451 Research® | PATHFINDER REPORT

RDP Exposure Index

RDP EXPOSURES REMAIN PREVALENT ACROSS THE FORTUNE 500

COMMISSIONED BY

EXPANSE

NOVEMBER 2019

About this paper

A Pathfinder paper navigates decision-makers through the issues surrounding a specific technology or business case, explores the business value of adoption, and recommends the range of considerations and concrete next steps in the decision-making process.

ABOUT THE AUTHOR

ERIC HANSELMAN

CHIEF ANALYST

Eric Hanselman is the Chief Analyst at 451 Research. He has an extensive, hands-on understanding of a broad range of IT subject areas, having direct experience in the areas of networks, virtualization, security and semiconductors. He coordinates industry analysis across the broad portfolio of 451 Research disciplines. The convergence of forces across the technology landscape is creating tectonic shifts in the industry, including SDN/NFV, hyperconvergence and the Internet of Things (IoT). Eric helps 451 Research's clients navigate these turbulent waters and determine their impacts and how they can best capitalize on them. Eric is also a member of 451 Research's Center of Excellence for Quantum Technologies.

Executive Summary

While the level of information security investment varies across enterprises, many would expect there to be highly effective protections in place among top-tier organizations. It might be surprising, then, to understand the extent to which serious security vulnerabilities exist within Fortune 500 companies' IT assets that are directly accessible via the Internet. Asset management and security tools can help organizations manage and secure Internet assets that they already know about, but it can be challenging to discover and secure unknown assets that have been deployed outside of managed processes.

To help organizations understand the breadth of the security challenges facing them, Expanse – a company that helps IT operations and security teams discover, manage and secure their global Internet assets – has been collecting data on the prevalence of Remote Desktop Protocol (RDP) exposed interfaces. The data from Expanse shows a startling prevalence of exposed RDP instances on the networks of Fortune 500 companies, including exposures at organizations within what are expected to be technologically sophisticated and well-financed industries. This paper explores these findings, which should serve as a wake-up call to companies large and small that they need continuous discovery and monitoring of their global Internet attack surface if they want to protect their networks.

Key Findings

- A majority (53.4%) of the Fortune 500 had at least one RDP exposure over a two-week period in April 2019.
- Even Fortune 500 companies in the most technologically sophisticated and well-funded industries had an RDP exposure, including 75% of aerospace and defense, 74.4% of technology, 55% of business services and 51.2% of financial services organizations.
- Higher IT spending does not appear to indicate that a company is significantly more protected from having an RDP exposure. Companies that reported higher IT spending as a percentage of their total annual revenue had a similar proportion of RDP exposures as the lowest relative spenders.

Digital Transformation Presents New Security Challenges

Digital transformation means that businesses today are operating at a faster cadence. Enabling teams to get the right capabilities in the right locations and at appropriate price points can give great competitive advantage because these teams are able to be more agile and effective. Whether that activity is organizationally sanctioned or is what's come to be labeled as 'shadow IT,' it's generally driven by users simply trying to get a job done. Such flexibility comes with a set of risks, though. The fact that it's easy for users to build infrastructure outside of the traditional datacenter, in public clouds or in other hosting environments, opens the possibility that those systems may escape proper IT security review and monitoring of their configurations and functions.

Before the easy availability of public clouds, systems that were independently deployed tended to turn up within the confines of the enterprise. The server under the desk became a common trope for IT admins. Those systems were protected by the enterprise perimeter, though, and sloppy configurations or insecure management had at least a modicum of protection. But in today's world, server instances are created in public clouds with the swipe of a credit card – meaning the bad habits of those historical practices are now exposed to a much more hostile environment.

Just as it has become orders of magnitude simpler and cheaper for organizations to spin up capacity, attackers have benefited from these same technology advances, allowing them to find and exploit systems at Internet scale at very low cost and technical complexity. Along with cloud-scale decreases in the costs of bandwidth, storage and compute resources, attackers have also benefited from the easy availability of software that allows them to perform rapid Internet-wide scanning for exposed systems. For example, the ZMap Project and the open source tools associated with it have been supported by the University of Michigan since 2013, and these resources pale in comparison to some of the more aggressive tools available to attackers. The ability to rapidly scan and assess any Internet-connected device is a reality today.

