UNITRENDS MSP

The Unitrends MSP State of Ransomware Survey Report 2021

msp.unitrends.com

Introduction

Unitrends MSP surveyed more than 200 IT professionals from MSP organizations worldwide to learn about how they are adapting to the threat of ransomware and advanced cyberthreats to protect clients and internal organizations. The result is a wealth of data and insight that ranges from identifying how ransomware is targeting their clients and strategies for prevention and mitigation, to ways to help clients recover from ransomware attacks.

Our research ensures strong representation from MSP organizations of varying size throughout the Americas, EMEA and Asia Pacific regions. We've included a Table of Figures at the end of our report, which breaks down respondents by organization employee size (Figure 1), number of endpoints managed (Figure 2) and vertical/industry focus (Figure 3).

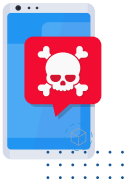
AMERICAS
84%

EMEA
3%

APAC
13%

RESPONDENTS BY REGION

How to mitigate ransomware for clients



Key Findings

1. A majority of MSP customers have experienced a ransomware attack

It's estimated that an organization falls victim to a ransomware attack every 11 seconds. Over the past year, ransomware attacks have grown increasingly sophisticated. Some of these methods include increased lateral movement through an infected client to disable as many machines as possible, the persistence of human-operated ransomware, and highly targeted spear-phishing campaigns through the use of techniques such as domain spoofing. Only 4.59% of our respondents reported that they've had no clients affected by ransomware.

2. The majority of MSPs report that their clients are either somewhat prepared or not prepared to face a ransomware attack

About 49.71% of respondents reported their clients are only somewhat prepared to handle this threat while 6.94% reported their clients are not prepared at all. See Figure 7 in the appendix for full results. It's no surprise then that ransomware cases spiked globally during the COVID-19 pandemic, with many employees working under a completely new set of parameters since then. Work from home (WFH) employees even in hybrid models have adopted new environments rife with distractions that lead to lax safety precautions and poor IT visibility, including the increasing use of Shadow IT. As a result, these poorly prepared corporate servers face high potential risks as users connect from less secure WFH networks.

3. Healthy levels of MSSP partnerships indicate that MSPs aren't combating current threats alone

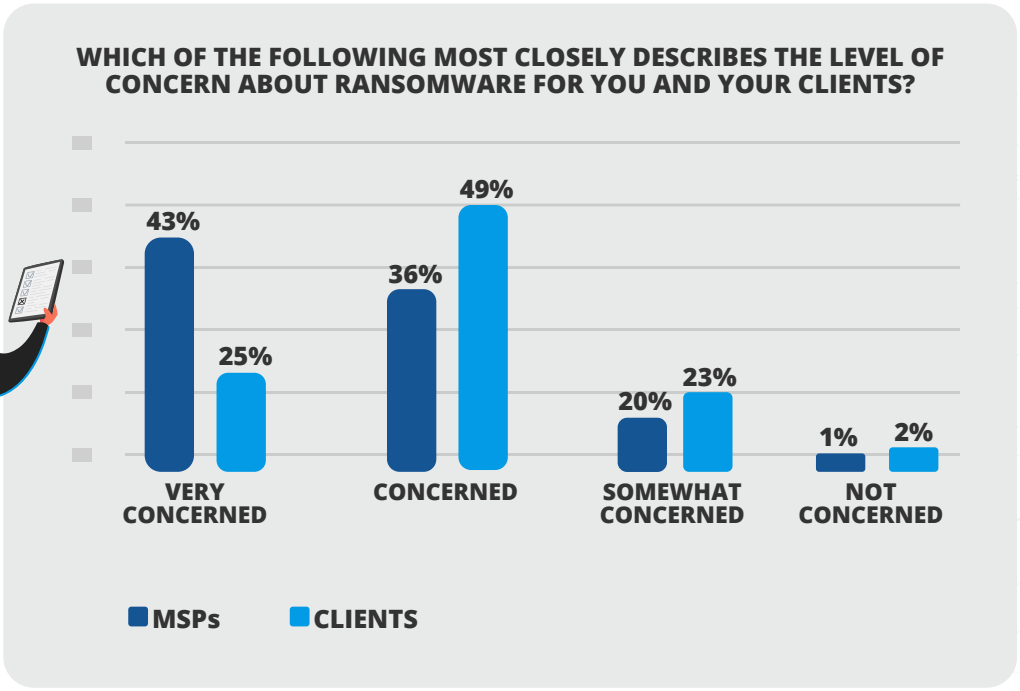
About 80.39% of respondents indicated that their organization has partnered with a managed security services provider (MSSP). Whether to minimize costs, extend their team, or gain visibility and insights into advanced threats, many MSPs are leveraging the benefits of partnering with an MSSP. With cybersecurity concerns increasing across organizations, MSSPs provide expertise on tactical threat hunting, monitoring and analysis, enabling internal security teams to focus on more strategic security projects.

