Spin.ai

eBook

The Ransomware Prevention Guide for Enterprises

In the space of a few years, ransomware has gone from a niche security issue to a significant mainstream concern. The threat vector has grown more sophisticated and damaging at a terrifying pace. Today, no vertical and no company are safe. A successful attack can be devastating, incurring both a financial and a reputational cost.

How can enterprises protect themselves? With ransomware, the adage "an ounce of prevention is worth more than a pound of cure" applies. In this guide, we examine trends, costs, and targets – and lay out how businesses can protect themselves from a ransomware infection.

Table of Contents

Ransomware: **An Ever-Expanding Threat**

Cybercriminals love ransomware because, as a form of attack, it is highly effective and extremely lucrative. It has rapidly become a favorite tool among attackers because of the high likelihood that a victim will pay up.

Among organizations, 66% reported getting hit by ransomware in 2021, up from 37% in 2020.

Ransomware is a real threat to enterprise data: it can lead to unauthorized access to enterprise networks and cloud services, allowing threat actors to steal, destroy, or even replace files. Furthermore, cybercriminals often threaten to leak data to the Internet, which may lead to loss of business due to damaged customer confidence.

The spread of COVID-19 started a new wave of ransomware as more and more organizations began implementing remote workforces and sacrificing security.

Bolder, More Frequent, More Complex

The evolving business landscape, highlighted by the rapid adoption of remote/hybrid work, emerging computing technologies, IoT, and more, has expanded the ransomware threat environment.

Bad actors are getting bolder than ever. Among organizations,

66%

reported getting hit by ransomware in 2021, up from 37% in 2020, clearly signaling adversaries' evolving capabilities and scale.

Nearly

60%

of organizations reported an increase in the overall volume of cyberattacks, while 59% said cyber attacks had grown more complex. Cybercriminals are also increasingly becoming successful in encrypting data in their attacks: from 54% in 2020, data encryption in attacks rose to

65%

in 2021.

Since 2020, cybersecurity groups and government agencies have identified over

130 ransomware strains

Unfortunately, in recent months, we have seen some new variants take the headlines, **recording 722 attacks**. Here are some of them:

LockBit 2.0

LockBit has been around since 2019, formerly known for its "ABCD" ransomware because of how it would change file extensions. LockBit 2.0 is self-spreading and does not require any manual direction after being introduced to an environment.

Once LockBit successfully exploits vulnerabilities in a network — whether through social engineering, phishing, or other tactics — it begins its automated propagation, escalating its privileges through admin mimicking tools to gain further access.

Conti

Conti ransomware commonly makes its way into an environment through phishing emails. Threat actors craft emails that seem to come from reputable sources but contain corrupted links. When a user clicks such a link, it will push them to install TrickBot and BazarLoader Trojans, giving machine access to cybercriminals.

In addition, Conti is known for using the double-extortion strategy, where besides encrypting an organization's files, it copies some or all of the information and threatens to make them public unless the victim pays the ransom. Conti managed to obtain more than **$50 million** as a result of its ransomware tactics, according to a report. It has also become one of the most prolific ransomware types.

PYSA

The PYSA ransomware, retaining its name due to encrypting files with the .pysa extension — which stands for "Protect Your System Amigo" — implements a human-operated ransomware strategy. It is commonly known for picking high-value targets with system vulnerabilities or other weaknesses. These targets usually can and are willing to pay ransoms due to the sensitivity of the data they hold. PYSA attackers have a **58% success rate** of receiving the ransom payment after breaching an organization, according to an IndustrialCyber report.

A PYSA analysis by cyber intelligence company Prodaft found **747 victims** of this ransomware attack, which leaked confidential files of 309 victims in their public leak server. **The success (ransom/payment) ratio of the ransomware group is around 58%**.
The growing sophistication of ransomware fueled a show of confidence from threat actors. Last year, they launched ransomware attacks against 14 of the 16 US critical infrastructure sectors.

