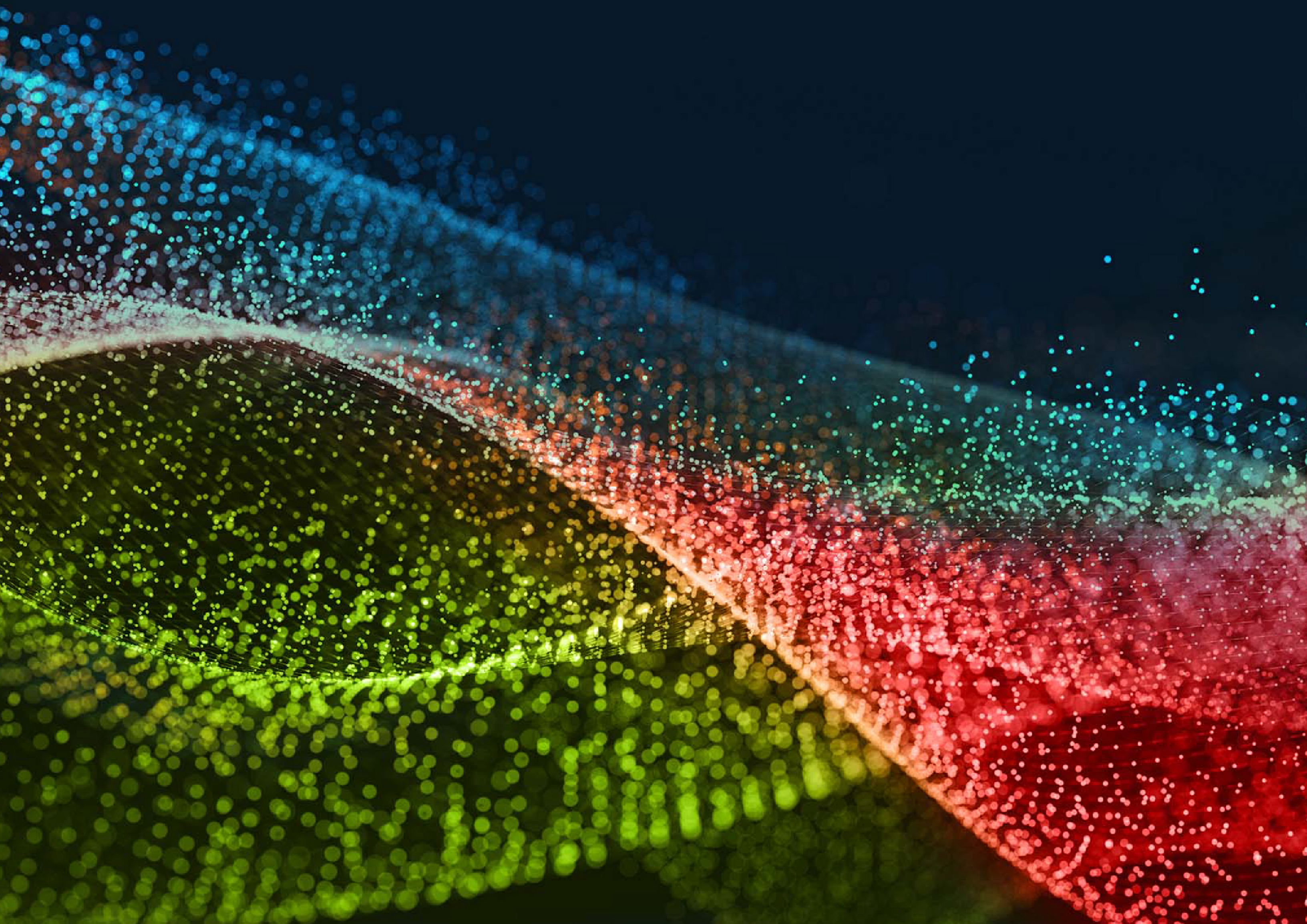
thycotic Centrify

2021 State of Ransomware Survey & Report

Mitigating the Impacts of Ransomware



INTRODUCTION: Ransomware attacks are on the rise. Are you prepared?

