Six key cybersecurity trends you need to know about





As the world becomes more connected and digital, cybersecurity is becoming more complicated. As an experienced technology provider, we know how challenging it can be to prioritize where to focus security efforts. Between infrastructure, data, and apps in the cloud, there's a lot more to protect. We can help.



an attacker to begin moving laterally within a corporate network once a device is compromised¹

median time it takes

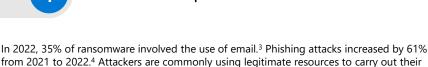
98%

protected against with basic security hygiene²

of cyberattacks can be

Keeping up with today's threats means securing every area of vulnerability, including email, identity, endpoint, Internet of Things (IoT), cloud and the external attack surface. Here are six things you need to know to prevent compromise.

You're only as strong as your weakest link



Email remains a top vector—and a focus area for defense

campaigns. It's getting harder to tell the difference between real and malicious emails. Using safeguards like URL checking and disabling macros will help strengthen your security posture. Tackling more advanced email threats requires that you correlate email signals into broader incidents, visualize the attack, and understand how attackers are taking

advantage of other parts of the environment to leverage legitimate resources. We can help you keep your guard up as threat actors increase the quality of social engineering in their attacks, using AI and other tools to be more persuasive. 72 minutes



The expanded identity landscape also

median time it takes an attacker to access private data if you fall victim to a phishing email⁵



Attackers are getting more creative in circumventing multi-factor authentication (MFA) and phishing kits have made it even easier to steal credentials. The fact is, managing the identity attack surface is more than just securing user accounts. You also need to cover

cloud access and workload identities too. For instance, attackers frequently get access to

expands opportunities for threat actors

third-party accounts and then use those credentials to infiltrate the cloud and steal data. Often, this is accomplished through workload identities, which can be overlooked in permissions auditing. Attacks targeting identity will continue to grow in volume and variety. Let us help you ensure that you have complete visibility into your identity and access.

Password attacks per second in 2022, a 74% increase from 20216



93%

revealed insufficient privilege access and lateral movement controls⁷

of Microsoft investigations during ransomware recovery engagements



more challenging. Unmanaged servers and BYOD personal devices contribute to the shadow IT landscape—and are particularly appealing to threat actors. And it only continues to grow. We are ready to help you improve endpoint visibility and security hygiene.

Hybrid environments and shadow IT have increased endpoint blind spots

3,500 æ, Average number of connected devices in an enterprise that are not protected by an endpoint detection and response agent8

The sheer number of devices in today's hybrid environments has made securing endpoints



IoT devices are proliferating, and so are IoT threats

dangerous vulnerabilities, such as outdated, unsupported software.

more visibility into all your attack surfaces—and that includes IoT devices.

of the least secured aspects of their infrastructure1

IoT devices are an often overlooked endpoint attack vector. Interestingly, as organizations harden routers and networks to make them more difficult to breach, IoT devices are becoming a threat target of choice. For instance, an IoT device can exploit vulnerabilities to turn IoT devices into proxies—using an exposed device as a foothold onto the network. Frequently, organizations often have no visibility into IoT devices, and can even contain

41 billion -0 IoT devices expected in enterprise and consumer environments by 2025¹⁰

There are emerging regulations for IoT security in various countries, but it's vital to gain

Protecting the cloud is critical, but complex

Organizations are increasingly moving infrastructure, application development, workloads, and data to the cloud. This radical shift has increased the number of new attack vectors for

For app development, we recommend embracing a "Shift-left" security approach—that is, thinking about security at the earliest phases of app development. We can help you

> man-in-the-middle phishing attacks detected per month by Microsoft Defender for Cloud Apps, on average12

integrate your cloud and multi-cloud assets with your security tooling.



60%

cybercriminals to exploit, with many gaining access through gaps in permissions security. Cloud app development is a top cloud attack vector. So is cloud storage. And sometimes, cloud services providers themselves can be affected.

of security practitioners say IoT and operational technology (OT) security is one

of organizations that suffered ransomware attacks did not integrate their multi-cloud environments into security operations tooling 13



acquired organizations. Fact is, the internet is now part of the network, and despite its almost unfathomable size, security teams must defend their organization's presence throughout the internet to the same degree as everything behind their firewalls.

entirety of your environment and extended ecosystem.

Securing the external attack surface is an internet-scale challenge

1.613 X cyberattack-related data compromises in 2021; more than all data compromises in 2020¹⁴

Are you aware of your external connections and exposure? Let us help you gain more visibility into your external attack surface and identify vulnerabilities throughout the



caused by a third party from 2018-2020¹⁵

53%

Our services and solutions help to keep your business protected As a Microsoft partner, we're here to help you take advantage of the Microsoft Security

of organizations experienced at least one data breach

solutions that give your business the security strategies you need to keep up with evolving threats. We have the expertise to assess, pilot, and deploy the right Microsoft security solutions for your business, along with a variety of managed services to help streamline

your security operations. Learn more about what we can do to help secure your business.

rt-reveals-more-than-255-million-attacks-in-2022-signaling-a-61-increase-in-phishing-year-over-year-301659518.htm

Contact us today

2022 Microsoft Digital Defense Report, p. 92

**Digital Defense Report, p. 92

**Digital Defense Report, p. 93

**Digital Defense Report, p. 93

**Digital Defense Report, p. 95

**Digital Defense Re

6612948827