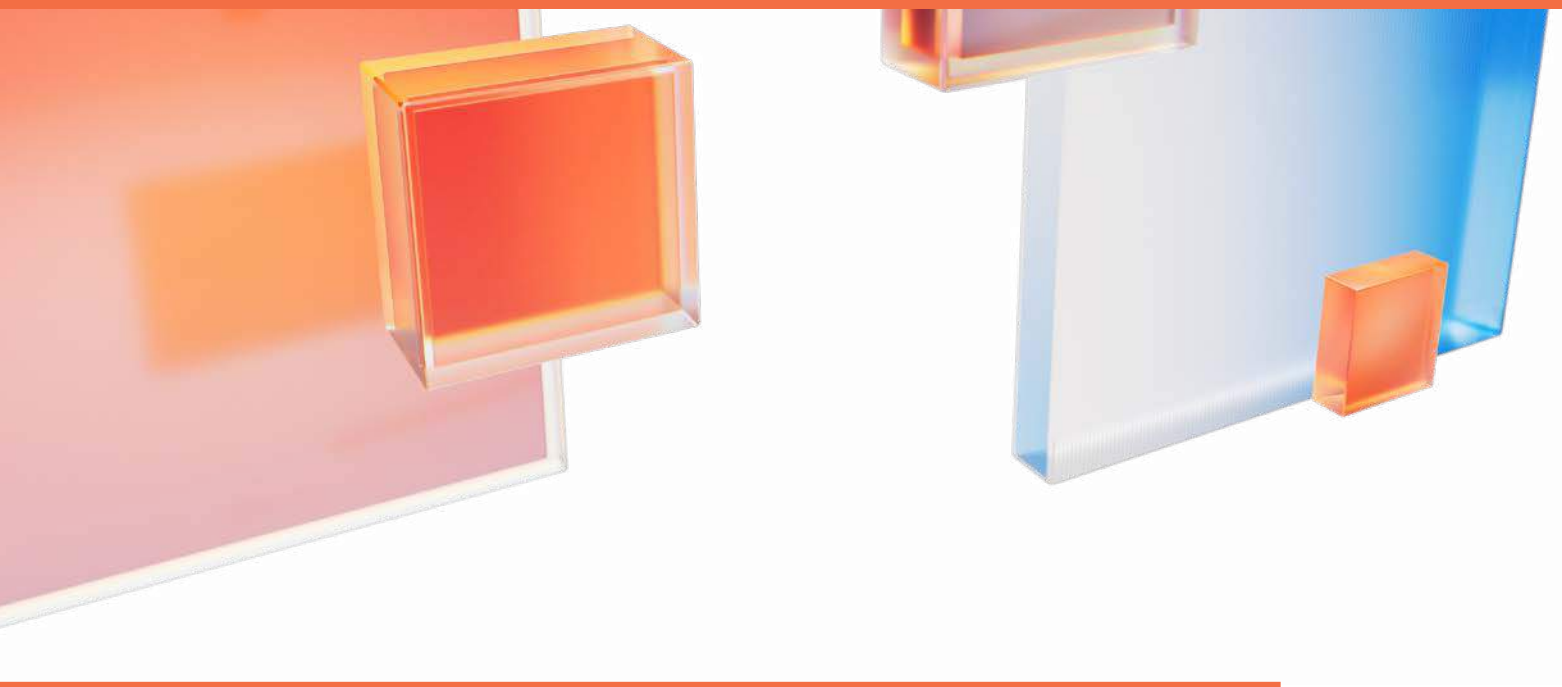
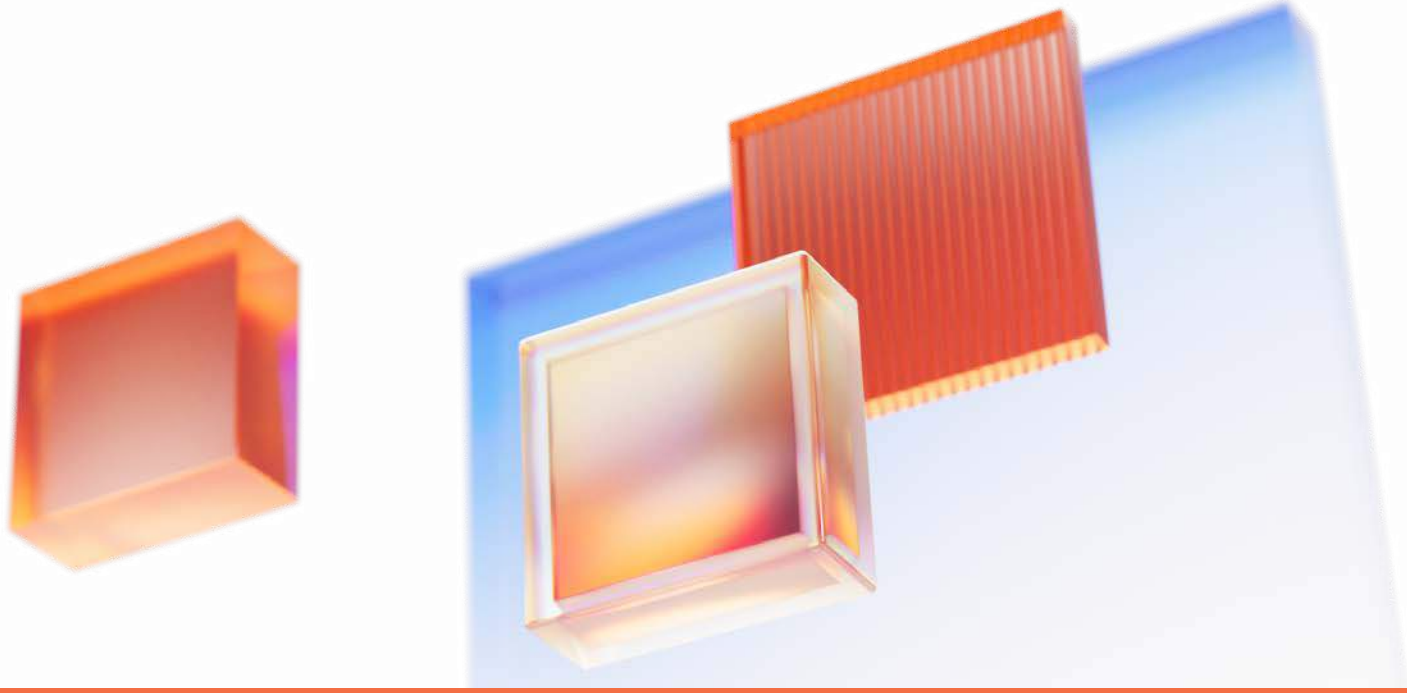
SONICWALL®



2024 Mid-Year Cyber Threat Report

ACTIONABLE INSIGHTS FOR EVOLVING THREATS



INTRODUCTION

LETTER FROM THE CEO

In today's dynamic threat landscape, our customers rely on us more than ever to protect their sensitive data, systems and operations from increasingly sophisticated cyber threats. From ransomware attacks to malware to cryptojacking, the adversaries we confront are relentless and evolving, requiring us to be continuously vigilant and proactive.

To further empower our partnership and enhance our collective efforts, I'm excited to present the SonicWall 2024 Mid-Year Cyber Threat Report. It shows how the threat landscape has continued to evolve with our relentless focus on supporting our partners and customers. Threat actors are adding more efficient and sophisticated tactics. Malware has increased 30% as compared to the same time last year, and we're seeing significant spikes in IoT malware (+107%) and encrypted threats (+92%) – all of which are laying the groundwork for the evolution of threat actors around the globe.

