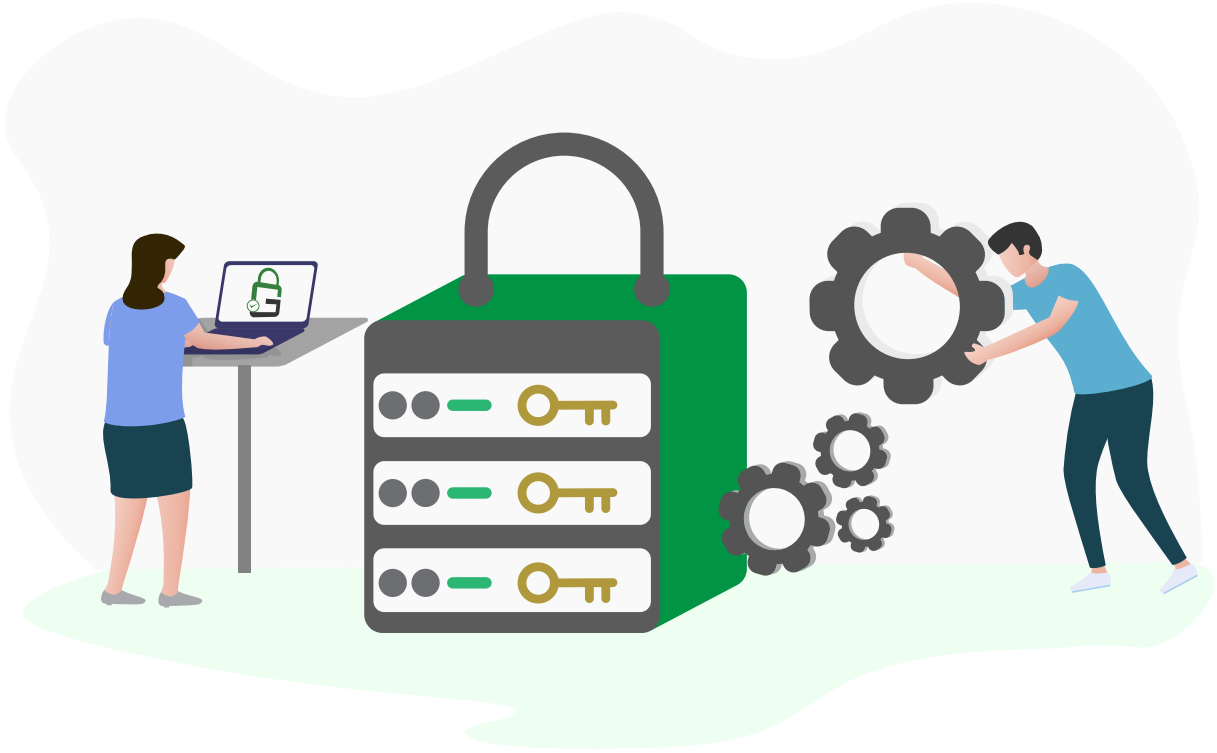
Garantir

1041 Market Street #302
San Diego, CA 92101
(858) 751 - 4865
info@garantir.io



Securing Enterprise Data From Ransomware Attacks

Preface

In the midst of a global pandemic and the resulting economic turmoil, cyber criminals launched ransomware attacks at an unprecedented rate in 2020. Throughout the year, ransomware attacks were both larger, in the magnitude of the ransom demands, and more frequent, with the prevalence of attacks reaching new heights.

Ransomware attacks have left no sector of the economy unscathed, with cyber criminals targeting everything from hospitals and universities to local government offices and private enterprises of all stripes. In many cases, the victims are forced to make payments to the attackers as quickly and quietly as possible.

As we look forward to 2021, ransomware attacks are a primary concern for all cybersecurity leaders. Many organizations are taking a hard look at their own weaknesses and vulnerabilities. If there is any silver lining to 2020's barrage of ransomware attacks, it is that many organizations are now ready to dedicate additional resources to improving cybersecurity. While there is no such thing as impenetrable security, there are steps that every organization can take to improve their overall security posture and significantly reduce the risk of a major breach.

This e-book will serve as a high-level guide to defending against ransomware attacks. The specifics will vary depending on your infrastructure-- whether it's fully in the cloud or a hybrid infrastructure of legacy data centers and clouds, either private or public or both-- but the recommendations laid out here are applicable for organizations of all sizes and in all industries.

> *"At least 966 entities were successfully attacked in 2019 at the cost of $7.5 billion."*
>
> Emsisoft State of Ransomware in the US: Report and Statistics for Q1 and Q2 2020

$233,817

The average ransom payment in Q3 2020 was $233,817, an increase of 108% from Q1 2020.

47%

In Q3 2020, 47% of ransomware attacks included a threat to publicize exfiltrated data.

19

On average, a ransomware attack caused 19 days of downtime in Q3 2020, up 19% from Q2.

