the criminal actors had access to Langs' systems. They kicked off the malicious attack at 2:00 AM when they knew no one would be around.

"Rubrik is particularly useful for ransomware attacks in which you have tens of thousands, or hundreds of thousands of files being encrypted, or deleted, in the span of minutes like we experienced. It really helps you assess the scope of the threat and where we needed to start targeting our recoveries," Aaron Pritchard, Langs' IT Systems Analyst, stated. "With Rubrik, we were able to analyze the impact, quickly identify what data was encrypted and where it resided in our environment. We did not have to pay the $15M ransom. We had zero data loss. And we were fully recovered, up and running in less than 24 hours. Rubrik really saved us."

Microsoft and Rubrik have partnered to make it easy for customers to restore their data, minimizing business disruption and damage to brand reputation without having to succumb to the demands of cybercriminals.

Building on their long-standing partnership, Rubrik and Microsoft now provide Microsoft 365 with hybrid cloud data protection and integrated cloud services on Microsoft Azure. Rubrik, the Zero Trust data security company, addresses the most pressing data challenges for organizations: Rapid recovery from ransomware, automation of data operations, and the transition of data to the cloud. The Rubrik and Microsoft collaboration brings these offerings to the next level, providing Zero Trust data protection for hybrid cloud environments spanning data center, edge, and cloud, including Microsoft 365.

“Customers across industries are migrating to the cloud to drive business transformation and realize growth,” says Nick Parker, Corporate Vice President, Global Partner Solutions, Microsoft. “End-to-end application and data management is critical to business success, and we believe that integrating Rubrik’s Zero Trust data management solutions with Microsoft Azure and Microsoft 365 will make it easy for customers to advance their Zero Trust journey and increase their digital resilience.”

Adding Rubrik to your existing Microsoft tools provides an extra layer of security and saves copies of critical user data outside of the Microsoft ecosystem—all done in tandem with Microsoft. Both engineering teams work together to best protect your data.

Rubrik reinforces Microsoft environments with full data protection for VMs running in Azure and storage volumes provided by Azure Managed Disks. API-driven integration between Rubrik and Azure storage services offers secure, immutable archiving for long-term retention. Additionally, protection for Microsoft 365, OneDrive, SharePoint, and Teams creates a logical air gap for Microsoft data.

> “When we were hit by ransomware in February 2021, it could have been a debilitating disaster for the county; however, one of the few moments of satisfaction during weeks of discomfort was knowing that Rubrik was backing up our data and that we wouldn’t have to pay the ransom for data recovery.”
>
> **Paul LaValley**
> Former CIO, Yuba County

Peace of Mind—Guaranteed

“As the pioneer of Zero Trust data security, Rubrik is helping the world’s leading organizations manage their data and recover from ransomware,” said Bipul Sinha, Co-founder and CEO of Rubrik. “Together with Microsoft, we are delivering tightly integrated data protection while accelerating and simplifying our customer’s journey to the cloud.”

Rubrik is so sure of its ability to protect your data that they’ve guaranteed it. Rubrik delivers the ultimate peace of mind by warranting up to $5M in ransomware recovery for Rubrik Enterprise Edition customers.

> “Backups are one of the most, if not the most, important defenses against ransomware. Rubrik’s file system was built to be immutable, meaning backups cannot be encrypted or deleted by ransomware. I am very fortunate to say that 100% of what we had on Rubrik we were able to recover.”
>
> **Paul LaValley**
> Former CIO, Yuba County

Meet with Our Experts

Cybercriminals are hatching plots as we speak. Time to smash some eggs. You’ve begun your datatude adjustment and realized that backup is just the beginning of what the Rubrik and ePlus solution can do for you. Now it’s time to take the next step by meeting with our experts. During the meeting, we’ll discuss your current infrastructure, needs, and processes. We’ll make strategic recommendations that show you a path to simpler data management, smart automation, and considerable cost savings.

datatude.eplus.com

References

1 U.S. Department of Justice (accessed through YouTube), “Justice Department Press Conference Regarding Ransomware Attack on Colonial Pipeline.”https://www.youtube.com/watch?v=fS-uiSxHcAQ&t=275s

2 The Next Web, “Why is ransomware on the rise?”
https://thenextweb.com/news/why-ransomware-on-the-rise-syndication

3 The Next Web, “Why is ransomware on the rise?”https://thenextweb.com/news/why-ransomware-on-the-rise-syndication

4 Threat Post, “Ransomware volumes hit record highs.”https://threatpost.com/ransomware-volumes-record-highs-2021/168327/

5 The New York Times, “White House Warns Companies to Act Now on Ransomware Defenses (2021).”
https://www.nytimes.com/2021/06/03/us/politics/ransomware-cybersecurity-infrastructure.html?searchResultPosition=23

6 Sophos, “The State of Ransomware 2021.”https://secure2.sophos.com/en-us/content/state-of-ransomware.aspx

7 Cybereason, “Ransomware: The true cost to business.”https://www.cybereason.com/hubfs/dam/collateral/ebooks/Cybereason_Ransomware_Research_2021.pdf

8 SonicWall, “SONICWALL: RECORD 304.7 MILLION RANSOMWARE ATTACKS ECLIPSE 2020 GLOBAL TOTAL IN JUST 6 MONTHS.”https://www.sonicwall.com/news/sonicwall-record-304-7-million-ransomware-attacks

9 Sophos, “The State of Ransomware 2021.”https://secure2.sophos.com/en-us/content/state-of-ransomware.aspx

10 ZDNet, “Most firms face second ransomware attack after paying off first.” https://www.zdnet.com/article/most-firms-face-second-ransomware-attack-after-paying-off-first/

11 Sophos, “The State of Ransomware 2021.”https://www.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-2021-wp.pdf?cmp=120469

12 Sophos, “The State of Ransomware 2021.”https://www.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-2021-wp.pdf?cmp=120469

13 TechRepublic, “The many ways a ransomware attack can hurt your organization.”https://www.techrepublic.com/article/the-many-ways-a-ransomware-attack-can-hurt-your-organization/

14 MS-ISAC, “Ransomware Guide 2020.”https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf

15 PurpleSec, “Cybersecurity Statistics 2021.”https://purplesec.us/resources/cyber-security-statistics/

16 Business Wire, “New Research Shows CIOs need Greater Cross Team Collaboration to Drive Digital Transformation.”https://www.businesswire.com/portal/site/home/news/

17 The Next Web, “Why is ransomware on the rise?”https://thenextweb.com/news/why-ransomware-on-the-rise-syndication

18 Coveware, “Ransomware Payments Fall as Fewer Companies Pay Data Exfiltration Extortion Demands.”https://www.coveware.com/blog/ransomware-marketplace-report-q4-2020

19 The New York Times, “Don’t Ignore Ransomware. It’s Bad. (2021)”https://www.nytimes.com/2021/04/29/technology/ransomware-attacks-prevention.html?searchResultPosition=5

20 Rubrik, “Rubrik Announces Strategic Agreement with Microsoft to Mitigate Ransomware Threats and Tightly Integrate Cloud Services.”
https://www.rubrik.com/company/newsroom/press-releases/21/strategic-agreement-with-microsoft-to-mitigate-ransomware-threats

21 Rubrik, “Rubrik Announces Strategic Agreement with Microsoft to Mitigate Ransomware Threats and Tightly Integrate Cloud Services.”
https://www.rubrik.com/company/newsroom/press-releases/21/strategic-agreement-with-microsoft-to-mitigate-ransomware-threats