2021 REPORT

"EXPOSED"

The world's first report to reveal how exposed corporate networks really are.

zscaler™

Table of Contents

The internet, the modern workplace, and their impact on attack surface

The modern workforce has resulted in an increase in users, devices, and applications existing outside of controlled networks, including corporate networks. As a result, the business emphasis on the “network” has decreased and the reliance on the internet as the connective tissue for businesses has increased.

Leveraging the internet as a means of connectivity has greatly benefited businesses in regard to scalability, reliability, and user experience. It makes it possible for healthcare providers to continue treating patients via Zoom and enables teachers to create a virtual learning environment for their students. While the internet has helped enable the modern workforce, we must remember that it is an untrusted network. The significant expansion of its use has led to a correspondingly sizable expansion in attack surface as remote workers and network access solutions have become a popular target for cybercriminals to exploit. In a recent survey, 94 percent of businesses said they are aware that cybercriminals are specifically targeting VPNs and other network-centric technologies to gain access to their corporate networks (**2021 VPN Risk Report**), resulting in attacks such as VPN exploits, Sodinokibi, and the recent HAFNIUM MSFT Exchange attacks.

To avoid becoming victims, IT leaders must eliminate areas of exposure and identify what resources are discoverable on the internet. For the 2021 "Exposed" Report, we analyzed 1,500 organizations’ visible attack surfaces to highlight and identify attack surface trends that are affecting businesses of all sizes across all geographies and industries. Our hope is that this report will raise awareness of companies’ attackable surface and ultimately compel organizations to take steps to reduce it.

Report findings

The timespan of the analysis for this report was February 2020 through April 2021, providing a first-ever look at the possible impact on attack surface due to remote work during the global pandemic. Here is an overview of what we found through our analysis:

202,316
Potential CVE Vulnerabilities

95,742
Potential SSL/TLS Vulnerabilities

392,298
Exposed Servers

214,230
Exposed Ports

60,572
Exposed Public Cloud Instances

85,380
Exposed Namespaces

Top CVEs discovered

The global report found a total exposure of 202,316 potential CVE vulnerabilities and identified 750 unique exploits.

We found that, on average, organizations are exposed to 135 known vulnerabilities, each carrying potential risk to the business. Of the discovered CVEs, 49 percent are classified as "Critical" or "High" severity.

The five most common CVEs we discovered include:

1. **CVE-2018-1312 – CRITICAL – 6.8 CVSS Score**
   In Apache httpd 2.2.0 to 2.4.29, when generating an HTTP Digest authentication challenge, the nonce sent to prevent reply-attacks was not correctly generated using a pseudo-random seed. In a cluster of servers using a common digest authentication configuration, HTTP requests could be replayed across servers by an attacker without detection.

2. **CVE-2017-7679 – CRITICAL – 7.5 CVSS Score**
   In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_mime can read one byte past the end of a buffer when sending a malicious content-type response header.

3. **CVE-2019-0220 – MEDIUM – 5.0 CVSS Score**
   A vulnerability was found in Apache HTTP Server 2.4.0 to 2.4.38. When the path component of a request URL contains multiple consecutive slashes ('/'), directives such as LocationMatch and RewriteRule must account for duplicates in regular expressions, while other aspects of the server's processing will implicitly collapse them.

4. **CVE-2016-4975 – MEDIUM – 4.3 CVSS Score**
   Possible CRLF injection allowing HTTP response splitting attacks for sites which use mod_userdir. This issue was mitigated by changes made in 2.4.25 and 2.2.32, which prohibit CR or LF injection into the "Location" or other outbound header key or value. Fixed in Apache HTTP Server 2.4.25 (Affected 2.4.1-2.4.23). Fixed in Apache HTTP Server 2.2.32 (Affected 2.2.0-2.2.31).

5. **CVE-2018-17199 – HIGH – 5.0 CVSS Score**
   In Apache HTTP Server 2.4 release 2.4.37 and prior, mod_session checks the session expiry time before decoding the session. This causes session expiry time to be ignored for mod_session_cookie sessions since the expiry time is loaded when the session is decoded.

Discoverable SSL/TLS risk

We found a total of 95,742 web servers that support the use of outdated and vulnerable SSL/TLS protocols, with an average of 64 outdated web servers per company. According to NIST guidelines, organizations should be supporting current protocols, such as TLSv1.2 or TLSv1.3, to avoid harmful man-in-the-middle attacks. However, we found that 47 percent of protocols supported on these servers are outdated, including support of SSLv3, SSLv2, TLSv1, and TLSv1.1 protocols.

Number of exposed servers and ports

The highest level of exposure we found came from servers, with 392,298 servers that were discoverable on the internet and possibly vulnerable. This means that an organization has an average of 262 servers exposed not only to bad actors, but to the entirety of the internet. Additionally, within these servers, we found a total of 214,230 ports exposed across 68 unique ports. The three most commonly exposed ports were:

Port 443 (HTTPS)
56.8%

Port 80 (HTTP)
38.8%

Port 22 (SFTP)
1.98%

Not surprisingly, web applications with HTTPS and HTTP traffic represent the vast majority of exposed ports, contributing nearly 96 percent of port exposure, followed by Port 22, which primarily hosts the Secure Shell (SSH) service used to transfer hypertext and share data.

Exposure across public cloud providers

The events of 2020 required many organizations to turn to cloud platforms for scale and agility to support the newly mobile workforce. While public cloud platforms themselves are not dangerous, having misconfigured cloud services and resources can increase the risk of visibility and exposure to the business. The report found that the 1,500 companies had a total of 60,572 internet-exposed public cloud instances, averaging 40 instances per company. Public cloud exposure is primarily seen across three cloud platforms: Amazon Web Services (AWS), Microsoft Azure Cloud, and Google Cloud Platform (GCP). Here is a breakdown of total found instance exposure across the public cloud platforms:

AWS
50%

Azure
35%

GCP
13%

Other
2%

This exposure could be due to a variety of things such as simple misconfiguration, spun-up services without IT knowledge, or long-forgotten or misplaced instances. IT security leaders need to own the usage of their public cloud assets across the organization and ensure cloud services adhere to deployment best practices to reduce attack surface.

TAKEAWAY

We have now analyzed global attack surface trends from a high level. The next sections of this report will take a more focused look into attack surface by company size, geography, and industry.

*The identified public cloud exposure in this report refers to instances/services which are hosted, run, and managed by customers, not services of the underlying public cloud provider. Customers run workloads on the cloud providers infrastructure and follow the shared security responsibility model.

