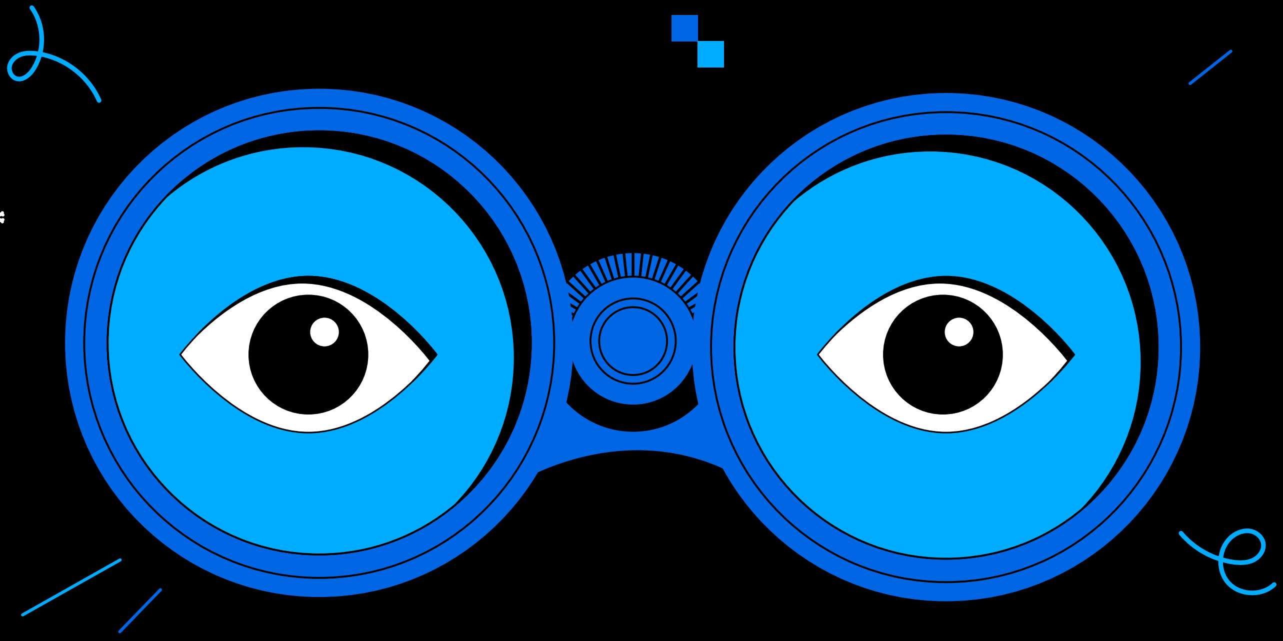


RUBRIK EBOOK

How to Catch a Hacker

The **4 Key Threat-Hunting Capabilities** You Need for Optimal Data Protection

rubrik

70%

The number of reported cyberattacks across all industries **increased by 70% YoY** between 2022 and 2023.

38%

The percentage of organizations with hybrid environments that suffered **at least one data breach.** Of these victims, 33% endured at least one ransomware attack.

20%

The percentage of organizations that **do not know what actions to take** in the event of a cyberattack.

Source: The State of Data Security, a 2024 Rubrik Zero Labs report

It's a troubling paradox: businesses across all industries are 67% more likely to experience a cyberattack than physical theft. Alas, the locks, fences, and surveillance systems that guard the perimeter of your business are not equally matched in the all-important realm of data protection.

Businesses are five times more likely to experience a cyberattack than a fire, but most lack the cyber resilience equivalent of smoke detectors and sprinkler systems. If you don't want to join the 94% of IT and security leaders who reported a significant cyberattack in 2023, you need to meet hackers where they are—living within your data and ready to strike.

Backup Data: Your Secret Defense Against Attack

Once you accept that it's a matter of when (not if) your organization will find itself under attack, it's time to start thinking like a hacker. Cyber criminals are creative and always looking to cover up their tracks. So cyber resilience hinges on the ability to go back in time and uncover the specifics of an attack.