1. https://purplesec.us/resources/cyber-security-statistics/
2. https://blog.morphisec.com/three-trends-ransomware-attacks-more-dangerous

Increased Concerns Over Ransomware

The majority of our respondents (89.02%) feel that ransomware has become a significant risk in the last 24 months. About 84.12% anticipate the rate of ransomware attacks to either worsen or remain about the same over the next year. Conversely, less than 2% of respondents believe the threat of ransomware has diminished and only 4.71% anticipate the threat of ransomware will diminish over the next 12 months. See Figure 5 in the Appendix for full results.

These sentiments are reflected in the respondents' level of concern about ransomware, with 42.77% of MSPs indicating they are very concerned about the threat. Respondents indicated that while their clients are aware of the threat, their level of concern is somewhat less so. Only about a quarter (25.43%) of respondents indicated that their clients are very concerned about the threat.



Interestingly, of the 1.73% of MSPs that stated they are not concerned about ransomware, all also indicated they are confident in their ability to recover from an attack. Many have done so first-hand. Increased confidence due to successful recovery has in part alleviated their concerns over the threat.

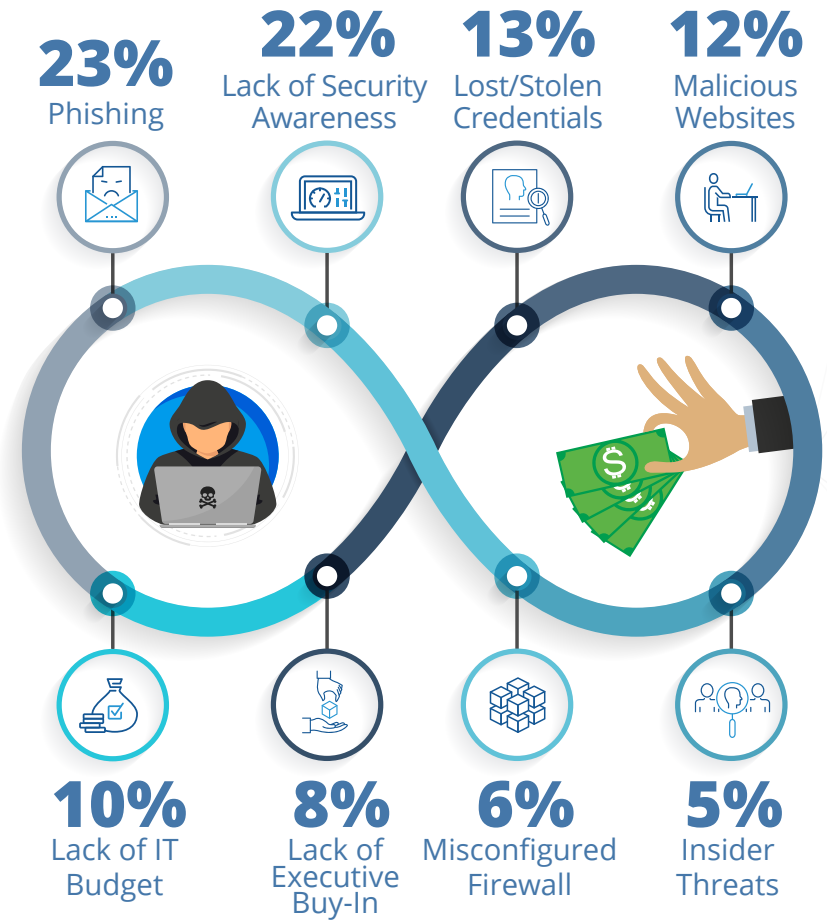
Causes of Ransomware

Ransomware attacks are increasingly diverse, sophisticated and dangerous. Attacks that rely on social engineering rather than technology (spear-phishing, brand impersonation and account takeover) are on the rise, making human activity, both by internal and external actors, a primary security risk. Rather than deploying a mass phishing attack with a broad approach, adversaries determine their intended target and customize their messages and delivery to be as realistic as possible in highly targeted spear-phishing attacks.

MSPs are aware of the changing threat landscape, citing phishing (22.97%), a lack of security awareness (22.56%) and lost/stolen credentials (13.21%) as the leading causes of ransomware attacks. Despite understanding these risks, only 17.91% of MSPs report implementing security awareness training while only 14.72% have implemented email/anti-phishing protection. See Figure 6 in the appendix for a full breakdown of environmental controls implemented.

Preventing or overcoming these attacks requires a multi-faceted, layered defense. Unfortunately, ideating a plan of defense is often easier than implementing one. About 9.55% of MSPs cited a lack of IT budget as a leading cause of ransomware attacks, with another 8.33% reporting a lack of executive buy-in.

WHAT ARE THE LEADING CAUSES OF INFECTION?