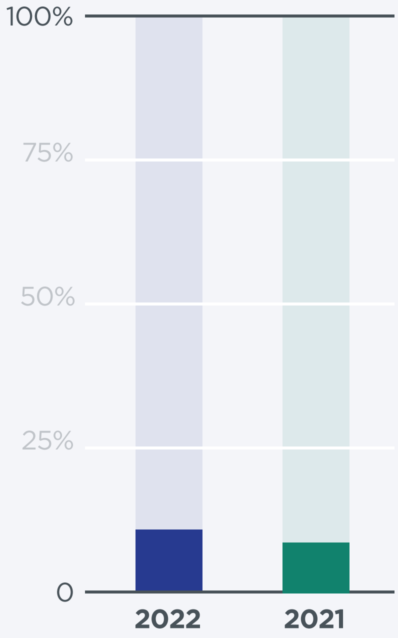
The evolving business landscape, highlighted by the rapid adoption of remote/hybrid work, emerging computing technologies, IoT, and more, continue to expand the already big ransomware threat environment.

The average cost of a ransomware attack sits at a huge $4.54 million, excluding the ransom cost.

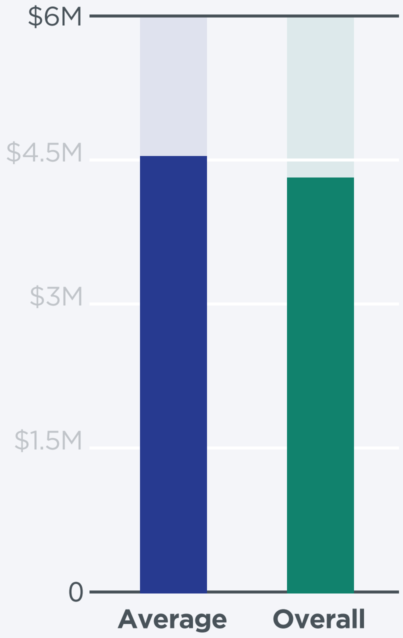
Ransomware Attacks Costing Companies More

In 2021, 11% of companies opted to pay a ransom of $1 million or more. This number ballooned from just 4% in 2020.

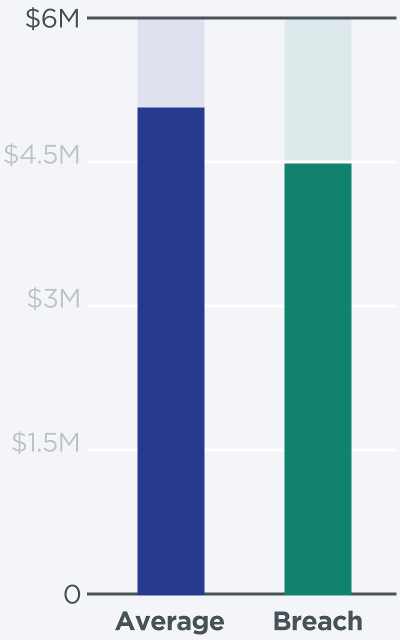
IBM's Cost of a Data Breach Report 2022 cites the following:



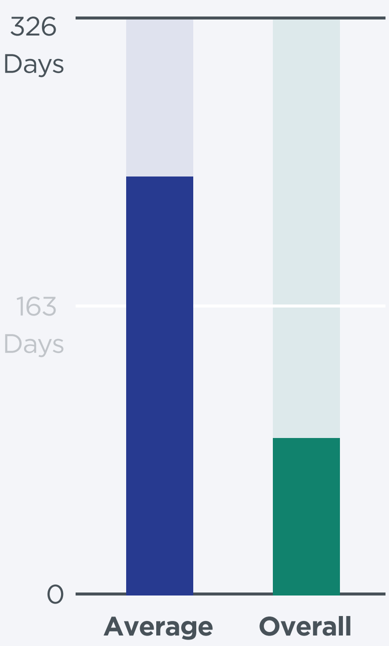
11% of breaches in 2022 were ransomware-based, compared with **7.8% in 2021.**



The average cost of a ransomware attack sits at $4.54 million, excluding the ransom cost. This number is higher than the **overall average cost of a data breach of USD 4.35 million**.