This report will provide partners, MSPs, MSSPs and customers actionable insights to help create and implement defensive strategies to combat these threats whether new or old. That is the primary reason we continue to provide the SonicWall Cyber Threat Report. And this year, we're more closely associating our threat data with credible business results that every organization should be able to relate to.

To further educate and inform our readers, we've added some new perspectives that feature feedback from our 24/7, 365 SOC analysts, market insight provided by a reputable cybersecurity insurance provider and even included the voices of some of our partners.

I encourage our partners to leverage this edition to engage with your customers around the necessary services and products that your customers need to safeguard their brands and businesses.

I am confident that this report will serve as a cornerstone in our joint efforts to secure our customers' environments effectively. Your feedback and insights have been and will continue to be instrumental in shaping our approach and direction.

On behalf of our global security network of trusted partners and the entire SonicWall team, including our Capture Labs threat researchers, we're excited to share this exclusive look at the most recent evolutions of the cyber threat landscape in the 2024 SonicWall Mid-Year Cyber Threat Report.

Bob VanKirk
President & CEO
SonicWall

Executive Summary

THREAT LANDSCAPE

125%

Our sensors detected 50 hours worth of critical attacks in a 40-hour work week. You read that right - our average firewall was under attack 125% during a 40-hour work week.

Organizations were saved from a potential 46 days of downtime in the first five months of 2024.

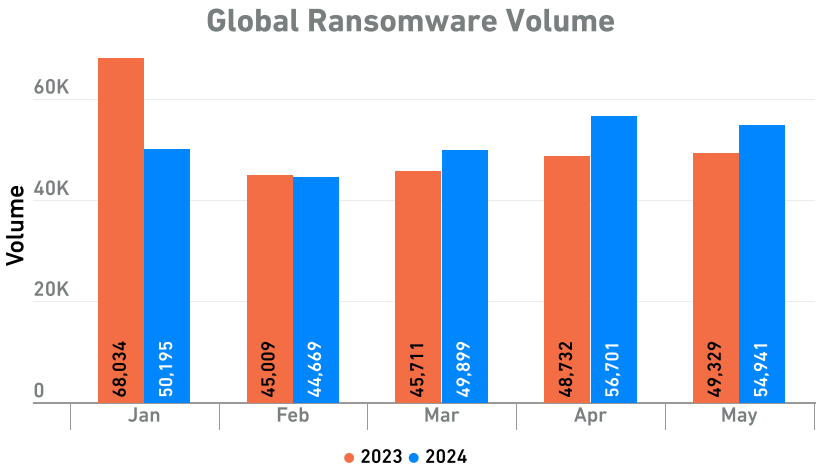
46 DAYS

12.6%

At a minimum, 12.6% of all revenues are exposed to cyber threats without proper protection. For a $10 million company that equates to $1.2 million.

RANSOMWARE

Ransomware is on the rise in the Americas (NOAM: 15%, LATAM: 51%). EMEA, however, is pulling the global numbers down, logging a -49% suggesting improved cybersecurity measures and law enforcement interventions are having a positive impact.



MALWARE

▲30%

Malware trended up from March to May, seeing a massive 92% increase in May alone.

15%

15% of all malware are leveraging software packing as the primary MITRE TTP.

IoT MALWARE

Attacked IoT devices spent an average of 52.8 hours under attack.

▲107%

ENCRYPTED THREATS

11001X
10XX11
001XX1
100X11
110X10

▲92%

Encrypted threats jumped 92%, which showcases growing sophistication from cybercriminals and the fact that they continue to increasingly utilize TLS-encrypted transfers to deliver malware and other threats over the network.

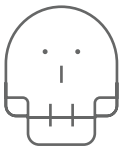
"The SonicWall 2024 Mid-Year Cyber Threat Report includes timely trends and provides our partners, MSPs, MSSPs and customers with insightful trends to help create and implement defensive strategies to combat these threats whether new or old."

-SONICWALL PRESIDENT AND CEO BOB VANKIRK

SOC

Eighty-three percent of customer-received alerts from our managed services team are related to cloud apps and compromised credentials.

RTDMI™



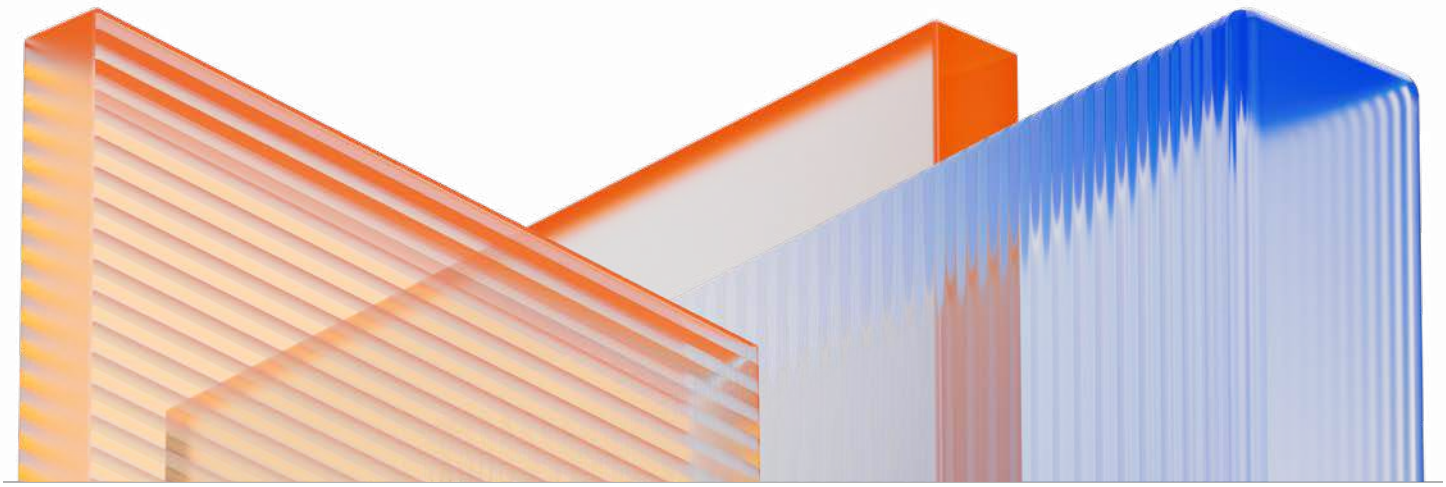
526
— NEW VARIANTS —
A DAY

SonicWall Capture Advanced Threat Protection (ATP) with Real-Time Deep Memory Inspection (RTDMI™) recorded 78,923 new variants.

CRYPTOJACKING

▼60%

After a record-breaking year, Cryptojacking dropped 60%. Most of the globe saw a decrease with the exception of India who saw a staggering 409% increase.



Evolving Metrics

As the SonicWall Threat Report matures, it's important that we consistently review and analyze the way we measure our data – it is crucial in adapting to the dynamic landscape of security threats. As new threats emerge, attack surfaces expand and the complexity of data increases. Traditional metrics can become deficient, leading to misinterpretations. By continually refining our analytical methods, we can better capture the nuances of evolving threats, reduce the impact of anomalies and ensure more accurate, timely and actionable insights. Today, we announce an evolution in the way we present data to the industry as we move from what has been referred to as the HITS metric to a new TICKS threat metric – which we believe will provide more meaningful insights to our partners and customers.

