ARCTIC WOLF

THE STATE OF CYBERSECURITY 2022 TRENDS

Table of Contents

© 2022 ARCTIC WOLF NETWORKS, INC. ALL RIGHTS RESERVED. | PUBLIC

01

FOREWORD

© 2022 ARCTIC WOLF NETWORKS, INC. ALL RIGHTS RESERVED. | PUBLIC

Foreword

In the first full year after the start of the pandemic, 2021 served as a year of reflection for organizations, IT and security professionals, and business owners.

The rapid changes made nearly overnight to infrastructure, applications, and access controls during 2020's huge shift to remote work came under scrutiny, while security teams were still busy defending against the litany of attacks and attack methods.

Arctic Wolf's 2022 Security Trends Report provides insight into the current and future state of these cybersecurity teams as they attempt to move their security programs forward while dealing with an ever-evolving threat environment.

Our research findings show that ransomware, phishing and vulnerabilities don't just monopolize headlines, they're taking up security professionals' headspace, too. Defending an increasing number of threats from attackers with far more resources feels like a lost cause to many businesses.

Organizations are also continuing to struggle to find, train, and retain cybersecurity talent as the rise of the "Great Resignation" in 2021 left IT and security leaders unable to fill their many vacant security roles.

Additionally, with 99% of organizations now using one form of public or private cloud, the rate of cloud adoption is quickly exceeding the internal capabilities of organizations to secure their cloud environments leaving them vulnerable to even more threats.

In 2022, executing on security fundamentals and dealing with perennial threats will continue to be top of mind for IT and security leaders looking to better secure their organizations.

Companies that can rely on a mature security operations practice will find themselves more secure, more resilient, and better able to adapt to the multitude of internal and external risk factors.

What monopolized headlines & took up security professionals' headspace in 2021?

Ransomware

Phishing

Security Vulnerabilities

© 2022 ARCTIC WOLF NETWORKS, INC. ALL RIGHTS RESERVED. | PUBLIC

02

NAVIGATING THE STATE OF CYBERSECURITY

- Financial Motivators Are Leading the Trend
- Some Organizations May Be Destined for Failure

© 2022 ARCTIC WOLF NETWORKS, INC. ALL RIGHTS RESERVED. | PUBLIC

Navigating the State of Cybersecurity

Financial Motivators Are Leading the Trend

To understand where security professionals and IT leaders rank themselves, their risk appetite, and their ability to mitigate cybersecurity risks, we conducted a survey of 300+ global IT security decision makers. Our goal was to understand what IT security leaders considered to be their top priorities and objectives for 2022, and to get first-hand perspective on their current challenges and future concerns.

02

Security product and service spending continues to climb to astronomical heights.

New markets, technologies, and acronyms appear on what feels like a daily basis, while VC funding for new cybersecurity tools shows no signs of slowing down.

For businesses, the dominant feeling is one of constant change.

Cloud adoption often occurs before proper cloud security is in place, the cybersecurity skills gap is a growing obstacle for many companies, and ransomware, phishing, and targeted attacks continue to increase in number each year.

Overburdened and understaffed, organizations find themselves asking the same questions again and again: Where, how, and when will things improve? In what areas? What's most concerning right now, and in the future? How does this impact security strategy? Seeking answers, we've broken down our survey findings to focus on the most critical trends that security professionals must understand and react to over the coming months.

© 2022 ARCTIC WOLF NETWORKS, INC. ALL RIGHTS RESERVED. | PUBLIC

02 Navigating the State of Cybersecurity

Some Organizations May Be Destined for Failure

50%

of IT leaders in our survey confirmed that their cybersecurity budget fails to meet the minimum figure they need to remain on track with their security goals.

In this report we identify the continued trend of the well-documented security skills gap that forces many companies to operate with understaffed teams.

Without security budget growth that mirrors the growth of their cyber risk, many enterprises find themselves unable to attract the talent required to deliver a baseline security program.

This lack of human and financial resources compounds with the ever-growing scale and breadth of cybersecurity activities, such as cloud monitoring, security awareness, and vulnerability management, leaving these firms with a weak security posture by default. This ensures they fall behind in their security goals before they even get started.