For those organizations that didn’t pay the ransom, the **average cost of the breach was USD 5.12 million**. Conversely, the **breach cost was USD 4.49 million for organizations** that paid the ransom.

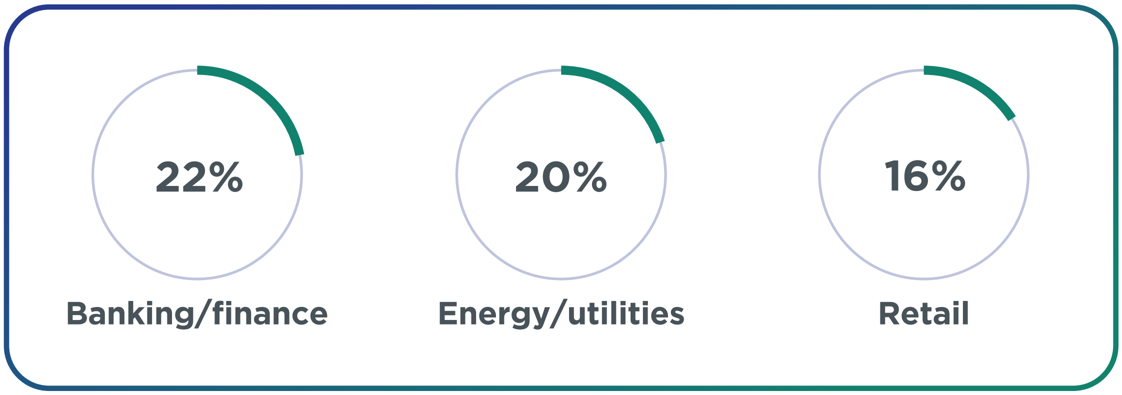


A ransomware attack took 237 days to identify and 89 days to contain, for a total lifecycle of 326 days.

Enterprises: **More Vulnerable Than Ever**

The average duration of ransomware attacks against enterprises has accelerated by 94%.

Ransomware attacks intensified in 2021, but **specific industries bear the bulk of the threat**. The most ransomware-attacked industries as of 2021 are:



These sectors accounted for **58%** of all ransomware incidents in 2021.

Cybercriminals are also improving their ransomware deployment. The average duration of ransomware attacks against enterprises has accelerated by **94%**. From initial access to successful decryption at scale, the whole process comes down from two months to less than four days.

5 Biggest Ransomware Attacks of 2022

A hacking group demanded a $1-million ransom plus a percentage of an unspecified fee from Nvidia to allegedly prevent the online leak of encrypted 1TB in exfiltrated company data.

Nvidia

Ransomware group Lapsus$ executed a ransomware attack against Nvidia in February 2022. The hacking group **demanded a $1-million ransom plus a percentage of an unspecified fee** from Nvidia to allegedly prevent the online leak of encrypted 1TB in exfiltrated company data.

The Government of Costa Rica

The national government of Costa Rica declared a national emergency because of a cyberattack. Ransomware group Conti claimed responsibility, targeting the country's Ministry of Finance. **Conti initially demanded a ransom of $10 million but increased it to $20 million**.

Another attack was launched in May 2022, this time perpetuated by the group HIVE. The group managed to breach Costa Rica's social security fund, **adversely impacting their healthcare infrastructure**.

Bridgestone Americas

In March 2022, Bridgestone, one of the world's leading tire manufacturers, suffered a ransomware attack. The incident **forced its computer networks to temporarily shut down production facilities in Latin America and North America**. Ransomware group Lockbit took responsibility for the attack.

SpiceJet

India-based airline SpiceJet experienced a ransomware attempt against its systems in May 2022. Although SpiceJet's IT security team successfully contained the attempted attack, it had already **forced the airline to delay many of its flights, inconveniencing hundreds of passengers**.