The problem: Many organizations feel their only option is to scan their production systems for malware. This process can be difficult, time-consuming, and bad for network performance. And that says nothing of the resources required to spot and deflect novel, zero-day cyberattacks.

But what if you could monitor your backup data for new threats?

The solution: Analyze several of your most recent point-in-time backup snapshots. This spares your production systems the burden of adding threat monitoring and scanning activities, instead using an out-of-band process on existing backup data.

And since the investigation happens away from the site of the attack, you can perform your investigation without alerting the attacker.

Bottom line: If your threat hunting uses backup data instead of production data, your active systems stay nimble as you work quietly to uncover clues about a potential attack.

Glossary of Terms

Air-gapping

A security measure used to isolate and protect critical data by creating a separation between the data and the rest of the network. Logical (versus physical) air-gapped environments are protected by **immutability**, encryption, and access controls, preventing unauthorized modifications or deletions of backup data that is kept separate from the production environment.

Immutability

A characteristic of data that ensures it cannot be altered—crucial for ensuring data integrity and security in the face of cyber threats such as ransomware attacks.

File hashes

Fixed-size strings or numbers generated from the contents of a file using a hash function. Because file hashes uniquely identify a specific file's contents, they are invaluable for detecting malicious files. (See **Indicators of compromise**.)

File patterns

Specific characteristics or attributes of a file that can be used to identify or classify them. File patterns such as naming conventions or file extensions can indicate the presence of malicious files. (See **Indicators of compromise**.)

Indicators of compromise (IOCs)

A piece of digital forensic evidence that suggests a system or network has been compromised. Key IOCs include **file hashes**, **file patterns**, and **YARA rules**.

Threat hunting

The process of searching a company's systems for **indicators of compromise**, alerting users to changes and taking affected files and systems offline at the first sign of a malware attack.

Threat monitoring

A proactive form of threat hunting that allows you to detect threats early by automatically identifying indicators of compromise within backup snapshots using up-to-date threat intelligence.

YARA rules

A form of coding that malware researchers use to identify and classify malware samples. Yara rules are created for threat hunts and focus specifically on unique and characteristic strings or patterns that are unlikely to occur in benign files. (See **Indicators of compromise**.)

Key Capability #1: Finding the point of attack

If you fear your systems have been compromised, you face an urgent need to find the point of attack. You must discover what servers and data have been affected, gauge the extent of the damage, and quickly restore the business.

But before you can assess the damage, you need to be aware of the attack—and you need to gain this awareness before the hackers complete their attack. Scanning for and finding indicators of compromise (IOCs) is especially powerful when you are able to remediate the threat early—ideally before the malware detonates.

Still, minimizing downtime while analyzing IOCs to discover threats is a daunting challenge for IT organizations. They're racing to track down all compromised files and revert to the last-known clean copy from their catalog. But:

- How do they know when the malicious code was delivered and executed?
- Can they even identify the malware variant?
- Do they have the right personnel, tools, and skillset to execute the forensic analysis in time and keep the hacker in their sight lines?
- Has an intruder accessed any sensitive or regulated data, and do you need to notify the proper authorities?

IRON MOUNTAIN®
DATA CENTERS

Upwards of 70% of attacks now incorporate a social engineering component, such as phishing, baiting, and impersonation, according to Iron Mountain Data Centers (IMDC), which operates a worldwide colocation platform with over 20 facilities across seven countries for customers to meet their digital transformation needs. These attacks bypass external controls by tricking unsuspecting users unless these users recognize and report that they're being attacked.

IMDC was looking to further enhance its systems to track and prevent social engineering schemes. The company found the right solution with Rubrik Threat Hunting for data threat analysis.