Ransomware Targets

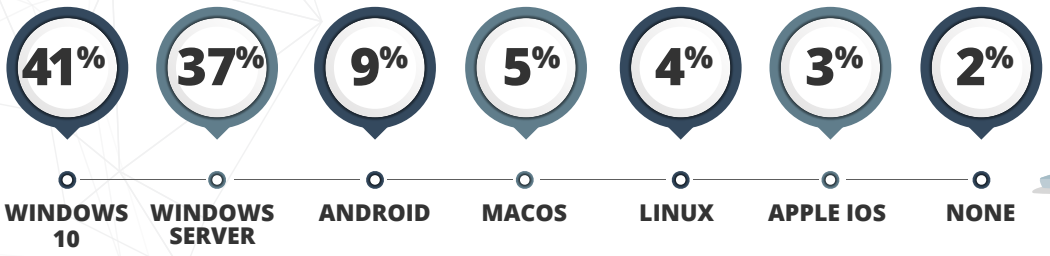
The Windows operating system (OS) represents a massive share of the global OS market, with more than 70% share of desktop OS and 72% of server OS.[3, 4] Despite massive adoption, ransomware security remains a major concern for organizations running the Windows operating system. As per the CVE database, as of 2020, more than 660 "dangerous" security gaps were attributed to Windows operating systems, with 357 of these vulnerabilities relating to Windows 10.[5] Beyond backdoors found in the OS, users may be at increased risk due to the transition to remote work, with the potential for threat actors to attack security vulnerabilities through connected devices. Being the world's most popular operating system has left a target on the proverbial backs of Windows systems, with Windows machines being the target of 83% of malware attacks during the pandemic.[6]

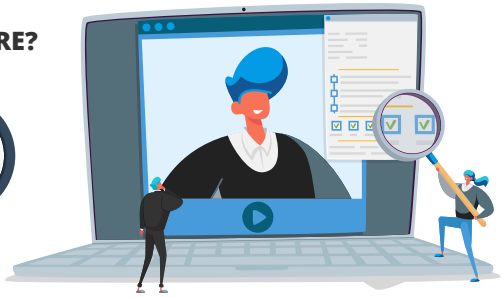
The experience of our MSP respondents echoes the sentiments of the security community at large; they've seen the greatest number of ransomware attacks targeted towards clients' Windows machines. Respondents indicated 40.77% of the observed attacks targeted Windows 10, with another 36.61% targeting various versions of Windows Server OS. Unfortunately, Windows is not the only OS under attack. Nearly 1 in 10 attacks targeted an OS other than Windows such as MacOS (4.46%) and Linux (4.17%).

Beyond servers and desktop machines, the proliferation of mobile devices, largely unprotected by antivirus or other security software, has led them to become the latest target for threat actors. Koler, a malware that spreads via text message, has been observed displaying localized ransomware messages in at least 30 countries, with 75% of their infections being in the U.S.[7]

Regarding mobile OS, our respondents noted that the Android operating system was targeted by ransomware at nearly three times the rate of Apple iOS. About 8.63% of all observed attacks targeted Android compared to 2.98% for Apple iOS.

WHAT CLIENT OPERATING SYSTEMS HAVE YOU SEEN TARGETED BY RANSOMWARE?



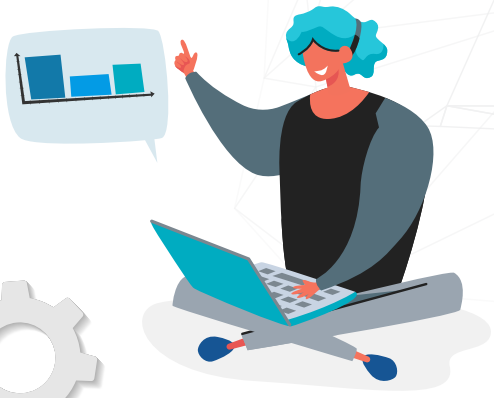


3. https://www.statista.com/statistics/268237/global-market-share-held-by-operating-systems-since-2009/
4. https://www.statista.com/statistics/915085/global-server-share-by-os/
5. https://www.pcmag.com/news/windows-computers-account-for-83-of-all-malware-attacks-in-q1-2020
6. https://www.pcmag.com/news/windows-computers-account-for-83-of-all-malware-attacks-in-q1-2020
7. https://blog.knowbe4.com/evolution-of-mobile-ransomware