Attack surface by company size

To identify attack surface trends on the basis of company size, we broke down the data into four size categories:

Majors (20,000+ employees)
Large Enterprise (6,000–20,000 employees)
Enterprise (2,000–6,000 employees)
Commercial (<2,000 employees)

47%
Large Enterprise

31%
Major

12%
Commercial

10%
Enterprise

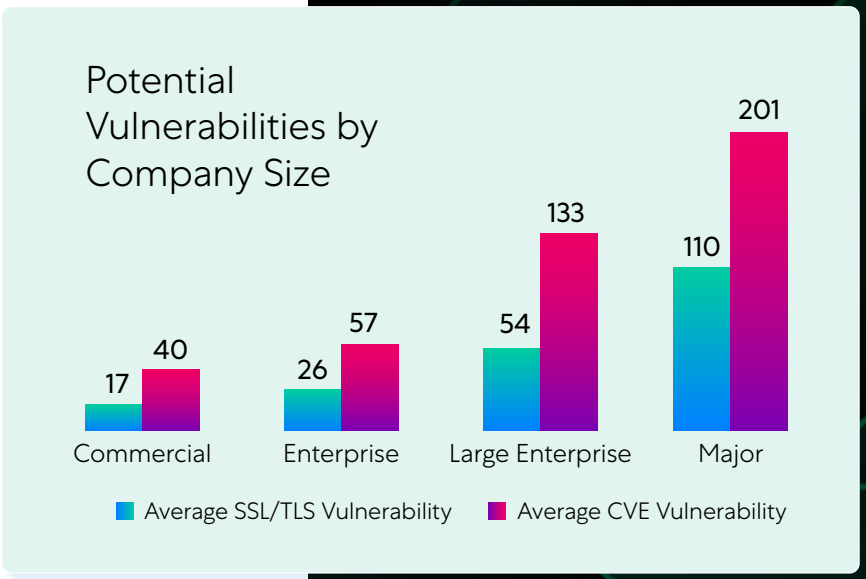
We found that 78 percent of the organizations in our analysis were majors or large enterprises.

SSL and CVE vulnerabilities by company size

Looking at the average number of known vulnerabilities, we can immediately see that major companies by far have the highest average for realized CVE vulnerabilities (201), as well total potential SSL/TLS vulnerabilities (110).

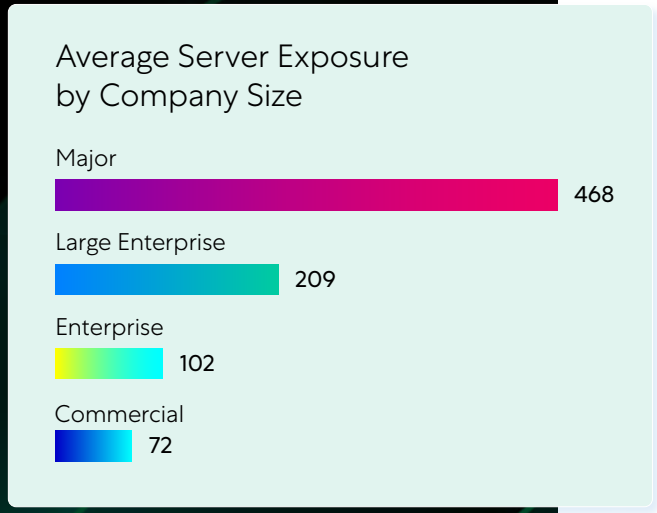
While we can see that organizations with 20,000+ employees have the most possible vulnerabilities, we also see the relationship between company size and exposure and it's dramatic. There is a 51 percent increase in CVE count and a massive 104 percent increase in outdated SSL/TLS protocols from large enterprises to majors.

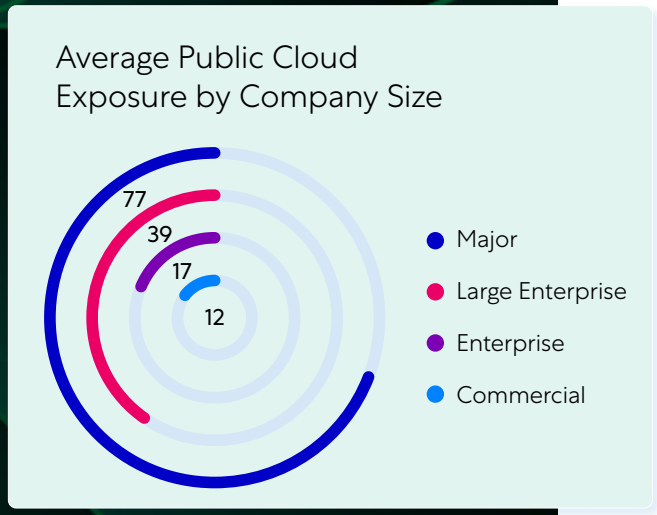
One reason for these increases is obvious: large and major organizations have more employees, more servers, and more applications to manage, therefore having an increased attack surface and exposure to potential vulnerabilities. Conversely, while smaller organizations have fewer IT resources, they also have fewer employees to secure and servers to manage.



TAKEAWAY

Company size is a significant factor in vulnerability risk. Larger companies have a higher likelihood of risk due to the sheer size of their attack surface.





Major companies have high server exposure

With an average of 468 servers exposed, we can see that again the majors segment has a significantly larger average than large enterprises and enterprises. While 468 is the average, 75 percent of major companies have 547 or fewer servers exposed. This could be due to majors having more servers to support the high-capacity demands of a large workforce.

On the other end, we see smaller commercial companies still have an average of 72 exposed servers. This is significant considering that commercial companies have fewer than 2,000 employees. This means that on average, one server is exposed for every 28 employees (or less).

When looking at public cloud instances exposed to the internet, we see that major companies have more than double the amount of exposure as large enterprises, enterprises, and commercial companies combined, with an average of 77 exposed public cloud instances.

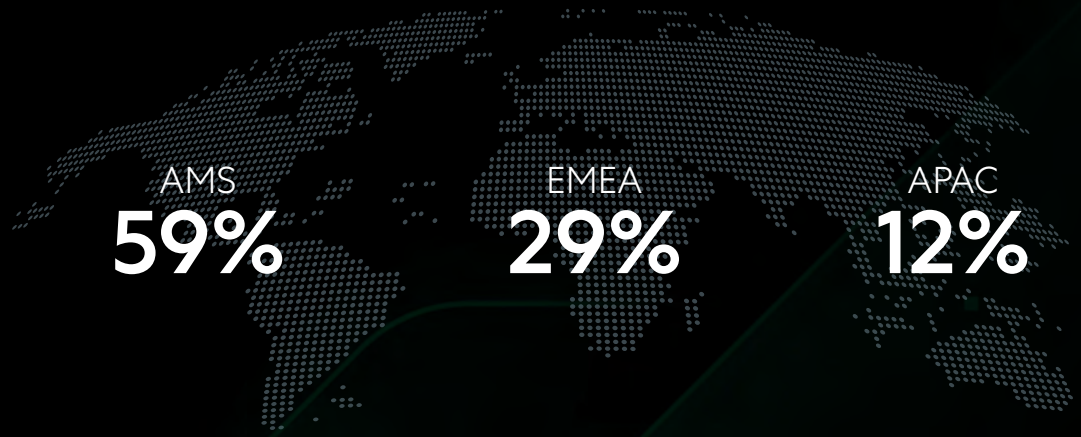
Additionally, the data shows that the majors segment has internet-exposed instances across the three main cloud platforms, with 52 percent of exposed instances in AWS, 36 percent of exposed instances in Azure, and 11 percent of exposed instances in GCP. Since majors have more diversified exposure across clouds than the other segments, this potentially shows there is a wider adoption of a multicloud strategy which can contribute to the breadth of attack surface.