In the past, many organizations put their faith in 'security by obscurity' – a strategy for defense based on the idea that the Internet is a vast space where individual IP addresses are not quickly discoverable as long as they aren't referenced in public domain name services or applications. But the arrival of machine-speed Internet scanning means that any exposed device now faces a significant risk of rapid compromise.

The collision of all of these factors means that just as organizations have more assets and services on the Internet than ever before, attackers have inexpensive and effective methods to probe those assets and services for weakness. Organizations have to find ways to mitigate this risk, but even the apparently best-financed and most sophisticated companies in the world often struggle with securing the entirety of their perimeter.

Existing security management offerings can fall short in solving this problem because they only secure the assets they are directed to secure. Vulnerability management tools, for example, scan the assets organizations tell them to scan for any indicators of vulnerability. Similarly, asset

management tools only discover and manage assets in areas where the organization expects them to exist. So without a complete, current and accurate inventory of their Internet assets, organizations can't achieve comprehensive coverage with existing security and IT operations tools.

Fortunately, these problems can be addressed with the right intelligence into and analysis of an organization's global Internet assets. Because RDP and other exposures show up in unexpected places outside of the known enterprise network perimeter, organizations need a global, real-time approach to discovering these vulnerabilities. The prevalence of RDP exposures in Fortune 500 companies can be used as a lens through which to view the ongoing security challenges that organizations face in today's environment.

The Challenges of Securing the Remote Desktop

The Remote Desktop Protocol was developed by Microsoft to allow users to share access to Windows computers via a network connection. The protocol is extremely useful and, beyond its intended multiuser role, fell into wide use by administrators as a way to quickly manage Windows servers. While more secure, scalable and comprehensive server management tools have become available, many organizations continue to use RDP because of its simplicity. The downside is that having direct access to an administrator-level console was a significant enough risk for servers within a traditional perimeter-based environment; in today's world, that risk becomes critical.

Security advances have reduced the risk from exposed RDP servers in recent years, but, like any software, the protocol still contains vulnerabilities, some of which are severe. Early RDP vulnerabilities, like man-in-the middle attacks, have since been mitigated through transport-layer encryption, but attackers are now finding other ways to target exposed ports. In May 2019, Microsoft disclosed vulnerability CVE-2019-0708, nicknamed BlueKeep. The critical severity of this vulnerability is based on the fact that the attacker does not need to be authenticated, and the user does not need to take any action in a successful exploit. This also means that the vulnerability is 'wormable.' (Worms are viruses that spread across networks and replicate automatically, with no interaction required from the user.) Because of this, the vulnerability could be leveraged to launch attacks rivaling the scale of the NotPetya and WannaCry ransomware outbreaks.

Network-level authentication (NLA), which improved some aspects of the authentication process, has also been shown to cache credentials to allow broken sessions to be resumed without reauthentication. While that can accelerate the reconnection process for the client in the event that it loses connectivity, it allows prospective attackers to sidestep the Windows lock screen by hijacking connections.

In a review of two months of RDP exposures across the entire Internet (not just limited to the Fortune 500) in 2018, Expanse found that 90.7% of the time, RDP exposures were live for under one week. In short, RDP exposures are almost always ephemeral – a snapshot of your attack surface on one day doesn't mean that an RDP exposure couldn't pop up the following day. It is simply not possible for organizations to obtain a full grasp of their Internet asset inventory (and associated attack surface) without taking the perspective of the entire Internet and updating that inventory continuously.

Research Methodology

The data in this study was derived from Expanse Platform, which continuously collects and correlates petabytes of active and passive data on every system connected to the public Internet using a globally distributed, dynamically changing sensor network. This study examined RDP exposures associated with all Fortune 500 companies over a two-week period in April 2019. Researchers also examined the prevalence of RDP exposures across industries, as well as the relationship between IT spending as a percentage of company revenue and RDP exposures. The analysis of the Expanse data set should be of great interest to organizations looking to improve their cybersecurity posture and reduce the risks associated with unknown exposures on their network.

