WHITEPAPER

HOW TO PROTECT YOUR DATA FROM RANSOMWARE

The Register® | Lenovo

1. EXECUTIVE SUMMARY

The last decade has seen ransomware move from being a largely theoretical problem that affected a limited number of unlucky victims, to a pervasive problem for most organizations and an existential threat for an unfortunate few.

This has happened as the volume of data being generated and retained by organizations has exploded, driven in part by new workloads like AI and machine learning and advanced analytics.

Meanwhile, the pandemic gave bad actors a chance to raise their game. As companies switched to hybrid and remote working, stretched security teams left workers and their data more exposed.

This whitepaper sets out the scale of the ransomware threat, including how attackers are extending their targets beyond larger enterprises and critical infrastructure, putting medium and smaller organizations increasingly in the firing line.

It also explains why organizations need to adopt a defense in depth strategy, in order to protect their most valuable assets – their data and critical infrastructure – as well as their business overall. This means not just focusing on prevention, but on detection and mitigation, and, crucially, recovery to ensure they can get back to business quickly.

We will also explore how the underlying storage infrastructure has an increasingly key role to play, particularly when it comes to recovery, to ensure that a ransomware attack is an irritation, rather than a complete disaster.

2. INTRODUCTION

The roots of ransomware stretch back to the 1980s, when an unscrupulous individual first allied the idea of a Trojan that encrypted file names to an extortion scheme. But it was not until the mid-1990s that researchers conceived of adding public key cryptography to the mix, raising the possibility of victims permanently losing their data if they did not pay up.

By 2010, ransomware was a viable threat, though the real-world impact was perhaps dwarfed by hyperbolic headlines. However, recent years have seen a steady increase in the financial impact of ransomware gangs, fueled in part by the rise of Ransomware-as-a-Service (RaaS) gangs, and in part because cryptocurrencies have made it easier for them to collect and transport the ransoms.

Ransomware is a problem for everyone, not just large enterprises or critical infrastructure operators

The result is increasing activity by ransomware gangs, and more high-profile attacks, such as 2021's Colonial Pipeline and JBS USA attacks.

This all adds up to ransomware becoming not just a technical or business concern, but a national security concern.

The White House notes that victims paid up $400m in ransomware payments globally in 2020, with $81m in the first quarter of 2021[1].

The average ransom cost in 2021 was $170,404, according to the Sophos State of Ransomware 2021 report. But the total cost of remediating an attack grew from an average of $761,106 in 2020, to $1.85m in 2021. That's because of business downtime, lost orders, and operational costs.

Research by insurance giant AIG predicted $20bn of ransomware damage costs in 2021, compared to just $325m in 2015. Total global cybercrime damage costs are predicted to hit $10.5tn by 2025, AIG added. In cases where data is extracted by hackers, AIG reported that ransom and extortion claims costs had doubled[2].

AIG also noted that network outages due to ransomware attacks are getting longer, with seven to ten days being typical. And while lost orders in the short term are an obvious headache, how do you account for the longer-term impact on customer confidence? Likewise, what about the impact on suppliers, investors and other stakeholders?

Ransomware is a problem for everyone, not just large enterprises, or critical infrastructure operators. AIG said it had seen a 150 percent increase in the frequency of ransomware and extortion claims since 2018, and these were coming from "all sizes of company...across all types of industry."

A joint advisory from US authorities and the UK's National Cyber Security Centre earlier this year, said that attackers were "shifting away from 'big game' hunting in the United States", and towards mid-sized organizations. Meanwhile, the European Agency for Cybersecurity's most recent threat landscape assessment rated ransomware "as a prime threat" for the period.

FOOT NOTES:

1. https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/13/fact-sheet-ongoing-public-u-s-efforts-to-counter-ransomware/

2. https://www.aig.com/content/dam/aig/america-canada/us/documents/business/cyber/aig-ransomware-global.pdf

So it is important to understand the threat, acknowledge that anyone can be a victim, and ensure that systems are primed to detect ransomware, and put in place a strategy to respond if ransomware does breach their defenses.

3. YOU HAVE BEEN HIT BY A RANSOMWARE ATTACK? WHAT'S THE BEST OUTCOME YOU CAN HOPE FOR?

Ransomware is a pervasive, ongoing threat and it might seem tempting to default to a bunker mentality in response, banking on a fortress-like perimeter and constant surveillance to keep bad actors out of your systems.

