The ASX 200 Attack Surface

Research by Erick Galinkin, Principal Researcher, Rapid7

Executive Summary

Overall, the companies listed on the ASX 200 have a respectable security posture. The attack surface of ASX 200 companies in general is on-par with their counterparts in the FTSE 350 and the Fortune 500. There is still definite room for improvement, but the overall security posture of ASX 200 companies have measurably improved since the Industry Cyber-Exposure Report (ICER) Rapid7 conducted on the ASX 200 in 2021.

- The industrial sector of the Australian economy leads all industries in their exposure of risky services to the internet.
- Australian companies which expose Nginx web servers could do better with managing version dispersion risk by keeping their Nginx installations up to date.
- Microsoft Exchange remains a popular on-premises email server, despite the recent spate of high-impact remote vulnerabilities.
- More ASX 200-listed companies have a valid DMARC configuration than ever before, which helps protect email and brand integrity among these companies.

Introduction

This report examines the attack surface of the 200 largest publicly traded companies listed on the Australian Securities Exchange, also known as the ASX 200. This report follows our 2021 Industry Cyber-Exposure Report (ICER) on the ASX 200 that considered one year's worth of historical data from 2020 into 2021. While that report followed a defined methodology and was part of a cycle examining large public companies around the world (*e.g.* FTSE 350, Fortune 500), this report is a snapshot in time taken at the beginning of October 2022.

The report surveys a number of factors that provide a picture of what an "average" company in the ASX 200 looks like from the internet. These factors include:

- **Internet-facing attack surface**: Overall port counts and high-risk port counts provide insight into how accessible corporate networks are to outsiders.
- **Web server type and version complexity**: Web servers by necessity are internet-facing, so we do not typically consider them part of the attack surface in the same way as other services. However, the variety of software types and differing versions between servers offers a proxy for how an organization manages complexity and patching generally.
- **Microsoft Exchange patching**: Given the spate of high profile Microsoft Exchange vulnerabilities and the popularity of Microsoft Exchange as an enterprise email server, this serves as a leading indicator of overall vulnerability management.
- **Email and Domain safety**: The use of Domain-based Message Authentication, Reporting, and Conformance (DMARC) and Domain Name Service Security Extensions

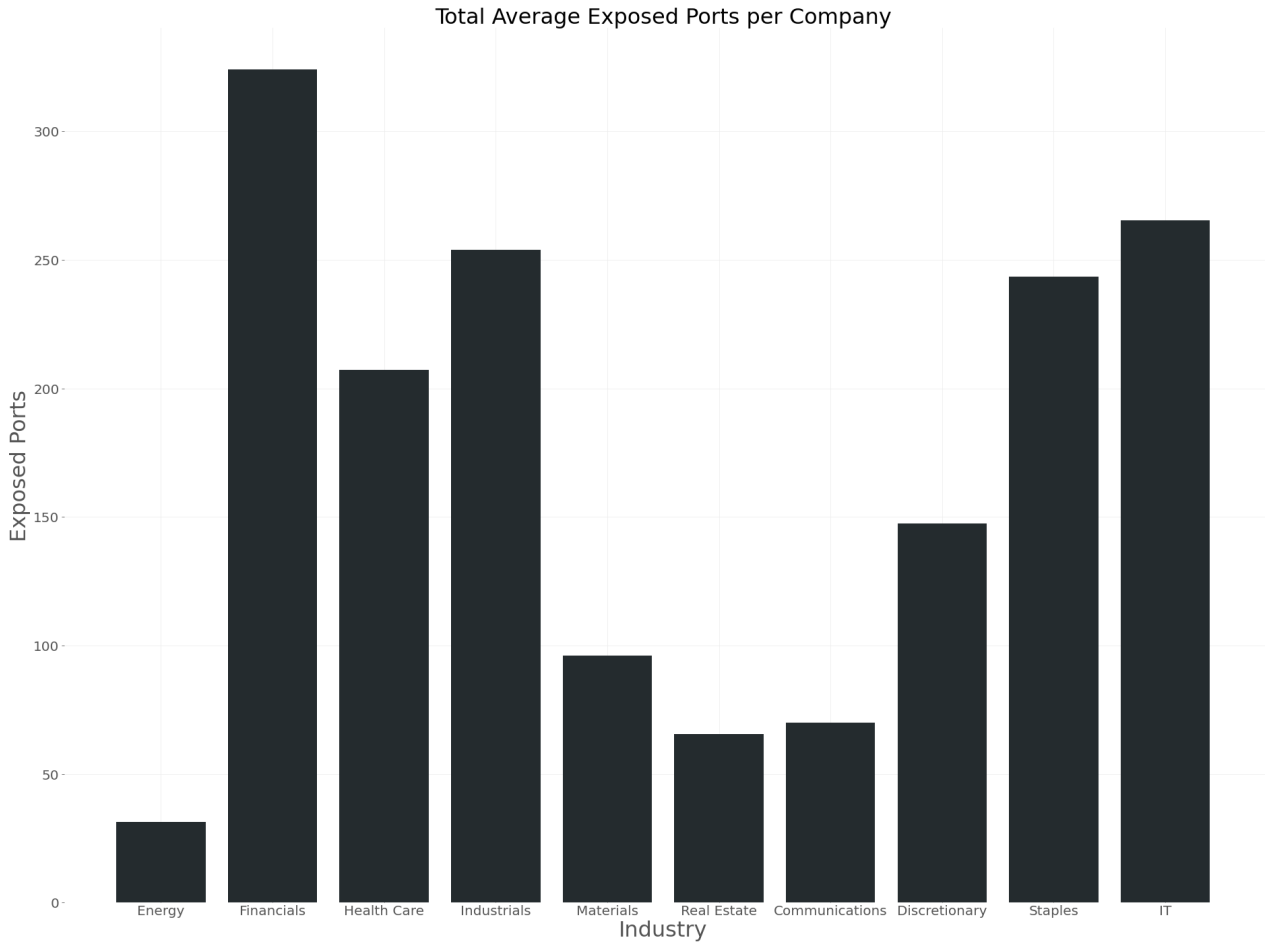
(DNSSEC) helps mitigate email-based attacks like phishing by flagging illegitimate senders and preventing spoofing.