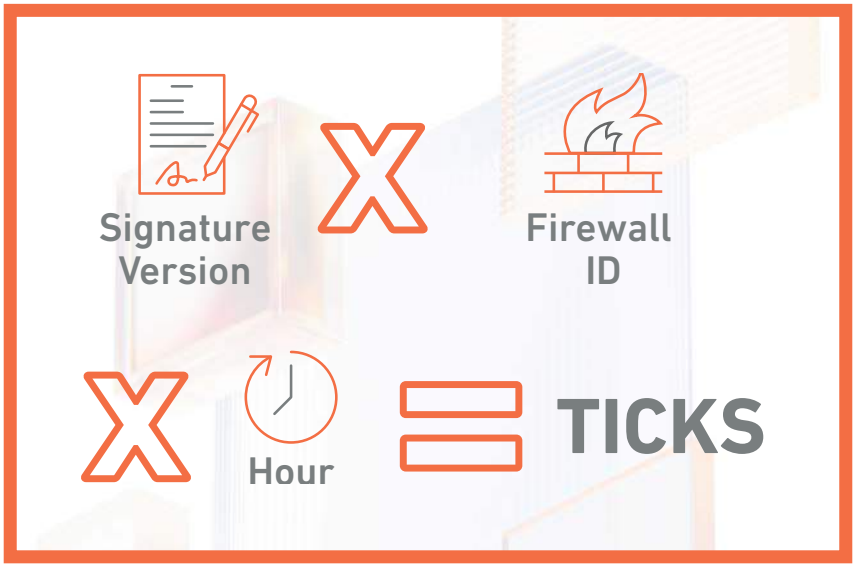
The shift to the TICKS metric for reporting telemetry data is driven by the desire to improve accuracy, reliability and clear ways to measure firewall activity. **TICKS represents the number of hours during which one firewall was under attack from any given threat.**

The absolute count of HITS can vary depending on how the signature is written, which is not a property of the actual threat, rather it is a property of the threat detection technique.

TICKS normalizes detection events to a logical value (true/false) for any threat over our default unit of time, which is hourly.

The TICKS metric counts the hours a firewall is under attack by receiving at least one hit per hour, rather than counting the total number of events. This normalizes data to reduce sensitivity to outliers and focuses on the duration of attacks rather than their intensity, highlighting sustained threats more effectively. This approach reduces the impact of occasional spikes in attack intensity and emphasizes sustained threats that may require immediate attention. It enhances the accuracy and reliability of assessing cybersecurity threats, thereby supporting better decision-making and more effective protection strategies for networks and systems.

This ongoing evolution also allows us to leverage advancements in data science and technology, improving our ability to detect patterns, predict trends and make informed decisions. Ultimately, staying at the forefront of data analysis and measurement practices is essential for maintaining robust security postures, optimizing performance and fostering innovation.

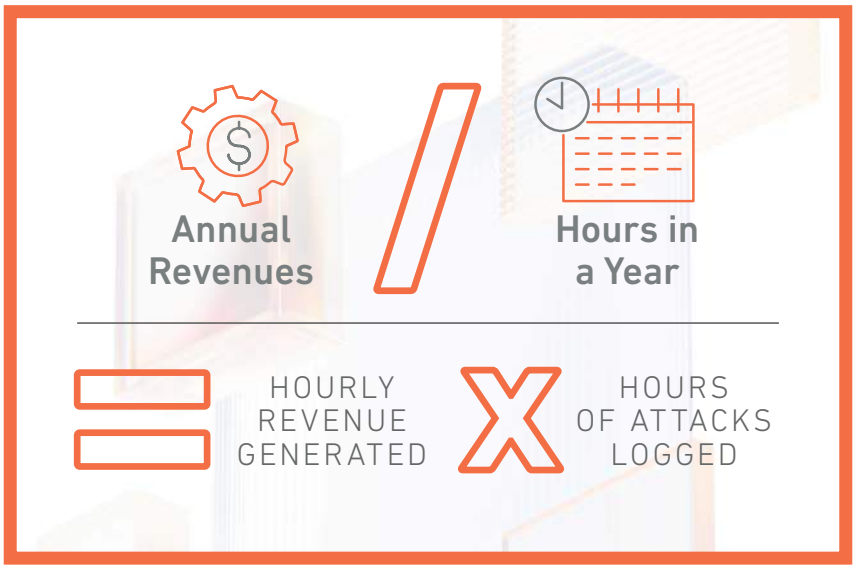


Methodology

As mentioned previously, our metrics have evolved to a point where we can assign an approximate dollar amount for the revenue our products have protected from malicious attacks. To determine hourly revenue generated, we divided annual revenues by hours in a year.

In this formula, we divide annual revenues by hours in a year to determine the hourly revenue generated. Leveraging our newly introduced TICKS data, that number is multiplied by the critical attack hours our sensors saw attacks.

The final number represents the minimum total revenue that was exposed to risk from these known nefarious attacks. It does not include potential additional costs of repairing or replacing infected systems, remediation of the vulnerability, quarantining compromised hardware and software, etc.



Unveiling the Latest Trends

Our partners lean on the mid-year threat report to identify the latest security trends stemming from the first half of the year, making it possible for them to more accurately comprehend bad actor behavior and to help them enhance their security strategies.

Supply Chain Attacks Intensify

Supply chain attacks have solidified their status as a significant cybersecurity threat, growing in sophistication and impact. These attacks exploit the interconnectedness of modern enterprises, targeting vulnerabilities in third-party software and services to compromise broader networks. The first half of 2024 has seen numerous highly-publicized incidents, such as the JetBrains TeamCity authentication bypass - underscoring the widespread nature and severe consequences of these attacks.

SonicWall's analysis highlights that older vulnerabilities remain a significant risk, particularly for small businesses (SMBs) with limited resources. As previously reported, by the end of 2023, three of the top five most widespread attacks were supply chain-related, with over 50% of customers affected by supply chain vulnerabilities, including older issues such as Log4j and Heartbleed.

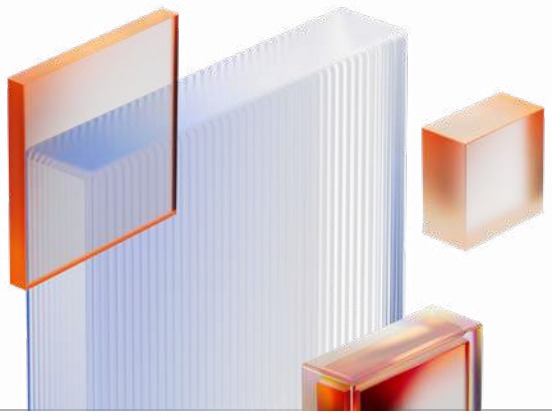
The Intricacy of Supply Chain Attacks

Supply chain attacks infiltrate a company's network through vulnerabilities in third-party suppliers or partners. Threat actors exploit weaknesses in software updates, libraries or interconnected systems, gaining unauthorized access to sensitive data or systems. This method is particularly effective as it bypasses traditional security measures focusing on direct attacks, challenging detection and prevention.