TAKEAWAY

Larger companies tend to have more exposure across servers and public cloud instances. Further, larger companies seem to have greater adoption across public cloud platforms, with additional environments adding to the attack surface, which needs to be minimized.

Attack surface by geography

It's important to see the effects of attack surface across varying geographies. The report includes findings from companies based across 53 countries, which have been broken down into three geographical categories: AMS, which includes both North and South America; EMEA, which includes much of Europe, the Middle East, and Africa; and APAC, which includes Asia, Australia, and the Pacific Island nations.

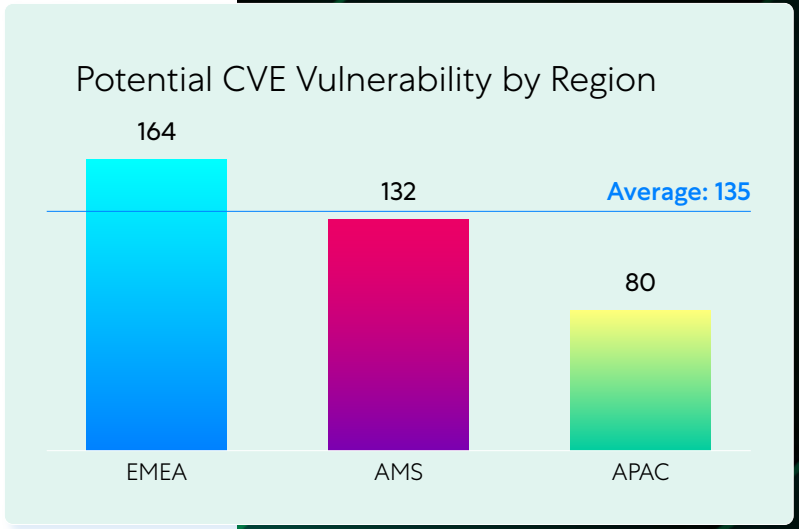


Our distribution includes a notable portion of organizations headquartered in the Americas with 59 percent, followed by 29 percent of companies headquartered in EMEA and 12 percent headquartered in APAC. However, as our findings have shown, more than 75 percent of companies are majors or large enterprises, meaning that while a company may be based in a particular region, there is a high likelihood that these companies have a global presence.

EMEA companies have the highest potential CVE vulnerability

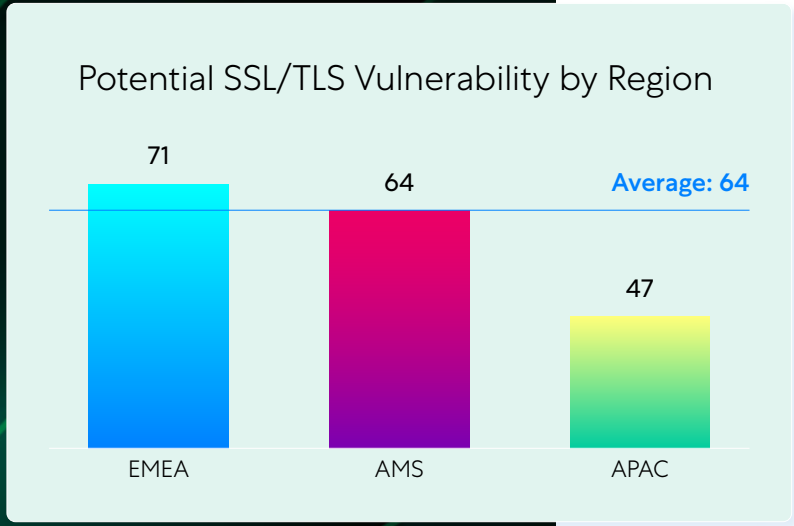
Out of the three regions, we found that EMEA based companies have the highest average of potential risk, with 164 CVE vulnerabilities. EMEA is followed by AMS, with 132 CVEs (20 percent lower than EMEA), and APAC, with an average of 80 CVE possible vulnerabilities (51 percent lower than EMEA).

When looking at CVEs by individual country, we see that Finland has the highest average worldwide, with 355 potential CVE vulnerabilities, followed by Brazil with 300 and Italy with 257. The high averages from Finland and Italy are likely contributing to EMEA's high vulnerability average, as well as the fact that seven out of 10 of the top exposed countries come from the EMEA region.



TAKEAWAY

While companies headquartered in EMEA have the highest potential CVE vulnerabilities, each geo still averages more than 135 vulnerabilities per organization. Businesses, especially those based in EMEA, should consider adopting security best practices, including taking regular inventory of installed software products and assessing for identified vulnerabilities within their environments.



EMEA companies have the highest risk of SSL/TLS vulnerability

We see that EMEA companies have an average of 71 servers with SSL/TLS vulnerabilities, meaning they support more outdated SSL/TLS protocols than the other regions. When looking at individual countries, we see that Hong Kong has the highest average of possible SSL/TLS risk with 107 vulnerable servers, followed by Finland with 98, and Switzerland with 91. Two of the top three exposed countries are EMEA-based, which contributes to EMEA's higher SSL/TLS vulnerability average.

