Microsoft Security

Cyber Resilience:

9 in 10 security leaders who reported feeling vulnerable to attacks believe security is an enabler of business.

Microsoft Security conducted a survey of more than 500 security professionals to understand emerging security trends and top concerns among CISOs.

Learn how security leaders are tackling the most sophisticated threat landscape they've ever seen and why they're optimistic about the future.

5 steps to cyber resilience:

1. Embrace vulnerability as a fact of hybrid work and move to resilience
2. Limit how far ransomware attackers can get
3. Elevate cybersecurity into a strategic business function
4. Recognize that you may already have what you need to manage rising threats
5. Implement the fundamentals of security

The past few years have accelerated three existing trends and the tension among them: (1) how to be competitive in a fast-evolving business landscape, (2) how to defend against increasingly serious cyber threats, and (3) how to achieve both goals while reducing complexity and digitally transforming.

With the adoption of hybrid work, corporate networks are becoming more dispersed, complicated, and ambiguous. If businesses are to manage risk in this hyper-connected virtual space, cybersecurity strategy must evolve. Fundamentals like multi-factor authentication (MFA) and patching are still the cornerstone of security, but a perimeter-based approach to security is no longer viable. Instead, organizations can undermine the impact of escalating security threats by shifting to a posture of resilience.

Our recent survey of more than 500 security professionals shows this shift is underway, as leaders now focus on preparing for threats and attacks rather than preventing them. The emerging approach elevates security into a strategic business function that enables how we work today while mitigating the risk and minimizing the impact of attack.

1 Embrace vulnerability as a fact of hybrid work and move to resilience

Hybrid work has propelled businesses of all types into the cloud, dispelling any illusion of a perimeter. More than ever, work happens in difficult-to-defend spaces—across platforms, cloud applications, personal devices, and home networks. It's no wonder that two out of three security leaders say hybrid work has made their organization less secure. Cloud and network vulnerabilities are the top security concern for security leaders today, superseding even the perennial threat of malware. 61 percent of security leaders identify cloud infrastructure and cloud applications as the feature of the digital environment most susceptible to attack, followed by networks. About half point to email and collaboration tools—the instruments of remote work—as their most vulnerable digital feature.

45% of security professionals identify email and collaboration tools as the aspect of their organization most susceptible to attacks.

61% of security leaders say the cloud is the digital feature most susceptible to attack.

2 out of 3 say hybrid work has made their organization less secure.

40% of all attacks last year—and half of all cloud attacks—significantly impacted the business.

These leaders are right to be concerned. In our research, breaches due to cloud misconfiguration are just as common as malware attacks—and are even *more associated with significant damage to the business.* About one in three businesses reported a cloud misconfiguration issue in the past year, a higher incidence than any other attack and on par with malware. But cloud and malware attacks diverged in the severity of their impact. Whereas about half of cloud and IoT breach victims reported significant business impact (operational downtime, sensitive data stolen, and reputational damage) from security attacks, fewer than a third of malware and phishing victims suffered this level of damage. Altogether, about 40 percent of security breaches in the past year significantly impacted the business, according to security decision makers.

Top concerns and recent attacks

Security leaders concerns mirror recent attacks

	Top concerns	Attacks last year
Cloud misconfiguration	37%	30%
Malware	36%	28%
Phishing	31%	24%
IoT device attacks	30%	24%
Ransomware	28%	17%
Denial of service attacks	26%	20%
Social engineering	24%	23%
Zero day exploits/attacks	24%	20%
Supply chain compromise	23%	21%
Compromised credentials	19%	21%
None of these	0%	14%

Organizations significantly impacted when attack type present

Impact of recent attacks show the importance of both prevention and detection and response

Denial of service attacks	57%
Social engineering	49%
Cloud misconfiguration	49%
Zero day exploits/attacks	49%
Supply chain compromise	48%
Ransomware	48%
IoT device attacks	47%
Compromised credentials	36%
Malware	34%
Phishing	27%

Today's hybrid networks, deployed across multiple platforms and cloud environments, elude traditional security measures. Security leaders and practitioners alike identify "difficulty managing a multi-cloud environment" as their single biggest security challenge. About a third report challenges securing the organization across multiple platforms. These dispersed cloud networks are inherently difficult to secure; for instance, there can be thousands of policies which can make it challenging to figure out which ones are active.