© 2022 ARCTIC WOLF NETWORKS, INC. ALL RIGHTS RESERVED. | PUBLIC

03

TECHNOLOGY TRENDS

- Modernizing the Traditional Technology Stack
- Endpoint Tools Are Essential
- Cloud Adoption Is Outpacing Cloud Security

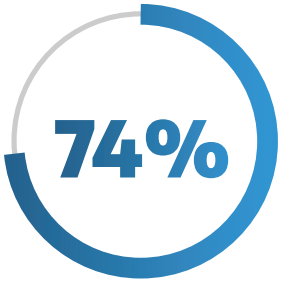
© 2022 ARCTIC WOLF NETWORKS, INC. ALL RIGHTS RESERVED. | PUBLIC

Technology Trends

Modernizing the Traditional Security Stack

Despite the introduction of new technologies and products into the security marketplace, we have found that most organizations still choose to base their cybersecurity technology stack on the traditional "moat and castle" model, with a firewall as the center of their program. This is understandable since firewalls have long been considered the front-line defense of a security program.

03



In our research, we discovered that 74% of those surveyed have invested in either the maintenance or acquisition of one or more firewall/UTM solutions within the last 12 months.

Purchasing and maintaining a firewall is an important step in securing most environments, but we must be careful in how we use them.

First, firewalls should be seen as a key element in a defense-in-depth strategy. They should not, however, be considered the only necessary piece of security technology. While firewalls are key to controlling access and traffic within an environment, they lack many important capabilities that are essential to modern security programs.

In the past year, popular firewall vendors have suffered from security concerns and vulnerabilities. For instance, several high-severity vulnerabilities were identified within commonly used firewalls that, when exploited, give attackers remote attack capabilities. In the surprisingly high number of situations where an organization relies upon a firewall nearly exclusively as its sole security measure, an exploit of this nature renders the firewall almost completely defenseless.

Therefore, firewalls must be supported by additional technologies within a stack to provide a well-rounded defense strategy. They must also be actively monitored and reviewed on a regular basis to ensure they are secure and operate effectively. Furthermore, as the traditional network boundaries become blurred due to evolving architectures and work-from-home business models, the legacy approach of all data processed on ingress and egress through a firewall is obsolete in many cases. This had led some businesses to think beyond the idea of a firewall as the first line of defense for a security stack.

© 2022 ARCTIC WOLF NETWORKS, INC. ALL RIGHTS RESERVED. | PUBLIC

03 Technology Trends

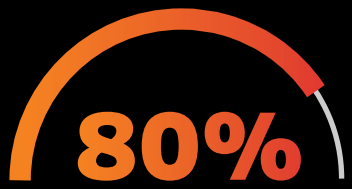
Endpoint Tools Are Essential

Endpoint solutions are another important element of the defense-in-depth strategy, as they are designed to monitor and secure the endpoint devices within a network. This can include laptops, desktops, servers, and in some cases virtual or cloud systems. When considering an endpoint solution, it is important for an organization to understand the goals they hope to achieve since there are a range of purposes and designs within these technologies.

With Microsoft providing Defender by default in Windows, and with macOS/Linux still a relatively small footprint in the world of interactive, laptop, and desktop endpoints, the remaining 20% of IT leaders may use endpoint technology but are either confused with the ever-changing marketing buzzwords (AV, EPP, EDR, XDR, etc.), or are just not sufficiently staffed to use them in a meaningful way. All these possibilities are plausible, as practitioners often forget that organizations without a dedicated security staff far outnumber those that do.

Antivirus and endpoint protection platforms were primarily designed to prevent malicious activity.

They may use a variety of methods to identify threat activity—such as machine learning, signature matching, or behavioral analysis—but their end goal is to stop a potential threat before it can be executed. Endpoint detection and response is a parallel technology that is designed to observe and detect threats that occur on the endpoint rather than prevent them altogether. This ultimately places responsibility on the security analyst to verify and resolve alerts faster than the adversary can achieve its goal.



A surprising data point in our research is that only 80% of surveyed decision makers claim to currently use some form of endpoint technology within their environment.

© 2022 ARCTIC WOLF NETWORKS, INC. ALL RIGHTS RESERVED. | PUBLIC

03 Technology Trends

Endpoint Tools Are Essential

In most cases, EDR is seen as a more holistic and granular technology since, again, it is designed to observe the activities taking place on the endpoint and issue alerts when potential threats are identified, rather than terminating processes.