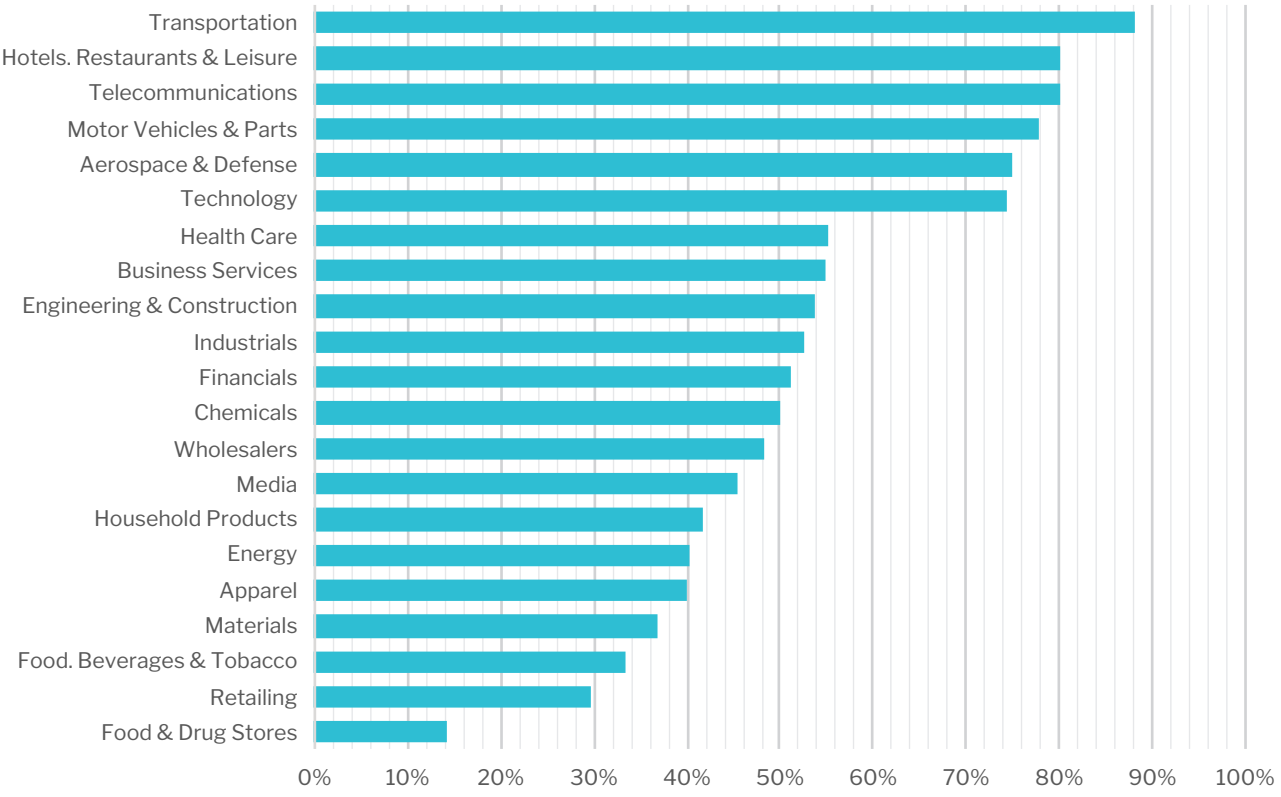
The attribution of identified assets to specific enterprises is achieved via Expanse's proprietary technology. It dynamically attributes all Internet assets back to organizations and requires only a single piece of data related to an organization – for example, the name of the organization – as input. The technology operates recursively. Given a collection of digital identifiers associated with a specific organization – a set that begins with just one element – it searches over dozens of Internet-wide data sets that Expanse collects. Then it automatically nominates new possible identifiers associated with the organization to be added to the organization-specific collection, at which point the process is repeated. In this way, the algorithms driving attribution dynamically learn and adaptively discover all the ways an organization configures and deploys its IT systems on the Internet. The power of this technology comes both from running it over the deep, planetary-scale data indexed by Expanse – over a petabyte a day, including multiple data sets that Expanse uniquely has access to – as well as from its computational intelligence that enables it to find organizations' Internet assets that do not have traditional identifiers, such as a domain name, that are missed by more rigid, rules-based attribution methods.