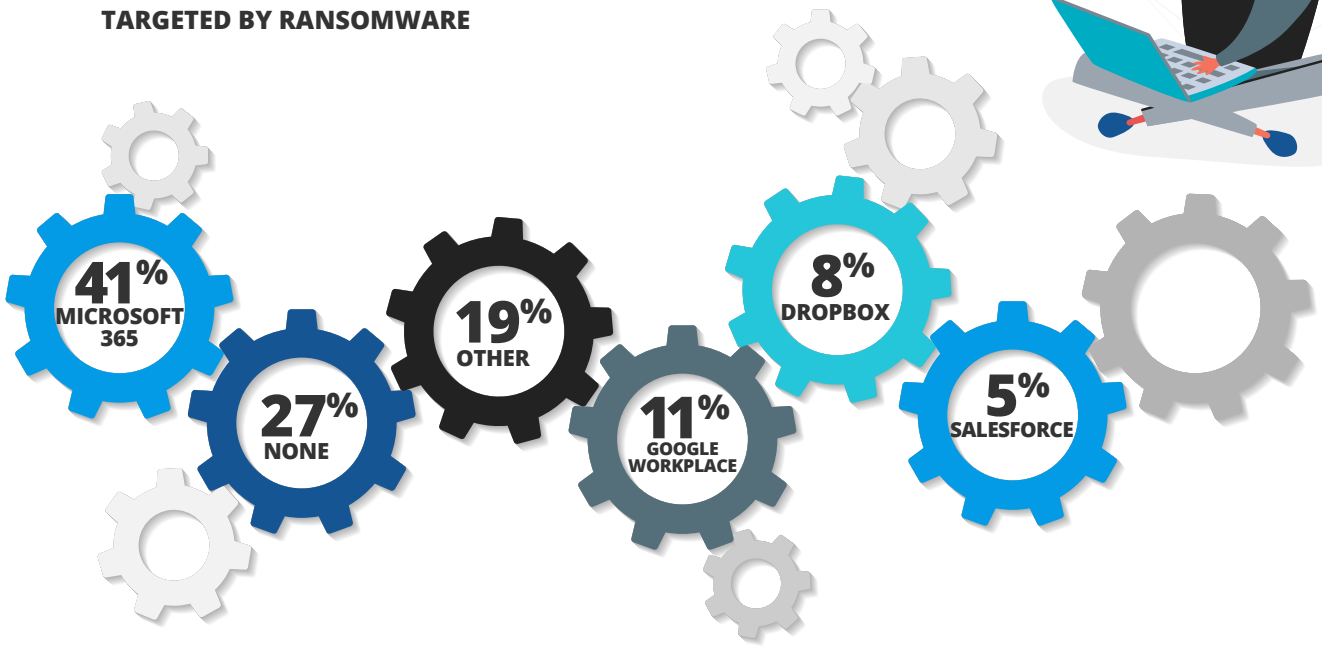
Respondents identified human activity, such as phishing and lack of security awareness, as a leading cause of malware attacks. Threat actors are changing tactics to adopt to today's distributed enterprise. Organizations must be prepared to protect all workloads, not only on-premises systems.

Nearly three-quarters of all respondents revealed their clients' SaaS applications are under attack. SaaS applications that serve as important document stores, privy to potentially private and sensitive data, are leading targets. About 29.82% of attacks observed were against the Microsoft 365 platform with another 10.55% against Google Workplace. About 7.80% and 5.05% of observed attacks were against Dropbox and Salesforce respectively.

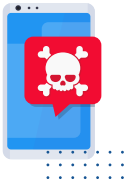
Microsoft and other SaaS providers operate under a model of shared responsibility.[8] This means that accounts, identities, devices, information and data are the responsibility of the customer to secure. Microsoft, Google and other SaaS providers cannot protect your data from the deluge of socially-engineered attacks that proliferate the threat landscape today. Security awareness, anti-phishing tools, and ways to identify and secure accounts at risk is paramount.



TOP CLIENT SAAS APPLICATIONS TARGETED BY RANSOMWARE



8. https://docs.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility



Ransomware Prevention and Recovery

Defending clients or organizations against ransomware requires a multi-pronged, continuous effort that combines end-user training and awareness, security and environmental controls, and a thoroughly tested business continuity and disaster recovery (BCDR) strategy.

Our respondents have implemented a series of measures to secure users, networks and backups from adversaries. About 69.66% of respondents employ multiple layers of defense (i.e. a combination of end-user training, immutable off-site backups and file system monitoring).

The two most popular prevention strategies to secure backups involve getting a copy of backups stored in an alternate location (35.95%), split between 22.44% of respondents who remove backups from the network on removeable media (i.e. HDDs) and 13.51% who leverage immutable cloud storage. About 19.61% of respondents have implemented end-user cybersecurity training.

Another popular technique is proactively monitoring file systems for anomalous activity (16.56%), a counter to more recent ransomware techniques such as gestation and dormancy, where the malware attempts to disable machines, backups and accounts by spreading through the network leveraging stolen credentials before locking machines and launching the ransom demand. [9]

About 15.69% of respondents have deployed a non-Windows-based backup solution to differentiate the backup environment and camouflage backup files signatures from malware seeking Windows-based extensions, increasing the level of difficulty to access the system for potential attackers.