Coveware Q3 2020 Ransomware Marketplace Report

Garantir

A Brief Synopsis Of Ransomware

Ransomware comes in many different flavors, but ultimately it all falls into one of two categories:

- **Confidentiality Attack** - ransomware that exfiltrates the victim's data with the intention of releasing it to the public, if the victim refuses to pay the ransom.

- **Availability Attack** - ransomware that seizes and encrypts the victim's data so the victim will never be able to regain access, unless they pay the ransom.

Of course, both varieties of ransomware are designed to extract financial resources from the victim. They only differ in their approach to achieving that goal.

Further, the two tactics are not mutually exclusive. Exceptionally ruthless attackers will demand one ransom in exchange for the return of hijacked data, then demand a second ransom in exchange for guarantees that a copy of the data will not be released to the public.

Common Delivery Methods

Cyber criminals use a number of different techniques to distribute their ransomware but email is by far the most common delivery method. The 2019 Verizon Data Breach Investigations Report found that a whopping 94% of malware is delivered through email. And, while this figure includes all forms of malware, not exclusively ransomware, data from the 2020 Verizon DBIR shows that 27% of all malware is, in fact, ransomware. Other ransomware distribution methods include sending infected files on social media and making infected files available for download on a public website, often one that is designed to look like the legitimate site of a trusted company.

In many cases, cyber criminals will not deploy ransomware immediately after gaining access to a corporate network. Instead, the attackers will move laterally within the network to gain access to the enterprise's decryption keys and backup databases before launching the attack.

If the decryption keys aren't properly protected, the attackers can steal the keys and simply decrypt data as they please, rather than going up against the virtually impossible task of breaking the encryption or brute forcing the key. Additionally, even if attackers can't compromise decryption keys, they will often corrupt or destroy backups before deploying their ransomware. This process doesn't allow the attackers to view or publicize the encrypted data, but it still compounds the impact of the ransomware, as the enterprise cannot restore their most recent backup to avoid making ransom payments.

Fortunately, there are a number of ways that enterprises can defend against ransomware. The following pages will describe 10 steps every security leader can take to keep their data and infrastructure secure.

Securing Data From Ransomware

1. Backup Your Data

To ensure that you can properly recover from an Accessibility Ransomware Attack, be sure to backup your data regularly. Systems that are critical to the enterprise should be backed up more frequently than systems that are less so. Backups should be stored offline in read-only fashion to ensure that attackers cannot delete, overwrite, or otherwise destroy the backups. For on-premise backups this means writing the backups to Write Once Read Many (WORM) storage devices and moving that storage device offline. For cloud backups, this means applying read-only controls to data and/or using cold storage.

2. Encrypt Data At Rest With A Self-Managed KMS

Encrypt data at rest using a self-managed Key Management Service (KMS), wherever possible. Using third-party encryption is better than not using any encryption, but it doesn't prevent the third-party from decrypting the data. This is especially important when the third-party is the one storing the data, as is the case with cloud providers. By encrypting the data before it is sent to the storage provider, you are able to take advantage of the storage provider's scale without sacrificing the confidentiality or integrity of your own data.

3. Protect Data At Rest With An Envelope Structure

Use enveloped encryption with an asymmetric master key (or key encryption key) to protect your backup files. Stated simply, this means encrypting your backup with a symmetric key and then encrypting the symmetric key with an asymmetric key. This technique comes with a significant added benefit: your backup systems do not need to have an online channel to the KMS because only the public keys are being used from the KMS. This significantly simplifies deployments and increases performance.

4. Keep Decryption Keys In A Disabled State

With enveloped encryption the public key used for encryption is separate from the private key used for decryption. Since the private (decryption) keys are only needed when restoring backups and are therefore not needed frequently, it is best practice to keep them disabled by default. Only when a restore is about to happen should these private key(s) be enabled, and then immediately disabled after they are used. The process for enabling, disabling, and using private keys should be tightly controlled and auditable. A tool like GaraSign provides out-the-box support for this.

5. Timestamp Your Data Prior To Encryption

While encryption is great for protecting the confidentiality of data, on its own it does very little to protect the integrity of data. In order to prove that your backups haven't been tampered with since they were created, cryptographically timestamp the backup before encrypting the data. This is useful later on to ensure that attackers haven't compromised the backups as well as to prove compliance during e-Discovery or other legal or audit proceedings.

6. Protect Data In Transit With TLS

Always protect data in transit with TLS 1.3, or at least TLS 1.2. First published by the IETF in August 2018, TLS 1.3 is considered the strongest security currently available for data in transit, though TLS 1.2 is currently considered acceptable if your enterprise has not yet made the update. Anything below TLS 1.2 should not be utilized.

7. Use Storage Provider Encryption Controls

Wherever available, use storage provider encryption controls, in addition to self-managed encryption. This adds an extra layer of encryption to your data and may provide more assurance to auditors of your environment.

