Microsoft Security

Anatomy of an external attack surface:

Five elements organizations should monitor

The cybersecurity world continues to become more complex as organizations move to the cloud and shift to decentralized work. Today, the external attack surface spans multiple clouds, complex digital supply chains, and massive third-party ecosystems. Consequently, the sheer scale of now-common global security issues has radically shifted our perception of comprehensive security.

The internet is now part of the network. Despite its almost unfathomable size, security teams must defend their organization's presence across the internet to the same degree as everything behind their firewalls. As more organizations adopt the principles of Zero Trust, protecting both internal and external surfaces becomes an internet-scale challenge. As such, it's increasingly critical for organizations to understand the full scope of their attack surface.

Microsoft acquired RiskIQ in 2021 to help organizations assess the security of their entire digital enterprise. Powered by the RiskIQ Internet Intelligence Graph, organizations can discover and investigate threats across the components, connections, services, IP-connected devices, and infrastructure that make up their attack surface to create a resilient, scalable defense.

For security teams, the sheer depth and breadth of what they need to defend may seem daunting. However, one way to put the scope of their organization's attack surface into perspective is to think about the internet from an attacker's point of view. Below we highlight five areas that help better frame the challenges of effective external attack-surface management.

1 The global attack surface may be bigger than most think

The global attack surface grows with the internet

And it is growing every day. In 2020, the amount of data on the internet hit 40 zettabytes, or 40 trillion gigabytes.[1] RiskIQ found that every minute, 117,298 hosts and 613 domains[2] add to the many interwoven threads making up the global attack surface's intricate fabric. Each of these web properties contains a set of elements, such as its underlying operating systems, frameworks, third-party applications, plugins, and tracking code. With each of these rapidly proliferating sites containing these nuts and bolts, the scope of the global attack surface increases exponentially.

Both legitimate organizations and threat actors contribute to this growth, which means cyber threats increase at scale with the rest of the internet. Sophisticated advanced persistent threats (APTs) and petty cybercriminals alike threaten businesses' safety, targeting their data, brand, intellectual property, systems, and people.

In the first quarter of 2021, CISCO detected 611,877 unique phishing sites,[3] with 32 domain-infringement events and 375 new total threats emerging per minute.[2]

These threats target organizations' employees and customers with rogue assets, looking to fool them into clicking malicious links and phishing for sensitive data, all of which can erode brand confidence and consumer trust.

The global attack surface grows every minute

117,298 hosts created each minute.

613 domains created each minute.

375 375 new threats each minute.[2]

2 Sometimes, threat actors know more about an organization's attack surface than their SOC does

The rise in vulnerabilities from a remote workforce

The rapid growth of internet-exposed assets has dramatically broadened the spectrum of threats and vulnerabilities affecting the average organization. With the advent of COVID-19, digital growth accelerated once again, with almost every organization expanding its digital footprint to accommodate a remote, highly flexible workforce and business model. The result: attackers now have far more access points to probe or exploit.

A new vulnerability landscape

+41% growth in RDP use.

+33% growth in VPN use.

18,378 vulnerabilities reported in 2021.

The use of remote access technologies like RDP (Remote Desktop Protocol) and VPN (Virtual Private Network) skyrocketed 41 percent and 33 percent[4] respectively, with most of the world adopting a work-from-home policy. The global remote desktop software market size, USD 1.53 billion in 2019, will reach USD 4.69 billion by 2027.[5]

Dozens of new vulnerabilities in remote access software and devices have given attackers footholds they never had before. RiskIQ surfaced many vulnerable instances of the most popular remote access and perimeter devices, and the torrential pace of vulnerabilities hasn't slowed. Overall, 18,378 vulnerabilities were reported in 2021.[6]

With the rise of global-scale attacks orchestrated by multiple threat groups and tailored for digital enterprises, security teams need to mitigate vulnerabilities for themselves, third parties, partners, controlled and uncontrolled apps, and services within and among relationships in the digital supply chain.

3 Threat actors don't have to compromise assets to attack an organization or its customers

Digital supply chains, M&A, and shadow IT create a hidden attack surface

Most cyberattacks originate miles away from the network; web applications comprised the vector category most commonly exploited in hacking-related breaches. Unfortunately, most organizations lack a complete view of their internet assets and how those assets connect to the global attack surface. Three significant contributors to this lack of visibility are shadow IT, mergers and acquisitions (M&A), and digital supply chains.

