# How to improve cybersecurity posture and overall cyberresilience

Insights and best practices for staying ahead of the threat
by NTT and Microsoft

Continue

# The reality of today’s cybersecurity landscape: defensive strategies aren’t enough

Despite the plethora of available tools and technologies, cybersecurity remains a constant battle for corporations around the globe thanks to the growing sophistication of cybercrime and an ever-changing threat landscape. Bad actors from nation states to professional cybercriminals to disgruntled employees can devastate any given company in mere seconds, without warning, before any internal system can detect them. A recent report from Microsoft shared a sample snapshot of the malicious activity that’s possible in just one 60-second window: 34,740 password attacks, 1,902 Internet of Things (IoT)-based attacks, 1,095 distributed denial-of-service (DDoS) attacks and a host of other attacks ranging from phishing to SQL injection to ransomware and beyond. All in a span of a minute.

So, what’s a company to do – how can organizations possibly stay ahead in an environment where threats are more prevalent than ever and can wreak havoc before they’re detected? The only winning cybersecurity strategy in this day and age is a proactive one. In other words, the best defense is a strong offense and taking that approach requires a combination of battle-tested, frontline experience and deep technical knowledge, along with the agility to respond quickly and mitigate the threat.

# Real-world perspectives from the leaders in managed detection & response

NTT and Microsoft are pre-eminent in managed detection and response (MDR). They've been advising businesses around the globe on their cybersecurity strategies for more than 20 years, working closely with client leadership and security teams to strengthen security postures and increase overall cyberresilience.

The following outlines the insights and best practices these cybersecurity experts have cultivated across thousands of client engagements. Their recommendations underscore the criticality of choosing a comprehensive cybersecurity platform – one that simplifies security across devices, networks, applications and data, while still delivering the swift and robust threat detection, protection and mitigation businesses require.

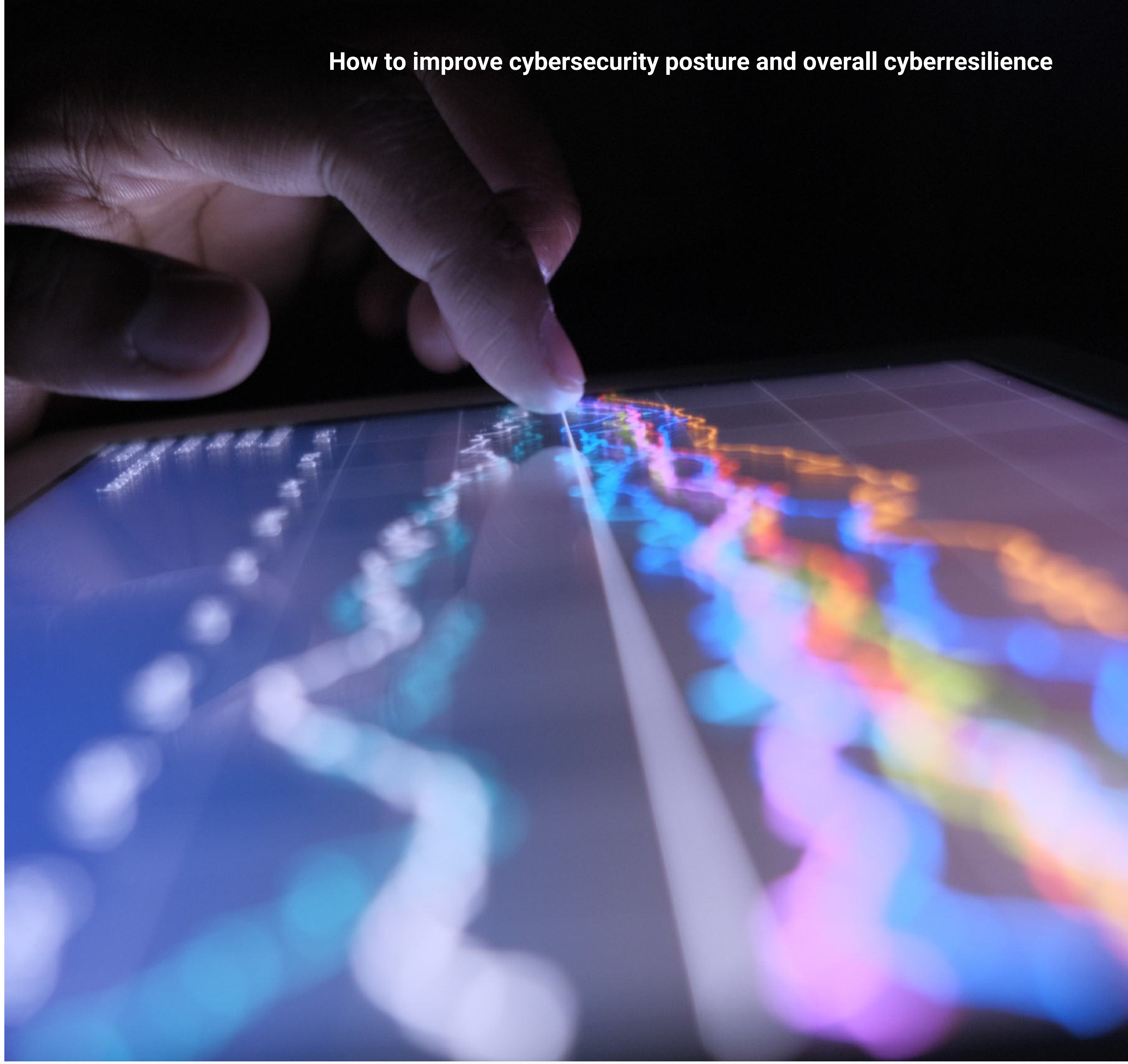
## What are the insights that cybersecurity-focused companies need to consider in planning for the year ahead? Our experts have prioritized the top ten:

1

**Business resilience depends on cyberresilience –** Cybersecurity has taken a permanent place on board meeting agendas for corporations of all sizes and across all industries. Cyberattacks are increasing in frequency and sophistication and are deliberately targeting core business systems to maximize the impact of the attack or likelihood of a ransomware payout. Executives and investors have come to realize that the success of a business – from customer relationships and brand reputation to compliance and operations – is only as secure as the infrastructure on which it runs. For that reason, companies will make cyberresilience a cornerstone of their growth strategy in the months and years ahead.

2

**Visibility is essential to a successful security strategy –** With workforces growing increasingly distributed and attack surfaces expanding in parallel, organizations are plagued with more cybersecurity blind spots than ever before, which cybercriminals know to look for and exploit. Companies will need to invest in services that give them unrestricted ongoing visibility into every corner of their environment, inside and out, to manage such vulnerabilities and detect and prevent attacks.



3

**Security at the speed of cloud is the new standard –** The cloud has become the great enabler for modern business environments where speed and agility are the expectation, whether that means accessing and managing business applications, processing and storing data, or collaborating with colleagues who sit on the other side of the world. But companies need to rethink their security stack to incorporate cloud-based security controls and services. Benefits include the ability to easily scale, automated deployment and updates, and greater agility and flexibility from the power of the cloud.

4

**Turn to an integrated security model to reduce complexity –** To uncover shifting attack techniques and threat vectors and stop them before they do real damage, organizations must be able to see across their applications, endpoints, network, and users. Facing a new economic reality, organizations will also be driven to reduce costs by adopting more of the security capabilities built into their cloud and productivity platforms of choice. To maximize the effectiveness of security organizations, these tools and technologies must be fully integrated to improve efficacy and provide true end-to-end visibility.

5

**The industrialization of cybercrime and the underground ransomware economy is driving an increase in attacks –** Cybercrime has evolved into an industry all its own, a status that brings with it a proliferation of products and services deliberately designed to support today's cybercriminals, like "organizations" that only focus on selling credentials (e.g., initial access brokers). There's also an entire ecosystem of tools that are evolving in a similar way to the microservices architectures being used by organizations to build applications. They are modular with feature sets and service tiers.

6

**Cloud migration is shaping global attacks –** With more companies moving data and infrastructure to the cloud, the preferred approaches to cybercrime are also shifting. For example, a sharp decrease in attacks targeting platforms and network services is giving way to a rise in web-application and application-specific attacks. This will force businesses to refocus, since traditional network security models are losing their effectiveness.