With hybrid work here to stay, businesses won't have the option to retreat to the walled castle of an internal corporate network. Instead, security leaders must embrace vulnerability as a feature of the hybrid work environment and seek ways to minimize the business impact of attacks.

What security leaders can do: Hire cloud experts.

Securing the cloud is a different game than securing an internal network, with different rules and stakes. Some of our survey respondents count on their practitioners to be "jacks of all trades," while others lean on cloud experts—even cloud engineers who might sit outside the security team. Given that the chief cloud vulnerabilities are administrator errors like misconfiguration and inconsistent application of security policies, our research suggests that it is a good idea to have specialists working on cloud security who understand cloud systems inside and out (even if they don't have traditional security expertise).

2 Limit how far ransomware attackers can get

In a perfect storm of security peril, ransomware is escalating just as corporate networks proliferate across the cloud multiverse. Nearly **one in five** security leaders report being a victim of a ransomware attack in the last year and about a third rank ransomware among their top security concerns. Ransomware grew by 1,070 percent between July 2020 and June 2021, according to the Fortinet 2021 Ransomware Survey Report.

The severity of attack is growing too: ransomware caused an estimated $20 billion in damages in 2021; by 2031, that number is predicted to exceed $265 billion (Cybersecurity Ventures, 2022 Cybersecurity Almanac). The average cost of a ransomware attack is $4.62 million (in escalation, notification, lost business, and response costs—not including the ransom), according to Ponemon Institute's Cost of a Data Breach Report 2021.

The financial cost is only part of the story. About half (48 percent) of ransomware attack victims in our study report that attacks caused significant operational downtime, exposure of sensitive data, and reputational damage.

1 in 5 businesses surveyed experienced a ransomware attack last year.

Half of those attacks significantly impacted the business.

65% Victims that paid the ransom recovered only 65% of their data, and a third got back less than half.

48% of ransomware attack victims report that attacks caused significant operational downtime, exposure of sensitive data, and reputational damage.

On average, organizations that paid the ransom **got back only 65 percent of their data,** with 29 percent getting back no more than half their data.

"Ransomware as a service" is behind the meteoric rise of this crime. Maturing cybercrime supply chains are enabling cybercriminals to buy proven cybercrime kits and services for as little as $66, according to our security researchers. These cheap kits give any criminal opportunist access to better tools and automation to enable scale, increase the sophistication of their attacks, and drive down costs. As a result, the economics behind successful ransomware attacks are fueling their rapid trajectory.

What security leaders can do: Adopt Zero Trust principles.

Ransomware attacks come down to three primary entrance vectors: remote desk protocol (RDP) brute force, vulnerable internet-facing systems, and phishing. Organizations can limit the scope of damage by forcing the attackers to work harder to gain access to multiple business-critical systems. By establishing least-privilege access and adopting Zero Trust principles, attackers who breach a network are less able to travel across the network and find valuable data to lock up (Microsoft Digital Defense Report).

3 Elevate cybersecurity into a strategic business function

Knowledge is power in today's security threat landscape. Our research revealed dramatic correlations between the awareness of vulnerability and a mature security posture that treats security as a strategic business function. More than **half** of security leaders feel vulnerable to a significant cyberattack. And by an overwhelming margin, those who feel most vulnerable are also the most mature in their security posture—83 percent compared to 35 percent of all respondents. Furthermore, nine in ten security leaders who reported feeling vulnerable to attack perceived security as "an enabler of the business."