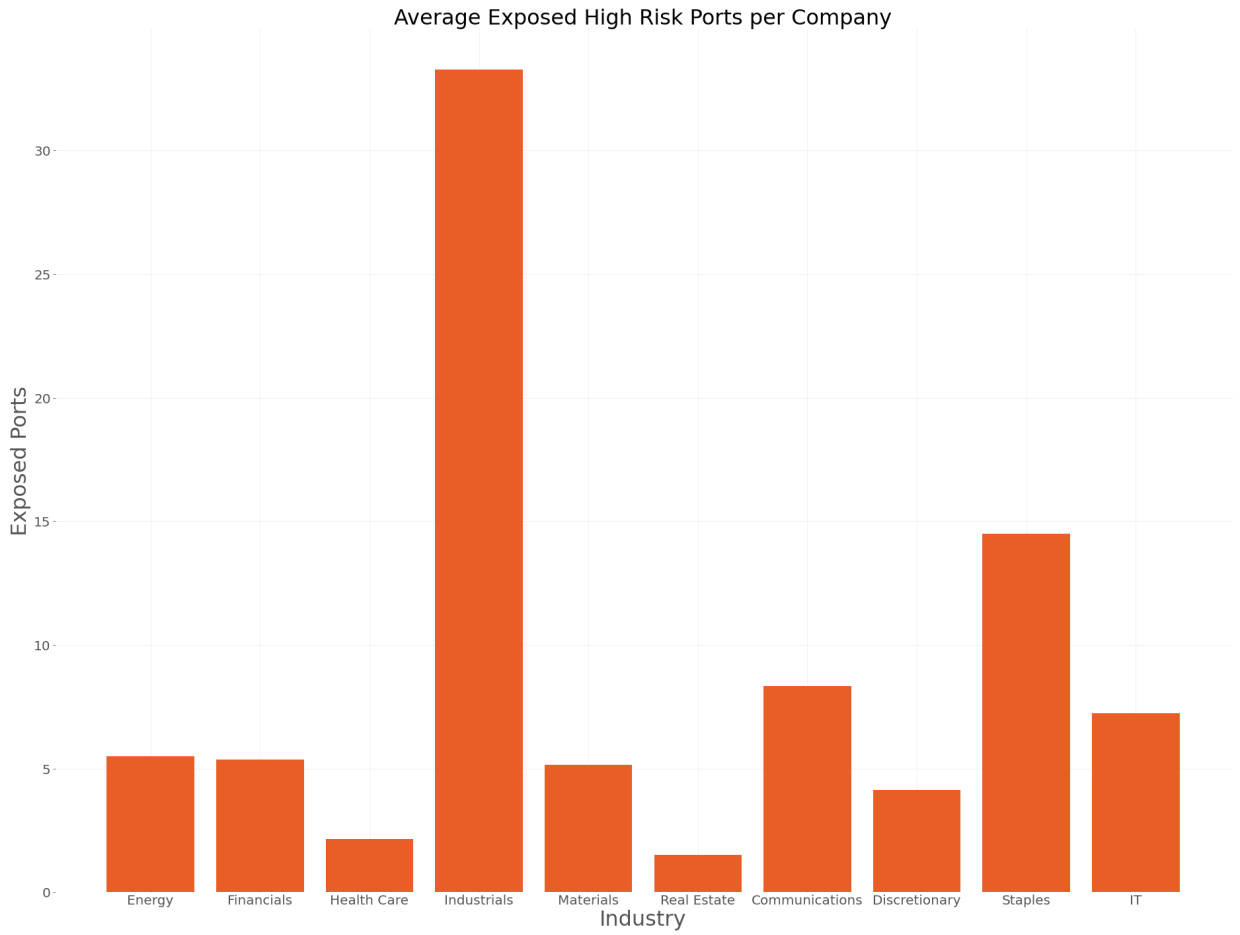
Findings

Attack Surface

From an attack surface perspective, one metric we are concerned with is which ports are exposed to the internet. We consider two metrics: the total number of exposed ports, and the number of exposed high-risk ports. We define “high risk” as the ports commonly associated with FTP, SSH, Telnet, SMB, and RDP. For more on why RDP and SSH are high risk, see our recent October, 2022 report on automted attacks targeting of these services: Good Passwords for Bad Bots. Telnet suffers from a similar usage as SSH but is actually worse since the traffic is unencrypted and server authentication is generally impossible. FTP, the file transfer protocol, is another cleartext protocol and files stored on FTP can easily be downloaded by motivated attackers. SMB is a protocol that has been associated with high-profile exploits like EternalBlue and is broadly recommended not to be exposed to the internet.

The two charts below normalize the number of exposed ports by company and industry, such that the number of ports in the chart is a reflection of the average number of exposed ports a company in that industry would have – we do this to mitigate the issue of overrepresentation of certain industries within the ASX 200.





Based on the charts above, we find that although financial services, health care, and information technology have a substantial number of ports exposed overall, their relative exposure of risky ports is actually very low. By contrast, industrials leaps out ahead of the pack with an average of 33 exposed high risk ports per company. This exposure is largely due to the substantial number of exposed SSH ports among industrial companies, combined with being the leading exposer of RDP, with an average of five exposed RDP servers per company.