7

**Basic hygiene can never be overlooked –** Companies can invest in every piece of technology on the market, but none of it will work effectively without an unwavering commitment to the fundamentals of strong cybersecurity. Unfortunately, "the basics" are all too often skipped over, and it's an oversight that cybercriminals are just waiting to exploit. Companies must practice good cyber hygiene if all other aspects of their cybersecurity strategy are going to be successful. This includes implementing solutions and workflows that support the principles of Zero Trust and ensuring cyber risk management is integrated into every aspect of the business.

8

**Attacks on identity systems are making detection and response more difficult –** Identity exploitation is on the rise – this includes credential theft and attacking and attempting to exploit the identity system itself – and it's especially hard to detect. That's because the bad actor's newly "acquired" identity gains them unprecedented levels of system access, seemingly from inside the business, making detection and response significantly more difficult.

9

**Ransomware is more prevalent than ever, with Trojans leading the charge –** Ransomware typically is the first thing that comes to mind when someone thinks about a cybersecurity breach, and with good reason. Ransomware is everywhere, with emails embedded with malicious links or attachments as the most common method of infection. Trojan deployments, specifically, have become especially problematic with the re-emergence of botnets, and accounted for 65% of all malware in 2021. Ransomware is such a popular form of attack, that it's become its own cybercrime cottage industry. For example, specialization within the cybercrime circles has fueled offerings such as ransomware as a service (RaaS). And cybercriminals are renting or selling their ransomware tools for profit, rather than performing attacks themselves.

10

**Deeply embedded supply chain vulnerabilities present a huge risk to entire ecosystems and economies –** With the goal of imposing widespread chaos and disruption, cybercriminals are targeting critical supply chain infrastructure at every level, from manufacturing to transportation and distribution. The underlying technology infrastructure, including IoT, operational technology (OT) and integration with the broader digital supply chain ecosystem, create plenty of opportunities for bad actors to gain access. Such vulnerabilities are deeply embedded and often extremely difficult to detect. Adding to the urgency is the fact that thousands of applications or devices may be simultaneously impacted by a single attack elsewhere in the supply chain.

# Advanced preparation and the right partnerships are the key to cyberresilience

To effectively insulate themselves from cyberattacks, companies must rethink the tactical band-aid point-solution approach that has led to so much of the complexity now leaving them vulnerable. Instead, they need to adopt a comprehensive cyberresilience strategy. This is why proactive IT and cybersecurity organizations are embracing MDR services to augment and reinforce their internal teams. MDR services are designed to give businesses real-time detection, response and mitigation capabilities, all delivered remotely 24x7. And they're becoming a staple in security strategies everywhere. According to Gartner®, the MDR market is projected to reach $2.15 billion by 2025, up from $1.03 billion in 2021, a compound annual growth rate of 20.2%.[1]

NTT is a global leader in MDR services with a proven track record of successfully protecting and defending mid-to-large enterprises facing a dynamic and unpredictable threat landscape. In collaboration with Microsoft, NTT provides a scalable, intelligent, cloud-native MDR solution that goes far beyond traditional alerting and notification to deliver swift and remote incident response, investigation and containment. And this turnkey service is fast and easy to deploy, allowing companies to immediately identify hard-to-find threats, disrupt complex and sophisticated cyberattacks and improve cyberresilience. No lengthy and time-consuming implementation or configuration required.

Moreover, with NTT MDR, companies gain visibility across their entire IT environment, so they can see and remove every potential point of vulnerability. There's complete transparency at every turn from alerts to escalations and any other actions within their environment. And because the cloud sits at the core of everything they do, NTT has purpose-built this cloud-native MDR offering with Microsoft to ensure speed, agility and performance for even the most mission-critical environments.