Ransomware attacks are increasing drastically on a global scale. The US, for example, has seen a rise of nearly 200% in the past two years. And the cost to recover data from the cybercriminals has soared, now averaging more than $100,000---ten times what it was only a year ago.*

Cybercriminals are getting more sophisticated and ransom demands continue to skyrocket. Attack surfaces are increasing while the costs for hacking tools are decreasing. Payouts have become so lucrative that ransomware developers have emerged to sell or establish an affiliate program for their tools and expertise, offering Ransomware-as-a-Service (RaaS). Ransomware could further evolve into a subscription model where you pay the criminal gangs not to target you. This ThycoticCentrify report indicates two out of three companies surveyed were victims of a cyber attack in the last 12 months, and more than four out of five felt they had no choice but to pay the ransom demands.

As the odds for experiencing a ransomware attack grow, it's not a matter of if an attack will happen, but when it will happen. This means that while you are trying to prevent becoming a victim of ransomware, you must also be prepared to respond to attacks with a proven incident response plan that you test regularly.

*https://www.insurancethoughtleadership.com/how-to-combat-surge-in-ransomware-attacks/

Ransomware dwell time poses a major risk

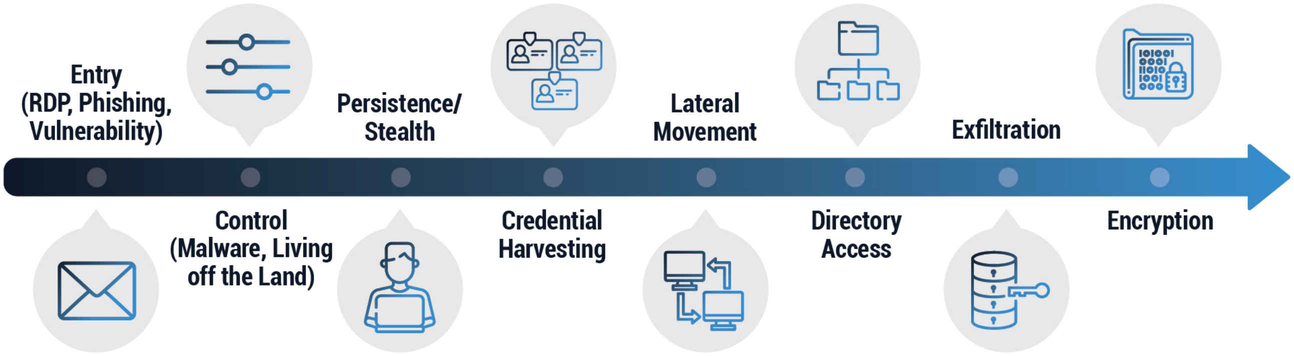
In the past, ransomware attacks typically targeted a single computer or limited network. When an employee clicked on a link, they unknowingly downloaded malware which would then encrypt the computer or server. A backup restore could usually help fix the problem.

Today, attackers focus on compromising user credentials and passwords to gain an entry point from which they can exploit our vast connected networks. Once inside the network, undetected, the cybercriminals seek to elevate credential privileges, traverse the network, locate sensitive data, and plan how to exfiltrate and encrypt the data.

This dwell time - the time from the point of entry until the actual launch of ransomware and detection of the attack - enables attackers to understand the network, find and exfiltrate critical data. They will then leave crypto-locking malware on your systems to launch when they are ready. Typically, once an attacker gains access to domain administrator privileges, it is usually only a matter of hours before the ransomware is deployed and business comes to a halt.

In many cases, organizations see the only realistic way to get their network back up and running is to pay an exorbitant ransom demand or risk devastating damage to their operations and reputation.

Figure 1: Ransomware attack dwell time spectrum



Source: UltimateITsecurity.com

This diagram illustrates the stages of a ransomware attack with dwell time from the point of entry to encryption measured in days. The longer the attacker is allowed to roam at will undetected, the greater the risk for exfiltration of critical data and the deployment of crypto-locking malware that leaves few options but to pay the ransom.

Prevention and mitigation built on early detection

The key to prevention and mitigation is to detect a breach as early as possible, block the escalation of privileged access, and prevent directory access. Privileged Access Management (PAM) solutions that enforce least privilege are designed to prevent credential harvesting and lateral movement, reducing attacker dwell time and making it much more difficult to use ransomware tools.

In addition, PAM security solutions are essential to understand a ransomware attack that's underway and conduct a post-mortem analysis to help make sure it can't happen again. Forcing the attackers to take more risks will result in the attackers making more noise on your networks, giving you a better chance at detecting them before they gain domain administrator privileges.