TAKEAWAY

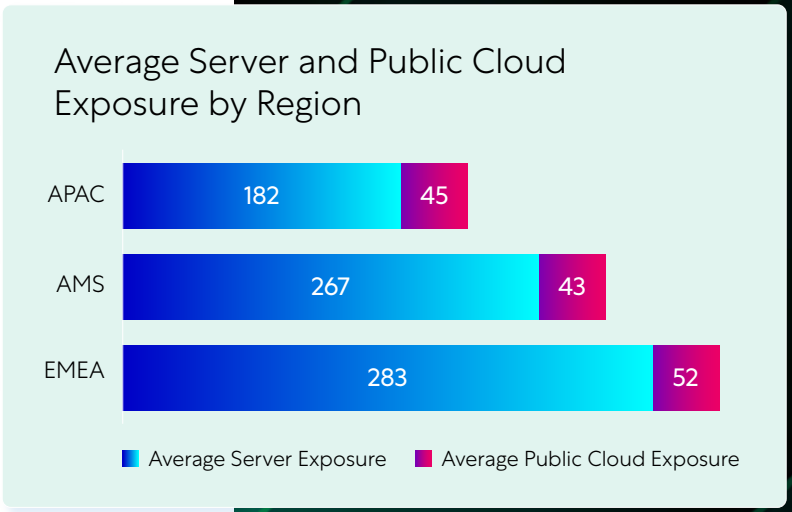
Companies in EMEA have the highest SSL/TLS risk from a regional perspective. This could be due to EMEA companies supporting older devices with older protocols, or, in some cases, they may have simply neglected to maintain server hygiene. Companies in EMEA, and globally for that matter, should be mindful of what protocols their servers are supporting and minimize support of SSLv3, SSLv2, TLSv1, and TLSv1.1.

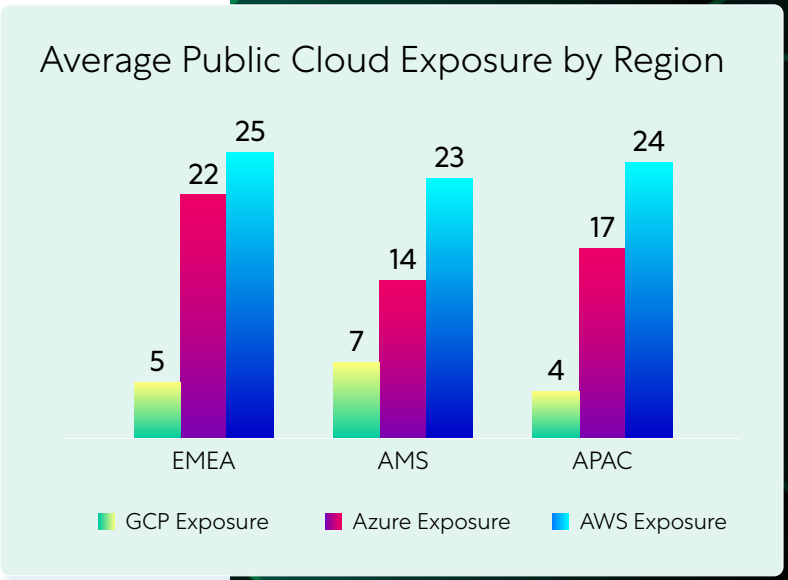
EMEA companies lead in overall exposure

When analyzing regional exposure, we see EMEA companies lead again with an average of 283 servers and 52 public cloud instances exposed to the internet. Drilling down into the distribution of public cloud exposure, we see that instances in AWS have the most overall internet exposure, averaging 23 to 25 instances across all regions; however, we also see slight variance in distribution for instances in public cloud platforms across geos. The biggest variance is the high average of instance exposure hosted in Azure for EMEA based companies with 22 instances, versus the lower averages seen in AMS (14) and APAC (17).

TAKEAWAY

From a geographical perspective, EMEA based businesses consistently have higher averages of exposure compared to AMS and APAC, but not by much. IT teams should look to adopt best practices, including zero trust security, to minimize the attack surface and eliminate exposure.





Attack surface by industry

The 1,500 companies in our study were diverse, spanning 23 industries, with top organizations and industry leaders being represented. The industries with the highest representation included manufacturing (199), financial services (195), services (167), high-tech (144), and healthcare (134). Although 23 industries were represented, we decided to focus on the top 15 most-vulnerable.

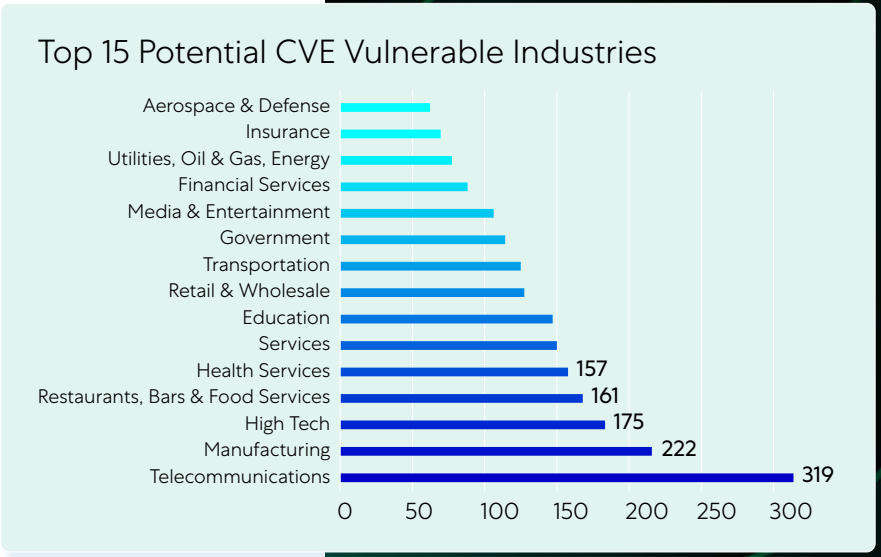
Telecommunications leads in vulnerability risk

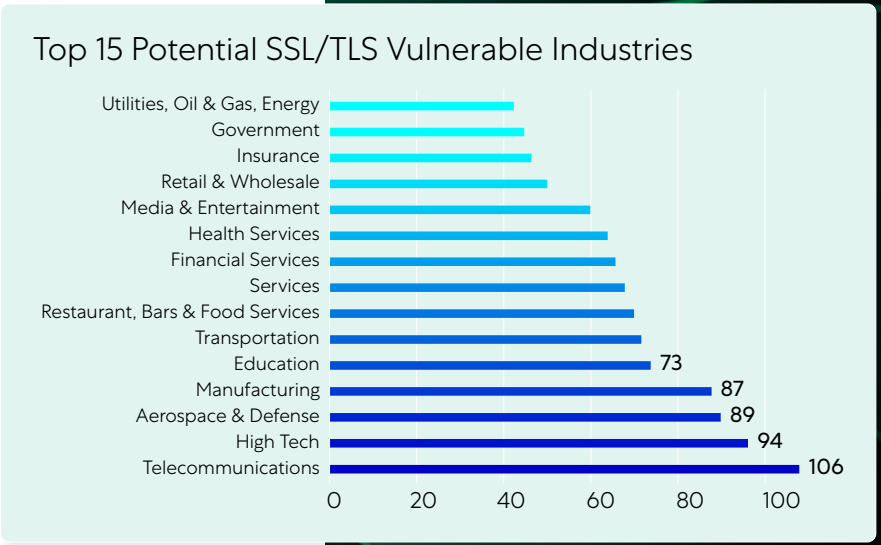
When analyzing possible CVE exposure side-by-side, we can immediately see that the telecommunications industry has more exposure than other industries, with an average of 319 CVEs. In fact, between telecommunications at the top, there is a 30 percent decrease in potential vulnerability to the second-highest industry, manufacturing.