Many EDR tools are also the basis of threat hunting activities since they catalog large datasets for analysis. Successful use of an EDR tool does require that it is effectively managed by a well-trained set of analysts to achieve the most value from the tool.

The dependency on security analysts is why we found that, of the 80% of surveyed decision makers using endpoint solutions within their environment, only 23% use standalone EDR.

During our analysis we also identified that—of those organizations not currently using EDR—only 12% have current plans to evaluate and implement an EDR solution. This may also result from some vendors consolidating EDR and endpoint protection platform (EPP) capabilities into a single endpoint solution, which eliminates the need for single-purpose EDR.

© 2022 ARCTIC WOLF NETWORKS, INC. ALL RIGHTS RESERVED. | PUBLIC

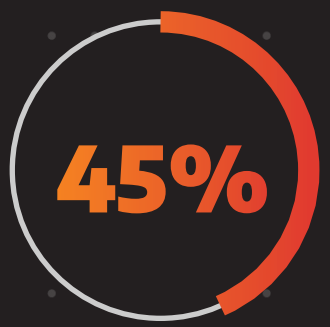
03 Technology Trends

Cloud Adoption Is Outpacing Cloud Security

A recent report on cloud technology noted that 99% of organizations currently use at least one public or private cloud.[5]

This could include anything from cloud storage to SaaS applications to full cloud infrastructures.

Due to the ready availability of cloud solutions, this percentage is expected to grow as barriers to cloud usage decrease.



In fact, a recent Gartner report estimates that, by 2024, more than 45% of IT spending on system infrastructure, infrastructure software, application software, and business process outsourcing will shift from traditional solutions to the cloud.[6]

Unfortunately, our survey found that only 19% of responding organizations use cloud security posture management (CSPM) as a way of securing their cloud resources.

Furthermore, of the 81% of organizations not currently using some form of CSPM, 28% stated that cloud security was their primary concern, but only 22% currently have plans in place to add this capability to their security program.

Coinciding with this, the demand for cloud security skills is expected to increase by 115% in the next five years, and companies can expect these positions to command salaries that are $15,000 higher than security analyst roles with average-growth skills.[7]

© 2022 ARCTIC WOLF NETWORKS, INC. ALL RIGHTS RESERVED. | PUBLIC

03 Technology Trends

Cloud Adoption Is Outpacing Cloud Security

One way cloud providers seek to address cloud security is through the shared responsibility model embraced by technologies like Amazon Web Services (AWS), Google Cloud Platform, and Microsoft Azure.

These providers invest in technologies to further secure these cloud resources, but the shortage of cloud expertise within companies means these security features are not fully and successfully utilized. We find this a troubling trend due to possible security implications of organizations blindly adopting cloud capabilities and infrastructure without having proper safeguards in place.

47%

In a review of Arctic Wolf operational data, we have found that 47% of all customer incidents investigated by our SOC analysts included at least one cloud component.

With the rapid pace at which many organizations integrate these cloud capabilities into their architecture, practitioners must ensure they don't unintentionally deploy misconfigurations and vulnerable entry vectors for attackers, especially when they lack the proper detection and response capabilities.

© 2022 ARCTIC WOLF NETWORKS, INC. ALL RIGHTS RESERVED. | PUBLIC

04

THREATS AND CONCERNS

- Ransomware Concerns Continue
- Phishing Remains a Primary Threat
- Attack Surface Management
- Staffing Obstacles

© 2022 ARCTIC WOLF NETWORKS, INC. ALL RIGHTS RESERVED. | PUBLIC

Threats and Concerns

Ransomware Concerns Continue

As expected, the threat of ransomware and targeted attacks against their business is top of mind for almost everyone. This year saw yet more high-profile ransomware incidents, with an estimated 700 million attacks using ransom or extortion in 2021.[8]

$40 MILLION

This includes some of the highest ransom demands on record, with one financial institution paying $40 million to decrypt its data.

04

Our research found 70% of those surveyed rank ransomware as their top concern entering 2022.

This is likely due to several ransomware trends: the increase in ransom demands are often more than many organizations can pay; the sophistication of ransomware and the social engineering used to deploy it are increasingly complex and successful; and the uptick in criminal gangs using ransomware-as-a-service has lowered the entry barrier even further for would-be attackers.

Gartner's forecast for worldwide security products spending in 2021 was $78 billion,[9] but despite the ongoing increase in product spending, ransomware continues to be the number one threat to most companies. IT leaders must quickly accept that tools and products alone will not resolve this problem and it might require more state-level interference—such as the recent operations targeting REvil and other ransomware actors.