Shadow IT
Where IT can't keep pace with business requirements, the business looks elsewhere for support in developing and deploying new web assets. The security team is frequently in the dark regarding these shadow IT activities and, as a result, cannot bring the created assets within the scope of their security program. Unmanaged and orphaned assets can become a liability in an organization's attack surface over time.

This rapid proliferation of digital assets outside the firewall is now the norm. New RiskIQ customers typically find approximately 30 percent more assets than they thought they had, and RiskIQ detects 15 expired services (susceptible to subdomain takeover) and 143 open ports every minute.[2]

Mergers and acquisitions
Everyday operations and critical business initiatives such as M&A, strategic partnerships, and outsourcing create and expand external attack surfaces. Today, less than 10 percent of deals globally contain cybersecurity due diligence.

There are several common reasons why organizations are not getting a complete view of potential cyber risks during the due diligence process. The first is the sheer scale of the company's digital presence they're acquiring. It's not uncommon for a large organization to have thousands—or even tens of thousands—of active websites and other publicly exposed assets. While IT and security teams in the to-be-acquired company will have an asset register of websites, it's almost always only a partial view of what exists. The more decentralized an organization's IT activities are, the more significant the gap.

Supply chains
The enterprise is increasingly dependent upon the digital alliances that form the modern supply chain. While these dependencies are essential to operating in the 21st century, they also create a cluttered, layered, and highly complicated web of third-party relationships, many of which are outside the purview of security and risk teams to protect and defend proactively. As a result, quickly identifying vulnerable digital assets that signal risk is a massive challenge.

A lack of understanding and visibility into these dependencies have made third-party attacks one of the most frequent and effective vectors for threat actors. A significant amount of attacks now come through the digital supply chain. Today, 70 percent of IT professionals indicated a moderate-to-high level of dependency on external entities that might include third, fourth, or fifth parties.[9] At the same time, 53 percent of organizations have experienced at least one data breach caused by a third party.[10]

While large-scale supply chain attacks become more common, organizations deal with smaller ones daily. Digital credit card skimming malware like Magecart affects third-party e-commerce plugins. In February 2022, RiskIQ detected more than 300 domains affected by Magecart digital credit card-skimming malware.[11]

At risk dependencies

15 expired services per minute.[2]

<10% of deals contain cybersecurity due diligence.[7]

53% of organizations experienced at least one data breach caused by a third party.[8]

4 The mobile attack surface goes beyond major mobile app stores

App stores across the world contain apps targeting organizations and their customers

Each year, businesses invest more in mobile as the average consumer's lifestyle becomes more mobile-centric. Americans now spend more time on mobile than watching live TV, and social distancing caused them to migrate more of their physical needs to mobile, such as shopping and education. App Annie shows that mobile spending grew to a staggering $170 billion in 2021, a year over year growth of 19 percent.[12]

This demand for mobile creates a massive proliferation of mobile apps. Users downloaded 218 billion apps in 2020. Meanwhile, RiskIQ noted a 33 percent overall growth in mobile apps available in 2020, with 23 appearing every minute.[2]

App stores are a growing attack surface

+33% growth in mobile apps.

23 mobile apps appear every minute.

1 app blocked every five minutes.[2]

For organizations, these apps drive business outcomes. However, they can be a double-edged sword. The app landscape is a significant portion of an enterprise's overall attack surface that exists beyond the firewall, where security teams often suffer from a critical lack of visibility. Threat actors have made a living taking advantage of this myopia to produce "rogue apps" that mimic well-known brands or otherwise purport to be something they're not, purpose-built to fool customers into downloading them. Once an unsuspecting user downloads these malicious apps, threat actors can have their way, phishing for sensitive information or uploading malware to devices. RiskIQ blocklists a malicious mobile app every five minutes.

These rogue apps appear in official stores on rare occasions, even breaching the major app stores' robust defenses. However, hundreds of less reputable app stores represent a murky mobile underworld outside of the relative safety of reputed stores. Apps in these stores are far less regulated than official app stores, and some are so overrun with malicious apps that they outnumber their safe offerings.