But that is difficult to sustain in today's tech environment. Few experts think the traditional perimeter approach is sufficient, because the nature of ransomware attackers is to quietly slip into your systems and move, laterally, until they find the goods they are seeking.

Tech teams need automated scanning and detection, so that if intruders make it past the outer defenses, they can be unmasked and stopped before they do too much damage or exfiltrate data

A better approach is to adopt defense in depth, as recommended by government agencies such as the UK's NCSC[3], and the US' Cybersecurity and Infrastructure Security Agency[4].

This means organizations should practice basic security hygiene, to prevent attacks in the first place. This includes patching and updating systems and applications to minimize vulnerabilities; educating users about phishing and other threats; and requiring other safeguards such as multi-factor authentication, and strong passwords.

But tackling ransomware does not stop there. Some attacks will make it through, and this is where detection and mitigation come into play. Tech teams need automated scanning and detection, so that if intruders make it past the outer defenses, they can be unmasked and stopped before they do too much damage or exfiltrate data. And they should consider network level actions, such as segmentation, end-to-end encryption and least privilege.

And it is clear they need to increase their focus on remediation and recovery. Detection will count for little if the company is offline and unable to do business for hours, days, or longer. Recovery strategies should be in place and tested well before any attack, with staff drilled on exactly what they have to do.

WHAT DATA IS MOST AT RISK?

The first step is to analyze the organization's key data sources and their associated risk. What impact would losing access to a given data store have on the organization's ability to do business?

Large pools of historic data may be essential for training machine learning algorithms, but it might not

3. https://www.ncsc.gov.uk/news/joint-advisory-highlights-increased-globalised-threat-of-ransomware

4. https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C_.pdf

be immediately necessary to have this data back up and running in the immediate aftermath of an attack.

On the other hand, getting back in business might require a relatively small amount of data in the first instance – leaders need to know precisely what this is. For example, a financial firm's first thought might be to ensure its transaction records are safe. A manufacturing firm might have its PLM (product lifecycle management) data as the first order of business in any restore.

And an attack might have limited impact before it is detected. Companies need tooling that will allow them to identify the blast radius, and allow them to quickly restore only those files or volumes they need to.

HOW DOES THIS AFFECT YOUR RECOVERY?

Traditional backup approaches, typically with tape as the final destination, were focused on producing a complete record of all company's data, which would be held offsite. Although comprehensive, this approach can be unwieldy for quick business restoration.

Creating these backups is a time-consuming process which can interfere with production workloads. Worse, it might take days or weeks to carry out a restore.

Understanding the importance of particular data sources means the organization can think about how quickly they want to restore their data, and how much data – if any – they can afford to lose. It might not be necessary to have those pools of historic data up and running immediately. For historic data needed for compliance purposes, traditional backup approaches may be acceptable, even if recovery is measured in weeks.

$81m	**Ransomware fees paid out globally in Q120, The White House.**
$170k	**Average ransomware cost in 2021, Sophos.**
$1.85m	**Average cost of remediating an attack in 2021, Sophos.**
$20bn	**Predicted ransomware costs in 2021, AIG.**
$10.5tn	**Total global cybercrime damage costs in 2025, AIG.**

But if production data is disrupted, this affects the organization's ability to do business, right now. The victim will want to recover to a point minutes, or even seconds before the disruption hit.

SNAPSHOTTING

The answer to the backup/restore dilemma is snapshotting. A "snapshot" captures the state of the file system at the time it is taken, creating a read-only image of a volume. Subsequent snapshots record only the changes made since the previous snapshot.

