Ransomware & Business Continuity for Data Infrastructure

Protecting Against the Threats of Ransomware On-Premises and in the Cloud

Market Landscape

The threat of cyber-attacks and specifically ransomware is real and top of mind for many IT security professionals. In the early 2000s, ransomware was perceived to be a threat to only small to medium sized businesses (SMB) with studies like The Beazley Report[1] indicating 71% of the attacks in 2018 targeted SMBs. Ransomware has quickly shifted into large enterprise businesses over the years and is and was much more ubiquitous than many once believed. According to the Harvard Business Review[2], in 2020 ransomware attacks were up 150% over the previous year, and the momentum continued to grow through 2021 and 2022. While cyber-attacks continue to rise in number, it is the sophistication of the attacks and the impact on businesses around the globe that is staggering. According to an article by Cloudwards[3], ransomware has cost the world's businesses and governments $20 billion in 2021 and is expected to rise to $265 billion by the year 2031. Below is a list of the largest ransoms paid in 2021, but beyond the ransom is the cost of remediation.

CNA Financial	$40M
JBS	$11M
Acer	$10M (offered)
Colonial Pipeline	$4.4M
Brenntag	$4.4M

Companies that pay the ransom must still go through an extensive remediation process of decrypting potentially millions of files, which alone could take weeks or months. While 32% of ransomware victims have paid the ransom in 2021[4], only 65% of their data was able to be recovered during remediation and just 57% of businesses are successful in recovering their data using a backup. The recovery process from ransomware alone has cost businesses $1.85M on average in 2021[5].

Furthermore, according to a 2022 SpyCloud survey[6], 90% of organizations say they were impacted by ransomware over the past 12 months. This is up dramatically from last year's 72.5%. While companies have strengthened their cybersecurity measures across the board, the criminals continue to find gaps whereby they are able to perpetuate these attacks.

QUOTE

> "90% of organizations say they were impacted by ransomware over the past 12 months. This is up dramatically from last year's 72.5%."

