druva | SHI

Insider's Guide to **Defending Against Ransomware**

Evaluate the real risks, costs, and strategies for IT leaders

Introduction

According to Cybersecurity Ventures, global cybercrime costs are expected to grow by 15 percent per year over the next five years, **reaching $10.5 trillion USD annually by 2025**, up from $3 trillion USD over the last decade.[1] Security vendor Trend Micro predicts that there will be more data extortion in 2023, with attacks involving cloud-aware ransomware, as organizations are increasingly moving their most critical data assets to the cloud.[2]

No industry is immune to ransomware attacks. And attacks on one company's infrastructure can halt business operations for many others. For example, in February 2022, the Cybersecurity and Infrastructure Security Agency (CISA) reported that it is aware of ransomware incidents against 14 of the 16 critical U.S. infrastructure sectors.[3]

[1] Cybersecurity Ventures, "Cybercrime To Cost The World $10.5 Trillion Annually By 2025," Morgan, Steve.
[2] Trend Micro, "Security Predictions for 2023: Future/Tense," Trend Micro Incorporated.
[3] Cybersecurity & Infrastructure Security Agency, "2021 Trends Show Increased Globalized Threat of Ransomware," Cybersecurity & Infrastructure Security Agency (Revised 2022).

Backups in the Crosshairs

In another worrying trend, new variants of ransomware specifically target backup data for encryption or deletion to ensure that victims have to pay. Two ransomware variants with backups in their sights are SamSam and Ryuk.

In a recent indictment, the US Department of Justice charged two threat actors who had used the SamSam malware to extort more than $30 million from over 200 victims, including hospitals. The indictment stated that the attackers maximize their profits by launching attacks outside regular business hours and by "encrypting backups of the victims' computers".[4]

With ransomware attacks on the rise and new variants specifically targeting backup data, organizations of all sizes are struggling to reduce risk and recover quickly from attacks.

[4] The United States Department of Justice News, "Two Iranian Men Indicted for Deploying Ransomware to Extort Hospitals, Municipalities, and Public Institutions, Causing Over $30 Million in Losses," Office Public of Affairs.

“Should I be Worried?”

You may be tempted to cross your fingers and hope you won’t be targeted. Unfortunately, the chance of experiencing a ransomware attack is very high, with serious consequences for a lack of preventative action.

Over half of all enterprises have had at least one ransomware attack within 12 months. Out of those enterprises, most were attacked more than once. About two-thirds of the attacks succeed in infecting at least one endpoint, and more than half go on to infect more endpoints and cause more damage.[5]

It’s not so much a question of if, but when. When ransomware succeeds, your employees can’t be productive and your company can suffer costly downtime. Computers and file servers have to be disinfected, and then operating systems, apps, and data need to be restored. Even if you pay the ransom, there is no guarantee you’ll be able to recover all your data and your reputation takes a hit.

[5] Aberdeen Group, “Reducing impact of ransomware attacks via cloud-based approaches.”

Calculating the Real Costs of Ransomware

According to Sophos[6], in 2022, 66% of organizations were hit with ransomware, 86% of ransomware attacks in 2022 caused a loss of business revenue, and 90% of these attacks affected their ability to operate. Considering the spectrum of monetary and business losses caused by a ransomware attack, what's the real cost of ransomware?

Their research shows:

- It costs 1.4 million, on average, to remediate a ransomware attack
- It takes 1 month, on average, to recover from an attack
- Organizations, on average, that paid the ransomware got only 61% of their data back, down from 65% in 2020

[6] Sophos, "The State of Ransomware 2022," Sophos LTD.

When the Best Offense is a Good Defense

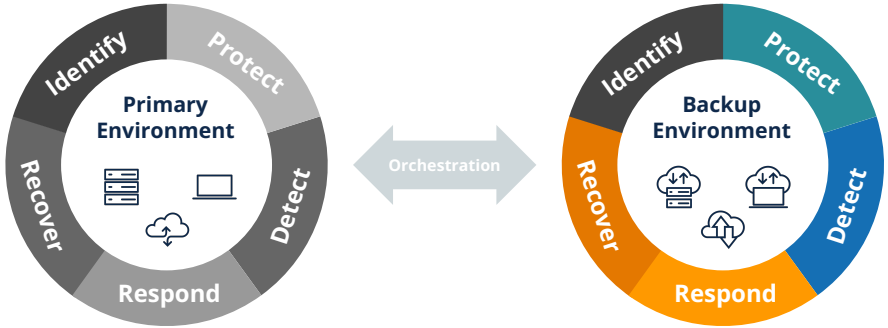
A proactive, cloud-based approach to ransomware protection and recovery can significantly mitigate the costly consequences of a ransomware attack.