This represents a paradigm shift in security: the value of a good security posture is in building awareness of the threat landscape and focusing on resilience, not in getting hyper-focused on preventing individual attacks.[1]

Over half of security leaders feel vulnerable to a significant cyberattack.

83% Vulnerability is highly correlated with a mature security posture (83%) and with viewing security as a strategic business function (90%).

78% of those who feel extremely vulnerable to attack have a comprehensive Zero Trust implementation.

This shift toward a security resilience model is shown by the Zero Trust adoption data in correlation to vulnerability and a strong security posture. Nearly all (98 percent) of respondents who felt extremely vulnerable to attack were implementing Zero Trust—and 78 percent already have a comprehensive Zero Trust strategy in place. Zero Trust assumes breach and optimizes for resilience rather than protection. In interviews, respondents who indicated maturity in their Zero Trust journey were also more likely to see attacks as an inevitability rather than a preventable threat. Our research confirmed that those with Zero Trust maturity did not report a lower incidence of attack. But Zero Trust has been shown to reduce the average cost of breach by 35 percent—from $5.04 million without Zero Trust to $3.28 million with a mature Zero Trust deployment (Cost of a Data Breach Report 2021).

74% of security decision makers that have a comprehensive Zero Trust implementation report that their security posture is significantly above their peers.

What security leaders can do: Assess your Zero Trust approach.

It is this resilient security posture that elevates security from a protective service to a strategic business enabler. In interviews, CISOs credit this proactive approach to security with facilitating hybrid work, improving consumer experience and confidence, and supporting innovation. Zero Trust adoption is integral to resilience. You can assess the Zero Trust maturity stage of your organization with targeted evaluation tools from Microsoft Security.

4 Recognize that you may already have what you need to manage rising threats

Mature security organizations are realistic about the threats inherent in today's increasingly complex digital environments—and *optimistic* about their ability to manage future challenges. Two years down the road, security leaders anticipate that even the most vulnerable aspects of their digital environment today will become less of a liability. For example, while nearly 60 percent of leaders see networks as a vulnerability today, only 40 percent see this issue persisting two years from now—in other words, a third of the leaders concerned today feel networks will no longer be a major issue in two years. Concern for all other features similarly falls off in the two-year outlook, with 26 percent less citing email and collaboration tools and end users as an anticipated concern; about 20 percent fewer seeing supply chain vulnerability as a top concern; and 10 to 15 percent fewer respondents citing endpoints and cloud applications as a top security concern in two years compared to today. Only **Operational Technology and IoT are expected to be the same or more of a challenge** two years from now.

Only IoT is expected to be as much of an issue in two years as it is today; all other security challenges are expected to diminish in impact.

28% fewer respondents see networks as a significant security concern in two years as they do today.

The decline in concern across nearly all security features is a noteworthy finding given the consensus that cyber threats are becoming *more* serious—higher impact and more difficult to elude. How can attacks be increasing in severity but declining as a risk? Implicit in these findings is a confidence among security professionals that today's approach to security will better protect their organizations in coming years as it is implemented across supply chains, partner networks, and ecosystems. In a recent study by the World Economic Forum, the vast majority of security leaders (88 percent) cited concerns about the cyber resilience of small and medium-sized enterprises (SMEs) in their ecosystems. SMEs are likely to be targeted as the weaker link until they achieve the same maturity in their security posture.

Concerns around threats, now and in two years

Security leaders feel optimistic about all threats—except OT/IoT

	Current threats	Threats in two years
Cloud infrastructure	61% to	50%
Cloud applications	59% to	53%
Networks	58% to	42%
Email/collaboration tools	45% to	34%
Endpoints	39% to	33%
End users	39% to	29%
OT/IoT	37% to	37%
Supply chain	37% to	30%
On-premises workloads	27% to	22%

What security leaders can do: Ensure comprehensive implementation of security tools.