Executive Summary

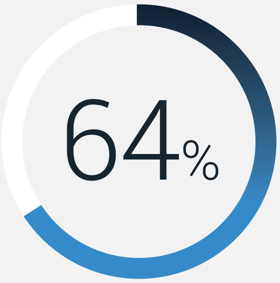
This report examines responses of 300 IT business decision makers in the US through a survey conducted in 2021 by Censuswide, a global research company. Key takeaways from the research include:

Key Takeaway

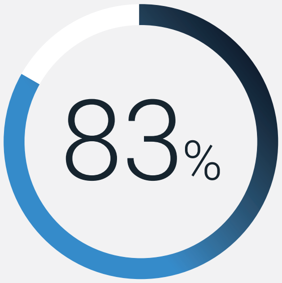
1 With nearly two out of three organizations victimized by a ransomware attack within the past 12 months *and more than 80% reportedly paying the ransom demands*, it is more important than ever that organizations prioritize creating an incident response plan.

2 Companies are increasing their cyber security budgets to mitigate the risk of ransomware attacks on their business. While turning to network and cloud security solutions for help, organizations must also understand and prioritize the requirements for preventing exploit escalation with PAM security that enforces least privilege access.

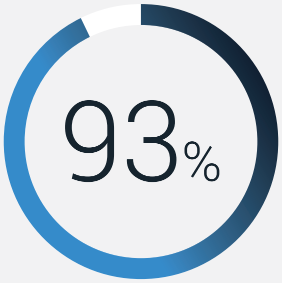
3 Organizations are on the right track to prevent the worst damages from ransomware attacks by practicing basic cyber security hygiene such as regular backups, timely patching, and password protection. However, you can't protect passwords adequately without making PAM policies for least privilege access a priority. This enables security teams to identify the attack entry point, understand what's happened, help remediate, and ultimately protect restored data.



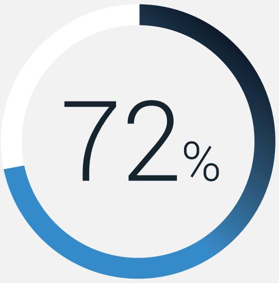
have been victims of a ransomware attack in the last 12 months



of attack victims paid the ransomware demand



are allocating special budget to fight ransomware threats

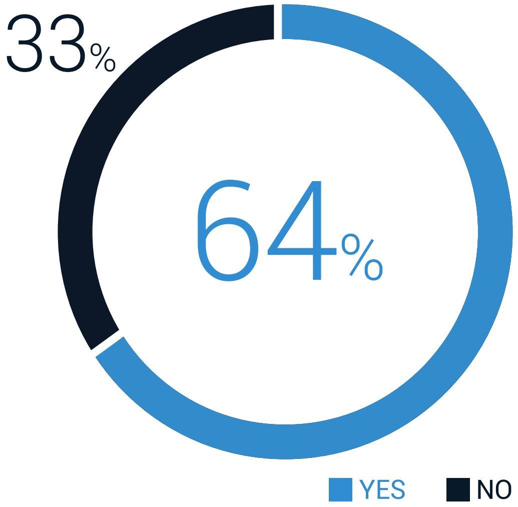


have seen their security budgets increase due to the ransomware threat

KEY TAKEAWAY #1

With nearly two out of three organizations being victimized by a ransomware attack within the past 12 months and more than 80% reportedly paying the ransom demands, it is more important than ever to prioritize creating an incident response plan. Your best defense is to prioritize prevention and incident response to contain the threat and limit the damage.