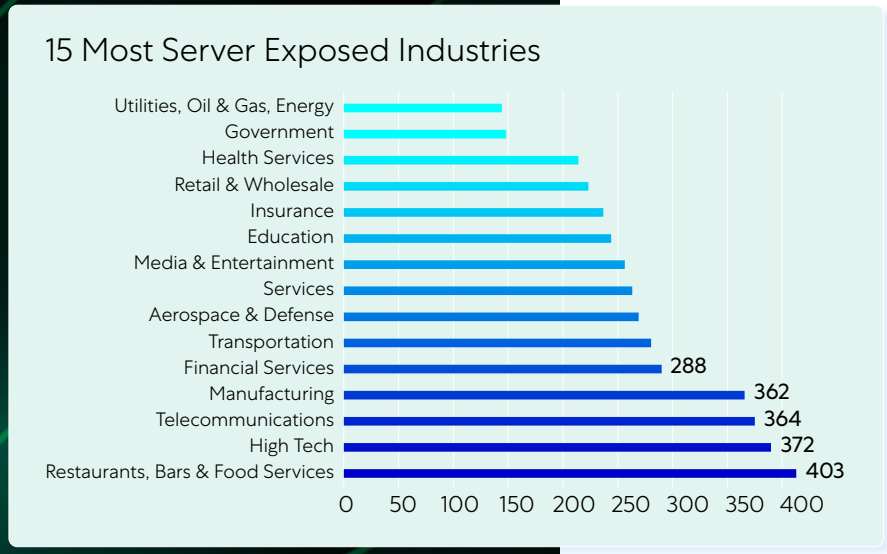
Telecommunications also has the highest risk resulting from servers with outdated SSL/TLS, showing an average of 106 such servers, followed by the high-tech industry with 94, and aerospace & defense with 89. In fact, the biggest difference we see from potential CVE vulnerabilities to SSL/TLS vulnerabilities is that aerospace & defense has the least exposure to CVE vulnerabilities, while it has the third-highest potential risk of SSL/TLS vulnerabilities. This is why it's important to assess vulnerability from multiple angles.

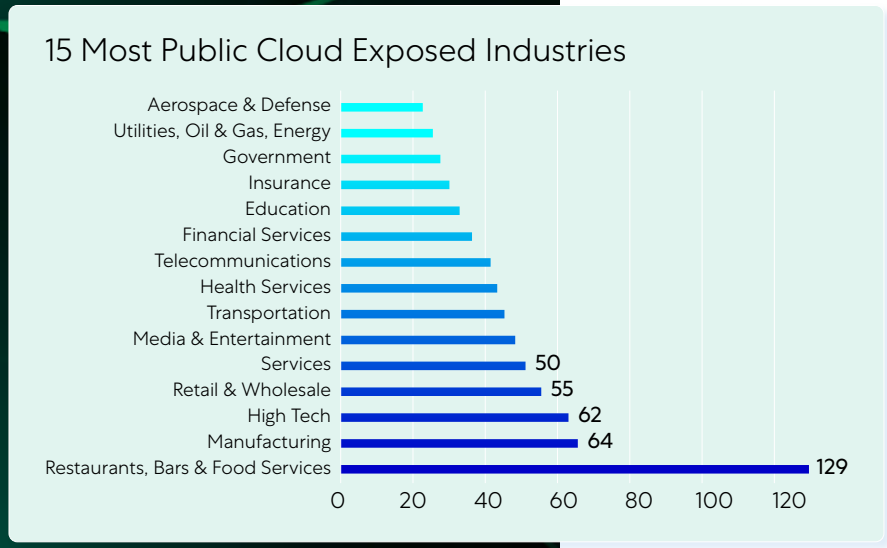
TAKEAWAY

Both potential CVE and SSL/TLS vulnerabilities vary across industries and can be more exposed in one area than another. Because of variability, companies should look at possible exposure from multiple perspectives.







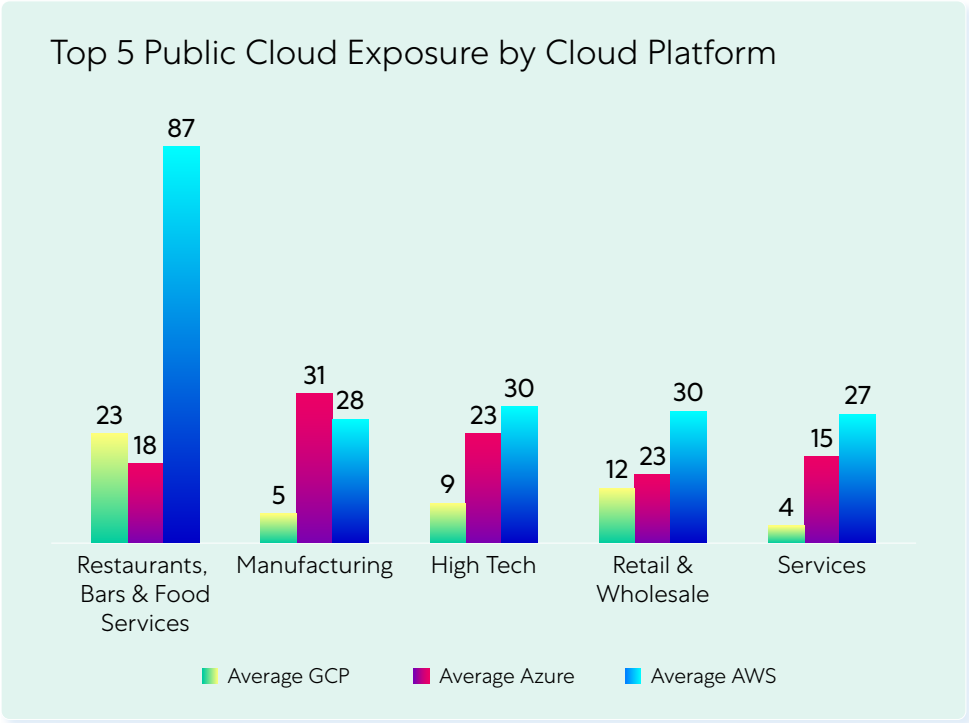


Restaurants, bars & food services have the most server and public cloud exposure

When analyzing exposure, we see the restaurants, bars, & food services sector has the highest number of exposed servers, with 403 on average, 54 percent above the overall average of server exposure. However, three industries follow closely behind with high averages of server exposure: high tech (372), telecommunications (364), and manufacturing (362). One interesting note is that financial services has the fifth-highest server exposure at 288, in spite of the strict compliance measures the sector has in place.