Information technology, in a meaningful change from 2021's ASX 200 ICER, now only exposes FTP and SSH as high-risk services, and only in fairly small numbers. Given the proclivity of information technology companies to expose SSH as a way to manage servers, this result is very promising for the sector and shows a meaningful improvement in security maturity over the last two years.

A final noteworthy industry: although the materials industry does not jump out on either chart, their particular exposure is dominated by SMB and RDP, two of the most worrisome protocols to

be exposed to the internet. On average, each company in the materials industry is exposing at least one SMB port and at least one RDP port to the internet.

Web Server Support and Version Complexity

Web server vulnerabilities can have tremendous impacts to an organization, so applying patches is crucial. Unsupported server versions will not receive these patches and so an impacted server will remain vulnerable until the underlying software is upgraded. Therefore, we wish to examine the deployment of supported versions.

The ASX 200 companies favor Apache and Nginx for web servers over IIS, and do so in approximately equal numbers – after all, what's a few hundred thousand servers among friends? While Nginx beats out Apache slightly in sheer numbers, it also beats Apache out in a more worrisome metric: the number of unsupported versions deployed on the internet. Only 26.75% of the Nginx servers deployed among ASX 200 are of a supported version (1.20 or above). Meanwhile, 88.13% of Apache servers are supported (version 2.4.x). IIS falls behind Apache, but well ahead of Nginx with 77.07% of deployed servers being of supported versions (8 or above).

