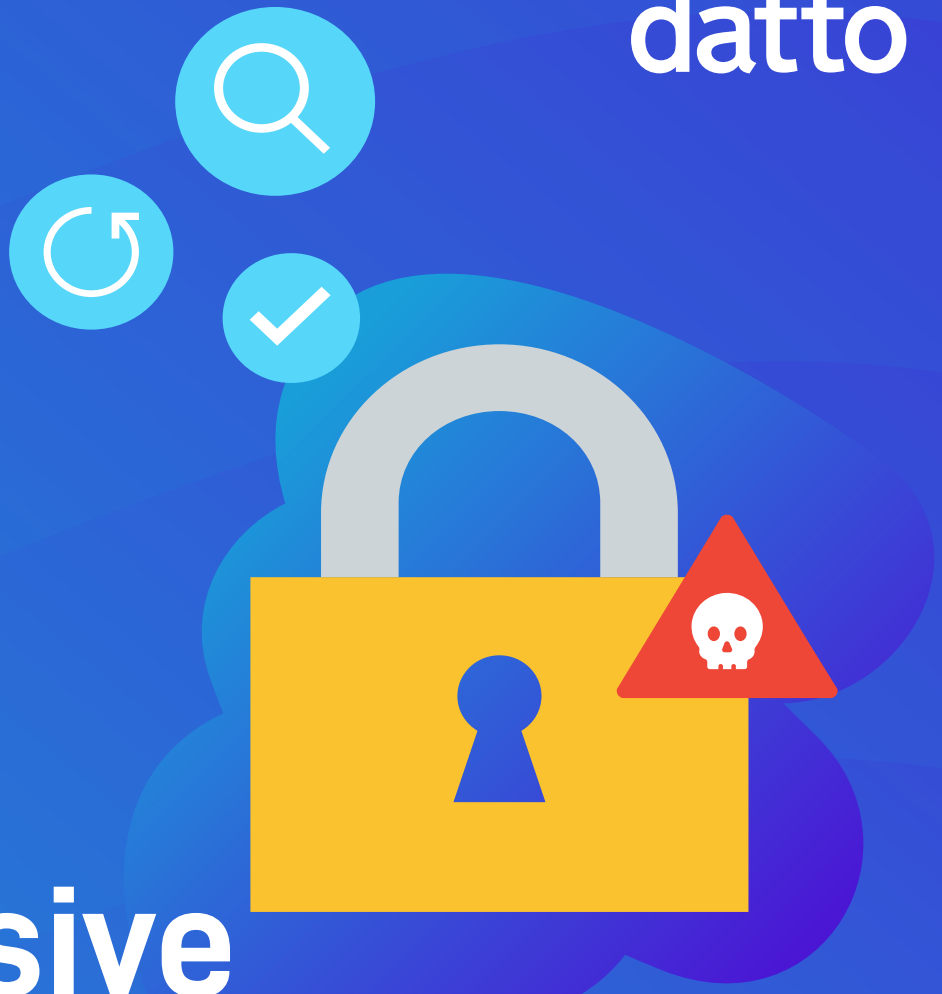
eBook

datto



A Comprehensive Ransomware Protection:

Detection, Response, and Recovery

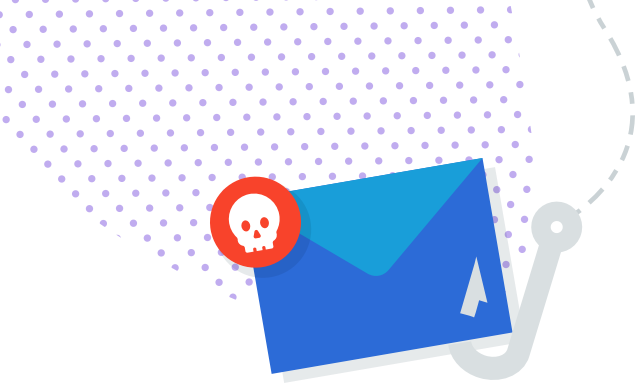
What is Ransomware?

Ransomware is a type of malware that encrypts files and folders and demands payment from victims to decrypt them. It is easily spread and has proven highly effective for cybercriminals for a number of reasons.

Ransomware strains are constantly modified and socially engineered to avoid detection by antivirus software. Some ransomware attacks incorporate worms that allow the ransomware to spread across networks, infecting devices beyond the initial source. Ransomware isn't limited to on-premises systems either, it can easily spread to software as a service (SaaS) applications as well. In fact, 1 in 4 MSPs reported ransomware attacks in SaaS applications, such as Microsoft 365, Google Workspace, and Dropbox.

Ransomware attacks can have serious financial implications for businesses, and ransom payment is just one complication. The business downtime associated with an attack can cripple revenue generation and the reputational damage to an organization that has been breached can take years to overcome.