The JetBrains TeamCity Incident

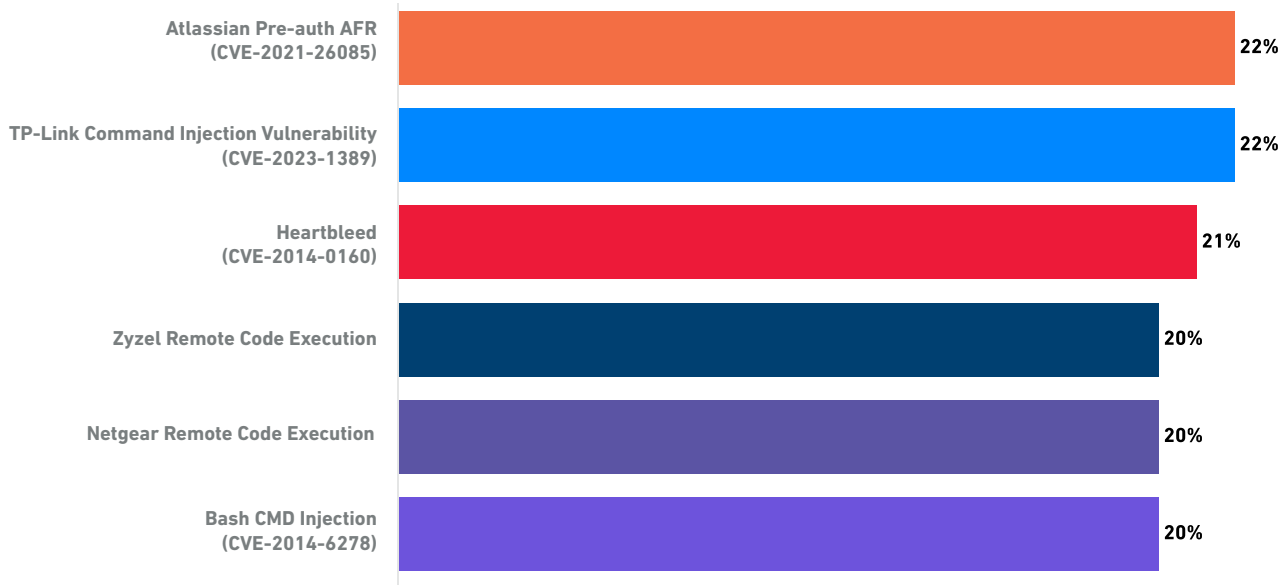
In March 2024, cybercriminals exploited vulnerabilities in JetBrains TeamCity, a popular CI/CD tool. Our research determined that attackers could bypass authentication mechanisms by rendering a 404 response and manipulating the JSP query parameter, potentially gaining full control over the affected systems. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) quickly added the JetBrains vulnerability (CVE-2024-27198) to its Known Exploited Vulnerabilities catalog.

Our telemetry data revealed that threat actors exploiting this vulnerability targeted 16% of all of our customers – displaying the ease of exploitation and the value this vulnerability had to threat actors. Eighty-three percent of these attacks, occurred in March, followed by a significant decline in subsequent months. This underscores the critical importance of prompt patching, as attackers frequently exploit the window of time organizations need to implement patches.



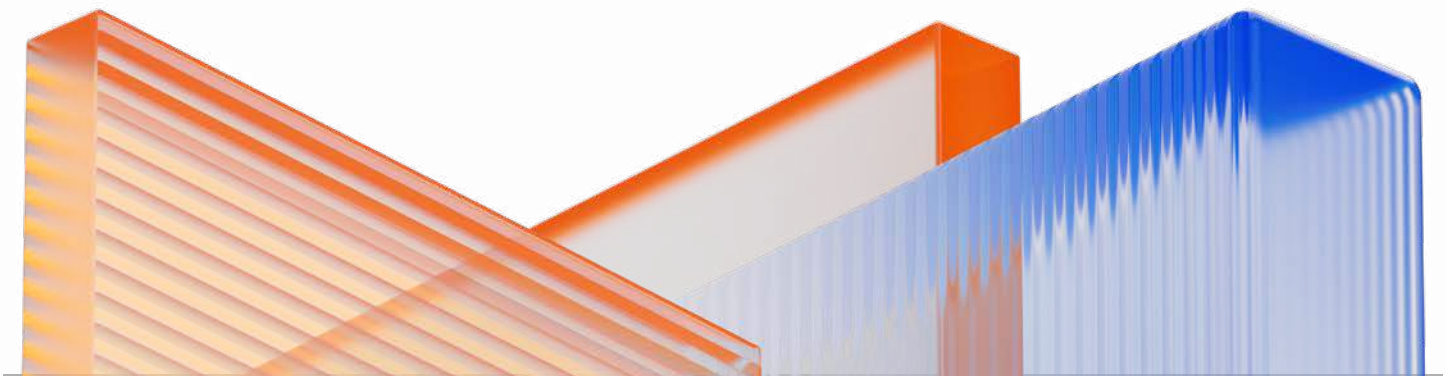
Reported exploitation of the JetBrains TeamCity vulnerabilities led to bad actors deploying Jasmin ransomware and the XMRig cryptocurrency miner, causing severe data breaches, heavy resource consumption, and operational disruptions. Despite SonicWall reporting a 60% decline in cryptocurrency miner attacks in the first half of 2024, the exploitation of these specific vulnerabilities demonstrates the ongoing cryptojacking threat.

2024 Top 5 Widespread Network Attacks



SOC POV

Preventing supply chain vulnerabilities requires thoroughness – you must know the ins and outs of your third-party software and services to ensure a strong security posture. Robust patch management protocols can help reduce your exposure to older vulnerabilities like Log4j and Heartbleed, which continue to be exploited. Industry reports show that on average it took organizations 55 days to patch even 50% of critical vulnerabilities. MSPs offer automated patching and expert security testing to provide you access to advanced security measures without the steep costs and in-house resources.



The Rise of Business Email Compromise (BEC) Attacks: From a Cyber Insurance Perspective

In recent years, cyber threats have evolved dramatically, with business email compromise (BEC) attacks taking center stage. On average, our insurance partner sees that there are now ten BEC events for every ransomware incident, and all signs point to this continuing to increase. Microsoft Office 365 (O365) misconfigurations, particularly at the Active Directory level, have also contributed to the rise in BEC incidents.

BEC attacks primarily rely on social engineering tactics, with 70% of reported incidents leveraging some type of social engineering. These sophisticated attacks often involve manipulating individuals into transferring funds or sensitive information. In one example, attackers gained partial control over a victim's email account, sending fraudulent invoice requests and routing replies to an RSS feed. This tactic makes it appear as though the victim is in control of their email, while the attacker responds to verification calls via email, falsely reassuring clients that it is safe to proceed with the wire transfer. This resulted in millions of dollars being wired to fraudulent accounts with little chance of recovery.

In another incident, a vendor was compromised, leading to a man-in-the-middle (MITM) attack. In this attack, the communication between the vendor and the customer remained legitimate, but the threat actor was able to alter the wire instructions. Consequently, the customers wired substantial sums – sometimes millions of dollars – to the wrong account, believing the transaction was legitimate.

These incidents pose issues for insurance claims. Typically, insurance policies require verification of any changes in wire instructions. However, when the communication appears legitimate, this step is often overlooked. Despite having robust email filtering services and security stacks, these attacks slip through due to the authenticity of the compromised communication channels.

INSURANCE POV

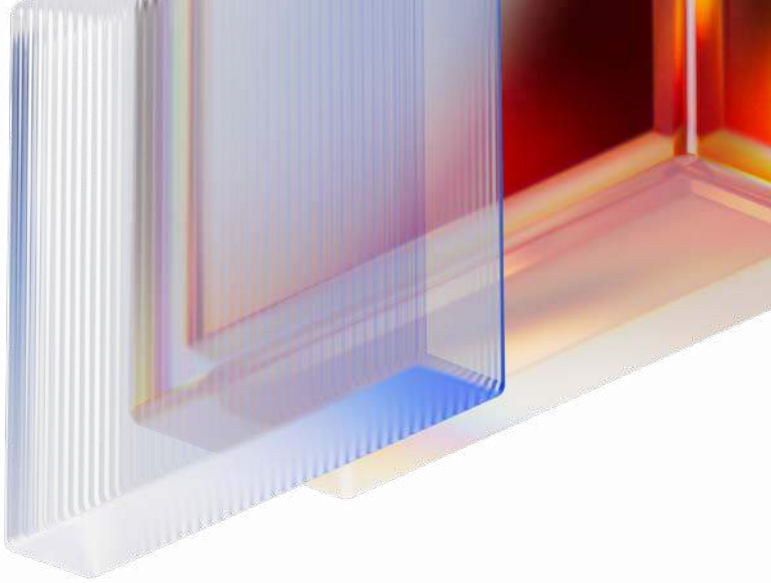
On average, our insurance partner sees that there are now ten BEC events for every ransomware incident.