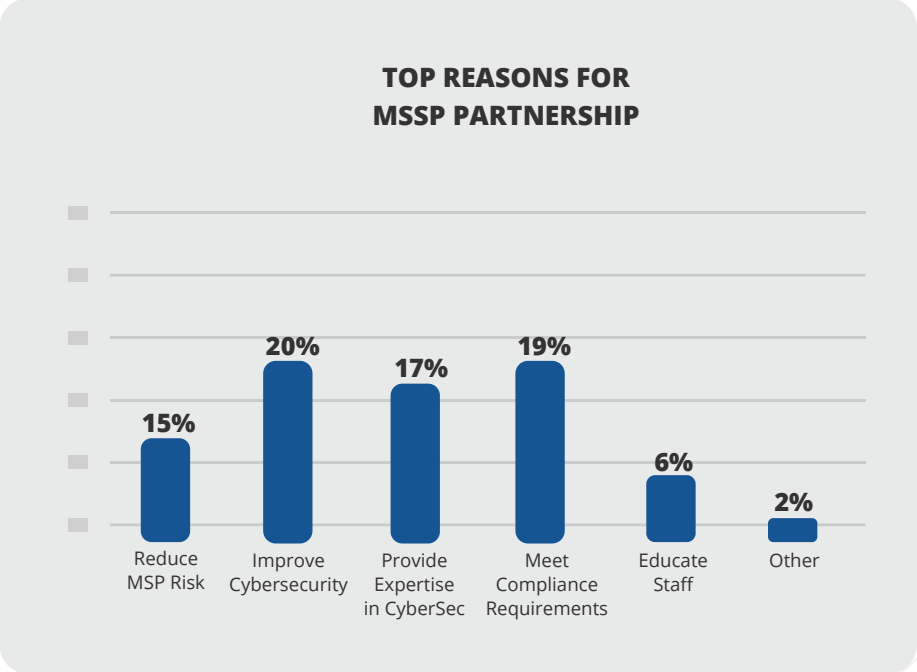
With backups often serving as the last line of defense, the ability to recover clean data from your backups is paramount. Nearly 1 in 10 of our respondents (9.80%) are automating their recovery testing, alleviating the historical challenges of manpower, budget and time, in order to certify recovery points for full proof and confidence in any potential restores to come. Only 2.40% of respondents have not implemented any of the preventative measures described in the survey.

Which of the following have you implemented to protect your backup environment from ransomware?

Copy of Backups taken off-network	**22%**
End-User CyberSec Training	**20%**
Proactive Monitoring for Anomalous Activity	**17%**
Deployed Non-Windows Solution	**16%**
Offsite Immutable Cloud storage	**14%**
Automated DR Testing	**10%**
None of the above	**2%**

9. https://securityboulevard.com/2020/10/ransomwares-next-target-backup-data/

Beyond environmental and security controls implemented by the MSP, many of our respondents indicate that they've partnered with a managed security services provider (MSSP) to augment a variety of areas, such as improving overall cybersecurity (20.17%), meeting compliance requirements (19.05%) and providing additional expertise in cybersecurity (17.09%), given the rise of today's advanced threats. Less than 1 in 5 (19.61%) respondents indicated that they're not currently partnered with an MSSP.



Facing a ransomware attack can be a career-defining moment for an IT professional — one's ability to identify, mitigate and recover from an attack may alter the trajectory of their organization. Respondents who have faced ransomware head-on, employed a variety of strategies for successful recovery.

Depending on the type of ransomware, the steps to remove it range from straightforward to near impossible. Lightweight scareware attacks install a malicious program that can be removed in minutes. In fact, the more popular variants that are classified as filecoders or encryption ransomware are much more challenging.

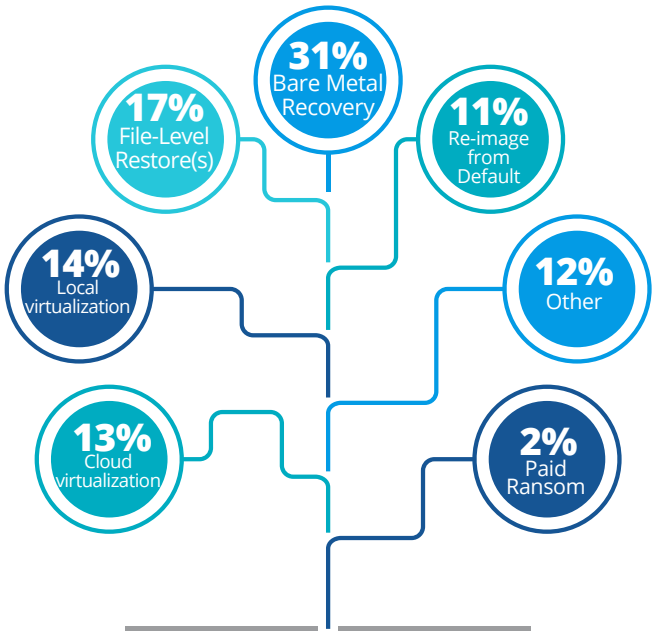
In cases where the infection is caught early on, removing the malware and recovering infected files may prove sufficient. For 17.06% of our respondents, removing and restoring infected files proved sufficient.

9. https://securityboulevard.com/2020/10/ransomwares-next-target-backup-data/

One of the more reliable ways to be certain that ransomware has been eliminated from a system is to completely wipe all impacted devices and reinstall them from scratch. Reformatting hard drives ensures no remnants of malware remain buried within the system. The most popular method of recovery among our respondents fell into this category, with 31.18% performing a bare metal recovery.[10] About 14.12% spun up new machine image(s) via local virtualization, another 12.94% performed virtualization on a cloud target and 11.18% of respondents reimaged their machines to their default.