8. Test Backup and Restore Procedures

Backups are only valuable if they can be restored. While ensuring the data can be decrypted is a critical aspect of the restoration process, other factors must also be considered, such as how to get the data from the backup location to where it is needed in order to be used. Verifying that this process works seamlessly is critical to ensuring minimal downtime, should the need arise.

9. Stop Attackers and Malicious Software

This is a subject all on its own that covers a wide range of topics. Topics include, but are not limited to, endpoint security, user training, log monitoring, and strong authentication.

10. Monitor, Maintain and Train

Like any system, your backup and anti-ransomware systems need to be monitored and maintained. The team members who use them need to be thoroughly trained. While keeping systems up-to-date with patches and upgrades is important, it must also be balanced with backwards compatibility, especially when dealing with long-term backups.

GaraSign: A Cryptographic Operations Platform

GaraSign simplifies ransomware protection by providing a secure and highly performant infrastructure for cryptographically protecting data that seamlessly integrates into your existing enterprise backup systems.

Superior Security For Private Keys

GaraSign is deployed on customer infrastructure between the HSM and signing clients, restricting those clients to proxied key access. The result is that private keys remain secured in the HSM at all times, while end-users can still use the keys to perform cryptographic operations like decryption.

Granular Security Controls

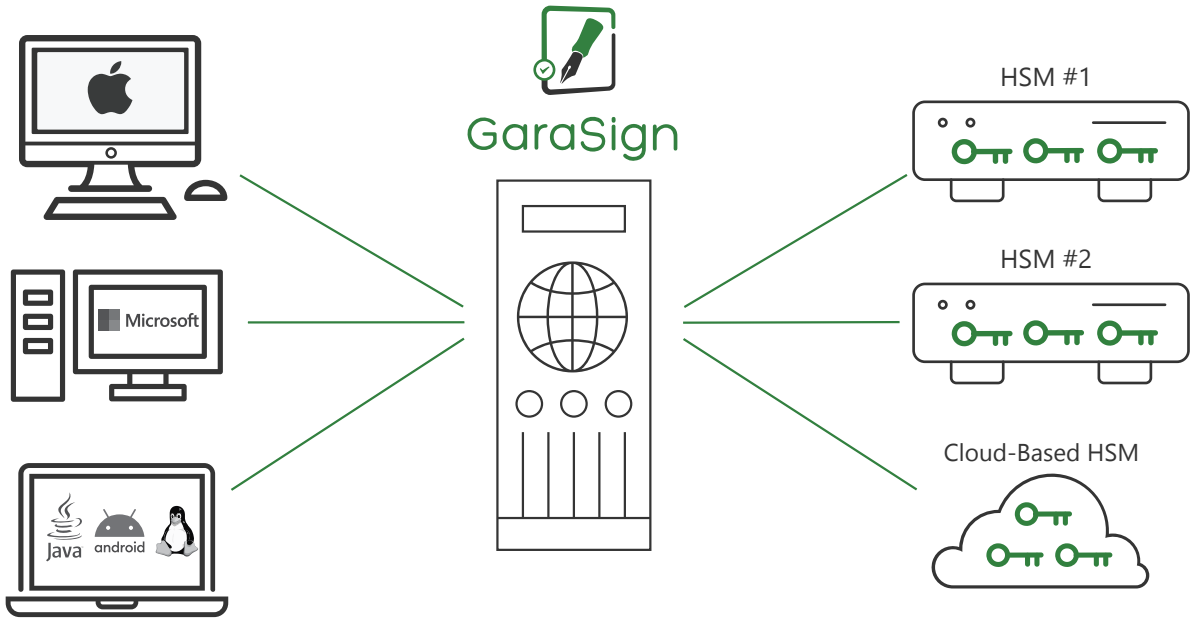
Since signing clients are restricted to proxied key access, GaraSign can integrate into existing processes to provide additional advanced security features: multi-factor authentication, device authentication, approval workflows, IP address whitelisting, notifications, and more.

Fast & Easy To Use

Using techniques like client-side hashing and enveloped encryption to keep the data sent over the network to a minimum, GaraSign provides extremely high performance. Additionally, GaraSign's native client integrations makes deployment easy while a centralized console ensures that key management is as simple as possible.

Native Client Integrations

GaraSign comes with a multitude of native client integrations, making it easy to deploy.



Garantir

Garantir is a cybersecurity company that provides advanced cryptographic solutions to the enterprise. The Garantir team has worked on the security needs of businesses of all sizes, from startups to Fortune 500 companies. At the core of Garantir's philosophy is the belief that securing business infrastructure and data should not hinder performance or interrupt day-to-day operations. With GaraSign, Garantir's flagship product, private keys remain secured at all times, while a client-side hashing architecture ensures high performance for all cryptographic operations, including code signing, SSH, S/MIME, document signing, TLS, secure backup, and more.

Garantir

1041 Market Street #302
San Diego, CA 92101
(858) 751 - 4865
info@garantir.io