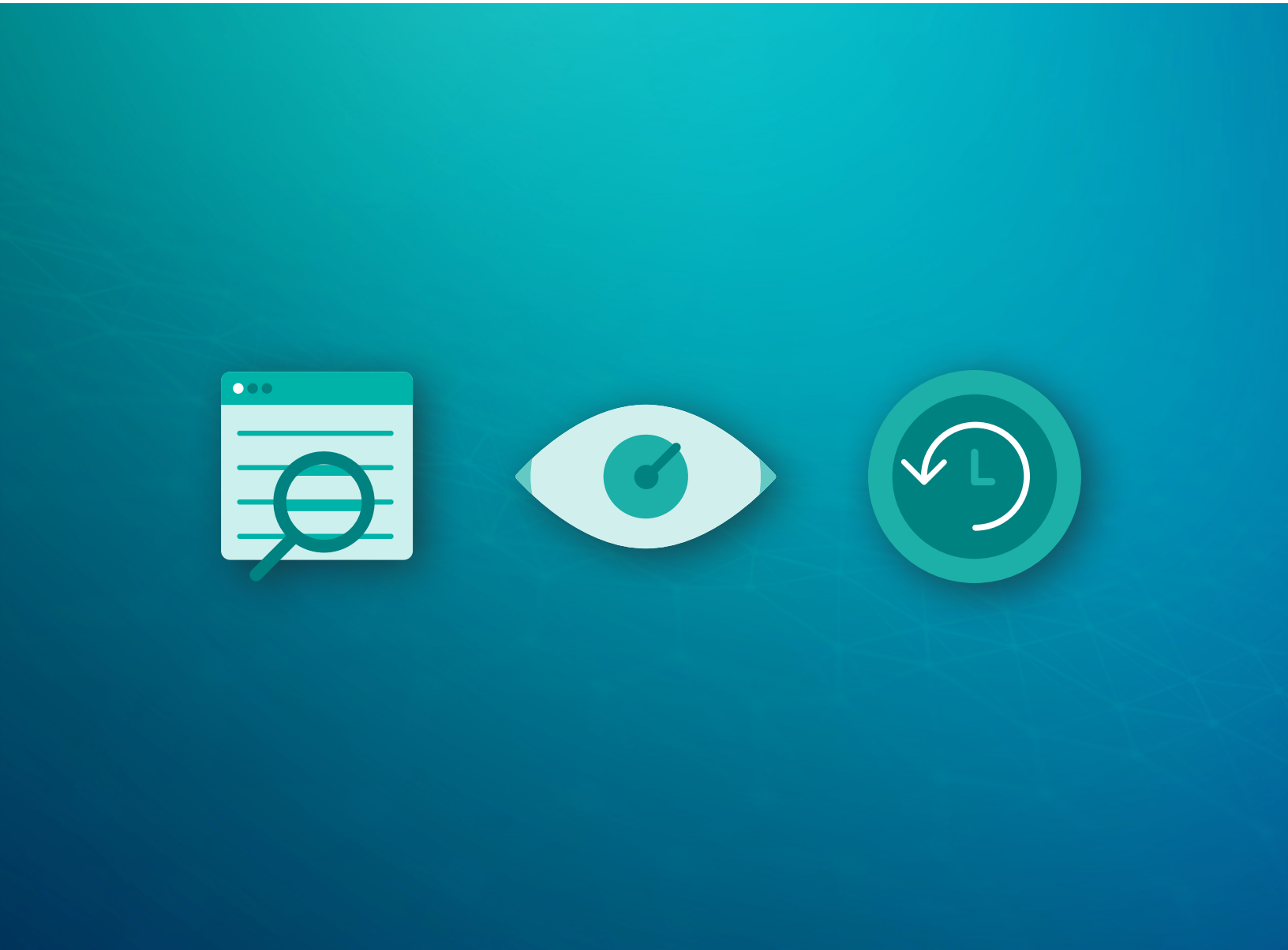
rubrik

WHITE PAPER

Report, Observe, Act: Cyber Recovery for Critical Infrastructure



Nation-state adversaries have set their sights on critical infrastructure—and that focus has only increased in the past year. A recent Waterfall Security report found a 140 percent increase in cyberattacks against critical infrastructure in 2022.[1] More recently, Volt Typhon, a state-sponsored threat actor based in China, launched a campaign to disrupt critical United States infrastructure.[2]

In response to this volume of attacks, a cybersecurity regulation has put pressure on critical infrastructure companies to report cyberattacks to the Cybersecurity and Infrastructure Security Agency (CISA): the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA).[3] The act encourages organizations to report cyberattacks, so CISA can help victims, warn other companies, and identify trends in the cybersecurity space.