Bandai Namco

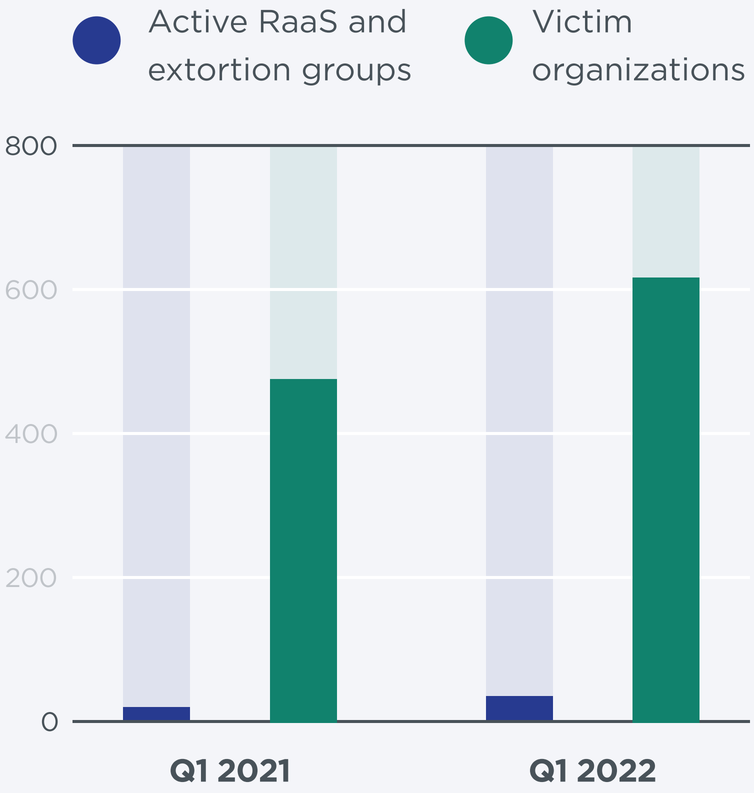
Japan's prominent video game studio Bandai Namco was also a victim of a ransomware attack. In July 2022, **ransomware group BlackCat breached Bandai Namco's computer networks and gained corporate and customer data access**.

Ransomware-as-a-Service: A Dangerous Development

Over an 18-month period, RaaS carried out over 60% of all cyberattacks.

Ransomware-as-a-Service provides would-be criminals with all the tools they need for carrying out a successful ransomware attack specific to a particular industry or business entity with little effort.

The number of RaaS and extortion groups **increased by 63.2% year-on-year** during the first quarter of 2022, inevitably resulting in more organizations falling prey to ransomware activity.



©2022 TREND MICRO

According to a study, more than

60%

of all cyberattacks in the 18 months until March 2022 were RaaS-based. The ease of use and the fact that this ransomware attack does not require technical expertise contributes to the growing appeal of RaaS.

Should you get **Ransomware Insurance?**

Enterprises planning to use insurance to hedge against a ransomware attack now face a harsh reality: higher premiums with minimized protection.

Organizations count on insurance carriers to cover losses and expenditures stemming from ransomware incidents, including data restoration, business disruption expenses, PR, and damage control.

Getting a cyber insurance policy against many cyber attacks, including ransomware, is a popular tactic for many businesses. In 2021,

75%

of all cyber insurance claims involved ransomware.

Are you willing to pay the price?

The costs of cyber insurance policies vary depending on factors such as industry type, size and nature of the business, annual revenue, and the kind and amount of information a company maintains. In the US, cyber insurance premiums range between **$500 to $5,000 annually**.

But as ransomware attacks continue to intensify, cyber insurance premiums have increased, **ranging from 50% to a 100% mark-up**.

Cyber insurance premiums increase, ranging from

50% to a 100% markup.

Insurance Providers are Getting More Meticulous

Enterprises planning to use insurance to hedge against a ransomware attack now face a harsh reality: **higher premiums with minimized protection**. Insurance providers are becoming more discriminating in the industries they are willing to cater to. Businesses in the government, education, healthcare, and utilities now struggle to secure an insurance policy.