Prioritize a strong Zero Trust strategy and ensure a comprehensive implementation to act as the foundation of your security model and guide future investments and projects. Ensure your existing security investments—like endpoint detection and response, email security, identity and access management, cloud access security broker, and built-in threat protection tools—are properly configured and fully implemented. For those who have Microsoft products, learn more about how to get the most out of your Microsoft investments and strengthen your Zero Trust strategy.

5 Implement the fundamentals of security

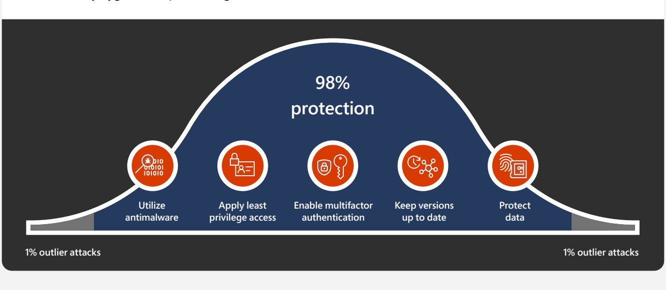
With staff and budgets stretched thin, it's more important than ever for security leaders to manage risk and set the right priorities. Many leaders tell us that strengthening their cyber hygiene to prevent the most common lines of attack, especially across their growing digital footprint, is their top priority. Our data and research support this sentiment—we estimate that basic security hygiene still protects against 98 percent of attacks (see page 124 in the Microsoft Digital Defense Report, October 2021).

98% Basic security hygiene still protects against 98% percent of attacks.

22% Only 22% percent of Azure customers have implemented strong identity authentication protection.

The cybersecurity bell curve

Basic security hygiene still protects against 98% of attacks



Nearly all cyberattacks could be thwarted by enabling multifactor authentication (MFA), applying least privilege access, updating software, installing anti-malware, and protecting data. Yet low adoption of strong identity authentication persists. Our internal research shows that across industries, only 22 percent of customers using Microsoft Azure Active Directory (Azure AD), Microsoft's Cloud Identity Solution, have implemented strong identity authentication protection as of December 2021 (Cyber Signals).

What security leaders can do: Start with identity.

Christopher Glyer, Principal Threat Intelligence Lead at Microsoft Threat Intelligence Center (MSTIC), urges organizations to place a higher security premium on identity: "Having secure identity protections, whether it's MFA, passwordless, or other defenses like conditional access policies, minimize the opportunity and make it much harder to raise the attack bar." Get guidance on identity and the rest of your systems with the Microsoft Security Best Practices.

The path to cyber resilience

The current moment is one of transition. As organizations have increased their reliance on workplace flexibility and accelerated their digital transformation over recent years, they have exposed themselves to new and more serious attacks. The perimeter has expanded and is increasingly hybrid, spanning multiple clouds and platforms. Although new technologies have been a boon to many organizations, enabling productivity and growth even in challenging times, the shifts have also presented an opportunity to cybercriminals, who work to exploit the vulnerabilities found in increasingly complex digital environments. To achieve resilience in the face of attacks, organizations must practice good cyber hygiene, implement architectures that support the principles of Zero Trust, and build cyber risk management into the business.

1 Interestingly, survey results did not reveal a correlation between those who experienced a significant attack and those with a stronger security posture or more comprehensive Zero Trust adoption. This could suggest that vulnerability is driving a stronger security posture, or that reducing attack is not the point—reducing impact is.

Learn more

Explore the latest cybersecurity insights and updates at Microsoft Security Insider.

Share this infographic

Microsoft

All cited Microsoft research uses independent research firms to contact security professionals for both quantitative and qualitative studies, ensuring privacy protections and analytical rigor. Findings included in this document, unless specified otherwise, are a result of Microsoft research studies. The Microsoft research for this report was conducted November, 2021.

© 2022 Microsoft Corporation. All rights reserved. This document is provided "as-is." Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. You bear the risk of using it.