Additionally, when we look at public cloud instances exposed to the internet by industry, we see restaurants with the highest exposure, with 129 public cloud instances exposed on average. That is 101 percent greater than the next-most exposed industry, manufacturing, with an average of 64 internet-exposed public cloud instances. This could reflect that the restaurant industry has a high adoption of cloud and, therefore, a higher average of cloud instances exposed to the internet.

When you look deeper into the individual public cloud platforms you can see something interesting. In the top five industries with public cloud exposure, we can see that the restaurants, bars, & food services industry has about 2.9x more internet-exposed instances hosted in AWS than other industries. This could mean that the restaurant industry has heavily adopted AWS over other cloud platforms. In contrast, we see that manufacturing's greatest area of internet-exposed public cloud is instances hosted in Azure, with 31 exposed instances on average. This is closely followed by internet-exposed instances in AWS with 28; however, this could mean that manufacturing has adopted more of a multicloud strategy.



TAKEAWAY

Be wary of server and public cloud exposure! IT must be mindful of exposure on two fronts, and as businesses continue cloud adoption, public cloud exposure is likely to increase.

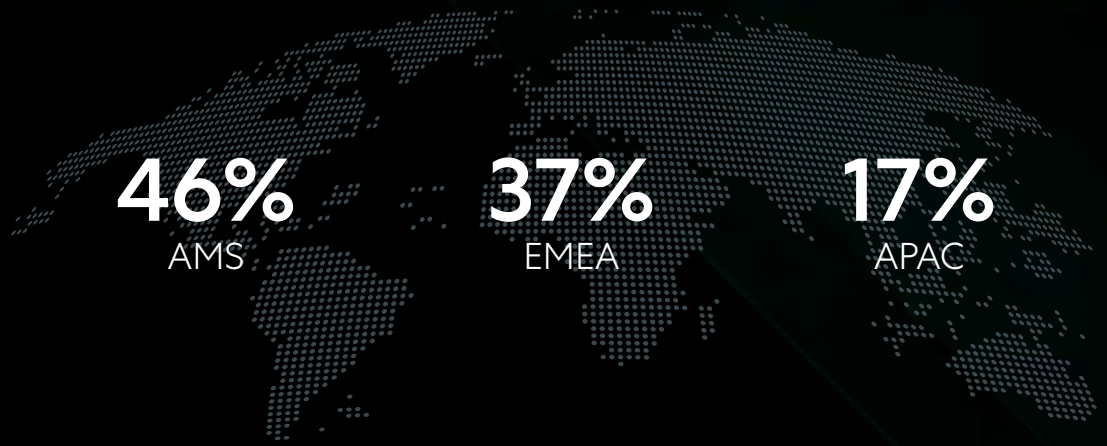
Attack surface snapshot by top exposed industries

We have presented an overview of the 15 most exposed and at-risk industries. Now, let's take a deeper look. This section will provide snapshots into some of the high-interest industries across the globe.

Telecommunications

The telecommunications industry includes companies that offer telecom services, telecom equipment, or wireless communications, the majority of which our report found to be in the large enterprise segment with 67 percent. While 46 percent of these organizations are based in AMS, we see that 37 percent are based in EMEA, primarily the Netherlands and UK.

67%	21%	8%	4%
Large Enterprise	Major	Enterprise	Commercial



106
SSL/TLS Vulnerability
↑ 66% average

319
CVE Vulnerability
↑ 136% average

364
Exposed Servers
↑ 39% average

43
Exposed Public Cloud Instances
↑ 7.5% average

77
Exposed Namespaces
↑ 35% average

Telecommunications

Straight off, we see that the telecommunications industry has significant exposure across all attack surface categories, the most significant being its CVE count, which is 136 percent above average, and possible SSL/TLS vulnerabilities that are 66 percent above average. Additionally, telecommunications has the third-highest average server exposure across all industries and is 39 percent above average.

That being said, the telecommunications industry has a unique responsibility, as its organizations can essentially be used as a gateway into multiple businesses, making them a significant target for cybercriminals. This means they also have a greater responsibility to not only protect themselves, but also their customers.

TAKEAWAY

Organizations in the telecommunications industry can be targets for cybercriminals to gain access to other businesses.

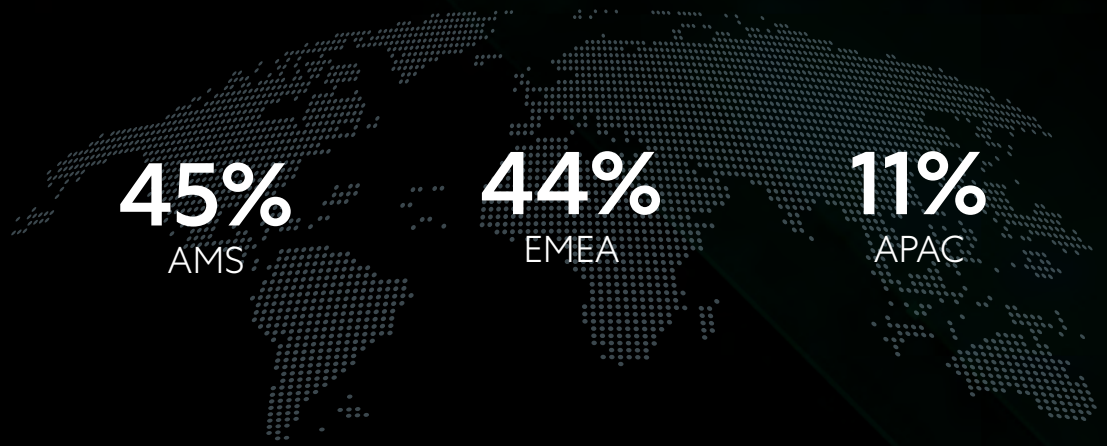
Telecommunications businesses have a greater responsibility to keep their infrastructure secure as a result.

Telecommunications should prioritize the minimization of exposed servers and public cloud services. First, eliminate the outward exposure, then implement software and server patches on a regular basis.

Manufacturing

Ninety-two percent of the manufacturing industry is categorized as either majors or large enterprise organizations. These manufacturing organizations span the production of automobiles, appliances, devices, and electronics, biopharmaceuticals, household products, heavy machinery, and more. Most of these organizations (89 percent) are located in the AMS or EMEA regions.