As ransomware continues to evolve, attackers have found numerous strategies to circumvent the defenses of traditional point products, giving way to the continued growth of these attacks.

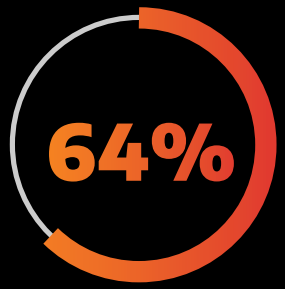
At Arctic Wolf, we have found that the best defense for ransomware is early detection through 24x7 active monitoring of all aspects of an environment along with an immediate response plan of action once a detection occurs.

© 2022 ARCTIC WOLF NETWORKS, INC. ALL RIGHTS RESERVED. | PUBLIC

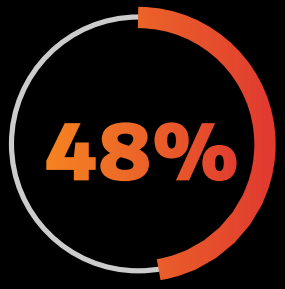
04 Threats and Concerns

Phishing Remains a Primary Threat

Following closely behind ransomware, we found that phishing is the second-most concerning threat for those surveyed.



of respondents listed phishing as one of their primary areas of concern



listed phishing as the cybersecurity topic they would be most interested in learning more about in the coming year.

This trend has real-world validity when we consider that operational research shows 90% of cyber-attacks target an organization's employees.

Attackers have found phishing and social engineering are often a low-risk, high-reward entry vector for initiating a breach. These types of attacks are still a threat even within heavily monitored environments, since they target weaknesses in human interactions rather than vulnerabilities in applications or devices.

Email is one of the oldest networking technologies still in use, and it continues to be one of the most prominent security concerns because many organizations have not taken the proper steps to address potential threats.

To combat phishing, it is important to have a strong security and phishing awareness program as part of your defense-in-depth strategy.

In our survey, we found that 62% of respondents currently use some form of security awareness program and training as a step towards reducing the likelihood of a phishing attack—or at least to encourage users to report potential incidents. We also found that 23% of respondents wish to add a security awareness program or improve their existing one.

© 2022 ARCTIC WOLF NETWORKS, INC. ALL RIGHTS RESERVED. | PUBLIC

04 Threats and Concerns

Attack Surface Management

81%

Our survey results show 81% of respondents rated vulnerabilities and unknown misconfigurations as the biggest security concerns within their environments.

These include both known software vulnerabilities and zero-day exploits, as well as systems which are either incorrectly configured or are not hardened to security standards. An attacker can leverage all of them.

In 2021 there were multiple high-profile exploits that remained unpatched threats long after their initial discovery was disclosed, and patches made available.

For example, a series of zero-day vulnerabilities identified within the Microsoft Exchange platform continued to be exploited throughout the year. Indeed, even as we enter 2022, Shodan.io shows over 30,000 MS Exchange servers are still vulnerable to CVE-2021-31206 and accessible from the internet. Too often many organizations overlook the importance of asset management and configuration management in terms of actively exploited vulnerabilities. When it comes to prioritizing remediation, if they don't have an authoritative list of devices and statuses, they are doomed to fail.

Identifying and addressing vulnerabilities or misconfigurations within an environment is a difficult task and requires a strong risk management program that includes vulnerability scanning and is built on a solid foundation of asset management.

Our survey showed that 30% of responding organizations look to either improve or expand their risk management function as a way of addressing these concerns.

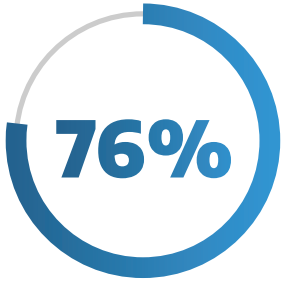
Developing asset identification, software inventories, 24x7 managed detection, and a streamlined patch management process are common ways in which companies can improve along these lines. Initial attack surface reduction can be relatively straightforward, and the most impactful steps are well documented. For example, our operational research showed organizations can prevent 80% of threats just by implementing the top 5 CIS controls, and we also found that 60% of organizations suffered an attack using methods described in the OWASP Top 10.