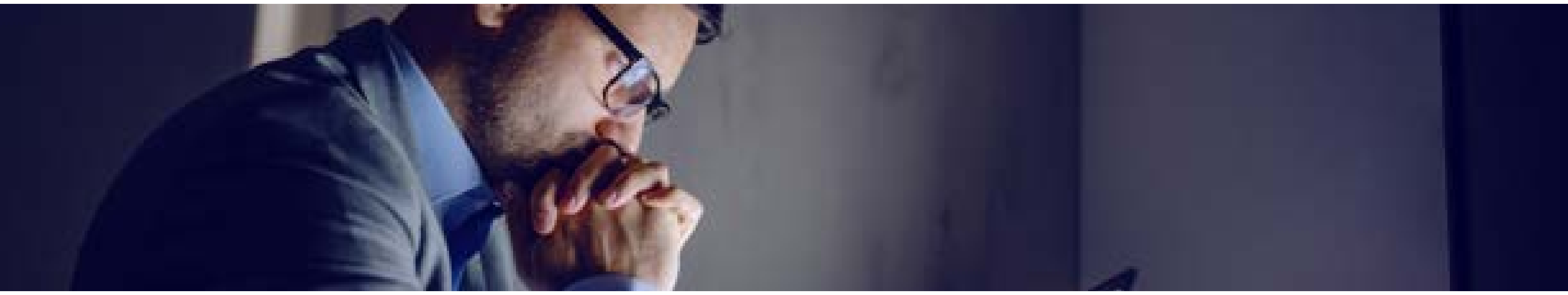
Providers also trimmed their insurance limits in response to the growing ransomware threat. The most they'll cover for a claim is now

$5 Million.

Tighter screening protocols are in place to ensure enterprises meet essential cyber insurance prerequisites. However, these protocols do not automatically reject companies that don't tick all the boxes. Instead, they receive offers of policies with higher rates and reduced coverage.

Providers also trimmed their insurance limits in response to the growing ransomware threat. The most they'll cover for a claim is now **$5 million**, down from their previous ceiling of **$10 million**. Meanwhile, other insurers have also closed shop and withdrew from the cyber insurance market.

Cybersecurity insurance is not a silver bullet. Instead, it's just one piece of the puzzle regarding comprehensive ransomware protection.



Should you **Pay The Ransom?**

Only 4% of enterprises that opted to pay the ransom successfully retrieved their data.

According to many law enforcement experts, including the FBI, organizations should not pay the ransom. Paying a ransom demand only encourages this type of cybercrime and funds it. However, having unreachable data due to ransomware encryption can be disastrous for many businesses.

When ransomware successfully infects an enterprise environment, there are only two ways to recover data:

- **Restoring from backup**
- **Paying the ransom**

However, there is no guarantee that attackers will uphold their end of the bargain once they receive the ransom payment.

Why do businesses pay the ransom?

Restoring from backups is preferable to paying ransom to cybercriminals in exchange for data restoration. Unfortunately, many organizations have found themselves in a position where ransomware has also infected their backups and business-critical production data. Hackers know that if they can encrypt backup files, they have a better chance of receiving the ransom payment.

Here are two main reasons why enterprises prefer to pay the ransom instead of restoring:

1. **The cost of downtime is too high.**
   Restore Time Objective (RTO) is a term used in data protection that describes the amount of time acceptable to the business without business-critical data. During this time, they may be able to operate in a degraded state.

   If the business has decided upon an RTO of 24 hours and restoring data infected by ransomware would take significantly longer – perhaps an entire week – paying the ransom becomes a more simple business decision.

2. **Cybersecurity insurance will offset the ransom.**
   Another factor that can weigh into deciding to pay the ransom demanded by cybercriminals is cybersecurity insurance.

   Since cybersecurity insurance can help any business offset the cost of paying a ransomware demand, many companies opt for paying the ransom instead of restoring data.

Does paying the ransom guarantee getting all your data back?