Ultimately, reporting attacks goes a long way in defending other critical infrastructure organizations from similar incidents, but reporting represents just a third of what CISA recommends in the plight against cybercrime. In addition, CISA reminds organizations to observe suspicious activity and act in a timely manner to mitigate threats.[4]

To help you observe suspicious trends and proactively mitigate potential threats, you need to understand where your critical data is and who has access to it. The best way to address each of CISA's three recommendations is to establish strong data security capabilities. This paper will show you how the right data security partner can help you gather cyber incident information to render a comprehensive report, provide data visibility to help you minimize risk, and help you recover quickly with your data intact when a cyberattack happens.

1 2023 Threat Report – OT Cyberattacks With Physical Consequences
2 Volt Typhoon targets US critical infrastructure with living-off-the-land techniques
3 Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)
4 Sharing Cyber Event Information: Observe, Act, Report

REPORT: Report Cyber Incidents

In the midst of a cyberattack, you need quick insights into what is happening with your data and how the attack has progressed. As you analyze potential data security partners, look for data observability capabilities that help you detect deletions, modifications, and encryptions, so you analyze backup data for unusual behavior and changes caused by a cyberattack.

You should also be able to use time series analysis to understand when malicious files were introduced, when they were introduced, and how they spread. Similarly, you need to be able to assess the blast radius of the attack, so you can get a clear picture of which files and applications were affected using forensic analysis.

The information these kinds of capabilities offer can help you create richer reporting. Your incident response team can use that report to quickly identify what was impacted and recover just what you need without forcing a wholesale restoration. And when you pass that report on to CISA, you are also providing valuable threat insights that other critical infrastructure organizations can use to prepare for similar attacks.

But just as one attack ends, another may be waiting for you. That's why CISA recommends observing potential vulnerabilities to reduce risk later on.

OBSERVE: Minimize Risk

While CISA can offer help if you are a victim of cybercrime, staying proactive and maintaining a strong security posture can help you prepare for an attack well before it happens, so the effects of the attack aren't nearly as devastating.

Global access or "open shares" are often the biggest risks for an attack or theft of certain types of sensitive data. Look for security capabilities that give you instant visibility into high-risk data, such as over-permissioned access or sensitive data stored in unauthorized locations. With greater awareness of user permissions, you can reduce the risk of data breaches.

The more you know, the better equipped you will be to recover from cyber incidents—every time.

ACT: Recover Quickly

Now is the time to reevaluate your cyber recovery strategy. A recent Microsoft study found that 92 percent of organizations that were victims of ransomware did not have an effective data loss prevention strategy in place, resulting in critical data loss. The same study found that 44 percent of affected organizations did not have immutable backups for their critical assets.[5]

Organizations need both a data security solution and immutable backups to ensure recovery. First, a proper cyber recovery solution will improve cyber readiness and accelerate incident response by creating, testing, and validating your cyber recovery plans in isolated recovery environments. You should be able to measure the time taken for recovery and provide detailed historical performance reports to auditors and insurers, so you can prove you're actually ready to recover.

The second part of proving you're ready to recover involves having immutable backups in place to help your data survive a major event. An immutable backup is one that can't be modified, deleted, or changed in any way. Because immutable backups can't be altered, you can deploy them to your production servers right away when a cyberattack strikes and know you'll be able to recover to a known, clean state.[6]

5 Microsoft Digital Defense Report 2022
6 What is Immutable Data Backup?

HOW RUBRIK CAN HELP

Rubrik is a data security company that delivers a suite of data security services to ensure you can understand the scope of a cyberattack, stay proactive against future incidents, and recover from cyber incidents quickly.

Rubrik gives you the ability to continuously monitor for threats to your data, including ransomware, data destruction, and indicators of compromise. Rubrik also proactively identifies and monitors sensitive data exposure and uses intelligent insights to mitigate risks to this data. And you can quickly return to business as usual within hours or days, not weeks or months using orchestration and quarantining to contain threats and rapidly recover your apps, files, or objects while avoiding malware reinfection.

Rubrik backs up its solutions with a $10 million ransomware recovery warranty offering for qualified customers, which gives the ultimate peace of mind that data and services are protected. Rubrik Security Cloud for Government is also in the process of achieving Moderate authorization by the Federal Risk and Authorization Management Program (FedRAMP®), a government-wide program that provides security assessment, authorization, and continuous monitoring of cloud products and services. Rubrik's upcoming FedRAMP® authorization validates its "...commitment to delivering cyber resilience for the largest, most regulated organizations in the world."[7]

To learn more about how Rubrik can help you protect your critical assets, click here.

7 Rubrik Security Cloud – Government Is On the FedRAMP® Marketplace

rubrik

Global HQ
3495 Deer Creek Road
Palo Alto, CA 94304
United States

1-844-4RUBRIK
inquiries@rubrik.com
www.rubrik.com

wp-report-observe-act-cyber-recovery-for-critical-infrastructure / 20240107