Spending information on IT budgets was derived from enterprise data from DiscoverOrg. Data was available for 475 of the 500 enterprises that compose the 2019 Fortune 500, and comparisons were made within that set.

RDP Exposures Abound in the Fortune 500

Despite Fortune 500 companies being some of the most elite organizations in the world, they had a surprising and concerning number of RDP exposures in this study. Over the course of a two-week time frame in April 2019, Expanse researchers found that 53.4% of the Fortune 500 had at least one RDP exposure. Because RDP exposures can be quickly located and breached by attackers, one would expect organizations in the Fortune 500 to not have any of them on their networks. This is clearly not the case.

Figure 1: Percentage of Fortune 500 Companies With RDP Exposures by Industry (2-Week Window)
Source: Expanse



The industry breakdown above shows where some of the most significant problems lie. The RDP exposures were most prominent among the transportation, hotels/restaurants/leisure, and telecommunications sectors. There are a number of possible explanations for this heavy weighting. For transportation, organizations are likely to have highly distributed and mobile networks, leading to a greater reliance on RDP for remote connectivity. Hotel, restaurant and leisure businesses are also likely to have distributed networks, as well as a strong focus on connectivity with customers that may be bypassing security protocols. Telecommunications companies may be providing IP hosting services for other organizations, and thus have a larger network perimeter. Whatever the root cause, it clearly is a situation in need of repair.

Interestingly, even Fortune 500 companies in the seemingly most technologically sophisticated and well-funded industries had at least one RDP exposure: 75% of aerospace and defense, 74.4% of technology, 55% of business services, and 51.2% of financial services organizations had at least one RDP exposure in the time period examined.

No matter the industry vertical, the level of exposure indicated by the data is cause for concern. It's a clear indication that systems are being deployed outside of traditional protections, creating risk for the organizations to which they're connected. Efforts to improve this situation must include effective means of locating, identifying and remediating these exposures.