Unfortunately, a recent survey has found that only **4%** of enterprises that opted to pay successfully retrieved their data.

One prime example is the Kansas Heart Hospital in Wichita, KS. The ransomware that hit the hospital held several non-critical systems hostage with a ransom. Even though patient data and other business-critical systems were unaffected by the ransomware, hospital officials decided to pay a "small amount" demanded as ransom.

However, after paying the initial ransom demand to the hackers, they did not send the decryption key/tool as promised and demanded even more money.

Ransomware **Prevention Methods**

An estimated 54% of ransomware infections worldwide originated from spam and phishing emails.

As mentioned, preventing ransomware is undoubtedly much more desirable than recovering from a ransomware infection.

The following are some of the most effective ransomware prevention methods:

Have backups of business-critical data

Backups are arguably the most **effective means of preventing, protecting, and recovering from a ransomware infection**. Note that backups should also be protected by a layer of cybersecurity to protect it from ransomware infection, as well.

Educate end users

Train employees to identify suspicious and potentially malicious emails, files, websites, or applications. Poor user practices and lack of cybersecurity training account for 53% of ransomware's most common delivery methods.

Implement good email phishing/SPAM filtering

Filter infected links, attachments, and other files from spam emails. Spam and phishing emails are primary threat vectors for ransomware infection. An estimated **54%** of ransomware infections worldwide originated from SPAM and phishing emails.

Implement endpoint security

Endpoint security is necessary because every endpoint has more than **11 security controls** installed, which decay over time. When this happens, it creates various potential attack vectors. Endpoint security includes antivirus, anti-malware, and anti-ransomware solutions that scan and protect end-user clients.

Use firewalls

Block known malicious connections and IP addresses. Firewalls can read from IP threat lists which can help block malicious source network traffic, including those used by ransomware.

Use least privilege access

Ransomware can exploit overprovisioned privileges and access levels to spread across network environments. Having the least privileged access in place helps mitigate the spread of ransomware into the system. Least privileged access means users only have the absolute minimum required level of permissions to access resources on the network.

Use application whitelisting

Ensure that ransomware executables and other malicious codes will not be approved to run if it makes their way to an end-user workstation.

Secure or disable Remote Desktop connections

RDP vulnerabilities, like "Bluekeep," allow attackers to compromise and take control of remote RDP servers. If RDP connections exposed to the Internet are required, make sure to patch RDP servers: use multi-factor authentication to validate the RDP, and restrict access as much as possible via network or other means.

Logically and physically separate networks

Having an enterprise's network segmented and logically/physically separated helps limit potential widespread infection across all connected devices in a network environment.

Creating an Action Plan for **Ransomware Attack**

The ransomware threat has grown so large and significantly more sophisticated than ever. Cybersecurity experts urge organizations to have an action plan in case of a successful ransomware attack.

The following are a few recommended actions enterprises should take when infected by ransomware:

Isolate the infected device immediately

Take the device off the network as soon as possible. One of the quickest and easiest ways to do this is by disconnecting the network cable.

Isolate devices that are not infected

If a device has not been affected by ransomware, isolating it from the network can be a great way to ensure it is protected. This also helps contain and remediate ransomware infection.

Secure cloud drives and synchronization access

Disable synchronization of OneDrive or Google Backup & Sync for all users to avoid the spread of ransomware infection.

Verify backup systems and isolate those ASAP

Many variants of modern ransomware are looking for backup files. Take backup systems off the network or isolate them completely. Verify backup file integrity and backup repositories.

Enforce password changes of network accounts

As a proactive measure in case sensitive data or passwords have been leaked, enforce a password change for all accounts across the board.

Contact law enforcement

Immediately contact the Federal Bureau of Investigation (FBI) or local law enforcement authorities upon learning of a ransomware attack.

Comprehensive Enterprise Security: **The Best Defense**

Invest in an enterprise-grade cybersecurity solution

Regardless of size and industry, business enterprises will always be prime targets for ransomware attacks. Companies must invest in advanced technologies and tools to quickly detect ransomware-laced emails and applications and prevent infection.