Instead of playing a game of catch up, **consider implementing an *in-depth cybersecurity and data protection strategy* that covers both your primary and backup systems**. A robust security infrastructure (including network and email security as well as SIEM and SOAR tools) can help prevent ransomware from entering your network. A cloud backup and restore solution can help you respond and recover quickly in the event of an attack. **Integrating your backup solution with your primary security ecosystem can enable orchestration and automation at each step of your in response process ultimately leading to less downtime and lost business opportunity.**

The type of backup solution you use can also have a huge impact on your ability to recover from a ransomware attack. If you are using an on-premises or Windows-based solution, your backups may be more vulnerable to encryption or deletion by new variants of ransomware due to vulnerabilities and common misconfigurations. Consider switching to a cloud-native backup solution that is resistant to ransomware attacks.

Identify, Protect, Detect, Respond, Recover

An in-depth cybersecurity strategy should span both your primary environment and backup data and include a comprehensive ransomware playbook that covers each step of protection and recovery. The National Institute of Standards and Technology (NIST), recommends following the Cybersecurity Framework (CSF), which defines five essential functions: **Identify, Protect, Detect, Respond, and Recover**.



Identify

Identify your critical functions and data landscape across your environment, ensure the backup platform is a tier 1 application, and align critical applications and protection policies across backup and security teams.

Protect

Ensure you always have safe, unencrypted backup data you can use for recovery with best-in-class platform security, immutable air-gapped backups, and zero trust architecture.

Detect

Pinpoint unauthorized activity with insights into access attempts. Get alerts for data anomalies using an entropy-based machine learning algorithm that understands your unique environment.

Respond

Stop the spread of ransomware immediately with API-based SIEM and SOAR integrations that automate response activities like quarantining infected resources and snapshots.

Recover

Avoid reinfection by scanning individual snapshots before recovery to ensure data is clean. Or use automated recovery tools to find the most recent clean version of every file within a specified date range.

A Powerful Ransomware Recovery Service

Druva's ransomware protection and recovery offerings are aligned to the NIST framework and support organizations in implementing all five of these functions.

Partnering with a cloud data protection leader like Druva, can help support your in-depth cybersecurity strategy by providing multi-layered defense and advanced recovery options.

Your teams will not only prevent data loss and save costs, but also accelerate response and recovery times so you can get your company back to normal in days, not weeks or months after you've been hit by a ransomware attack.

Prevent infection of backups through air-gapped backups, single sign-on and multi-factor support.

Detect anomalous activity Monitor suspicious events through unusual data activity, and monitor unauthorized access attempts and restores/downloads.

Respond through standardized playbooks APIs block and resume backups and restores and delete/quarantine infected snapshots based on date.

Recover with confidence and agility including blocking infected files from being recovered and proactively orchestrating cloud disaster recovery.

Next Steps

IT and infosec teams that understand the risks of ransomware are in the best position to defend their companies from attacks. By selecting the right ransomware recovery solution, you can ensure that your organization has a rock-solid multi-layer defense plan in place to reduce the impact of ransomware or malware. You'll also be far less vulnerable to costly ransom demands and debilitating downtime.

Check out druva.com/solutions/ransomware/ to learn more.

druva

Sales: +1 888-248-4976 | sales@druva.com

Americas: +1 888-248-4976
Europe: +44 (0) 20-3750-9440
India: +91 (0) 20 6726-3300
Japan: japan-sales@druva.com
Singapore: asean-sales@druva.com
Australia: anz-sales@druva.com

Druva is the leading provider of data security solutions, empowering customers to secure and recover their data from all threats. The Druva Data Security Cloud is a fully managed SaaS solution offering air-gapped and immutable data protection across cloud, on-premises, and edge environments. By centralizing data protection, Druva enhances traditional security measures and enables faster incident response, effective cyber remediation, and robust data governance. Trusted by nearly 7,500 customers, including 75 of the Fortune 500, Druva safeguards business data in an increasingly interconnected world. Visit druva.com and follow us on LinkedIn, X (formerly Twitter), and Facebook.