COMMVAULT

WHITEPAPER

Ransomware: 4 ways to protect and recover

We all hear the news – ransomware attacks are an unfortunate part of cyber life. To make matters worse, business is so good for these criminals, they're developing more and more sophisticated threats. This results in organizations losing access to their data, potentially putting their entire business at risk. These poorly-protected organizations are often forced to pay the ransom – with the "hope" that their data is actually released – or attempt an ad hoc recovery effort without any guarantee of reliable recovery. To maintain access to your critical data, consider these four best practices to protect and recover from ransomware attacks with confidence.

4 ways to protect and recover from ransomware attacks

Implementing a multi-layer security strategy – including anti-malware, personal firewall, file encryption, data loss prevention software (DLP) and more – is critical to protect your endpoints and infrastructures against growing cyber threats. However, even with all of these protection solutions, there's still a modest chance of a breach, which is why backing up your data is key!

"Making regular copies of files to a separate device is the only effective way to minimize damage in a cyber attack event. A reliable backup enables people to return to their normal use of the computer with all their files intact at the soonest possible time."

The Threat Report, Myths In Cybersecurity That People Needs To Forget, 2019

To protect even the most data-intensive business environments from ransomware, we've put together the following best practices:

1 Have an effective information security program

If your organization is new to information security, or if you've only partially implemented your information security plan, consider taking the following steps to put an effective security program in place.

Table 1: Components of an effective security program

Feature	Integration
Know where critical data is stored	Complex environments mean maintaining awareness of data location is harder than ever. • Data center • Remote facilities • Cloud • Service Provider
Inventory systems	• Know which systems handle critical data: store, process and transmit • Understand the data flow • Determine which systems present the highest risk to your operations
Assess risk	• Include electronic records, physical media, and the availability of key systems, services, or devices
Apply security controls	• Select, apply and manage security controls based on risk

Feature	Integration
Monitor effectiveness	Prepare for the evolving threat landscape • Proactively evaluate the effectiveness of risk- based information security strategy, the security controls applied, and the proper implementation of security technologies • Apply corrective actions, remediation, and lessons learned
Educate users	• Make sure employees are educated on what to do when they receive emails from unknown senders with suspicious attachments or links (see Appendix for recommended steps)

2 Protect data with technology best practices

With the growing number of threats, coupled with increasing sophistication of attacks, businesses need to clearly understand the cost tradeoffs of investing in cybersecurity and employee education, against loss of access to critical data and the resulting impact on your business and reputation.

55% of respondents said detection of advanced threats (hidden, unknown, and emerging), was a top challenge for their security operations centers.

Domain Tools
The 2019 Threat Hunting Report

Network security is a good first line of defense in guarding against ransomware attacks. And by implementing effective technology best practices, organizations can further protect their data and IT infrastructure. Table 2 outlines key technology strategies to help eliminate the potential for infection by ransomware attacks.

Table 2: Technology best practices

Feature	Integration
Detect and prevent	Employ a multi-faceted security solution: • Keep systems and software updated with relevant patches • Protect against file-based threats (traditional antivirus), download protection, browser protection, heuristic technologies, firewall and a community sourced file reputation scoring system
Use external certification groups (computer emergency response teams)	• Can often identify a problem before the virus infects companies • Can make recommendations on immediate steps for manual filtering (software companies may require hours or days to release a patch)
Identify and stop infection	Define a comprehensive prevention and recovery readiness policy: • Includes endpoint and network policies and protection products, such as antivirus, antispyware, and firewall-type products • Limits execution of unapproved programs on workstations • Limits the write capabilities of end users so that, even if they download and run a ransomware application, it is unable to encrypt files beyond the user's specific files • Include electronic records, physical media, and the availability of critical systems, services, or devices
Keep a "gold" image of systems and configurations	A fundamental element of data management policies: • Easily clone infected system with master
Maintain a comprehensive backup strategy	Prepare for the evolving threats: • Proactively evaluate the effectiveness of risk-based information security strategy, the security controls applied, and the proper implementation of security technologies • Apply corrective actions, remediation, and lessons learned
Educate users	• Make sure employees are educated on what to do when they receive emails from unknown senders with suspicious attachments or links (see Appendix for recommended steps)

3 Employ effective backup strategies

Recognize that a ransomware event is almost always a progressive hack. It works over time, and can run in the background while learning the behavior of your backup routines. As such, it is important to maintain a persistent copy of the data in other locations as part of your recovery readiness strategy and disaster recovery procedures.

Those companies who only rely on snapshots as backup are at a higher risk. When the snapshot or the other instance is replicated, the source is corrupted too — as it follows the replication. Having a preserved version of the data from prior recovery points in a protected location is a must.

Table 3: Data protection best practices

Steps	Action
Employ backup and DR processes	• Directly call out a backup copy rather than versions stored on the same system • Have external backup copies of the data beyond simple snapshots that are maintained on the source system

Using a cloud library is another alternative for a good external collection. Since the cloud backup is not visible to the local administrator operating system account, it would require additional sophistication to gain access to your cloud user credentials. And while no one loves tape, it may prove to be a better alternative for some businesses, as the online nature of disk or cloud is what exposes the persistent risk.

4 Educate employees to secure the endpoint

Finally, educating everyone who touches your data on good security habits is essential to keeping businesses secure — remind them to use common sense. As described below, educate your users on the best practices from Symantec, outlined in Table 4.

Table 4: Employee and endpoint best practices

Steps	Action
Train users to practice security best practices	• Use a firewall • Enforce a password policy • Ensure that programs and users of the computer use the lowest level of privileges necessary to complete a task • Disable AutoPlay • Turn off file sharing if not needed • Turn off and remove unnecessary services • If a threat exploits one or more network services, disable or block access to those services until a patch is applied • Always keep your patch levels up-to-date • Configure your email server to block or remove email that contains file attachments that are commonly used to spread threats • Isolate compromised computers quickly to prevent threats from spreading further • Train employees not to open attachments unless they are expecting them • If Bluetooth is not required for mobile devices, it should be turned off Refer to **Symantec, security Best Practice recommendations, 2018** for complete details
Employ endpoint protection best practices	• Deploy URL-reputation plugins that display the reputation of websites from searches • Restrict software to corporate-approved applications, and avoid downloading software from file sharing sites. Only download packages directly from trusted vendors' websites • Deploy two-step authentication on any website or app that offers it • Ensure users have different passwords for every email account, applications and login - especially for work-related sites and services

Conclusion

Securing critical business information is certainly a necessity for any organization. And guarding that information from ransomware attacks should be a top priority for any business. So, protect that data by being attentive to security, technology, backup and employee best practices. As a result, your data will be secure and you'll better ensure business continuity — while mitigating ransomware risk.

COMMVAULT Be ready™

commvault.com | 888.746.3849
get-info@commvault.com