Survey Results

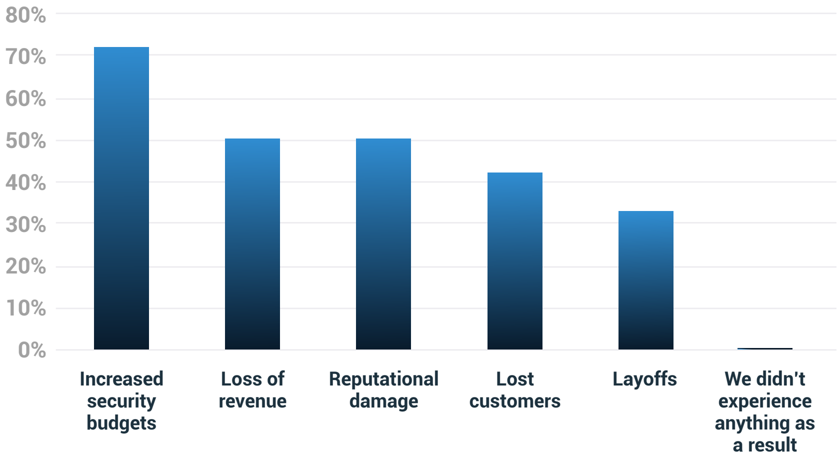


Q Has your company been the victim of a ransomware attack in the last 12 months?

64% of organizations in the survey reported being victims of a ransomware attack in the past 12 months.

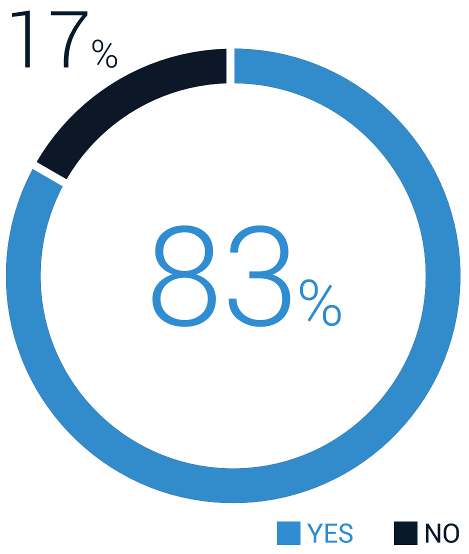
Q If your company has been the victim of a ransomware attack in the last 12 months, what, if anything, did your company experience as a result (check all that apply)?

The severity of the damage from ransomware attacks was clearly demonstrated by the severity of damage reported by survey respondents to their businesses. More than half of respondents suffered lost revenue and reputational damage, 43% lost customers, and one-third attributed the ransomware attack as the cause for employee layoffs.



Q If your company has been the victim of a ransomware attack in the last 12 months, did your company pay the ransom?

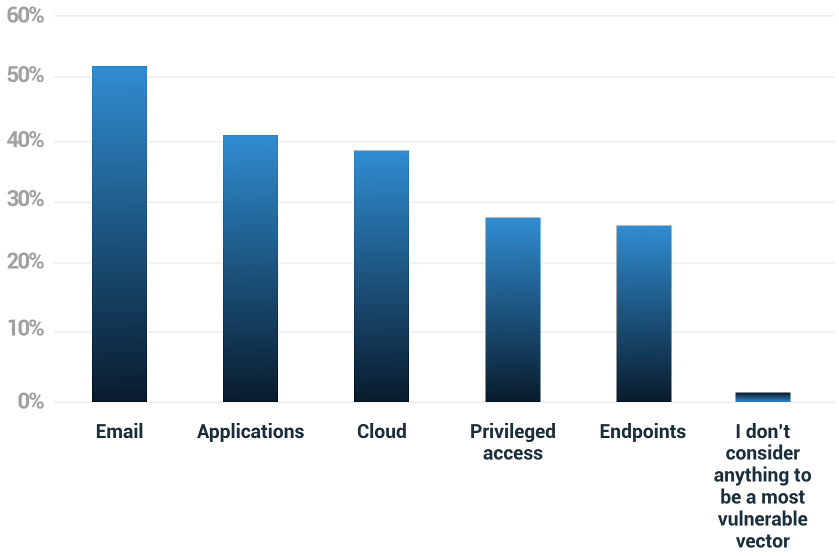
Most disturbing of all was the fact that 83% of companies victimized by ransomware paid the ransom to get their data restored. This is a strong indicator that companies experiencing a ransomware incident feel there are few, if any, options to paying the ransomware demand. Ransomware cybercriminals have also recognized that releasing crypto-locked data after payment only reinforces the sense that if companies do pay up, they are likely to get data restored.



Q What, if anything, do you consider the most vulnerable vectors for ransomware attacks? (Tick up to two)

The most vulnerable vectors for ransomware attacks, according to respondents, ranked Email first at (53%), followed by Applications (41%) and the Cloud (38%). This is likely due to attackers using phishing emails as a favorite technique whereby an unsuspecting user clicks on a link in an email that downloads malware and/or captures the user's credentials.