PARTNER INSIGHT

"The threat landscape is completely overwhelming for organizations and the teams who defend them. Most cybersecurity breaches include some degree of human error. Ultimately, there are two ways to battle this; reducing opportunity and educating users. The fewer opportunities there are for an error, the less users will be tested. And the more knowledge they have, the less likely they are to make a mistake even when they face an opportunity to do so."

STEVEN HUANG – COO, Fornida
SonicWall Partner

Hackers Take Aim at Lower-Severity Microsoft Product Vulnerabilities



Earlier this year, SonicWall published a review of Microsoft's released patches and vulnerabilities from 2023. The research demonstrated that despite a significant number of vulnerabilities, not all vulnerabilities should be treated equally. While Microsoft patched over 900 vulnerabilities in 2023, the real concern lies in how attackers exploited these weaknesses.

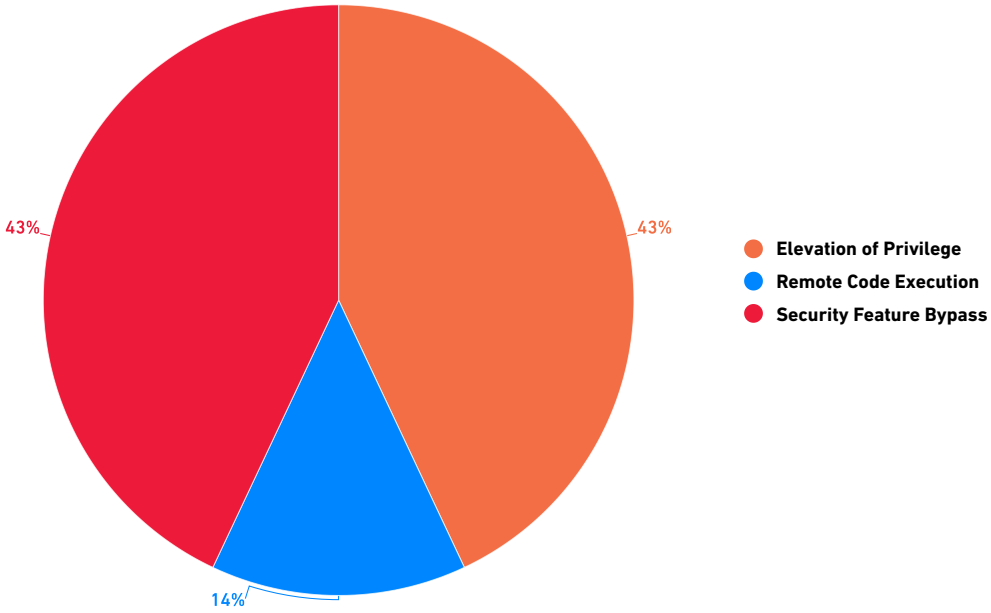
When considering the vulnerabilities that Microsoft patched, Remote Code Execution (RCE) accounts for 36%. Despite RCE vulnerabilities constituting a significant portion of the overall vulnerabilities, they were only exploited 5% of the time while Elevation of Privilege vulnerabilities were leveraged 52% of the time throughout 2023.

As of mid-2024, 434 Microsoft vulnerabilities have been reported and patched, putting them on track for a similar number when compared to last year. Interestingly, while almost 40% of reported vulnerabilities are categorized as Remote Code Execution (RCE), only one RCE vulnerability has been exploited. Eighty-six percent of exploited Microsoft vulnerabilities are Security Feature Bypass or Elevation of Privilege vulnerabilities. It underscores the need for cybersecurity strategies to prioritize these categories, even though they might seem less critical by sheer numbers.

SOC POV

Organizations should maintain a balanced approach, addressing both prevalent RCEs and the more frequently exploited Elevation of Privilege vulnerabilities to ensure robust security. Automatic patching allows software updates to be applied without requiring user intervention and is often implemented by MSPs. This approach enhances security by ensuring that vulnerabilities are addressed promptly, reducing the window of exposure to potential exploits and regardless of perceived severity.

Microsoft Exploited Vulnerabilities



Unlocking the Threat

Android devices are being targeted more and more by threat actors, particularly with RATs – no, not the cheese-eating kind. We're talking about Remote Access Trojans (RATs). These RATs disguise themselves as legitimate apps to gain permissions and then connect to command-and-control servers to steal credentials and bypass multi-factor authentication (MFA). Notable RATs like Anubis, AhMyth and Cerberus, all which have been widely used by threat actors this year, have adapted to bypass MFA. In April, we reported multiple campaigns where RATs used popular app icons to trick users into granting permissions, enabling them to capture two-factor authentication codes through accessibility services and gain unauthorized access to sensitive information.

Malware Upgrades

Anubis, a banking Trojan, now includes the capability to bypass MFA by capturing SMS messages with one-time passwords (OTPs), making it a significant threat on the Google Play Store.

AhMyth, a RAT from 2017 which is still in use, targets Android devices through infected apps on various stores, performing keylogging, taking screenshots and intercepting MFA OTPs.

Cerberus, which has been around since at least 2019, operates as Malware as a Service (MaaS) with features like SMS control, keylogging and audio recording, allowing it to intercept OTPs and bypass MFA for unauthorized transactions.

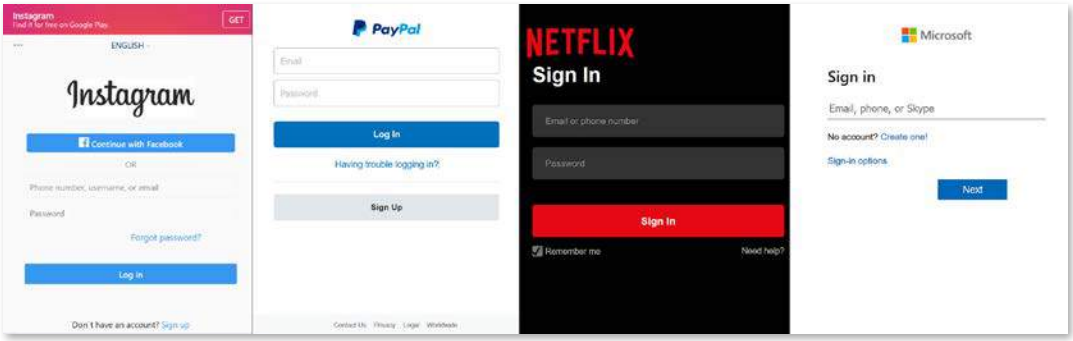


Figure 1: Real-life examples of fraudulent mobile login pages

SOC POV

From a Security Operations Center (SOC) perspective, location-based alerts are triggered by access attempts from unusual geographic locations, indicating potential security threats. For instance, an attempt from Russia when a user usually logs in from New York would trigger an alert. These alerts are vital for enhancing MFA security, helping SOC analysts identify and mitigate unauthorized access attempts, especially those involving compromised credentials or malware manipulating location data. Our managed services team has already seen over 7,400 location-based alerts, which is on track to outpace 2023 alerts by 10%.