46%	46%	7%	1%
Major	Large Enterprise	Commercial	Enterprise



87
SSL/TLS Vulnerability
↑ 36% average

222
CVE Vulnerability
↑ 64% average

362
Exposed Servers
↑ 38% average

64
Exposed Public Cloud Instances
↑ 60% average

63
Exposed Namespaces
↑ 11% average

Manufacturing

When it comes to exposure, the manufacturing industry ranks second highest in potential CVE vulnerabilities, at 64 percent above average, while ranking fourth highest in SSL/TLS risk with 36 percent above average. Meanwhile, manufacturing has a 38 percent higher average of exposed servers, while having a 60 percent increase in exposed public cloud instances. However, when looking at individual public cloud instances exposed within manufacturing, Azure has the highest level of exposure, averaging 31 exposed instances—94 percent higher than the overall average.

TAKEAWAY

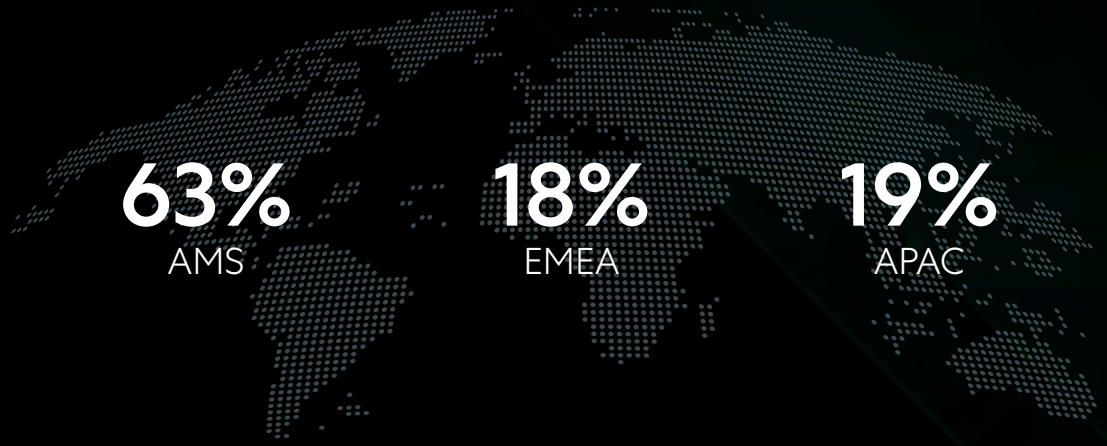
Manufacturing has high exposure regardless of what materials are being produced.

Manufacturing needs overall maintenance of its attack surface. Businesses should start by identifying any exposed servers and exposed namespaces and stop exposing them to the internet, followed by working on updating any outdated protocols.

High Tech

The high-tech industry has a healthy distribution across all company sizes, with the highest being large enterprises at 40 percent. The high-tech industry is broad, comprising companies that serve customers with either products or services that have a particular focus on innovation and technology. Some examples include software-based companies providing services or organizations focused on selling innovative electronics. We see that the majority of high-tech companies (63 percent) are based in the AMS region.

40%	31%	19%	10%
Large Enterprise	Major	Commercial	Enterprise



94
SSL/TLS Vulnerability
↑ 47% average

175
CVE Vulnerability
↑ 30% average

372
Exposed Servers
↑ 42% average

62
Exposed Public Cloud Instances
↑ 55% average

81
Exposed Namespaces
↑ 42% average

High Tech

The high-tech industry appears to have fairly significant risk of vulnerabilities, ranking second highest in SSL/TLS risk with an average of 94 and ranking third in CVE risk with an average of 175. The high-tech industry also ranks high in exposure, having the second-highest industry average for exposed servers, which is 42 percent above average while internet-exposure for public cloud instances is 55% above average. Forty-eight percent of their internet-exposed instances are workloads hosted in AWS, while Azure instances follows with 37 percent and GCP with 15 percent.

TAKEAWAY

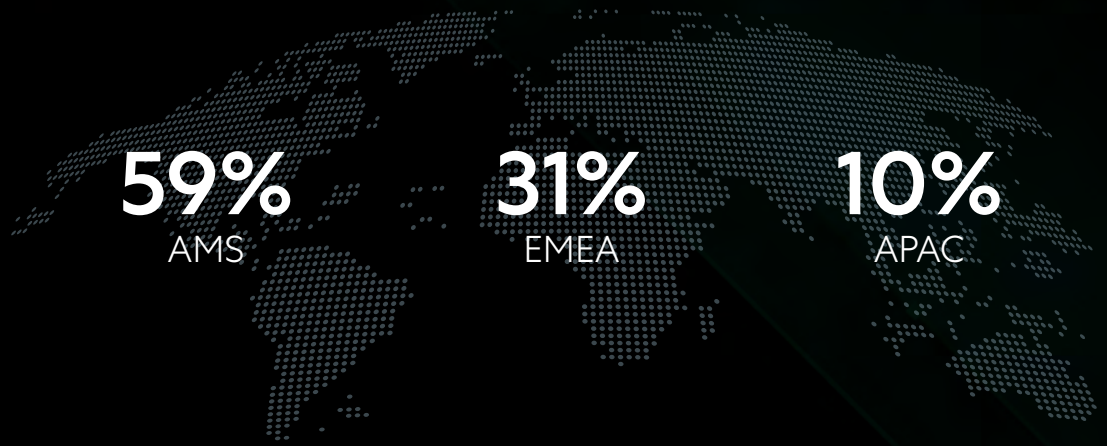
The high-tech industry has a high average of internet-exposed public cloud instances, especially with AWS. IT teams need to consider how to minimize the attack surface of these additional environments.

Exposed servers also are a significant contributor to high-tech's attack surface. Efforts should be made to eliminate server exposure to the internet.

Financial Services

The financial services industry has stricter compliance regulations than others, making it an interesting industry to dive into. The financial services industry mainly comprises majors and large enterprise organizations, the two categories making up 83 percent of all companies. Additionally, 59 percent of financial service organizations are based in AMS and 31 percent in EMEA.

42%	41%	11%	6%
Large Enterprise	Major	Commercial	Enterprise



65
SSL/TLS Vulnerability
↑ 1.6% average

84
CVE Vulnerability
↓ 38% average

288
Exposed Servers
↑ 10% average

37
Exposed Public Cloud Instances
↓ 7.5% average

59
Exposed Namespaces
↑ 3.5% average

Financial Services

We can see that while financial services companies are on par with the overall attack surface averages; however, some would expect that with the many security regulations that financial institutions must adhere to their attack surface averages would be lower. For example, while we see that potential CVE vulnerability is 38 percent below the average at 84, we also see that the number of exposed servers is actually 10 percent greater than average with 288. With all of its regulations, you would hope both exposure and risk of vulnerabilities to be far below average, especially considering the financial services industry handles a lot of customers' personal and financial information.