Partnering with the right security services provider gives enterprises a comprehensive security suite built on the latest technologies, including SaaS ransomware protection, application security, threat monitoring and detection, and backup and recovery. Traditional cybersecurity tools can no longer hold up against constantly evolving digital threats, particularly ransomware, so advanced solutions are a necessity.

Ideal ransomware protection features

AI-powered ransomware monitoring

Ransomware monitoring has grown beyond human capability. Integrating AI and other specialized machine learning techniques will help detect malicious files, processes, and applications as early as possible to mitigate any ransomware attack before it can even start.

Insider threat detection

People within the organization can be the greatest threat to data, whether the threat is accidental, negligent, or malicious. An enterprise security solution with insider threat monitoring can screen external and internal communications for potential ransomware files and attachments. It can also alert security teams of anomalous and malicious insider behavior indicative of an eminent data breach or attack.

Access management

Prevent ransomware infection by controlling and monitoring user access to data, applications, files, and devices. Grant privileges to specific individuals only when their work requires it.

Remote workforce visibility

Remote workers use devices and equipment outside the traditional cyber security perimeter, making them attractive targets for ransomware attacks. Mitigate potential ransomware infection by implementing proper data access controls and proactively monitoring remote devices.

Make the **Best Choice**

SpinOne – The Best Option for Ransomware Cloud Protection

SpinOne is an All-in-One SaaS data protection solution that combines four critical modules – Ransomware Protection, Application Security, DLP, and Backup – into one platform. As a result, enterprises can manage their cybersecurity initiatives and backups of cloud data from a single-pane-of-glass dashboard.

SpinOne utilizes a Machine Learning (ML) based cybersecurity that detects and responds to anomalous behavior in an enterprise's cloud environment.

As prevention is the recommended way to deal with ransomware, SpinOne provides many powerful cybersecurity features to help prevent ransomware from infecting files.

- **Fully Automated Ransomware Protection** – Through the ransomware protection module, SpinOne detects any anomalous behavior, blocks the source of the attack, and reverts any changes made to files automatically with no human factor or agent required.
- **Risky Apps Protection** – SpinOne thoroughly assesses all third-party apps and browser extensions, outlining business, security, and compliance risks and allowing organizations to automate blocklisting/allowlisting through security policies.
- **Insider Threat Protection** – SpinOne gives enterprises visibility of employees with unscrupulous intent or a compromised account.
- **Brute force login protection** – Attackers trying to drop ransomware in an enterprise environment often use brute force attempts to find compromised credentials. SpinOne provides brute force login protection and reporting, giving enterprises visibility to any potential attempt to breach security.
- **Active alerting and reporting** – SpinOne provides real-time alerting and reporting on security issues in cloud environments as they happen.

Bolster **Ransomware Defenses Now**

Ransomware is an ever-growing threat to data, both on-premises and in the cloud. However, protecting an enterprise's environment with various layers of security can significantly reduce ransomware's damage to business-critical data.

Educating users, using effective email filtering, and deploying endpoint security are just three practical steps to prevent a ransomware infection. Knowing what to do and acting quickly and decisively when infected by ransomware can help prevent its spread.

Remember not to neglect cloud environments when protecting valuable data assets. Solutions that provide cybersecurity and data protection for any domain are crucial to protecting data. SpinOne provides both means of data protection in a unique solution that leverages machine learning to fight ransomware.

About **SpinOne**

SpinOne provides a comprehensive enterprise-grade data protection platform for mission-critical SaaS Apps. Designed to simplify the complexity of cloud security, SpinOne combines four robust solutions into a single, more powerful suite: SaaS Ransomware Protection, SaaS Application Security, SaaS DLP and SaaS Backup and Recovery. In addition, SpinOne integrates seamlessly with Google Workspace, Microsoft Office 365, and Salesforce, making it the perfect on-premise, cloud, and remote work security solution for modern enterprises.

Spin.ai

@ info@spin.ai ☎ 1 888-883-2993

REQUEST DEMO