Privileged Access was selected as a top attack vector by one out of four (26%) of respondents, followed closely by Vulnerable Endpoints (25%). These responses may suggest that there is still a lack of awareness in how important exploiting privileged access can be in helping the attackers exfiltrate data, as well as knowing exactly where the ransomware should be targeted to cause the most concern or damage.



Recommendations

Ransomware attacks are often launched through phishing emails that contain malicious attachments or through drive-by downloading. Drive-by downloading occurs when a user unknowingly visits an infected website, and then malware is downloaded and installed without the user's knowledge. Other common techniques used by cybercriminals include brute-force attacks that guess known weak credentials used by employees or third-party contractors.

However, a ransomware attack should not be considered a single event but rather a process of exploitation that frequently begins with a simple breach and capture of a user's credentials through a phishing email that downloads malware. The dwell time between breach and ransomware lock up and money demands in an attack allows the perpetrator to explore your network undetected, conduct reconnaissance, and identify your most sensitive (and lucrative) data to target.

Prevention

To proactively prevent ransomware and ensure ransomware detection, there are several things you can do now.

- Make sure you are using multi-factor authentication on all internet-facing interfaces to prevent an easy takeover of user credentials.
- Focus on deploying and maintaining up-to-date assets, vulnerability, patch management, and configuration management programs.
- Develop and deploy a zero trust strategy that enables you to enforce least privilege access across all of your applications, cloud platforms, systems, and databases. It's your best way to prevent an attacker from escalating privileges and roaming your network undetected.
- Implement security tools and practices that minimize disruption to end users. Busy users are more likely to skirt security policies when security tools are difficult to use.
- Protect and isolate sensitive data, along with your backup and restore capabilities. Ransomware attackers often seek to disable your backup systems before locking up data.

Mitigation and Incident Response

- Ensure your security team has the visibility and processes in place to detect common malicious behaviors, including information about third-party software or devices.
- Use behavior analytics tools to detect and alert on high-risk behaviors associated with breaches and ransomware attacks.
- Familiarize your security team with the processes and techniques used by ransomware attacks and how to mitigate them once detected.

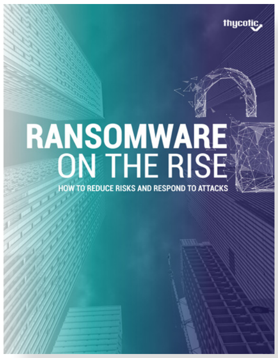
Make sure you have an incident response plan that has been tested in place so that you are prepared to respond to any suspected ransomware attack rapidly. Forensic follow up to any incident is a must to prevent future exploits.

Top tips to stop Ransomware and avoid becoming a victim

- Education & Cyber Hygiene
- Privileged Account Management
- Backup & Test
- Application Control
- Least Privilege
- Patch & Update Security

Resources

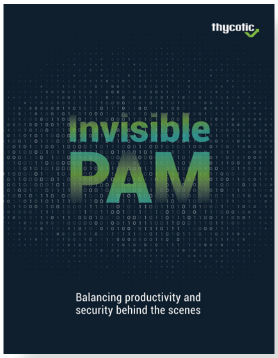
Free Guide: Ransomware on the Rise



Learn best practices recommended by the Cybersecurity and Infrastructure Security Agency (CISA) and the Multi-State Information Sharing and Analysis Center (MS-ISAC), plus PAM strategies that fortify your security controls and make your organization more resilient against ransomware.

https://thycotic.com/resources/ransomware-whitepaper-reduce-risks-respond-attacks/

Free Whitepaper: Invisible PAM - Balancing Productivity and Security Behind the Scenes



Traditional PAM solutions require users to interrupt their workflow to access privileged credentials. Frustrated, busy users are more likely to skirt security policies when PAM is difficult to use.

To realize the security benefits of enterprise PAM, software must be integrated and interoperable. PAM must be virtually invisible.

https://thycotic.com/resources/invisible-pam-balances-productivity-and-security/

Research Report: 2021 Cyberthreat Defense Report

CYBEREDGE GROUP
2021 Cyberthreat Defense Report
North America | Europe | Asia Pacific
Latin America | Middle East | Africa
Research Sponsors
PLATINUM
GOLD
SILVER

Cyberthreats at an all-time high in the wake of COVID-19.