© 2022 ARCTIC WOLF NETWORKS, INC. ALL RIGHTS RESERVED. | PUBLIC

04 Threats and Concerns

Staffing Obstacles

Recruiting and retaining IT security talent continues to be a difficult challenge across all industries.



of respondents said that the primary obstacle which keeps them from achieving their cybersecurity objectives is either the inability to hire staff or a lack of security expertise among their current staff.

This is commonly referred to as the "cybersecurity skills gap" and is expected to remain a concern for the foreseeable future.

This skills shortage places further strain on organizations when we consider a recent statistic that shows 65% of cybersecurity employees are actively considering leaving their current position.[10]

To address the shortage of skills in the workforce, many organizations now outsource security functions to a service provider.

Almost 30% of our respondents currently use a managed security service such as managed detection and response (MDR), and another 23% want to incorporate one of these managed services within the year. These services offer a simplified way of providing the same security benefits as an in-house security operations center (SOC) but at a much lower cost than hiring the equivalent number of full-time employees needed to do the job.

© 2022 ARCTIC WOLF NETWORKS, INC. ALL RIGHTS RESERVED. | PUBLIC

05

CURRENT STATE TRENDS

- Distributed Security Responsibility
- Lack of 24x7 Support
- Shift Towards Cyber Insurance

© 2022 ARCTIC WOLF NETWORKS, INC. ALL RIGHTS RESERVED. | PUBLIC

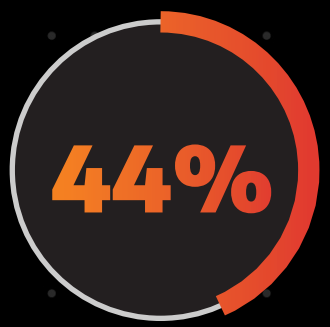
Current State Trends

Distributed Security Responsibility

The responsibility for establishing and managing a cybersecurity program should ideally be distributed among a team of dedicated and well-trained security professionals who can provide 24x7 coverage of the environment.

Unfortunately, due to the cybersecurity skills gap and to fiscal constraints, not all organizations are able to staff a full-time SOC. It typically takes a minimum of six dedicated full-time staff to maintain a high-quality 24x7 SOC operation, which is out of reach for most organizations.

05



We found that 44% of those surveyed do not have any staff members assigned to security as their full-time or primary function.

Without a dedicated cybersecurity team or SOC, security is often relegated to an afterthought for well-intentioned individuals with competing priorities.

Some organizations still try to buy their way ahead of adversaries by adding additional tools to their security stacks to minimize the security responsibility among IT staff.

In fact, 62% of responding organizations now look to add some combination of next-generation endpoint protection, deception technology, or user and entity behavior analytics as a way to identify threats and address security concerns. These can be useful technologies as part of a broader security strategy, but as with any tools, they require a team of analysts with the time and skills to use them effectively.

In most situations, the addition of more tools to a security stack without addressing the underlying staffing shortage presents a liability to an organization, since it increases the amount of potential noise, alert fatigue, and analyst burnout.

© 2022 ARCTIC WOLF NETWORKS, INC. ALL RIGHTS RESERVED. | PUBLIC

05 Current State Trends

Lack of 24x7 Support

For the remaining 56% of responding organizations who do not distribute security responsibilities among their IT staff, 23% employ only one to three staff members who are fully dedicated to the area of cybersecurity.

Maintaining a SOC with continual coverage and redundancy is difficult to achieve with such a limited staff. The minimum headcount of 6 or more full-time security operations team members is a luxury that cannot be afforded by 80% of our respondents.

In our findings we previously described how ransomware, phishing, and vulnerabilities constitute the largest concerns most organizations face when it comes to cyber threats. Many of these threats go undetected if an organization is not fully staffed and continually monitored.

70%

Our operational research shows that 70% of customer environments we defend had latent threats when we were brought onboard.

This means a large portion of company networks may already be infected with threats, but they have yet to be identified.

Even within organizations that can employ a fully staffed SOC, many plan to utilize a managed service provider as a means of assisting their analyst.

This way they can automate their initial triage and investigation tasks through a third-party who owns the work and delivers the guidance and insights needed for remediation. Within these environments and many others, a managed service provider can deliver 24x7 monitoring and response for threats and assist in the multiple support tiers needed to address security concerns. This leaves an organization's existing staff to pursue a more strategic approach to defense with blue, red, or purple team-type engagements.