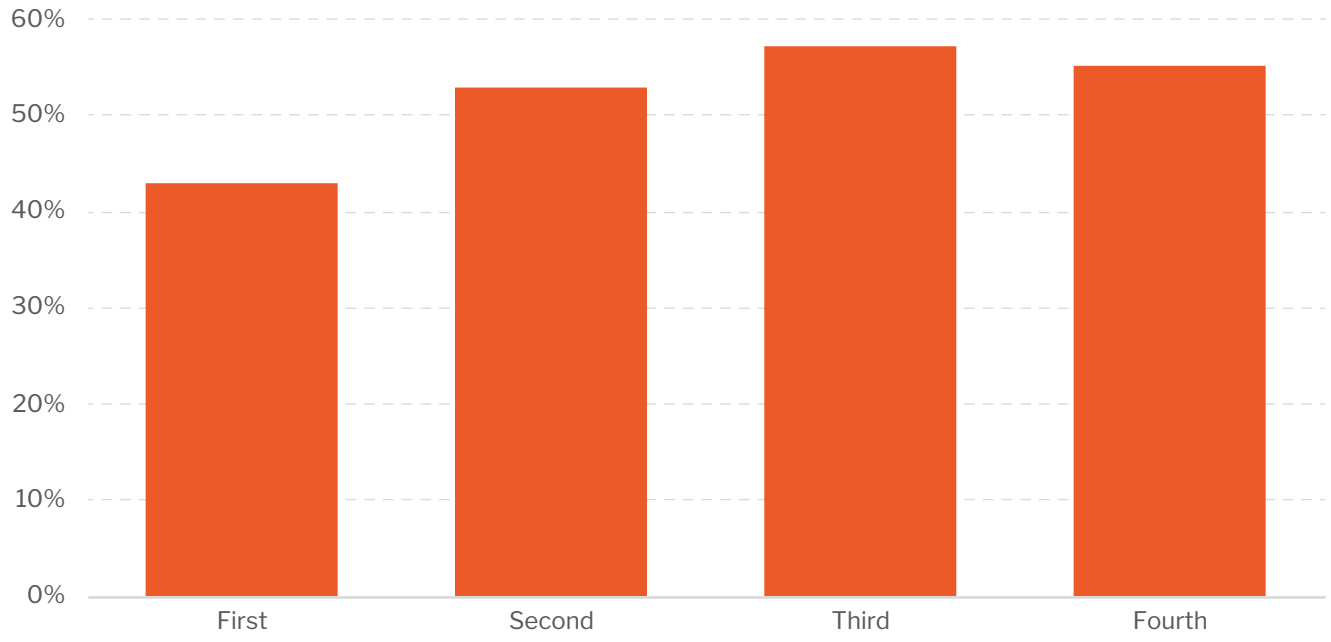
RDP Exposures and IT Spending

A casual observer might reasonably expect that companies with higher levels of IT spending relative to their overall budgets would have heightened security postures and be less likely to have RDP exposures on their networks. To test this, Expanse researchers divided the Fortune 500 into quartiles by reported IT spending as a percentage of total reported revenue, excluding 25 of the Fortune 500 that do not make their IT spending publicly available. Companies in the first quartile spent an average of 1.8% of their total revenue on IT, while organizations in the fourth quartile spent on average 6.1% of their revenue on IT.

Surprisingly, companies with higher reported IT spending were not less likely to have at least one RDP exposure. The third and fourth quartiles actually had a higher percentage of companies with at least one RDP exposure than the first and second quartiles, while the first quartile had the smallest percentage of companies with at least one RDP exposure of all the groups.

Figure 2: Percentage of Fortune 500 Companies With RDP Exposures by Relative IT Spending (2-Week Window)
Source: Expanse

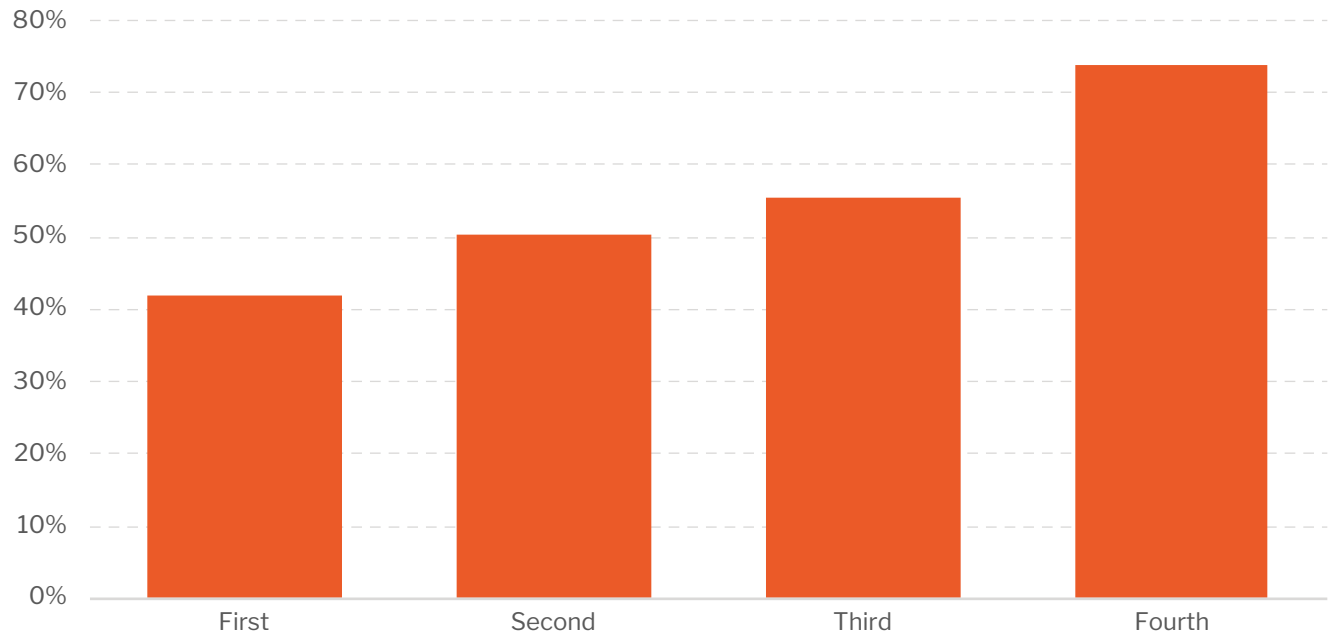
IT BUDGET/REVENUE PERCENT QUARTILE	AVERAGE BUDGET/ REVENUE PERCENT	COMPANY COUNT	NON-ZERO EXPOSURE COUNT	PERCENT W/ AT LEAST 1 EXPOSURE
FIRST	1.8%	119	51	43%
SECOND	2.8%	119	63	53%
THIRD	3.9%	119	68	57%
FOURTH	6.1%	118	65	55%