INSURANCE POV

While attackers constantly focus on how to bypass MFA, it is still prevalent to see organizations that have not deployed MFA. This drastically reduces the difficulty of attack and in many cases most insurance companies will *not* pay claims if MFA is not enabled on an impacted email, email system or server. Using MFA is like wearing a cyber seatbelt, it will not prevent a car crash, but it is a key component in protecting your organization and ensuring you're in the best position possible with your insurance company.

PowerShell: A Double-Edged Sword – Exploited by Over 90% of Malware Families

PowerShell has gained popularity among developers and system administrators due to its powerful scripting capabilities, object-oriented nature and rich interface for communicating with the Windows operating system. Its deep integration with Windows allows users to automate a wide range of tasks, making it a valuable tool for legitimate purposes.

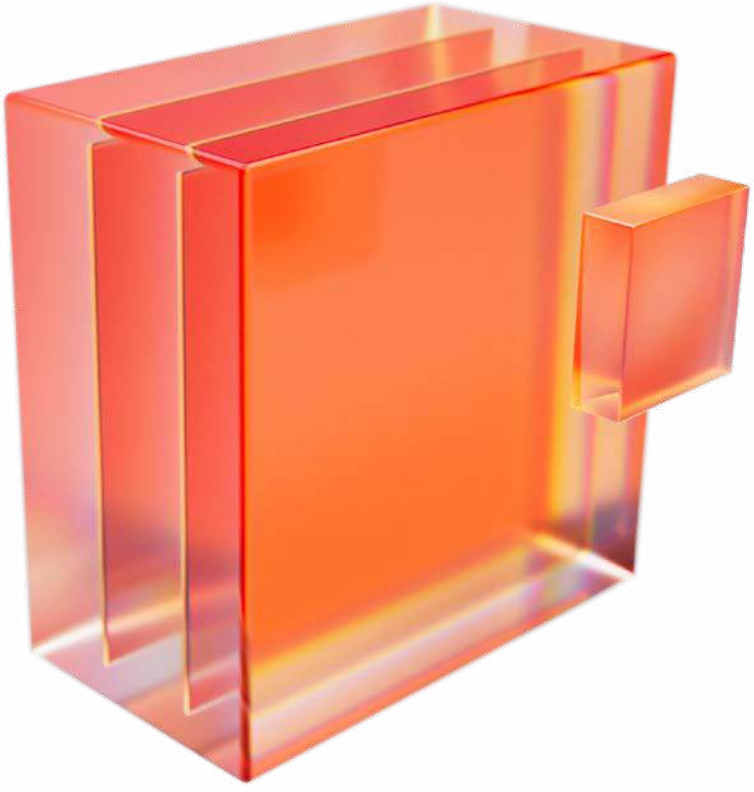
It's unfortunately these same, user-friendly features that make PowerShell an attractive tool for cybercriminals. More than 90% of prevalent malware families are leveraging PowerShell, with 73% using it to either download additional malware or evade detection. It's essentially a staple in any malware family diet. Prominent malware families such as AgentTesla, GuLoader, AsyncRAT, DBatLoader and LokiBot extensively use PowerShell scripts for various malicious tasks.

PowerShell has made extensive efforts to prevent the execution of downloaded scripts with restricted execution policies. Tragically, attackers have found ways to bypass these restrictions by invoking scripts locally or using command-line arguments to execute malicious code.

Recent reports indicate a significant rise in PowerShell-based attacks. The number of threats leveraging PowerShell grew by 208% in late 2020 culminating with its use by almost every malware family. This surge is driven by the increased use of PowerShell in various types of attacks, including process injection and privilege escalation techniques. The use of PowerShell in fileless malware attacks has also increased, as seen in numerous campaigns delivering payloads via PowerShell scripts embedded in spam emails or office document macros.

SOC POV

Our managed services are no strangers to the risks associated with PowerShell. In a 2024 incident, multiple machines were compromised by the Mimikatz tool, widely used by cybercriminals to steal credentials. Upon investigation, we discovered that an encoded PowerShell script was running across several machines. This script was responsible for downloading Mimikatz and executing additional malicious PowerShell commands. Unfortunately, the security policy at the time was set to alert rather than block such scripts, which allowed the malicious activity to spread and cause problems. Adversaries exploited a compromised, unprotected machine within the network to deploy and spread these harmful scripts internally. This incident highlighted the critical need for robust security configurations and a proactive response to security alerts to mitigate the misuse of PowerShell in cyber-attacks.



Escalating Risks of IoT Attacks

As we progress through 2024, the landscape of IoT security continues to develop, marked by a measurable increase in attacks targeting Internet of Things (IoT) devices. Our data reveals a dramatic 107% increase in IoT attacks year-over-year for the first half of 2024. This rise underscores that attackers are more frequently targeting IoT devices, likely due to the fact that IoT devices tend to be easier targets. These devices often lack robust security measures, while simultaneously the attack surfaces of mainstream systems such as Microsoft Windows continues to be hardened.

The TP-Link command injection vulnerability (CVE-2023-1389) has emerged as a significant threat among the numerous vulnerabilities exploited by cybercriminals. This vulnerability is one of the primary drivers of the drastic increase in attacks in 2024, with a notable spike in May. It ranks as the second most widespread attack, impacting 21.25% of small- to medium-sized businesses (SMBs). The exploitation of this flaw has been a driving factor in the spread of the notorious Mirai malware, which hijacks IoT devices to form botnets capable of executing large-scale Distributed Denial-of-Service (DDoS) attacks. Our team has reported on the increase in activity and the common features among the vulnerabilities exploited by threat actors. Although this vulnerability has existed since 2023, attackers have only began to leverage it in large quantities recently, aligning with the broader trend of exploiting older vulnerabilities.

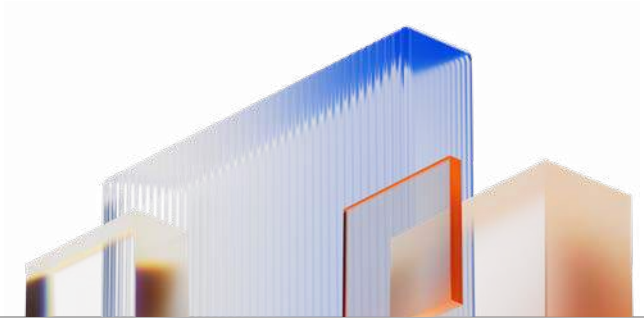
Another critical vulnerability being exploited is the Zyxel Remote Code Execution flaw, which ranks as the fourth most widespread attack in 2024. Affecting 20.5% of small businesses, this vulnerability also facilitates the spread of Mirai, further underscoring the pervasive nature of this malware.

The Impact of IoT Attacks

The rise in IoT attacks has become a significant concern for global cybersecurity leaders, with incidents like the Volt Typhoon botnet attack and the coordinated assault on Denmark's energy sector illustrating the growing threat. In the Volt Typhoon attack, a Chinese state-sponsored hacking group compromised hundreds of SOHO routers in the U.S., forming a botnet used to conceal further hacking activities targeting critical infrastructure. These compromised routers, primarily from Cisco and NetGear, were outdated and unsupported, making them particularly vulnerable to exploitation.

Similarly, in May 2023, a coordinated cyberattack targeted 22 energy firms in Denmark. Hackers exploited multiple vulnerabilities in Zyxel firewalls, gaining control over the systems and executing commands. This attack, identified as the largest against Danish critical infrastructure to date, highlighted the attackers' capability to disrupt energy operations and use compromised devices for DDoS attacks.