© 2022 ARCTIC WOLF NETWORKS, INC. ALL RIGHTS RESERVED. | PUBLIC

05 Current State Trends

Shift Towards Cyber Insurance

With ransomware continuing to be both a threat and concern, it is not surprising that many companies now turn to cyber insurance to minimize the financial impact of these attacks.

65%

Of those we surveyed, 65% currently work with some form of cyber insurance within the security program.

The limits of what these policies cover can vary greatly, but they often allow for reduced premiums if certain programmatic guidelines are met by the policy holder.

Of those who are enrolled in cyber insurance, 30% said their premiums have increased, or that their policy was canceled by the insurer within the last year. Such circumstances may be related to a series of factors, including a recent breach within the policy holder's environment, the results of a security audit, or an increased potential of a policyholder becoming the target of attackers.

The remaining 35% of organizations currently operate without any form of cyber insurance. This places them in a position where they become wholly responsible for the financial impact of a breach, including the cost of obtaining outside support for incident response or potentially covering ransom payments. This threat is likely the reason why 15% of those who currently do not have cyber insurance are actively working to obtain it.

© 2022 ARCTIC WOLF NETWORKS, INC. ALL RIGHTS RESERVED. | PUBLIC

06

IMPLEMENTATION AND OBSTACLES

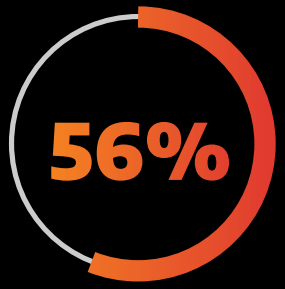
- Concerns with Managing Risk
- Support From Executive Leadership

© 2022 ARCTIC WOLF NETWORKS, INC. ALL RIGHTS RESERVED. | PUBLIC

Implementation and Obstacles

Concerns with Managing Risk

One of the key questions we sought to answer is what IT leaders feel is their primary concern related to the implementation of their cybersecurity strategy.



To that end, 56% of respondents identified the inability to adequately manage risk and the development of a risk management program.

They feel that they lack the ability to actively influence and implement programs that could lower the risk to their business.

06

All elements of the modern IT environment include some level of risk, and how a company chooses to address this risk has a direct correlation to its potential to suffer a serious security incident.

For example, as we stated previously, there is a vast trend today of organizations accelerating their adoption of cloud capabilities. This adoption comes with a series of risks, as it expands outside of traditional network boundaries, and businesses are forced to share infrastructure management and security responsibilities with cloud providers.

The development of an effective risk management program is crucial to the success of any security strategy.

Companies must first create a process of discovery to identify and categorize software and assets. Benchmarking their current risk posture then allows companies to assess the situation and identify areas for improvement. From here, patching and hardening systems can help safeguard them from future threats. To accomplish these tasks, a company must devote the time necessary to ensure these steps are completed correctly—or they can seek out a managed risk solution provider that can help.

© 2022 ARCTIC WOLF NETWORKS, INC. ALL RIGHTS RESERVED. | PUBLIC

06 Implementation and Obstacles

Support From Executive Leadership

74%

Despite the complaints—lack of staff, lack of budget—74% of respondents feel that they are well supported by their business leadership.

This confirms the growing trend for insight and oversight at the director and board level for current security concerns and cybersecurity initiatives.

In many cases, executive leadership may lead the charge in addressing security concerns.

With the recent increase in successful breaches and compromises and with the primary concern relating to the financial impact on a company, it is not surprising to see many executive sponsors take an active role in the delivery of their organization's security programs.

© 2022 ARCTIC WOLF NETWORKS, INC. ALL RIGHTS RESERVED. | PUBLIC

07

FUTURE STRATEGY

- Questioning the Impact of Work From Home
- Multifactor Authentication Goes Mainstream

© 2022 ARCTIC WOLF NETWORKS, INC. ALL RIGHTS RESERVED. | PUBLIC

Future Strategy

Questioning the Impact of Work From Home

2020 saw a significant shift towards a work from home (WFH) strategy, which many companies had to quickly adopt with the onset of the COVID-19 pandemic.

In many cases, the necessity of continuing business operations through whatever means available took priority over security concerns.

07

In 2021, some organizations transitioned back to physical office locations, while others continued to support the WFH approach.