A small percentage (1.76%) of respondents indicated the ransom was paid. Results varied — in 57.69% of cases, data was still lost. In 42.30% of cases where the ransom was paid, data was successfully restored.

If you've recovered from a ransomware attack, what technique did you use?



To pay or not to pay is a complicated, nuanced question. Authorities and industry experts agree it's generally a bad idea to give in to the ransom demand and pay up. Payment encourages further criminal behavior and emboldens the attackers with each successful ransom paid, perpetuating the cycle and increasing the ransoms demanded of future victims. Recent findings from cybersecurity vendor Cybereason report that 80% of organizations that paid a ransom experienced a second attack, and nearly half believe the second attack was carried out by the original perpetrator.[11]

10. https://searchstorage.techtarget.com/definition/bare-metal-restore
11. https://www.cybereason.com/press/new-cybereason-ransomware-study-reveals-true-cost-to-business

Consequences of an Attack

Even for those organizations that practice an abundance of caution and preparedness, a ransomware attack can wreak havoc before a successful recovery can take place. The average downtime an organization faces after a ransomware attack is 21 days.[12] This downtime ripples throughout the business, disrupting internal end users, external customers and stakeholders.

For our respondents who've faced ransomware head-on, data loss (22.34%) and downtime (22.13%) were the most widely reported consequences. Rounding out the top five most cited consequences were clients suffering reputational damage (15.24%), lost profits (13.57%) and compliance failure (9.39%).

What are the consequences of a ransomware attack for a client?

Downtime	**22%**
Lost Data	**22%**
Lost Profits	**14%**
Data Recovered (Paid Ransom)	**5%**
Data Lost (Paid Ransom)	**6%**
Reputation Damage	**15%**
Compliance Failure	**9%**
Other	**2%**
Clients Not Affected	**5%**

Restoring data and systems after an attack is merely the beginning of ransomware recovery. MSP organizations must harden client systems to prevent future attacks and complete repairs to systems damaged during the attack. These changes have the potential to negatively impact productivity, particularly when major changes such as a cloud migration are implemented. Should your organization implement additional controls or configurations before or after an attack, be sure you're communicating frequently with clients and their employees on progress, and are able to offer IT support to ensure they're able to remain as productive as possible during periods of change.

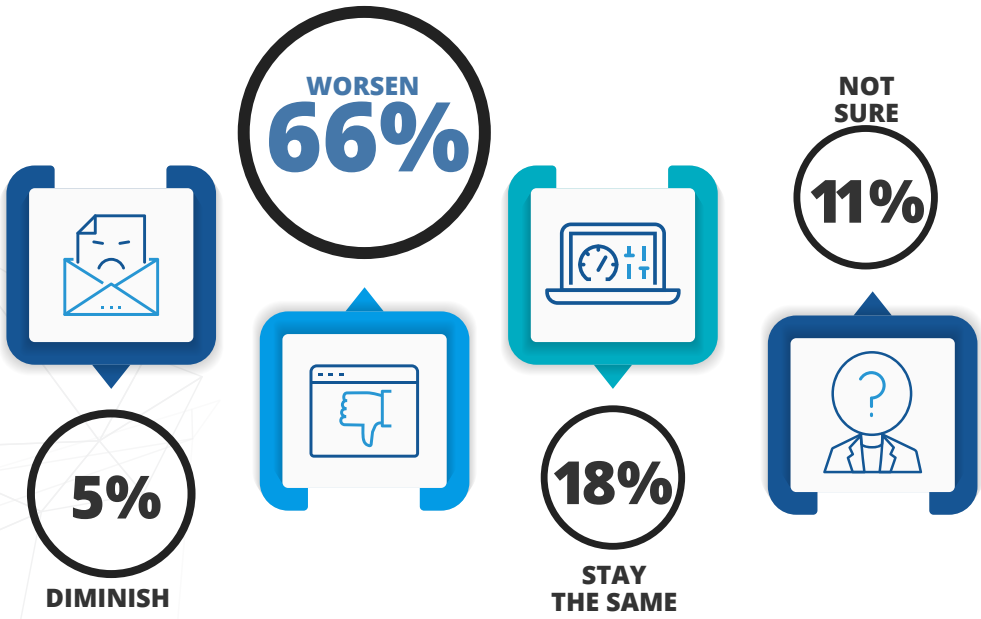
12. https://www.varonis.com/blog/ransomware-statistics-2021/

Future of Ransomware

The accelerated shift to hybrid work environments has proliferated social engineering attacks such as phishing schemes, malicious websites and the use of stolen or compromised credentials.

With this shift being permanent for many industries, it's no surprise our respondents anticipate ransomware will continue to worsen over the next year. About 84.12% of respondents expect ransomware will worsen or remain about the same while an optimistic 4.71% of respondents expect ransomware to diminish. However, the advent of technologies, such 5G and IoT, will bring about a new generation of threats.