Rubrik helped fill in other critical gaps in IMDC's legacy toolset, providing backup data immutability, Anomaly Detection, and Threat Monitoring. Together, these solutions support tighter lockdown for backups, data analysis to find indicators of ransomware or compromise, and surgical recovery to accelerate time to repair for complete cyber resilience.

Results:

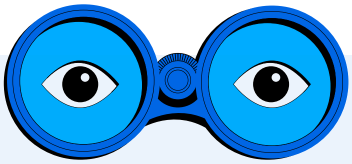
- 90% reduction in IT overhead associated with backup/recovery
- Zero impact to production data with Threat Monitoring and Threat Hunting
- Consistent procedures and compliance across data centers

Imagine you're an information security leader at a financial services company and you become aware that there's a threat targeting firms in your industry. Specifically, you're told by an industry group that these attacks began three days ago, carried out using executable files of a specific size. But that's all the information you have.

A cybersecurity analyst would get this tip and start looking for all executable files of that size that were active in the last 48 hours. Perhaps something fits that description, or perhaps they come up empty. They are essentially searching for a needle in a haystack—with very little information about what the needle looks like.

Threat-hunting software takes the pain out of this process. The solution may tell you, for example, that six matches have been found in a specific directory, as well as when they were created and last modified. Then you as a security leader can start making judgments based on that information. You might see something that was created three years ago and rule it out as your vulnerability—but suddenly you see something created three days ago, and you choose to investigate that more closely. If what you find is worrisome, your next step is to make sure what you've found is not on any other systems by doing a scan to look for a true negative. If those systems don't have it—phew, you're clean.

This scenario underscores the fact that a threat hunt isn't always about finding something bad. It can also be a way to validate that there's nothing sinister lurking in your systems. But the key is to have the tools you need to quickly do a comprehensive search using scant information.



> What I love about Threat Hunting is that it doesn't impact production or notify anyone. I can collect all the evidence, and the threat actor is never aware that it's happening.
>
> **Zoe Mora**
>
> Information Security Senior Manager at IMDC

Key Capability #2: Gathering Intel

The hypothetical financial services use case mentioned above is an example of a stealth "pre-attack"—the organization got a tip-off, searched appropriately, and was relieved to learn that its systems were clean. This happens all the time, and it's not the kind of attack that makes the headlines, such as one where a well-known organization gets hit by ransomware and a hacker has perhaps gone public.

In a ransomware scenario, ideally an organization will quickly turn to external data security experts to guide them through the right actions to take and what to look for. These experts understand that there's an art to knowing what to hunt for—how to gather intelligence on very specific file hashes and rules associated with a specific attack. With a narrowed data set in hand, the art gives way to the science of setting up exactly the right filters to increase the efficiency of the hunt.

File hashes and file patterns are unique identifiers that are among the most straightforward ways to search for a threat in your system. If you search for a specific file hash, soon enough you'll know which server cluster it can be found on, and within that cluster you'll know which objects it resides on. These hash matches are among the most common IOCs a threat-hunting solution looks for, along with suspicious file names/paths and YARA rules. With YARA—essentially a form of coding that malware researchers use to identify and classify malware samples—users can create descriptions of malware families based on textual or binary patterns.

Here's an analogy: Let's say three bank robbers have just escaped in a Tesla. In pursuit of these criminals, the police would of course want to narrow down that description—and various clues point to a Tesla Model Y. Soon enough it's revealed that the Tesla is red, which exponentially reduces the number of cars you're looking for. With YARAs and hashes, the specificity you gain is like being handed the license plate number. And nothing aids speed and efficiency like a perfect match.

> Threat Hunting for AmFam has been a game changer. It allows our security teams to look for specific malware or zero-day vulnerabilities across our entire ecosystem.
>
> **Nate Brooks**
>
> Technology Services Manager, AmFam Group

carhartt

Global premium workwear brand Carhartt relies on immutable backup capabilities from Rubrik that are specifically designed to protect data against ransomware and other threats. In a past incident, the Carhartt team discovered malware in backups from its legacy solution. What followed was more than two weeks of searching through endless data sets to manually complete an investigation into which files and servers had been corrupted.