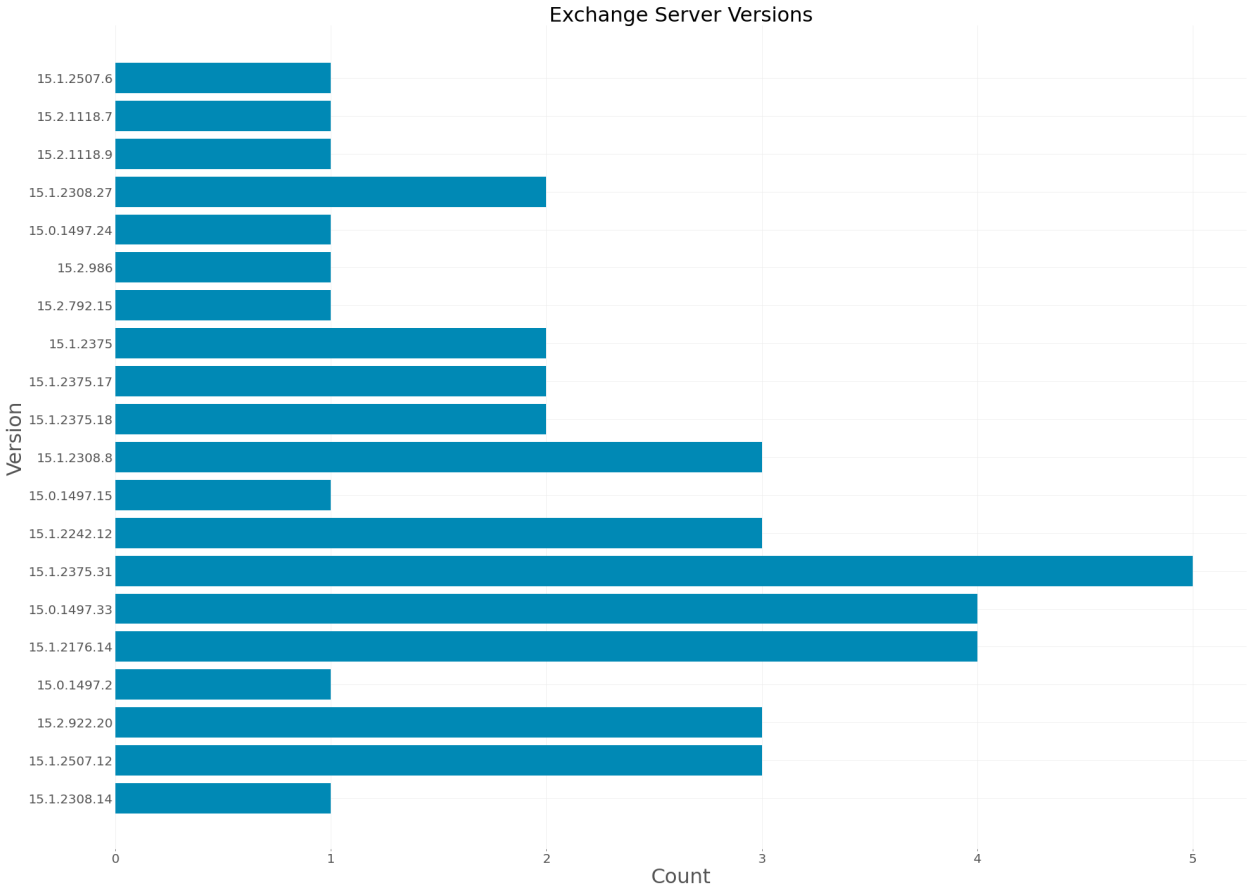
Looking more closely, in the last 12 months we see only two (actually one and a bypass) critical CVEs impacting these three pieces of software: CVE-2021-41773/42013 – a remote code execution vulnerability affecting Apache 2.4.49 and 2.4.50. While only 0.07% of Apache servers in the ASX 200 are still unpatched, this represents more than 10,000 servers vulnerable to a remote code execution known to be exploited in the wild.

In terms of version dispersion, we find that trends are fairly stable, with the majority of companies – particularly those on Nginx – running only a single version of a particular server, and a small number of companies running two, three, or even six versions of a particular server. In the version dispersion category, IIS is the leader, with only the communications and energy sectors having an average of one version per company.

