5 areas of network exposure you need to minimize immediately

The new 2021 "Exposed" report analyzed 1,500 organizations' visible network exposure over the last year to identify the attack surface trends affecting businesses today as a result of increased remote work. **The report highlights these 5 areas of exposure every IT and security team needs to consider:**

202,316
Potential CVE Vulnerabilities

Over 200K CVE vulnerabilities were discovered with 750 unique exploits identified. 49% of these discovered CVEs are classified as "Critical" or "High" severity.

95,742
Potential SSL/TLS Vulnerabilities

Out of all the web servers discoverable, 47% of all supported protocols are outdated and potentially vulnerable

392,298
Exposed Servers

There is an average of 262 servers per enterprise exposed and discoverable to the Internet. These servers are exposed not only to bad actors, but to the entirety of the internet.

214,230
Exposed Ports

Web applications with HTTPS and HTTP traffic represent the vast majority of exposed ports, contributing 96 percent of port exposure.

Port 443 (HTTPS)	Port 80 (HTTP)	Port 22 (SFTP)
56.8%	38.8%	1.98%

60,572
Exposed Public Cloud Instances

Businesses have an average of 40 exposed public cloud instances with 50% being AWS instances

AWS	Azure	GCP	Other
50%	35%	13%	2%

Want to learn more about how attack surface trends have impacted companies like yours across geographies and industries? **Download the full report.**

Read the Report →

Zscaler™