TAKEAWAY

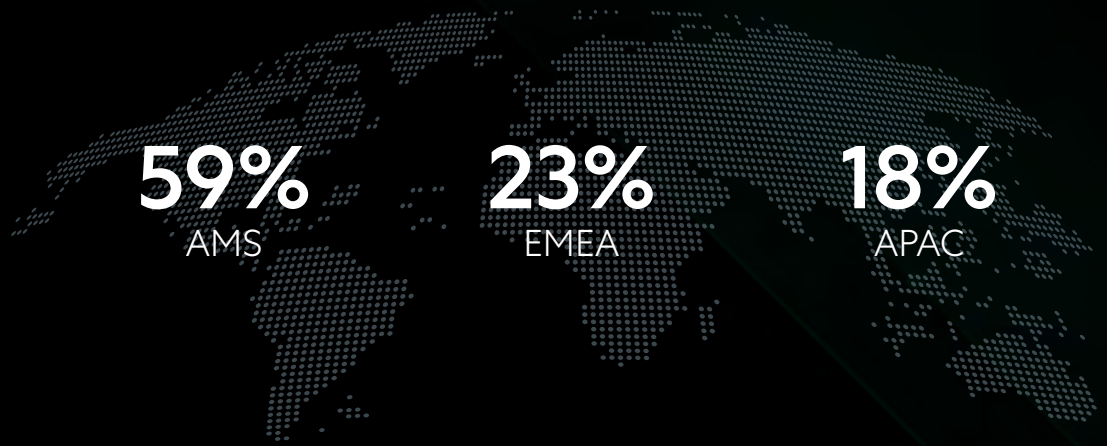
The financial services industry is consistent with overall attack surface averages for the most part, except for server exposure.

Considering the nature of the financial services industry, organizations should seek to minimize the attack surface for the sake of their customers. Additionally, IT should consider the use of zero trust for enhanced security.

Government

With recent targeted attacks towards government organizations, we thought it would be wise to take a deeper look into this segment. The first thing we see is that 88 percent of government organizations in our study meet the size of large enterprise and majors segments, with the majority (59 percent) located in AMS. We also see a variety of organizations at the state and federal level, not only in AMS, but across the globe.

61%	27%	8%	4%
Large Enterprise	Major	Commercial	Enterprise



44
SSL/TLS Vulnerability
↓ 31% average

111
CVE Vulnerability
↓ 18% average

149
Exposed Servers
↓ 43% average

28
Exposed Public Cloud Instances
↓ 30% average

47
Exposed Namespaces
↓ 18% average

Government

What we see in the government sector is exactly what we would hope to see, as it is below average in all areas, specifically in the number of exposed servers and public cloud instances. On the other hand, the government's highest exposure is in potential CVE vulnerabilities with 111, even though it is still 18 percent below average. However, if we recall recent attacks, such as HAFNIUM, which greatly impacted government agencies, we know that one CVE vulnerability could be responsible for shutting down operations.

TAKEAWAY

Government agencies are below average in all types of vulnerabilities. However, because government organizations (at all levels) are frequent targets of cybercrime, they should strive to eliminate any unnecessary attack surface to reduce the risk of it becoming exploited by HAFNIUM and other attacks.

Summary

With the number of cyberattacks rising every day, minimizing the attack surface needs to become a business-critical conversation. As organizations look to grow and innovate in enabling the modern workforce, public cloud adoption, and much more, IT must consider the effects that digital transformation will have on their attack surface and security risk. Consider these key takeaways from the report:

Key findings:

- ✓ Overall, we see it is nearly impossible to have a "zero attack surface." Businesses and IT teams need to be aware of this reality and remain diligent in minimizing this risk.
- ✓ Larger companies are more likely to have larger attack surfaces due to the sheer number of users, servers, and resources. If you are a larger company, beware of unknown attack surfaces and consider a security strategy that can secure the modern workplace at scale.
- ✓ Be mindful that cybercriminals are active across regions. While we see that EMEA has the highest level of potential vulnerabilities and exposures, attack surface only slightly varies across geographies. It's important to not only consider your own attack surface, but also your global partners as they contribute to third-party risk.
- ✓ Some industries are more exposed and potentially vulnerable than others simply due to the nature of the industry, such as telecommunications, high tech, or manufacturing. IT teams across all industries should begin initiating conversations about attack surface, especially in this high cyber risk climate. Consider what security strategy is right for your organization and address the topic of attack surface.
- ✓ Adopting the right security strategy is imperative in moving toward a zero attack surface, so take steps toward doing so. Be aware of the attack surface trends in your specific geo.

How does your attack surface compare?

Uncover your attack surface and see how you compare across company size, region, and industry.

Assess Your Attack Surface Now →

Next steps for businesses to consider:

Know your exposure – This can be tricky as more and more applications move to cloud or as new servers are set up, but knowing your visible attack surface is critical to mitigation. Remember, if it's exposed to the internet so it can be found by your employees, it can also be found by bad actors.

Know your potential vulnerabilities – Hidden exposure gives vulnerabilities a place to hide. Be consistent in checking the CVE database to remain up-to-date. Be sure to remove support of older TLS versions from servers to reduce risk.

Adopt best practices that minimize risk – This could mean adopting technologies that help provide visibility and adopting technologies that implement zero trust. But this should be technology that makes the IT team's life easier and the business safer.

Methodology

All data and facts presented in the 2021 "Exposed" report are sourced directly through **Zscaler's Attack Surface Analysis tool** which allows individuals to identify visible exposure based on domain name. Zscaler's Attack Surface Analysis tool does not actively probe the corporate network but alternatively identifies areas that are visible to the internet which may lead to risk. Note that exposure does not equate to actual risk, but rather potential risk.

The "Exposed" report consolidates and analyzes the raw data from a total of 1,500 attack surface reports from February 2020 through April 2021. Analyzing the data, we excluded outlier data so as to not skew results. We then calculated the average exposure across the varying segments like company size, geography, and industry to provide helpful benchmarks for viewers.

Zscaler's hope for the "Exposed" report is to help bring awareness to unknown areas of exposure so business and IT leaders can make educated decisions on minimizing excessive attack surface and exposure they may have.

Report Definitions

CVE Vulnerability – Lists the known CVE vulnerabilities that can pose a threat to internet exposed servers.

SSL/TLS Vulnerability – Lists the older SSL/TLS protocol version supported by internet exposed servers that can be exploited by nefarious actors.

Exposed Server – Lists the servers running within a network environment currently exposed to the internet. While some server exposure may be intentionally available for public and internet use, many are often private applications that need to be made invisible to the public internet.

Exposed Port – Lists the visible ports on the internet exposed servers.

Exposed Public Cloud Instances – Lists the managed public cloud instances that are currently exposed to the Internet. Again, while some of these public cloud instances might be intentionally available for public and internet use, many are often private applications that need to be made invisible to the public internet.

Namespace Exposure – Namespace exposure is calculated based on certain keywords matching your domain name/namespace. Within this report namespace exposure lists all servers that match a risky keyword.