OVER THE NEXT YEAR, DO YOU EXPECT RANSOMWARE TO:



Conclusion

As environments become more distributed and more complex, cybersecurity remains a priority, as does the ability to protect different sources of client data with a solution that's secure, easy to use and increasingly automated.

At Unitrends MSP, our Unified BCDR platform enables our MSP partners to address the challenges of today with a complete and agile solution designed to back up, secure and recover all client workloads regardless of where they live. The platform encompasses protection for traditional data center infrastructure as well as cloud-based workloads, SaaS data and the data being generated on endpoint devices such as small remote servers as well as laptops and remote PCs. Purposeful integrations with security tools provide end-to-end protection against cybercrime and human error, inject automation and artificial intelligence to simplify complex systems and provide a unified experience with visibility across a complete backup infrastructure.

Appendix/Table of Figures

Figure 1: How many staff work at your MSP?

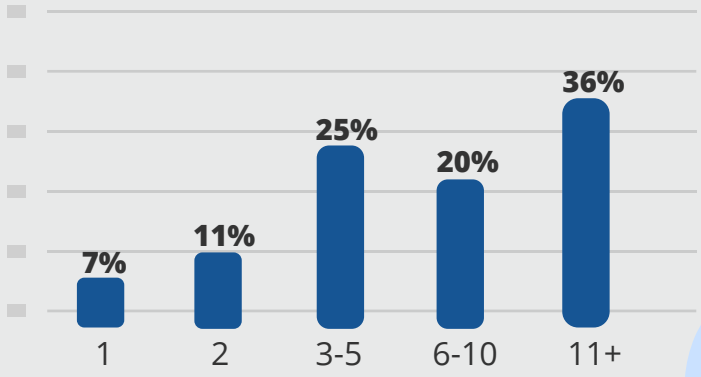
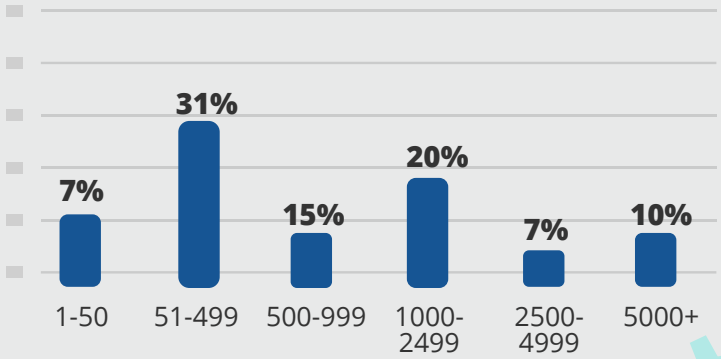


Figure 2: How many endpoints does your MSP manage?



Appendix/Table of Figures

Figure 3: Does your MSP focus on specific verticals?