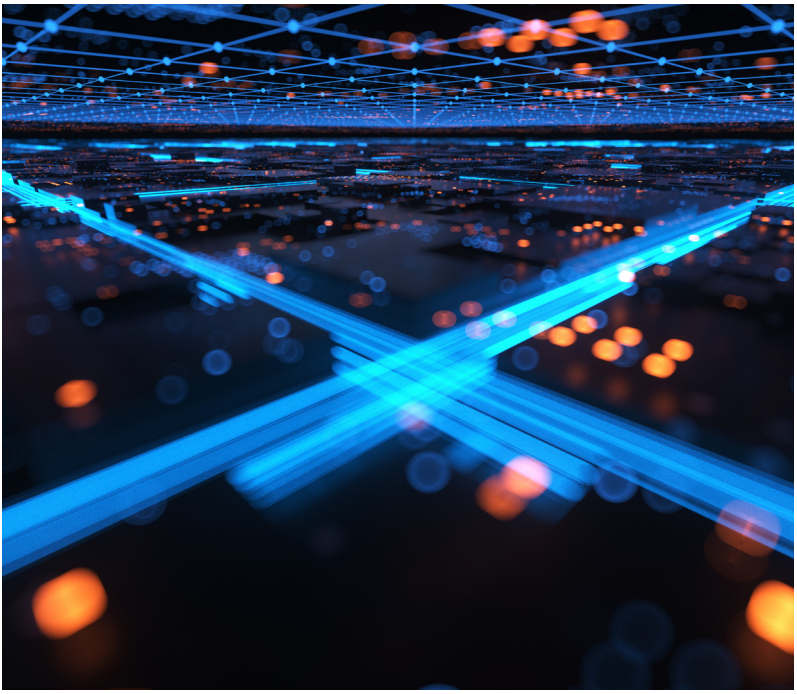
This provides the basis for an immutable record of the data at various points in time, allowing admins to roll back through previous versions to the latest safe version before an incident, such as a ransomware attack. It also allows for the recovery of not just entire volumes, but individual LUNS or files.

It is important to understand that not all snapshotting is created equal. Snapshots themselves can constitute a data management challenge, with organizations potentially looking to do 100s or 1000s of snapshots a day. In some systems, snapshotting is effectively a bolt-on, added on top of the underlying block structure. This is unlikely to be as time or space efficient as snapshotting that is integrated into the operating system.

Similarly, customers should consider how their data infrastructure's snapshotting capability integrates with other parts of their backup and recovery stack, such as Veeam, Veritas, or Commvault. This could entail reexamining backup and recovery options in the face of rising ransomware, but this does not necessarily mean existing investments and partnerships should go to waste.

WHAT ABOUT AIR GAPPING?

Air gapping has long been an essential part of backup and recovery strategies. The traditional rule was 3-2-1, meaning three copies of the data, on two different media, with one copy being held offsite.



But what does this mean in the modern world? Physically separate, non-networked media held offsite will of course be inaccessible to attackers. But, as we've seen, it's also inaccessible to the data pros looking to ensure an organization's systems are back up and running within minutes.

So, they will want to consider what constitutes a "virtual air gap." Immutable on-premises copies will be part of this – if an attacker does reach the data they are unable to change it – while preserving the ability to instantly restore.

Further security and peace of mind will come with off-premises capability in the form of immutable copies held in a private or public cloud, or clouds. Again, a platform's ability to integrate with other services comes into play here.

ATTACKERS CARE ABOUT YOUR DATA PROTECTION SYSTEMS TOO

Throughout this process, tech teams should bear in mind what their ultimate aim is. In the vast majority of cases this will be to get back up and running in minutes, without losing business, without losing vital data, and without paying the ransom.

Attackers know this too. They are known to analyze their victim's data infrastructure, identify potential weaknesses in recovery procedures, and set their ransom demands accordingly.

If a ransomware gang can be sure that an organization is relying on a physically separate tape backup, they know that the prospect of paying a high ransom might be more palatable than kicking off a data restore process that will take days or weeks, and which may not be ultimately successful. And if they find their way to a connected backup, you can guarantee that they will trash that before running the chance of detection by locking production data, virtually ensuring an even higher payout.

4. THE ROLE PRIMARY STORAGE SHOULD PLAY IN YOUR DEFENSE IN DEPTH STRATEGY

A ransomware attacker's ultimate destination is your organization's on-premises storage infrastructure. If this does not offer the performance or features needed to underpin your defense in depth strategy, including the appropriate snapshot and backup tooling, and the ability to quickly restore, all your other precautions may count for nothing.

Lenovo's DM series of all-flash arrays span entry level to high-end NVMe solutions. The CRN award-winning DM5100F All-Flash Array, in particular, is akin to plastic building blocks in that it offers the flexibility for businesses to start small and steadily build up capacity to meet most needs. It provides a path from a single SAN solution to scale up to a unified edge to cloud platform with enterprise class features. A single device scales up to 88PB of raw capacity, with up to 12 devices in a single cluster[5].