Worse yet, ransomware attacks have skyrocketed over the past few years. According to Datto's 2020 Global State of the Channel Ransomware Report, 78% of managed service providers (MSPs) surveyed reported attacks against their small and medium-sized business (SMBs) clients over the last two years.



Ransomware is typically distributed via a phishing email that dupes a user into clicking a link or downloading an attachment, which installs the malware on their system.

You may also be interested in:

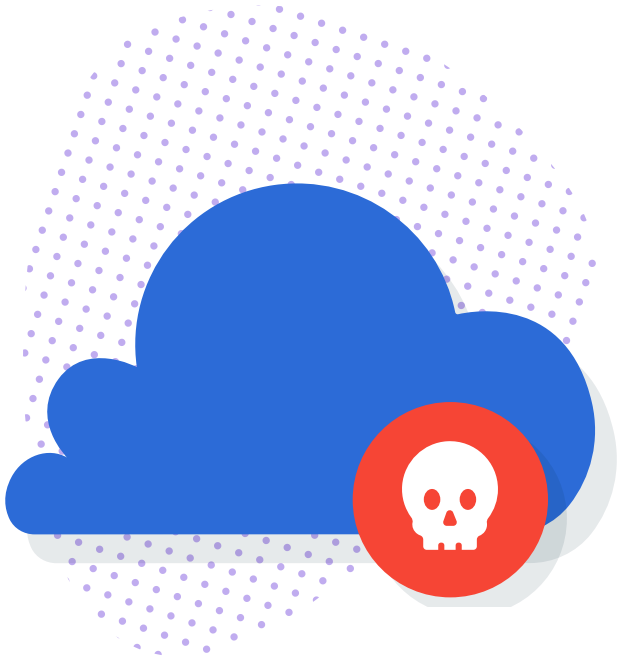
How Attacks Occur

To best understand how to protect against ransomware attacks, we must first look at how ransomware might spread across a business' local systems and SaaS accounts.

Delivery: Ransomware is typically distributed via a phishing email that dupes a user into clicking a link or downloading an attachment, which installs the malware on their system. In the early days of the ransomware boom, these attacks were generic and carried out on a wide scale. However, today's social engineering attacks are more targeted and customized for the intended victim.

Infection: An employee receives a phishing email and unknowingly clicks on a file that installs a "cryptoworm" variant of ransomware on their laptop, which begins searching for files on the device to encrypt. At the same time, the ransomware spreads across the network, infecting additional PCs and servers. Encryption does not begin immediately, instead the malware first spreads to as many systems as possible. This occurs in the background, so the business remains unaware of the infection.

Encryption: The command and control server operated by the cybercriminals generates a cryptographic key that will be used to encrypt the infected systems. Depending on the type of attack, this server may also be used to collect business information from infected systems. When the attackers are satisfied that the ransomware has been thoroughly distributed, the encryption process is triggered.



Spreading to SaaS: If employees have file synchronization turned on, encrypted files on a user's device are automatically copied to the domain on the SaaS provider's cloud. Phishing attacks in the cloud can be more sinister, as they often trick users into sharing administrative access to their account using OAuth with a simple click of a button. The MSPs surveyed saw 64% of ransomware infections occur in Microsoft Office 365 and 47% in Dropbox.

Ransom demanded: When encryption is complete, the attackers issue a ransom demand (in bitcoin or another cryptocurrency) and threaten to destroy data if the ransom is not paid, often within a specific timeframe to deliver a sense of urgency.

Ransom demands can vary depending on the nature of the attack. It's also important to note that the size of an organization or business has no bearing on whether they are a target for attackers. Additionally paying the ransom doesn't guarantee that businesses are in the clear, some can get hit multiple times from scenarios such as:

- **Ransom Size:** The ransom to unlock a single laptop will likely be much lower than the ransom demands of a business completely locked out.
- **Ransom Reactivation:** If ransomware remains dormant on infected systems, attackers may reactivate it at any time. This "double extortion" is an all-too-real concern where ransomware is concerned.
- **Ransom Restore:** Hackers may demand payment to return the stolen data - with no guarantees that 100% will be restored.
- **Ransom Value:** The relative value of what is compromised also holds substance. For example, healthcare records of customers can be a very lucrative revenue stream for a hacker.

Ransomware protection begins with end user education, perimeter protection, and antivirus software.

The business downtime associated with a ransomware attack though can be detrimental, especially for SMBs that may be less resilient to revenue fluctuations - not to mention the additional costs for violations under privacy protection legislations such as HIPAA (Health Insurance Portability and Accountability Act of 1996).

Detect, Respond, and Recover: Synthesized Ransomware Protection

Ransomware protection begins with end-user education, perimeter protection, strong email security, and antivirus software. However, if ransomware finds its way onto PCs, mobile devices, servers, or SaaS accounts the door opens for ransomware to enter a network. This is why MSPs in particular need a comprehensive strategy for ransomware.