These incidents align with the trends we observed in the first half of 2024, with a significant increase in attackers targeting and leveraging IoT devices. Since IoT devices are often integral to critical infrastructure, successful attacks can be highly lucrative for cybercriminals.



Phishing Tactics: How HTML, AI and QR Codes Are Redefining Cybersecurity

Phishing tactics have come a long way, becoming more sophisticated and leveraging advanced technologies. HTML phishing is still a widespread and effective method for stealing credentials. Our data shows more than 1,200 new threats a month on average from Q4 2023 through the first half of 2024. Attackers typically use alarming language to scare victims into entering their credentials to view important documents, sometimes pre-filling the email address and requiring only the password. Once entered, the credentials are sent to a malicious server, and the user is redirected to a legitimate website to avoid suspicion. These HTML files are often obfuscated using techniques like iframe redirection and JavaScript to evade detection.

We've recently noticed a trend with the rise of QR code phishing, or "quishing." In quishing, attackers embed QR codes in phishing emails, encouraging recipients to scan them with their smartphones. These codes typically lead to phishing URLs that mimic legitimate login pages, such as Microsoft's, to harvest credentials. Industry reports indicate a dramatic increase in quishing attacks, rising from 0.8% in 2021 to 10.8% of all phishing attacks in 2024. This method is particularly effective as it exploits the growing use of smartphones and QR codes. QR codes were once relatively niche, but you can now find them in department stores and on tables in restaurants leading to menus, coupons and more. It's likely that the rise in this type of attack aligns with the rise of QR code use in general.

Phishing attacks have also become more multi-faceted, utilizing various communication channels to increase their success rates. Artificial Intelligence (AI) is increasingly used to enhance the effectiveness of phishing attacks. AI tools enable attackers to craft highly personalized phishing messages that are more convincing and harder to detect. Attackers might start with an email and then follow up through Microsoft Teams, Slack or SMS, making the phishing attempt appear more credible. This multi-channel approach has been lucrative for bad actors, with platforms like Microsoft Teams accounting for a significant portion of these secondary attacks.

Phishing tactics have evolved to exploit human behavior more effectively. The landscape of phishing in 2024 presents complex challenges that require advanced detection and prevention measures.

Figure 1: Quishing Email

SOC POV

SOCs actively monitor configurations that facilitate credential compromise, such as when MFA is disabled or passwords are improperly accessed. In 2023, our SOC responded to over 800 alerts related to MFA being disabled. Alarmingly, in the first half of 2024 alone, we have already addressed over 650 alerts for the same issue, indicating that 2024 is on pace to nearly double the number of MFA-related alerts from last year. This trend is closely tied to the evolving landscape of phishing attacks, which often target weaknesses in MFA deployment. The significant rise in MFA-related alerts showcases the growing success of these phishing strategies. All of this combined underscore the importance of robust monitoring to protect against credential compromise.

INSURANCE POV

Most ransomware attacks reported to insurance are due to a successful phishing-style attack.

Actionable Insights for Today's Evolving Threats

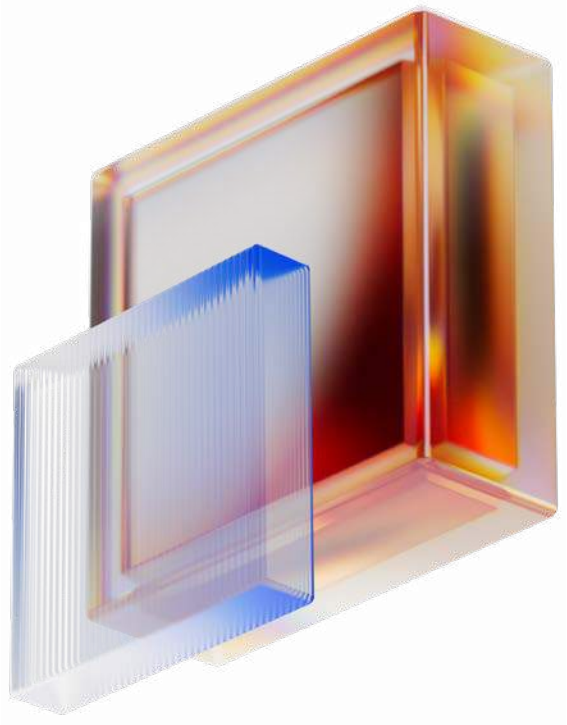
Challenges to Overcome When Developing a Healthy Security Posture

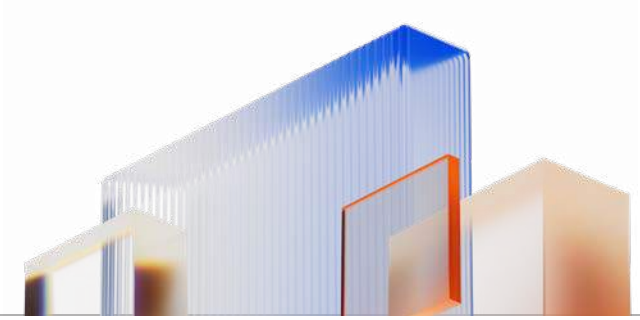
Understanding the challenges around creating good cybersecurity hygiene is crucial. Identifying the hurdles is the first step to addressing barriers that may hinder the implementation of effective security practices. Some common challenges include:

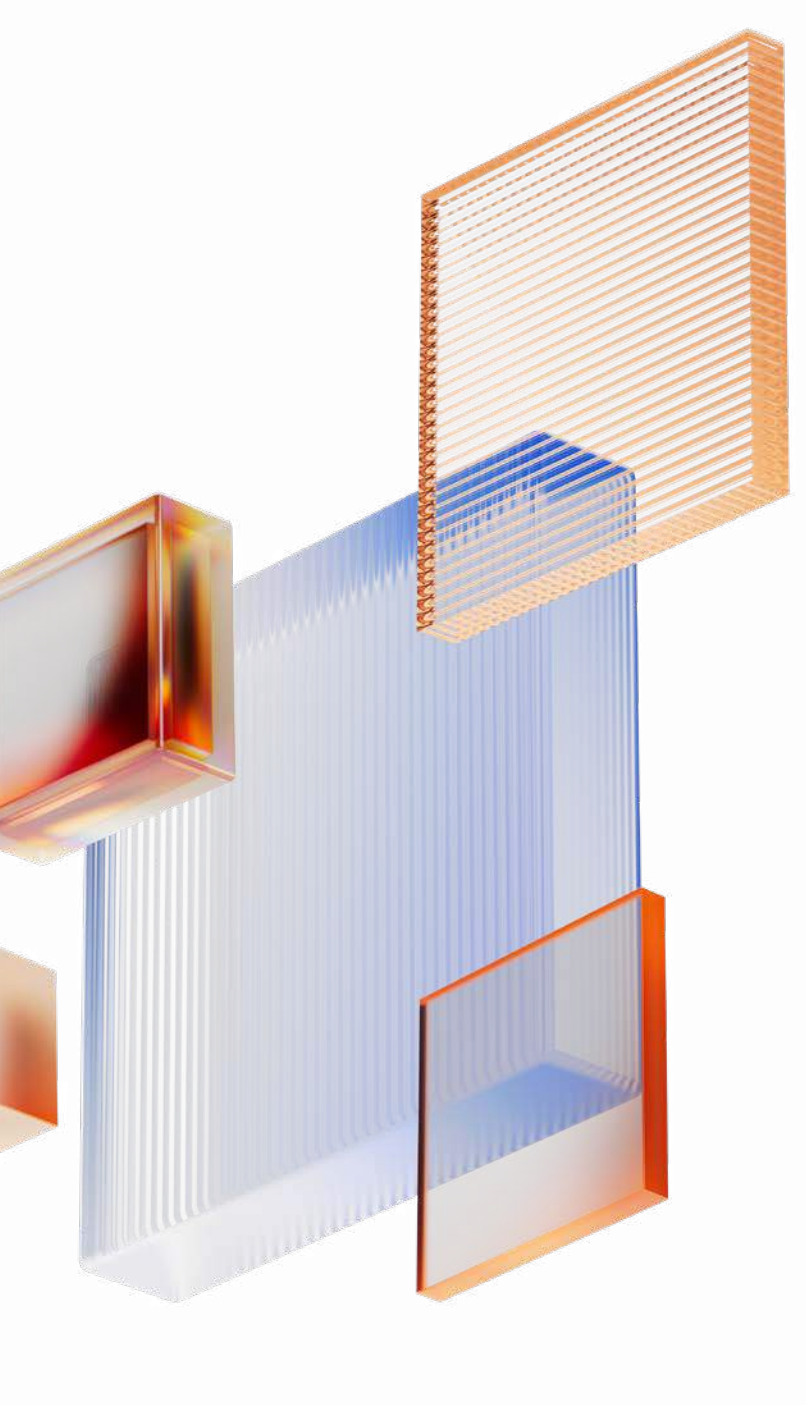
1. **Human Error:** Human error poses a significant cybersecurity challenge due to its potential to inadvertently expose vulnerabilities or mishandle sensitive information, thereby increasing the risk of data breaches or unauthorized access.
2. **Misconfigured Security Solutions:** Misconfigured security solutions, especially in cloud environments, can lead to critical gaps in defense mechanisms, leaving systems and networks exposed to cyber threats and unauthorized access.
3. **Blocking vs Alerting:** Choosing between blocking and alerting strategies in cybersecurity is crucial. Over-reliance on alerting can lead to unblocked threats, while excessive alerts can overwhelm analysts, causing alert fatigue and potentially overlooking critical security incidents.
4. **Procrastinated Patching:** In many cases, vulnerabilities and similar malware have been previously disclosed, but software or hardware remain unpatched due to delayed or absent updates. This leaves devices vulnerable to exploitation even after fixes are available.
5. **Default Configurations:** Often software and hardware are not designed to perform optimally out of the box. Taking the time to fine-tune a piece of hardware or device can ensure a higher level of security.