The DM series gives organizations of all sizes access to the sort of data resilience and management that were previously the preserve of high-end, enterprise systems

SNAPSHOTTING AT ITS HEART

The DM series is powered by the ONTAP operating system, which has snapshotting capability at its heart. As we've seen, some systems provide snapshotting capability as a bolt-on, which has implications for space efficiency, ease of management, and integration with other backup and recovery technologies and services.

The DM series snapshotting capability supports up to 1023 snapshots per volume. Snapshots are read only, providing protection against corruption by a ransomware attack. A snapshot takes less than a second to create and provides the basis for near instantaneous restores with flash-based arrays, whether the trigger is accidental deletion, or a full-blown ransomware attack. Restores can be at file, LUN or full volume level. This is, obviously, a far quicker option than a full backup and restore using a traditional architecture.

Snapshots can be scheduled but can also be triggered by the host system's own integrated security features.

The DM series gives organizations of all sizes access to the sort of data resilience and management that were previously the preserve of high-end, enterprise systems.

INTEGRATION

Lenovo's DM series provides integration with Veeam, Veritas, Commvault and other providers, who provide snapshotting and backup for VMs. So, admins are able to manage their data protection and backup for multiple data and application types from a single platform.

The DM series has partner-based solutions for additional built-in ransomware detection and

5. https://www.lenovoxperience.com/newsDetail/283yi044hzgcdv7snkrmmx9okesnwqxuzayrlke1e8sv4ubs

protection such as ProLion's CryptoSpike which uses AI to monitor file system behavior and block known ransomware signatures and file types. This gives admins the ability to track file "entropy" and changes, alerting them to suspicious activity that can be a precursor to a ransomware attempt.

Few organizations exist as an island. The DM series has built-in integrations with key enterprise cloud providers, including AWS, Microsoft, Google and IBM, allowing customers to migrate, replicate and tier data to multiple clouds, and providing the virtual air gapping needed to ensure complete protection against cyber attackers.

ALWAYS UP TO DATE

The DM series is available under Lenovo's TruScale Infinite Storage program. This means infrastructure can be procured on an OPEX basis, thus providing a cost-effective and immediate benefit to operational security.

The program includes regular health checks, and ensures upgrades and patches are automatically applied, to ensure that storage has the latest security updates to provide the most up to date protection.

With TruScale Infinite Storage, on-prem storage infrastructure is deployed with guaranteed technology upgrades that are transparent to the customers' operations and eliminate costly data migrations. In this way, organizations can focus on managing their data with the latest technology and avoid the limitations of aging hardware and the associated security risks this implies.

5. CONCLUSION

Ransomware is a clear and present danger, and most organizations are aware of the ramifications of an attacker successfully seizing control of their data.

With attackers going beyond "big game hunting", medium-sized organizations must understand that they too are squarely in the firing line.

They might think that if enterprises and national level organizations struggle to hold back the tide of ransomware, and recover when attackers do break through, what hope is there for them? They might imagine they simply don't have the resources to detect and mitigate the threat.

But they would be wrong. They can ensure they follow best practices around prevention, detection and mitigation, and recovery. They can be clear-eyed about what data is most critical to them, and make sure they understand the specific roles their data infrastructure choices play in protecting them from attack.

By combining the right practices, and the appropriate storage infrastructure and tooling, they can minimize the chances of being hit in the first place, maximize the chances of being back up in operation quickly, and eradicate the need to put "ransom" down as a cost of doing business.

6. ABOUT LENOVO

Lenovo Infrastructure Solutions Group (ISG) is a smart infrastructure solutions provider to organizations of all sizes. Our technology and insight power the data-centered heart of smarter retail, smarter manufacturing, smarter cities, smarter healthcare, smarter finance, and beyond. Through edge and cloud computing, analytics and artificial intelligence, and Infrastructure-as-a-Service via TruScale, we deliver Smarter Technology for All. We're the only data center provider with end-to-end manufacturing. We own our entire supply chain for everything we build, to deliver a level of security and seamlessness that no one else can, anywhere in the world.