When evaluating ransomware protection, MSPs should **look for solutions that protect data across all of the devices and services** their clients rely on **at multiple points in the networks** they oversee.

First Encounter Detection: Email Security

Traditional email security solutions depend on data of previously known cyber threats and their penetration modes, thereby leaving protection gaps for new, unknown threats. Zero-day threats are evolving every day, and hackers are sophisticated enough to penetrate attack vectors beyond email.

Unfortunately, many solutions fall short in protecting the entire Microsoft suite. In order to ensure comprehensive ransomware protection, it is vital to have an Advanced Threat Protection (ATP) solution in place that can detect malicious malware attacks as soon as they are encountered.

Ransomware detection is important, because early identification can mitigate the impact of an attack.

Recovery Time & Downtime Cost Calculator.

View Now

Datto SaaS Defense stops cyber threats at the first encounter by:

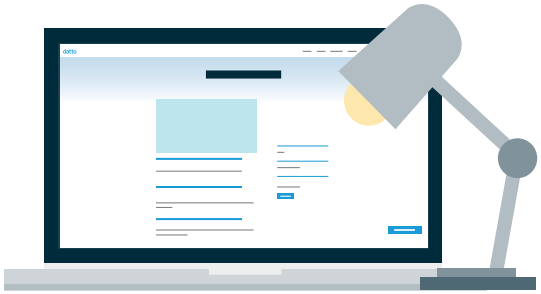
- **Identifies** and prevents threats that competitive solutions are missing including those that do not match any known malware signatures.
- **Defends** against malware and phishing threats that target Microsoft Exchange, OneDrive, SharePoint, and Teams.
- **Detects** unknown cyber threats at the first encounter with SaaS Defense and recover quickly from user error, ransomware, and other cloud data loss with SaaS Protection.

Ransomware Response, Perimeter Protection

Ransomware detection is important because early identification can mitigate the impact of an attack. Ransomware detection works by identifying patterns of change in the file types that are most likely to be encrypted by ransomware. One of the most effective defenses against ransomware can be found right inside of Datto RMM, which provides an **extra layer of security with native RMM Ransomware Detection.**

Datto RMM monitors for the existence of crypto-ransomware on endpoints using behavioral analysis of files and alerts you when a device is infected. Once detected, Datto RMM attempts to stop the ransomware process and isolates the device to prevent the ransomware from spreading. When Datto RMM is integrated with Datto business continuity and disaster recovery (BCDR) products, technicians can quickly recover from the ransomware outbreak by restoring the impacted endpoint to a previous state.

Partnering with a vendor that can deliver a unified ransomware protection solution can ease implementation and management.



Sign up for the Datto Blog today!

Sign Up Now

Recovery of Business Operations

Unfortunately, because ransomware has ever-changing tactics to gain entry into your networks the possibility still remains that a server or portion of your network can be compromised. This makes having a backup solution critical as a last means of defense in recovering from a ransomware attack.

This is where many modern server backup solutions offer a capability known as "instant recovery." If a ransomware attack takes down a primary server, a clean backup "image" is mounted as a virtual machine on the backup device or in the cloud. This allows normal business operations to continue while the primary server is being restored, reducing costly downtime to minutes rather than hours or even days.

Datto's Instant Virtualization enables this type of recovery where the backup server takes snapshots of physical or virtual servers, which are stored locally and replicated to the cloud. Point-In-Time Rollback for Servers, Endpoints, and SaaS applications. Point-in-time rollback or restore gives MSPs the ability to "turn back the clock" to a time before the ransomware attack occurred. In other words, you can restore systems to the state they were in immediately before the attack, ensuring minimal data loss. All Datto Unified Continuity solutions offer point-in-time rollback.

See how Datto solutions contribute to ransomeware protection.

View Now

Some backup solutions offer native ransomware detection capabilities. Since backup is an ongoing, scheduled process, adding ransomware detection makes a lot of sense to ensure the backup itself is free from ransomware as:

1. Some backup files are susceptible to ransomware, thus negating that ability to recover the infected system. Datto BCDR solutions utilize ZFS for creating backups that cannot be infected with ransomware.

2. It is important to ensure that no ransomware is lurking in the backed-up data, which is why a ransomware scan of the backup itself is critical.

Datto SIRIS, ALTO, and NAS devices feature ransomware detection by default

Choosing the Right Solution

Business data lives in many places—servers, desktops, laptops, and cloud-based applications. So, a solution that can protect your data wherever it resides is essential. Additionally, ransomware attacks can incur significant business downtime, cost, and distress if you aren't prepared. That's why it is important to deploy technologies that can get you and your clients back up and running quickly.

Ransomware detection, response, and recovery are important because early identification with comprehensive solutions can mitigate the impact of an attack. A complementary ransomware protection strategy requires a number of technologies and services. Partnering with a vendor that can deliver a unified ransomware protection solution can ease implementation and management.