Now, with Rubrik, the IT and Security teams are collaborating to zero in on malware and tie investigations into a central security operations center. If IOCs are discovered, these teams are prepared to quickly quarantine malicious snapshots within their backup catalog. This quarantine operation prevents a systems administrator from inadvertently restoring these files back into production using normal recovery operations—so Carhartt can now recover data with complete confidence that they are avoiding reinfection.

The company uses Rubrik Anomaly Detection to determine if individual files have been impacted by malware, and Sensitive Data Monitoring to aid in precision surveillance of critical data, such as personally identifying information. This helps Carhartt understand if any sensitive data has been compromised in the event of an attack—a scenario that would trigger looping in Legal and Privacy teams for swift and surgical next steps.

Results:

- 600+ workloads migrated to Rubrik Security Cloud
- 50%+ monthly cost savings

Key Capability #3: Isolating the Threat

For the purpose of ensuring that a system recovery is free of malware, threat-hunting solutions give users the capability to quarantine an infected snapshot—preventing reinfection during the recovery process.

Running threat-hunting and threat-monitoring solutions on a cloud-based data protection and management platform keeps those solutions separate from potentially contaminated workloads on your primary infrastructure. This allows companies to work through identifying the last-known clean snapshots (which may be hosted on the cloud, but are often preserved in the data center) and quarantine infected snapshots from a centralized data management control plane.

Since the control and data planes run on separated and logically air-gapped environments, the architecture itself reduces the risk of both planes being infected at the same time.

With the intelligence gleaned during the threat hunt about specific IOCs within the backup data, organizations can more accurately and surgically quarantine the threat and prevent reinfection during and after recovery. Having access to an archive of snapshots allows for a fulsome review of a system's history, expediting the investigation without impacting production and supporting rapid recovery when it's needed most. And with an immutable data management platform, it is impossible to delete data, including contaminated files, from a snapshot—a fundamental security feature and the reason infected files are quarantined instead of deleted.

Key Capability #4: Restoring Systems to Pre-Attack State

In the event of a successful attack, once you know which backups are clean and safe to recover from, you'll want to recover at speed. That's why recovery workflows should be built into threat-hunting and threat-monitoring technologies; Once a threat is discovered and isolated, it's just a matter of clicking the right buttons to restore to a clean state.

A sophisticated threat-hunting solution will take only the affected files and systems offline—minimizing impact on operations by focusing the hunt for IOCs on backup data and leaving production data alone. With the ability to quickly search backup snapshots for IOCs and proactively scan net-new recovery points, security operators and administrators can more accurately pinpoint the last-known clean snapshot to quickly restore data with the confidence that embedded malware will not reinfect production systems. This is a fundamental aspect of establishing data resilience.

Preparing for the next attack is an essential part of restoring the business. But many IT and Information Security departments lack the bandwidth to perpetually hunt for new threats. This is why it is essential to activate *threat monitoring* before the next attack.

Threat monitoring is a proactive form of threat hunting that allows you to detect threats early by automatically identifying IOCs within backup snapshots using up-to-date threat intelligence. A threat monitoring solution proactively scans for threats out-of-band from production

St Luke's
UNIVERSITY HEALTH NETWORK

St. Luke's cares for hundreds of thousands of patients every year with 2.5PB of data and millions of patient records they need to secure every day, across 14 campuses and 300 outpatient sites. Cyber recovery simulations revealed a ransomware attack would cause a major outage, costing the business millions of dollars and threatening patient care.

Data resiliency is essential to the survival of the business. St. Luke's needed to be able to recover from an attack in minutes or hours – not weeks or months.