When examined by reported total IT spending, rather than IT spending as a percentage of overall revenue, the data remained grim: 73.7% of companies in the fourth quartile of total IT spending had at least one exposure. Again, one could reasonably expect companies with larger reported IT budgets to have a corresponding increase in IT operations management and cybersecurity defenses, but in this case the opposite appears to be true.

Figure 3: Percentage of Fortune 500 Companies With RDP Exposures by Total IT Spending (2-Week Window)
Source: Expanse

IT BUDGET QUARTILE	AVERAGE IT BUDGET (MILLIONS)	COMPANY COUNT	NON-ZERO EXPOSURE COUNT	PERCENT W/ AT LEAST 1 EXPOSURE
FIRST	165.7	119	50	42%
SECOND	286.2	119	60	50%
THIRD	502.1	119	66	56%
FOURTH	2262.4	118	87	74%



Conclusion and Recommendations

Effectively managing the security of any large environment has always been challenging. Expanding cloud footprints, complicated enterprise networks with multiple chains of acquisitions and suppliers, and digital transformation initiatives have only increased this challenge. Most security and IT operations management offerings were not created to effectively manage the chaotic environment that today's enterprise has become. Compounding this risk is the expanding use of machine-speed, Internet-scale scanning by attackers, meaning that gaining global visibility into the attack surface is an operational and security imperative.

As the data explored in this study shows, even the largest, seemingly most sophisticated and well-financed organizations can have unknown exposures on their networks. While this study demonstrates the pervasiveness of RDP exposures within the Fortune 500, RDP is just one potential exposed system of many that could permit unauthorized entry by a malicious actor. While the rate of RDP exposure is troubling, it implies a broader issue that affects even leading enterprises in knowing, managing and securing all of their Internet assets.

Organizations that want to mitigate this risk need to adopt an approach that both presumes undiscovered assets exist and implements capabilities to find them as swiftly as possible. These capabilities must include continuous Internet-wide discovery and monitoring of connected assets and services to find those unknown assets that often present the greatest risk of compromise. Without this ability, modern organizations cannot be certain they will lock down exposed assets before attackers find them.

About 451 Research

451 Research is a leading information technology research and advisory company focusing on technology innovation and market disruption. More than 100 analysts and consultants provide essential insight to more than 1,000 client organizations globally through a combination of syndicated research and data, advisory and go-to-market services, and live events. Founded in 2000 and headquartered in New York, 451 Research is a division of The 451 Group.

NEW YORK
Chrysler Building
405 Lexington Avenue,
9th Floor
New York, NY 10174
+1 212 505 3030

SAN FRANCISCO
505 Montgomery Street,
Suite 1052
San Francisco, CA 94111
+1 212 505 3030

LONDON
Paxton House
30, Artillery Lane
London, E1 7LS, UK
+44 (0) 203 929 5700

BOSTON
75-101 Federal Street
Boston, MA 02110
+1 617 598 7200

451 Research®