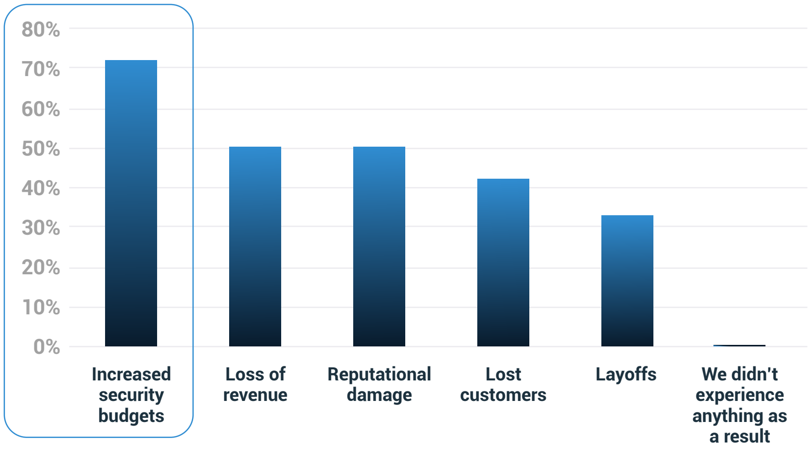
https://thycotic.com/resources/cyberedge-2021-cyberthreat-defense-report/

KEY TAKEAWAY #2

Companies are increasing their cyber security budgets to minimize the impact of ransomware attacks on their business. While turning to network and cloud security solutions for help, organizations must also understand and prioritize the requirements for preventing exploit escalation with PAM security that enforces least privilege access.

Survey Results

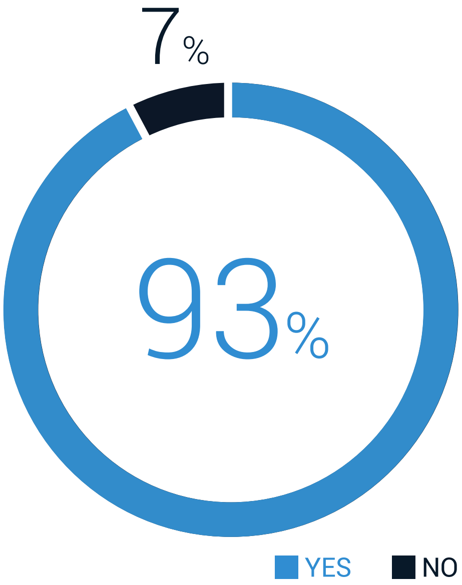
Q If your company has been the victim of a ransomware attack in the last 12 months, what, if anything, did your company experience as a result (check all that apply)?



Awareness has grown regarding the threat from ransomware, as incidents continue to grab headlines across the globe. So, it's not surprising 72% of respondents have realized increased security budgets among those victimized by a ransomware attack.

Q Is your company allocating budget to protect against ransomware in its annual budget?

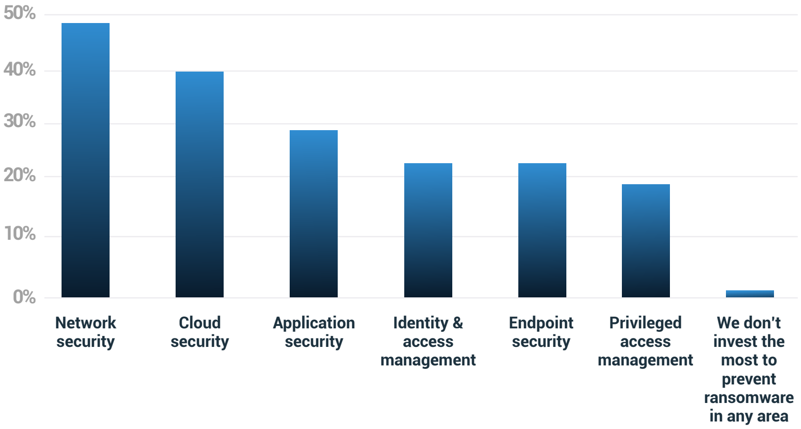
The importance of protecting against the ransomware threat is also reflected in how organizations now manage and allocate their cyber security budgets. Nearly all the respondents in this survey, or 93%, allocate budget to protect against ransomware as part of their annual security budgets.