Now, Rubrik Threat Hunting and Anomaly Detection alert the business in real-time about changes to the system, delivering a dynamic and integrated cyber defense to protect business operations and the well-being of its patients.

Results:

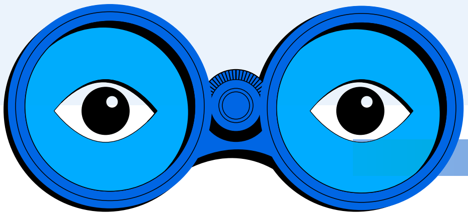
- 2.5 PB of data secured and protected with Rubrik
- Millions of patient records secured and protected
- 73% cost savings over three years
- Integration with Microsoft Sentinel & Azure

infrastructure based on vetted threat intelligence from multiple sources—accelerating the investigation process and reducing risk of reinfection.

Once you set up threat monitoring, it simply runs in the background—similar to antivirus software. It automatically downloads new signatures—unique strings of data or patterns that are characteristic of specific types of malware—and scans into them on your behalf.

Ideally, threat monitoring and threat hunting are used in tandem, so when an organization gets signals about new threats, they can then use threat hunting to confirm the results or determine which backups to explore further.

> With Rubrik, we have the ability to recover within minutes or hours as opposed to months. Threat Hunting and Anomaly Detection alert us of real-time changes in our environment so there is never a question about the integrity of our data. We have confidence in our data security night and day.
>
> **Paul de Vries**
>
> Senior Systems Engineer, St. Luke's University Health Network



How Rubrik Threat Hunting Works

Rubrik is well known for its backup technologies designed to address modern data control challenges across various environments, including cloud, on premises, and hybrid infrastructures. Rubrik Threat Monitoring and Threat Hunting are natural extensions of that investment in backup solutions that protect organizations from costly downtime in the face of increasingly likely cyberattacks.

Threat Monitoring is the source of a company's first alert, since this solution automatically scans for known threats based on an automatically updated threat feed. That company then confirms a clean recovery point using Threat Hunting and learns whether that specific malware is lurking on other systems. And if the malware payload detonated and encryption occurred, Anomaly Detection would generate alerts for that malicious activity and simplify recovery of only the impacted data

Threat Hunting can also be used to quickly and confidently determine that a particular threat is not present—establishing a true negative. Together, Rubrik's innovative Threat Hunting and Threat Monitoring capabilities allow organizations to reduce incident response times and strengthen their posture against malware attacks.

Both solutions leverage three different methods to identify IOCs in backups created on the Rubrik platform: YARA rule matches, file hash matches, and suspicious file name/path matches. With these three methods, Rubrik backups can be scanned for IOCs so security operators can understand which systems have been potentially impacted by an attack and identify when those IOCs were first present in the system.

These IOCs allow Threat Hunting to locate malicious files based on custom or predefined patterns within their backups and then help them identify a safe point to recover from, and safe data to recover. Predefined patterns are often developed by trusted third parties who study the signatures of common malware attacks, while custom patterns are created by IT teams to address an already identified threat. Rubrik brought this capability to its industry-leading data security platform so that organizations will now be able to easily search the backup environment for IOCs without any impact on production systems.

After the Rubrik Threat Hunt displays results about the hunt operation, a results table will include specifics on how many—if any—IOCs matched, as well as the earliest and latest snapshots where they were found. This key feature allows the user to pinpoint the exact location of IOCs and prevent the recovery effort from reintroducing the infection. The ability to take any corrupted backup snapshots and quarantine them comes courtesy of a feature of Rubrik Security Cloud called Threat Containment.

"With Threat Hunting, Rubrik equips us to search for security issues, helping us keep a clean data set for fast and secure data recovery that protects our reputation for dependable, trustworthy services," says Carhartt's Hopkins. "Rubrik isn't just a data security solution, it's peace of mind for our brand."

Are you ready to see Rubrik Threat Hunting in action? Take this product tour and see how you can stop an incursion and protect your data.