5 Threat infrastructure is more than what's on the network

The global attack surface is a part of an organization's attack surface, too

Today's global internet attack surface has transformed dramatically into a dynamic, all-encompassing, and completely entwined ecosystem that we're all a part of. If you have an internet presence, you interconnect with everyone else, including those that want to do you harm. For this reason, tracking threat infrastructure is just as important as tracking your own infrastructure.

Different threat groups will recycle and share infrastructure—IPs, domains, and certificates—and use open-source commodity tools, such as malware, phish kits, and C2 components to avoid easy attribution, tweaking and improving them to fit their unique needs. And with the rise of economies that sell crimeware-as-a-service and other cybercrime commodities, threat infrastructure can transcend threat actors and groups.

More than 560,000 new pieces of malware are detected every day, and the number of phishing kits advertised on underground cybercrime marketplaces doubled between 2018 and 2019. In 2020, the number of detected malware variants rose by 74 percent.[14] RiskIQ now detects a Cobalt Strike C2 server every 49 minutes.

The global attack surface is part of an organization's attack surface

560,000+ new pieces of malware are detected every day.[2]

+74% increase in malware variants.[13]

1 new Cobalt Strike server every 49 minutes.[2]

Summary

Traditionally, the security strategy of most organizations has been a defense-in-depth approach starting at the perimeter and layering back to the assets that should be protected. However, there are disconnects between that kind of strategy and the attack surface, as presented in this report. In today's world of digital engagement, users sit outside the perimeter—as do an increasing number of exposed corporate digital assets and many of the malicious actors. As such, companies need to adopt security strategies that encompass this change. Applying Zero Trust principles across corporate resources can help secure today's workforce—protecting people, devices, applications, and data no matter their location or the scale of threats faced. Microsoft Security offers a series of targeted evaluation tools to help you assess the Zero Trust maturity stage of your organization.

Stay on top of evolving security issues by visiting Security Insider.

Share this infographic

Microsoft

1 https://healthit.com.au/how-big-is-the-internet-and-how-do-we-measure-it/
2 https://www.riskiq.com/resources/infographic/evil-internet-minute-2021/
3 https://www.statista.com/statistics/266155/number-of-phishing-domain-names-worldwide/
4 https://www.zdnet.com/article/rdp-and-vpn-use-skyrocketed-since-coronavirus-onset/
5 https://www.globenewswire.com/news-release/2020/11/18/2128947/0/en/Remote-Desktop-Software-Market-to-Reach-USD-4-69-billion-by-2027-Rising-Popularity-of-E-learning-Distance-Learning-Platforms-to-Aid-Growth-Fortune-Business-Insights.html
6 https://www.zdnet.com/article/with-18376-vulnerabilities-found-in-2021-nist-reports-fifth-straight-year-of-record-numbers/#:~:text=Log%20Out-,With%2018%2C378%20vulnerabilities%20reported%20in%202021%2C%20NIST%20records%20fifth%20straight,was%20lower%20than%20in%202020.&text=Jonathan%20Greig%20is%20a%20journalist%20based%20in%20New%20York%20City
7 https://www.aon.com/unitedkingdom/insights/top-5-cyber-risks-in-mergers-and-acquisitions.jsp
8 https://www.securehalo.com/services/third-party-cyber-risk/#:~:text=A%20Ponemon%20Institute%20report%20notes,remediation%20costs%20averaging%20%247.5%20million.
9 https://www.slideshare.net/DeloitteUS/as-organizational-reliance-on-third-parties-increases-extended-enterprise-risk-management-to-be-a-focus-in-2019
10 https://www.securehalo.com/services/third-party-cyber-risk/#:~:text=A%20Ponemon%20Institute%20report%20notes,remediation%20costs%20averaging%20%247.5%20million.
11 https://www.riskiq.com/blog/external-threat-management/spoofed-sites/
12 https://techcrunch.com/2022/01/12/app-annie-global-app-stores-consumer-spend-up-19-to-170b-in-2021-downloads-grew-5-to-230b/
13 https://www.comparitech.com/antivirus/malware-statistics-facts/
14 https://www.comparitech.com/antivirus/malware-statistics-facts/