From a sectoral perspective, financial services and industrials stand out here, with the majority of companies in those two sectors deploying not only more than one type of server software, but multiple versions of each. This, of course, leads to significant complexity in deploying patches for potentially affected systems.

Microsoft Exchange

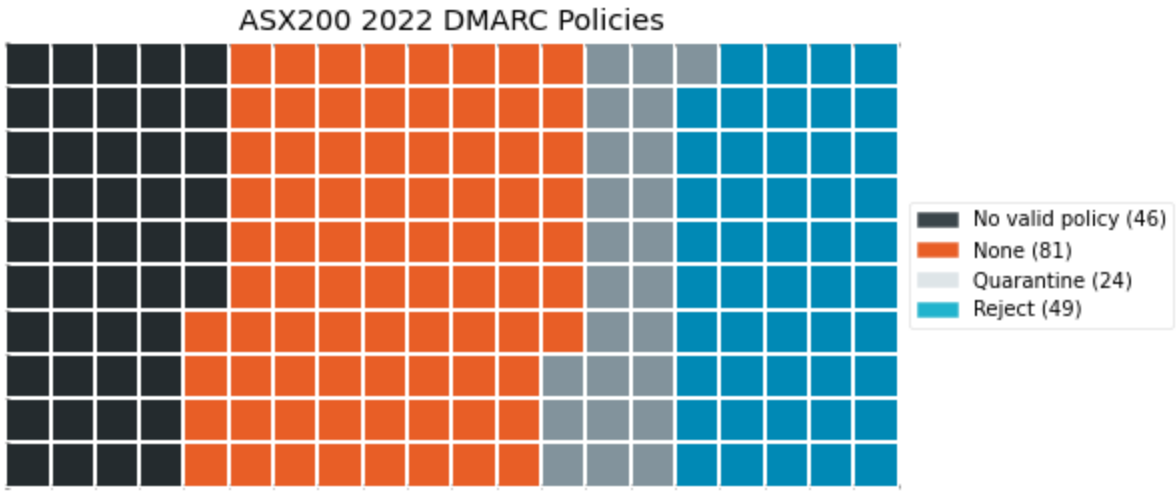
Microsoft Exchange has had a rough couple of years, between last year's string of vulnerabilities including the particularly nasty ProxyShell vulnerability, and the less terrifying, but still exploited in the wild CVE-2022-41040 and CVE-2022-41082 vulnerabilities that were patched on 30 September of this year. Despite this, Microsoft Exchange remains a very popular on-premises email server.



Examining the versions in the ASX 200, we found one company still vulnerable to ProxyShell (and have contacted them, since they are likely to have been exploited). The data presented here shows only four of 42 organizations running Microsoft Exchange on premises having applied the most recent, relevant patches, but the study that collected the data ran only a week after patches became available for the issues – it is likely that more organizations have patched, since this data represents only a snapshot in time. That said, large enterprises often face difficulty patching on-premises Exchange servers even in the most critical circumstances, with patch deployments often lagging patch releases by 60 days or more.

Email Safety

In 2020, 72 email domains had no valid policy, 81 had a policy of None, 18 had a policy of Quarantine, and 31 had a policy of Reject. There has been a meaningful shift to the point that 77% – up from 64.4% – of companies in the ASX 200 now have at least a valid, error-free DMARC policy, even if that policy is "None."



By contrast, only nine of the 200 companies have implemented DNS Security Extensions (DNSSEC). This is somewhat disappointing but worth noting that in 2020, not a single company in the ASX 200 had implemented DNSSEC, so this low count is still an improvement worth acknowledging.

Conclusion

As we can observe in this report's findings, there are significant differences in the security posture of individual companies; however, we have observed a shift in a more secure direction overall.

Despite these companies being the 200 largest listed on the ASX, there is still room for them to improve. Moreover, there are some key observations that can benefit all organizations:

- There are a number of services that can and should be exposed to the internet, and others that should never be configured in that way. Examining your external attack surface can provide useful insights about your organization's vulnerabilities.
- Patching everything all the time can be challenging – using proxies like web server version complexity may be helpful in identifying organizational difficulties.
- DMARC and DNSSSEC adoption is on the rise – this can help you build trust relationships with other organizations and protect your organization from phishing and other email threats.