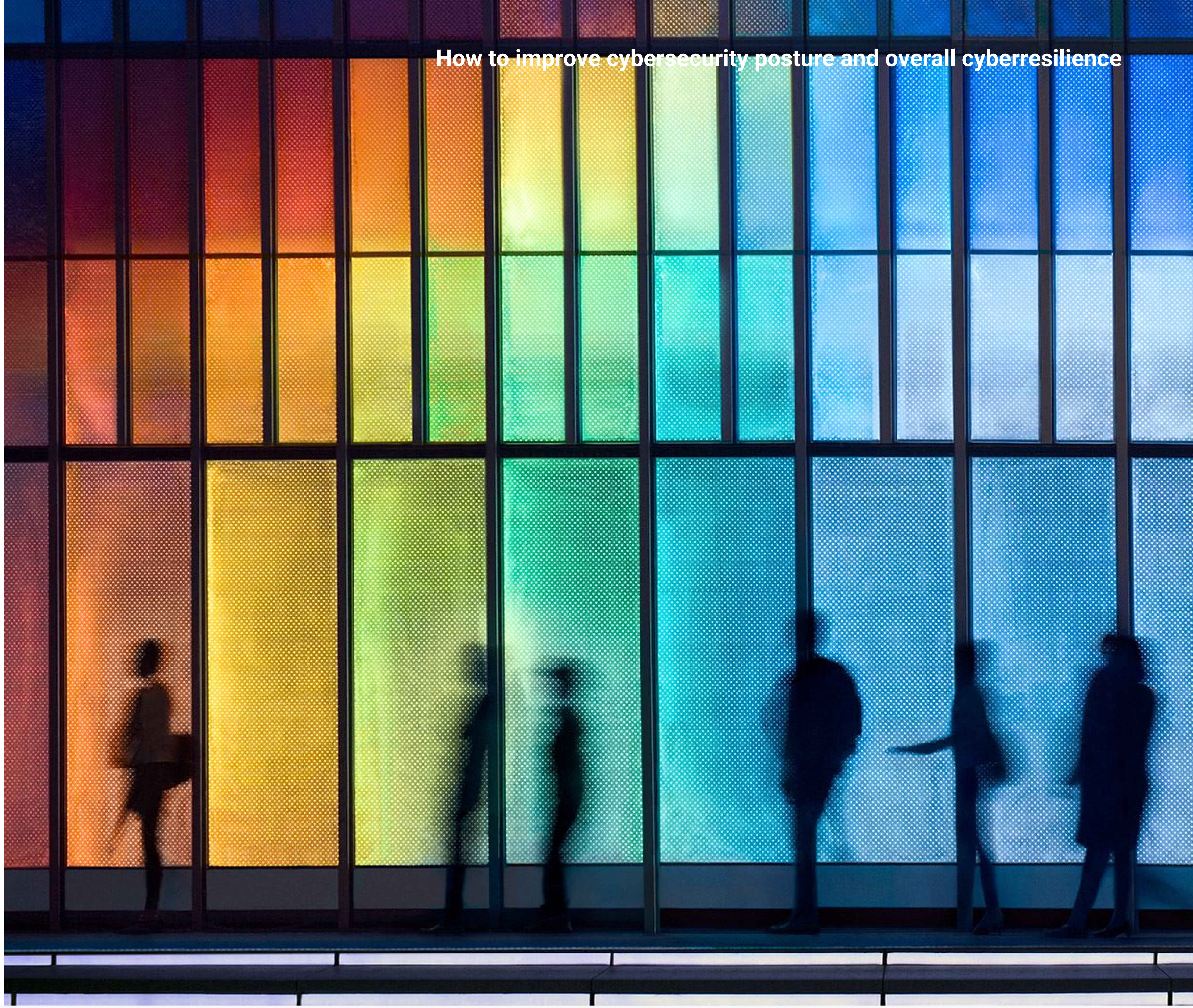
[1] Source: Gartner, Inc., Market Guide for Managed Detection and Response Services, 25 October 2021. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

# Why NTT and Microsoft?

## NTT and Microsoft have worked together to help organizations around the world harness the power of technology to innovate. The partnership boasts:

- Global experience for every local engagement across 47 countries
- Co-innovation centers across the globe to deliver client outcomes at greater speed
- Combined 6,000+ cybersecurity specialists around the world
- 9.5TB of data analyzed every day, helping you find the needle in the haystack
- Serving 5,000+ joint clients globally

Let us help you design, deploy and manage the cybersecurity environment your organization needs to protect and defend against all threats – while delivering the cyberresilience your business requires for strong, uninterrupted, long-term growth.



NTT