In what area, if any, do you invest the most to prevent ransomware? (Tick up to two)

Organizations are spending their increased cyber security budgets investing in ransomware prevention with Network Security (49%) and Cloud Security (41%) solutions.

It is interesting to note that in this survey, Identity Access Management (24%), Endpoint Security (23%) and Privileged Access Management (19%) are lower priorities for budget spend. Companies may not realize, or be underestimating how important these are to preventing against, mitigating or disrupting ransomware attacks.



Recommendations

When putting together your cyber security budget, keep in mind that you need to go beyond traditional security measures to effectively reduce the threat from ransomware attacks. Conventional signature-based antivirus programs, for example, are not able to keep up with the rapid variations of ransomware attacks.

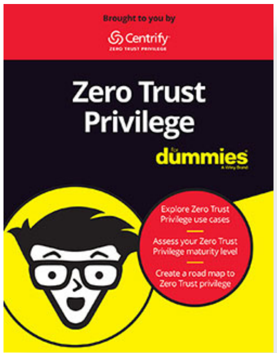
You should expect that, at some point, you will likely experience a breach of user credentials. But this kind of breach doesn't mean an attacker can escalate privileges and gain access to your network undetected. By budgeting for and implanting network segmentation, threat detection, and Privileged Access Management (PAM) solutions, you can prevent an attacker from roaming at will. This protects your most sensitive information, reduces the dwell time of a ransomware assault, and makes it more difficult to identify and exfiltrate critical data.

Assume all users are effectively privileged users. Consider a typical business user. They are likely reading emails, opening shared documents, browsing the internet, and plugging in USB devices. If your user has unmanaged local admin rights, they can readily install and execute any application regardless of where that application came from. That applies to unknowingly installing malicious software that gives attackers access to your entire network.

Your strategy to limit attacker escalation of privileges should include:

- Adopting a zero trust and least privilege posture
- **Restricting most users' permissions to install and run applications and programs by applying the principle of least privilege to all systems, devices, and services.**

Resources


Brought to you by
Centrify
Zero Trust Privilege
dummies
Explore Zero Trust Privilege use cases
Assess your Zero Trust Privilege maturity level
Create a road map to Zero Trust privilege

Zero Trust Privilege for Dummies

Zero Trust Privilege for Dummies explains how you can grant least privilege access by verifying who is requesting it, the context of the request, and the risks associated with access. In this free 46-page eBook from ThycoticCentrify, you'll learn what zero trust is, real-world use cases, and how to get started with your zero trust strategy.

https://www.centrify.com/resources/ebooks/zero-trust-privilege-for-dummies/

Webinar: Reduce your Ransomware Risks with Least Privilege and Application Control

Thycotic explains how specific application control solutions and other endpoint lockdown security can help you apply a "least privilege" strategy to protect your systems from ransomware and other targeted attacks.

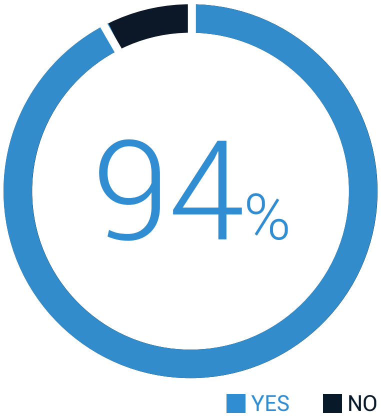
https://thycotic.com/company/blog/event/reduce-your-ransomware-risks-with-least-privilege-and-application-control/

KEY TAKEAWAY #3

Organizations are on the right track to preventing the worst damages from ransomware attacks by practicing basic cyber security hygiene such as regular backups, timely patching, and password protection. However, you can't protect passwords properly without making PAM policies for least privilege access a priority. This enables security teams to identify the attack entry point, understand what's happened, help remediate, and ultimately protect restored data.

Survey Results

Q Does your company have an incident response plan in place?