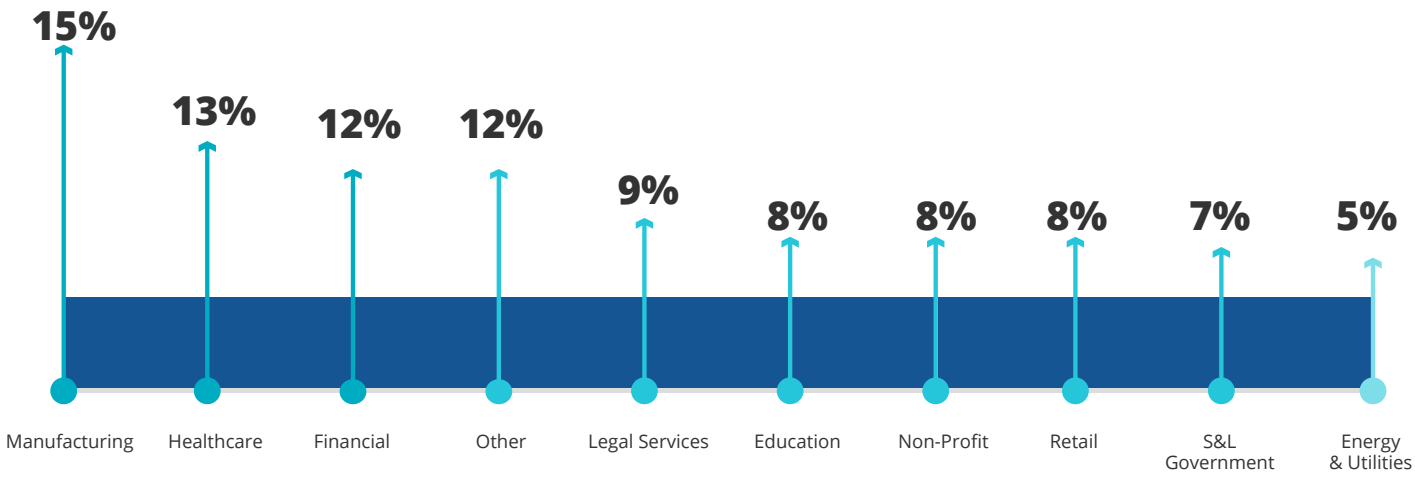
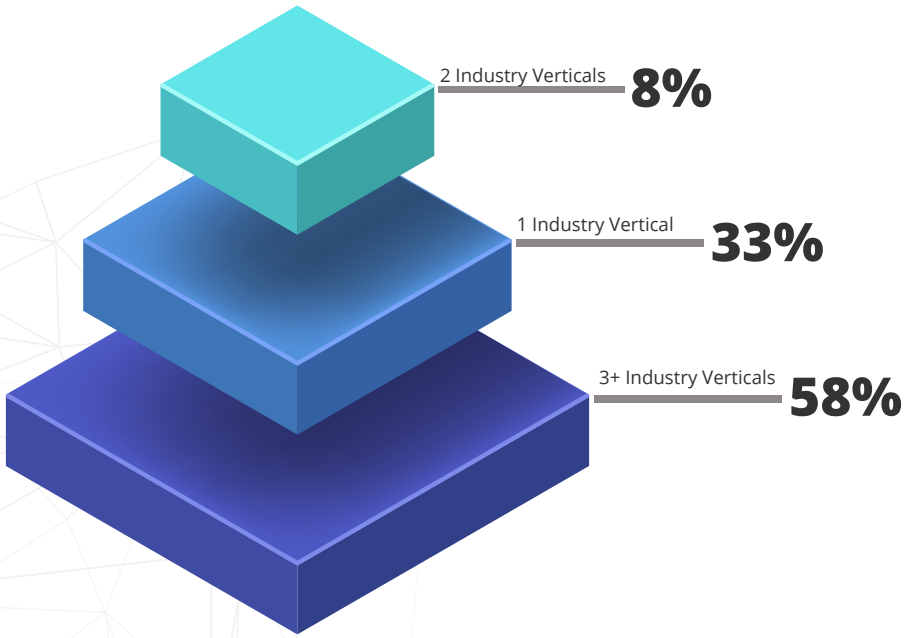


Figure 4: MSP Clients per Industry Served



Appendix/Table of Figures

Figure 5: In the last 24 months, ransomware has:

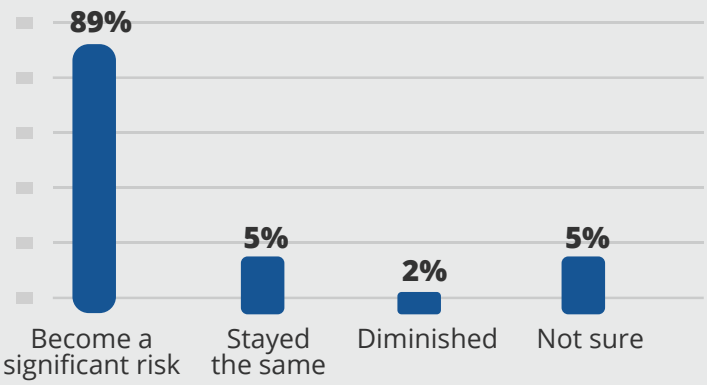


Figure 6: Which of the following have you implemented to protect your production environment from ransomware?

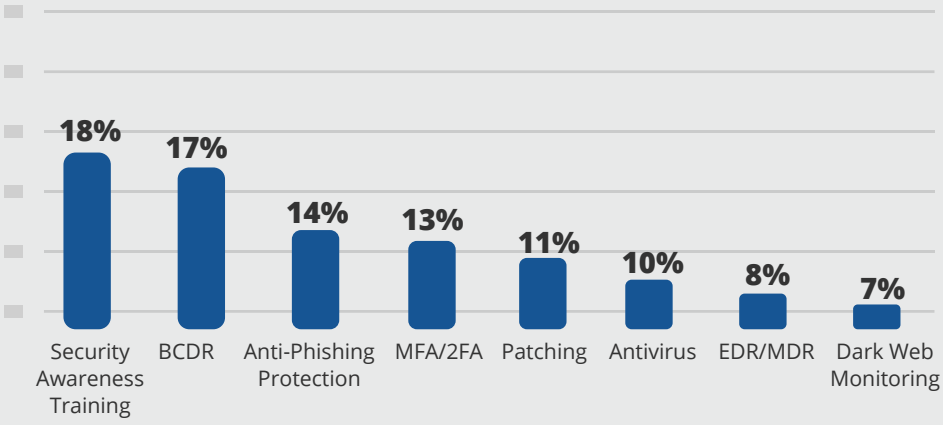


Figure 7: What most closely describes your clients' level of preparedness for ransomware?

Somewhat Prepared	**50%**
Mostly Prepared	**37%**
Extremely Prepared	**7%**
Not Prepared	**7%**

UNITRENDS MSP

msp.unitrends.com

Want to learn more?
GET IN TOUCH TODAY!