47%

In our survey we found that 47% of surveyed organizations are interested in learning more about what impact WFH has had on their overall cybersecurity posture.

As the traditional network perimeter vanishes, many established security technologies that organizations rely upon become less effective.

At the start of this report, we noted that many companies still use a traditional firewall within their security stack. With the shift to a remote workforce, these firewalls may provide little value in securing a fleet of endpoints residing outside of the network.

Continued adoption of cloud-based endpoint technologies and greater visibility into device and user behaviors are methods being used to help secure WFH devices. If these tools are supported by a skilled workforce of security analysts who can actively monitor them, they provide the benefits of securing both remote and on-site employees.

© 2022 ARCTIC WOLF NETWORKS, INC. ALL RIGHTS RESERVED. | PUBLIC

07 Future Strategy

Multifactor Authentication Goes Mainstream

Mirroring the continued concern over targeted threats, 38% of surveyed individuals stated an interest in learning more about how to integrate multifactor authentication (MFA) into their environments.

In addition, 29% state they currently have a plan in place to implement some form of MFA-based access control.

Growing interest in this area may also be due to many current cyber insurance providers requiring the use of MFA as a condition of their policy, as well as the general consumerization of MFA from social media companies who are keen to avoid account compromises and takeovers that can lead to market manipulation and crypto-currency boosting.

It's now widely accepted that any cybersecurity program can improve by orders of magnitude overnight with the implementation of access control technologies like multifactor authentication.

These tools ensure that a compromised password alone does not grant an attacker access to an environment. In 2020, Microsoft researchers indicated that 99% of the compromised accounts they track monthly didn't use multifactor authentication.[11] Also, in 2021, CISA added single-factor authentication to its list of exceptionally risky cybersecurity practices.[12] Taking this data into consideration, we highly encourage any organization not currently using MFA to adopt this technology.

© 2022 ARCTIC WOLF NETWORKS, INC. ALL RIGHTS RESERVED. | PUBLIC

How Arctic Wolf Can Help

As this survey reveals, cybersecurity continues to evolve at a rapid pace.

In a time of new sophisticated technologies, emerging threats, and a growing attack landscape, it's never been more important to ensure your organization's security. Keep the results of this survey in mind as you work with your team to build a stronger security posture for the rest of 2022 and beyond.

Arctic Wolf is a market leader in security operations, so we can help close the gaps in your cybersecurity defenses, manage your risks, and provide customized compliance reporting.

The Arctic Wolf® Platform delivers automated threat detection and response at scale and empowers organizations of virtually any size to stand up world-class security operations with the push of a button.

For more information about Arctic Wolf, visit **arcticwolf.com**

Additional Sources:

1. Bloomberg: https://www.bloomberg.com/news/articles/2021-07-30/amazon-given-record-888-million-eu-fine-for-data-privacy-breach
2. CNET: https://www.cnet.com/personal-finance/crypto/a-timeline-of-the-biggest-ransomware-attacks/
3. IBM: https://www.ibm.com/security/data-breach
4. Verizon: https://enterprise.verizon.com/content/verizonenterprise/us/en/index/resources/reports/2021-dbir-executive-brief.pdf
5. Flexera: https://www.flexera.com/about-us/press-center/flexera-releases-2021-state-of-the-cloud-report
6. Gartner: https://www.gartner.com/smarterwithgartner/cloud-shift-impacts-all-it-markets
7. Buring Glass: https://www.burning-glass.com/top-cybersecurity-skills-for-2021-apps-cloud-will-dominate-demand/
8. Sonicwall: https://blog.sonicwall.com/en-us/2021/10/cyber-threat-alert-ransomware-breaks-another-record/
9. Gartner: https://www.gartner.com/en/newsroom/press-releases/2021-05-17-gartner-forecasts-worldwide-security-and-risk-managem
10. Cybrary: https://www.cybrary.it/blog/talent-retention-for-top-cybersecurity-talent/
11. Microsoft: https://www.zdnet.com/article/microsoft-99-9-of-compromised-accounts-did-not-use-multi-factor-authentication/
12. CISA: https://www.cisa.gov/uscert/ncas/current-activity/2021/08/30/cisa-adds-single-factor-authentication-list-bad-practices

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

© 2022 ARCTIC WOLF NETWORKS, INC. ALL RIGHTS RESERVED. | PUBLIC