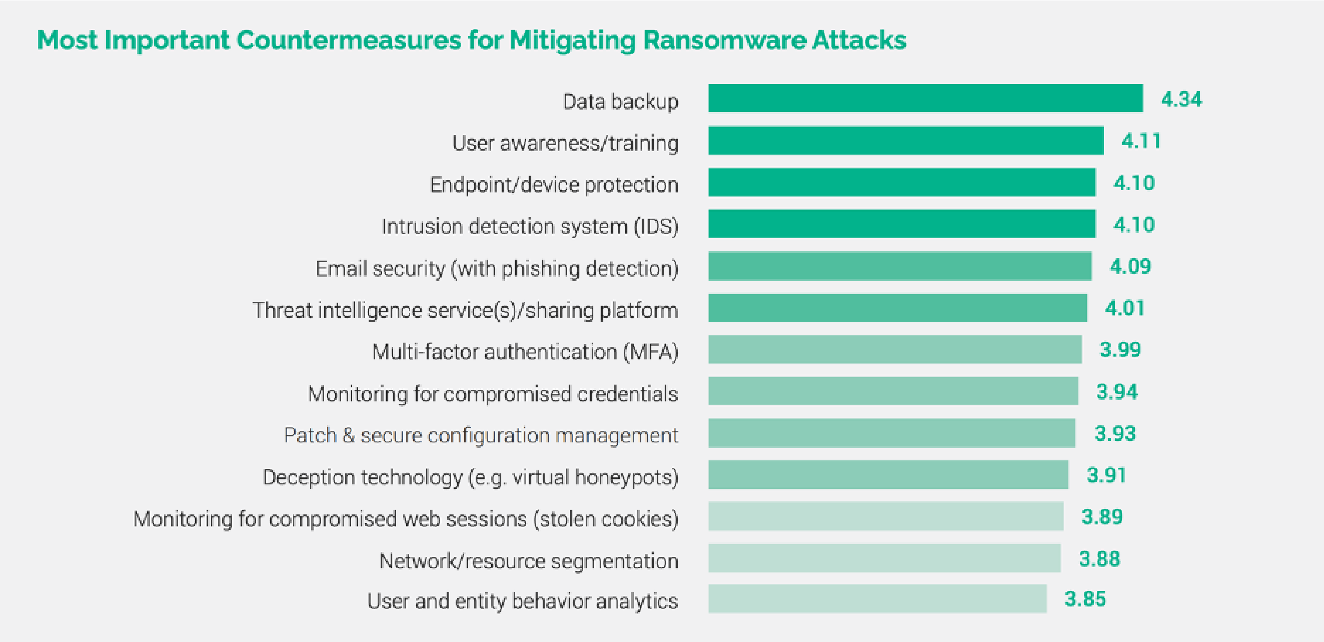

FIG. 1 The 2022 SpyCloud Ransomware Defense Report

The report goes on to show on a scale from 1-5, what these organizations say is the most important countermeasures for mitigating ransomware attacks. As you can see, data backup tops the list according to respondents with a score of 4.34.

Besides loss of data access, revenue, and the time of both employees and third-party agencies assisting in the remediation process, there is a more significant threat companies face: The impact on customer loyalty and trust. Another way of looking at this is "PR fallout". When organizations experience a disaster such as a ransomware attack and do not have the disaster recovery/business continuity plans and the operational tools in place to begin mitigation of the attack, including customer communication, it could have long lasting effects on the company overall. For example, the big retailer whose POS transactions were perceived as unsafe after an attack, may have turned customers away to competitors. Or the well-known financial institution with a long history of customer service is suddenly hit by ransomware and a data breach simultaneously where customer data was invasively collected and exposed, leaving customers questioning how secure their personal information truly is with this institution.

For those reasons and many others, organizations are looking for solutions to help increase their security score internally and keep their customers' data as secure and safe as they can. Now as you can see from this list in Figure 1, cyber resiliency is a multi-layered approach, and as the research has indicated the threat actors are becoming more and more sophisticated in their attacks.

THE DIFFERENCES BETWEEN RANSOMWARE AND DATA BREACH

A threat actor typically uses malware to encrypt an organization's data, which may include operational, financial, personnel, or customer data; the encrypted data then cannot be accessed by the organization until the ransom is paid and a decryption key is released by the attacker, hence the name ransomware.

SEE PAGE 4 TO LEARN MORE

The WEKA Data Platform

Beyond data backup, how does a data platform like WEKA help shore up your immunity to these attacks and strengthen your business continuity capabilities to mitigate extended loss or outage?

The WEKA Data Platform offers organizations additional layers of security that make it harder for would-be attackers to lock users out of their data and helps to ensure that the data can be recovered quickly and easily with authenticated mounts, encryption, snapshots, snap-to-object, and multi-tenancy segregation.

Authenticated Mounts

Admins can generate tokens that must be provided before mounting the filesystem. These tokens determine whether the client has permission to read/write and for how long before access is revoked prior to validating the permissions models on the filesystem, which provides an added layer of protection. Even if an attacker did manage to access a client system as an approved user, without these tokens they cannot mount any filesystem.

Encryption

The WEKA Data Platform supports encryption in-flight and at rest for all data while on the wire, as it lands on NVME storage, and when sent to backend object storage buckets. An attacker posing as a middleman to eavesdrop on the traffic will not be able to decipher the file data. Furthermore, the WEKA system is connected to the organization's Key Management Service, which constantly generates new keys as required, so that there is no single key that can be used to unlock all an organization's data. Data that is tiered to object storage or snapshotted and sent to object storage is encrypted as well.

Snapshots

WEKA supports instantaneous snapshots for all its filesystems, which is unique at exabyte scale. These snapshots can be immutable when sent to an object store WORM bucket and can always be used to instantaneously roll back a filesystem to its previous state within seconds.