SOC POV

In 2024, one of our MSPs responded to a financial customer who was breached and infected with ransomware due to RDP being left externally accessible. This known misconfiguration is still seen and can be extremely costly to an organization.







Proactive Steps to Bolster your Cybersecurity Posture

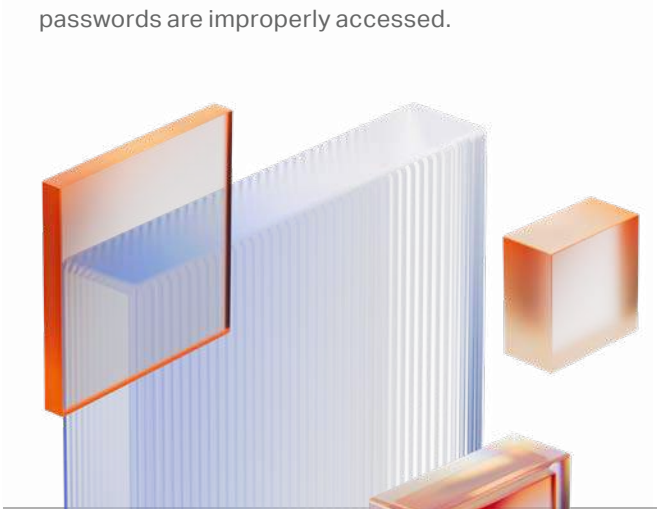
The modern threat landscape moves incredibly quickly, especially with the rise of AI – no organization is immune. But one thing that hasn't changed is that many of the attacks and threats outlined in this report can be avoided with proper cybersecurity hygiene. Some proactive steps that can significantly bolster your cybersecurity posture include:

- **Prioritize Rapid Patching:** Regular patching is essential as it mitigates vulnerabilities and reduces the risk of exploitation by malicious actors – who strike with alarming speed.
- **Add Multifactor Authentication (MFA):** MFA enhances cybersecurity by requiring additional verification steps beyond passwords, significantly strengthening access controls and thwarting unauthorized entry attempts.
- **Augment Cloud Security:** As businesses regularly push data and operations to the cloud, robust measures like Security Service Edge (SSE) and Zero-Trust Network Architecture (ZTNA) need to be in place to protect data and applications, ensuring comprehensive defense against evolving cyber threats in cloud environments.
- **Continuous Monitoring and Incident Response:** Deploying tools for real-time threat detection and developing a robust incident response plan can help mitigate and contain cyberattacks swiftly. Consider utilizing a Security Operation Center (SOC) to add a human layer as well as 24/7 threat detection.
- **Network Segmentation:** Divide networks into smaller, secure segments to limit the impact of breaches and unauthorized access.
- **Ongoing Training:** Continuous cybersecurity training is vital to keep professionals updated on evolving threats, defense strategies and regulations, enabling swift threat recognition and response to prevent data breaches and financial losses. It fosters a proactive cybersecurity culture, enhancing organizational resilience against emerging threats.

Takeaways

SOC Takeaways

- Effective patch management protocols can help reduce exposure to older vulnerabilities.
- Enhance security by deploying automatic patching, ensuring that vulnerabilities are addressed promptly, and the window of exposure to potential exploits is reduced.
- Tuesday morning between 3am and 6am is when the majority of critical attacks occur - outside of typical work hours.
- Location-based alerts are vital for enhancing MFA security and helping SOC analysts identify and mitigate unauthorized access attempts.
- Set security policies to block rather than simply alert, which prevents malicious activity from spreading and causing issues.
- SOCs actively monitor configurations that facilitate credential compromise, such as when MFA is disabled or passwords are improperly accessed.



Insurance Provider Takeaways

- Despite ransomware getting the lion's share of media headlines, business email compromise (BEC) attacks are alive and well; for every one ransomware event, we see ten BEC attacks.
- It is still prevalent to see organizations that have not deployed MFA, which drastically reduces the difficulty of attack.
- In most cases, insurance companies will *not* pay claims if MFA is not enabled on an impacted email, email system or server.
- Most ransomware attacks reported to insurance are due to a successful phishing-style attack.

Partner Takeaways

- Most cybersecurity breaches include some degree of human error.
- The best way to battle these errors is through reducing opportunity and increasing education.
- Limiting opportunities for error will help prevent common mistakes.

SonicWall Inc.
1033 McCarthy Boulevard
Milpitas, CA 95035

www.sonicwall.com

The SonicWall Threat Report could not be possible without the tireless efforts of the Capture Labs Team.

About SonicWall

SonicWall is a cybersecurity forerunner with more than 30 years of expertise and is recognized as a leading partner-first company. With the ability to build, scale and manage security across the cloud, hybrid and traditional environments in real-time, SonicWall provides seamless protection against the most evasive cyberattacks across endless exposure points for increasingly remote, mobile and cloud-enabled users. With its own threat research center, SonicWall can quickly and economically provide purpose-built security solutions to enable any organization—enterprise, government agencies and SMBs—around the world. For more information, visit www.sonicwall.com or follow us on Twitter, LinkedIn, Facebook and Instagram.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035

As a best practice, SonicWall routinely optimizes its methodologies for data collection, analysis and reporting. This includes improvements to data cleansing, changes in data sources and consolidation of threat feeds. Figures published in previous reports may have been adjusted across different time periods, regions or industries.