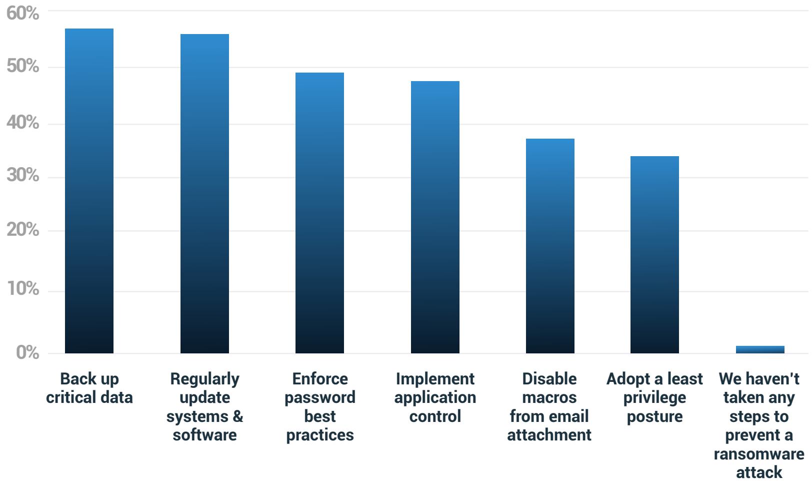


While the good news is that 94% of all respondents say their organizations have an incident response plan in place, it's unclear whether this resulted from a ransomware attack or was preparation prior to an attack. It is likely that the growing risk from ransomware attacks has spurred organizations to make sure they have a response plan in place.

In addition to an incident response plan, it is also critical to be incident-ready. Practicing your incident plans on a regular basis will allow you to quickly respond in the event of an attack.

What, if any, steps have you taken to prevent a ransomware attack? (Tick all that apply)

The most common steps taken to prevent ransomware attacks include Backing Up Critical Data (57%), Regularly Updating Systems and Software (56%), and Enforcing Password Best Practices (50%). Last on the list was Adopting a Least Privilege Posture (34%). However, enforcing least privilege is one of the best ways to prevent ransomware attackers from exploiting a simple breach to roam the network undetected and plan their lockdown and exfiltration of sensitive data.



Recommendations

Enforcing password best practices must recognize that most users today have far too many passwords and credentials to remember. In carrying out their daily tasks, cyber fatigue can easily occur whereby they neglect to follow password best practices. This makes it imperative that cyber security teams seek to push password management and hygiene into the background and make it as seamless as possible. With Privileged Access Management (PAM) solutions, most users don't even see their passwords. Instead, PAM tools automatically generate the passwords which are stored, rotated, and tracked.

PAM security software plays an integral role in deploying and enforcing security controls, making it more difficult for attackers to steal passwords and abuse privileges. Password randomization, rotation, and ongoing management are also effective in limiting an attacker's ability to explore your network and escalate privileges. Using a PAM solution forces attackers to take greater risks, increasing your ability to detect an intruder before they cause more damage.

Implement a strong Incident Response Plan and be Incident Response ready

Prevention is just one part of winning the battle with ransomware. No matter how many preventive controls you put in place to block malware, there's still a chance that sophisticated criminals will find ways into your organization. That's why you need an incident response strategy. It can prevent a cyber-attack from becoming a cyber catastrophe. With a solid plan in place, IT operations, security, and incident response teams will be able to form a united front against a ransomware attack, coordinate actions, and maintain business continuity.

Resources

Secret Server Free Trial

The road to PAM is a journey. Take your first step with a free trial of Secret Server. Get up and running fast with solutions for privileged account discovery, turnkey installation, out-of-the-box auditing and reporting tools, and endless customizations available for your team.

https://thycotic.com/products/secret-server/start-a-trial/

Free Template: Cyber Security Incident Response Plan Template

Thycotic's free Incident Response Plan Template helps to reduce the risk of a cyber breach from becoming a cyber catastrophe. It helps enable IT operations, security, and incident response teams to form a united front against an attack, coordinate a rapid response, and maintain your business continuity.

https://thycotic.com/resources/cyber-incident-response-plan/

thycotic

HOW TO BUILD YOUR INCIDENT RESPONSE PLAN

To contain a breach and protect privileged access

By Joseph Carson

Conclusion

Ransomware attacks are one of the most urgent threats to organizations today. As more ransoms are paid to restore data, cyber criminals are further incentivized to step up their efforts to compromise your networks. While companies are increasing their spending on cyber security solutions to prevent becoming ransomware victims, it is essential they protect all users as if they were privileged users. By safeguarding privileged access with PAM solutions to reduce or eliminate attacker dwell time, as well as implementing a robust incident response plan, organizations can minimize the risk from what appears to be a threat that will only increase for the foreseeable future.