Snap-to-Object

The WEKA Data Platform also supports sending snapshots to both local and remote object storage buckets. These snapshots can be used to send a copy to a remote version and/or write-once-read-many (WORM) bucket, where encrypting or deleting data is nearly impossible. A WORM bucket is an object storage bucket that is configured so that every dataset it contains has a retention period—once the dataset has been placed in the bucket it cannot be removed or changed before its retention period has expired. It is remarkably simple to periodically mount these WORM remote data copies and validate that the data is correct to catch a threat actor mid-attack. For example, once a week, provisioning a short-lived WEKA system that can mount the WORM remote data copy and confirm its accessibility and validity. The WEKA snap-to-object capability directly aligns with best practices for Backup and Disaster Recovery having multiple copies of data on separate media that is geographically separated from the primary source of data.

Multi-Tenancy Segregation

The WEKA Data Platform enables admins to create multiple separate organizations on a single system. Sub-organizations are allowed only to manage their own provided namespaces; the admin of the sub-organization cannot access other file systems across the organization, thereby limiting the potential scope of an attack even if a sub-organization is compromised.

Summary

Data security is a multi-layered challenge. Organizations must be vigilant about adding effective layers of protection to prevent ransomware attacks and take steps to ensure recovering backup data is a streamlined process should an attack occur. WEKA's enhanced security to reduce the risk and potential scope of ransomware attacks with advanced security features such as the ones mentioned above, help to simplify recovery even in a worst-case scenario.

As with other types of cyber threats, careful planning, the right tools, employee education, and multi-layer protection are all key to combating ransomware attacks—and WEKA's security and data protection capabilities can play an important role in helping to protect your organization's data. Additionally, IT organizations are adopting cloud technology for its fluid, on-demand scalability that supports diverse workloads at scale, such as data protection, and recovery. WEKA has built a software-only, high-performance file-based data platform that is highly scalable and easy to deploy, configure, manage, and expand. The design philosophy behind WEKA was to create a single data architecture that runs on-premises or in the public cloud with the performance of all-flash arrays, the simplicity and feature set of network-attached storage (NAS), the scalability and economics of the cloud, and the enterprise security and data protection features to mitigate data loss or data access in the event an attack occurs.

Common Cyber-Threat Situations

A threat actor typically uses malware to encrypt an organization's data, which may include operational, financial, personnel, or customer data; the encrypted data then cannot be accessed by the organization until the ransom is paid and a decryption key is released by the attacker, hence the name ransomware. In some cases, the attacker may make a copy of the data outside the target organization and delete the original data until the ransom is paid, at which time they restore all or part of it. This would be considered a data breach. The organization's challenge here is to detect when their data has been affected by the threat actors and if their data has been breached. This can be cumbersome given that these attacks usually take weeks to fully encrypt, copy, and delete the data.

Once the breach or attack has been confirmed, an additional challenge many face is identifying on what medium the backup sets available for recovery are stored, if they exist at all. The most common mediums are offline storage such as tape, nearline storage such as a backup appliance or an alternate storage cluster, or even a cloud repository. In sophisticated attacks, the threat actors may even delete remote copies of the backup sets' data that are intended for recovery.

According to the SpyCloud research report, organizations have implemented or plan to implement strict policies, processes, and procedures to thwart and prevent these types of attacks, such as user awareness/training (32.9%), multi-factor authentication (MFA) (50.5%), virus, malware, and phishing detection (52.4%), endpoint/device protection (45.9%), user and entity behavior analytics (UEBA) (33.1%), and more, but in many cases, threat actors are still outmaneuvering them.

[1] *The Beazley Report. https://www.beazley.com/news/2019/beazley_breach_briefing_2019.html*

[2] *Harvard Business Review. "Ransomware is spiking. Is Your Company Prepared?" https://hbr.org/2021/05/ransomware-attacks-are-spiking-is-your-company-prepared*

[3] *Cloudwards, "Ransomware Statistics, Trends, and Facts for 2022 and Beyond" https://www.cloudwards.net/ransomware-statistics*

[4] *"The Destructive Reality of Ransomware Attacks" https://www.avast.com/c-biggest-ransomware-attacks*

[5] *Sophos. "The State of Ransomware 2021"*

[6] *The 2022 SpyCloud Ransomware Defense Report*