Third-Party Security Signals

Exposing the reality of unsafe network services

A vast array of services form the underpinnings of enterprise network architectures that move and store data, enable administration of systems, and foster accessibility between entities. Though necessary in the era of digital transformation, such services arguably offer the most direct and tenuous pathways to an organization's critical assets. Attackers know this well and are quick to leverage unsafe network services to undermine a firm's cyber security posture.[1]

Though we colloquially dub data storage, network admin, and remote access services "unsafe," this is somewhat misleading, as their proper usage is not inherently dangerous. But when inadvertently or indiscriminately exposed to the internet, services like the ones above supply a seductive gateway for bad actors. A quick scan of a target's external infrastructure is all that's needed to reveal a not-so-secret entrance for opportunistic attackers. No sophistication or persistence needed.

Eliminating unsafe network services from your own infrastructure is challenging enough; ensuring your business partners and customers do the same is on another level altogether. Our data shows that one in three organizations in your third party population likely exposes unsafe services to the Internet. When your risk performance is interdependent with their risk performance, it's crucial to identify who's falling short of your standards.

In this report, we'll examine the prevalence of unsafe network services leveraging data from RiskRecon, which conducts scans of internet-facing hosts and the services they're running. The dataset includes millions of hosts across 40,000 commercial and public institutions—not home PCs and personal websites. Without tipping our hand, you might find it surprising what these organizations, which are responsible for protecting sensitive data, expose to the Internet for all to see. Perhaps even more importantly, we also look at whether these services forebode other, more inherently risky, security issues across the networks of the organizations in this analysis.

> "This is another example of the strong correlation between hygiene and health in cybersecurity.

33%
of firms expose unsafe network services to the Internet

5x
Firm exposing 9+ unsafe services have 5x higher rate of security findings

59%
of servers running unsafe services also run behind in software patching

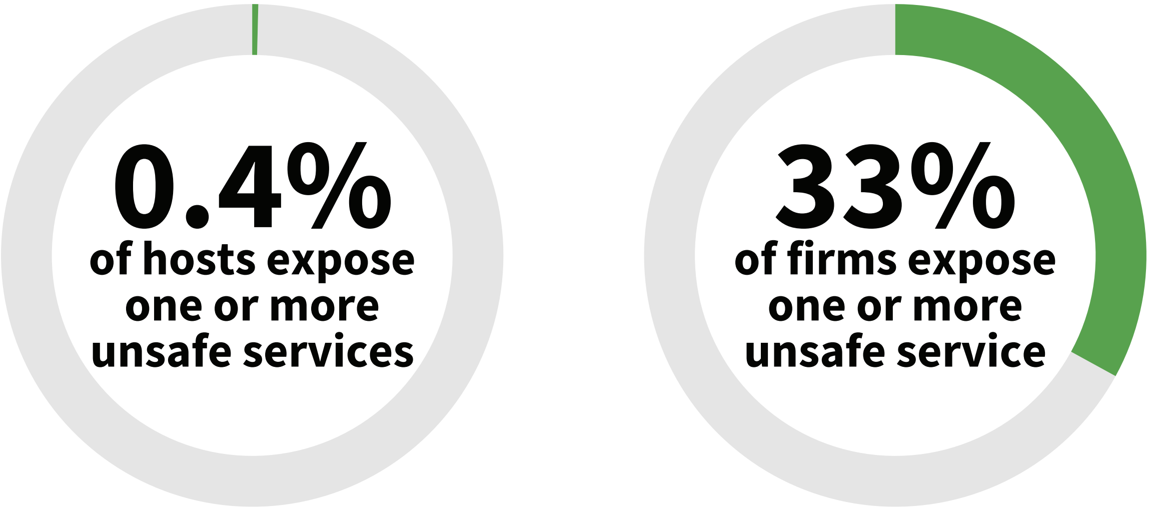
Analysis conducted by Cyentia Institute

[1] For example, automated attacks were recently discovered against users of publicly exposed RDP and Microsoft SQL Server and an attacker leaked more than 515,000 Telnet credentials online by scanning for exposed devices. Unfortunately, these attacks are not uncommon..

Prevalence of Unsafe Services

You might wonder just how widespread the problem of unsafe services is. Again, "unsafe" refers to instances where companies exposed data storage, network admin, or remote access services to the internet. There are two ways of analyzing the data: The first looks at the proportion of internet-facing hosts running these services, and the second looks at the percentage of companies that expose unsafe services somewhere across their infrastructure.

FIGURE 1: PERCENTAGE OF HOSTS (LEFT) AND FIRMS (RIGHT) EXPOSING UNSAFE SERVICES



Given the preponderance of errors we read about in other security reports, you might assume both categories tell a woeful tale. But our data shows that less than half a percent of commercial internet-facing systems expose one or more unsafe services. At first blush, this seems like everyone is doing OK. Keep in mind, though, that a half percent of millions of hosts is still a large number. Plus, each of these systems, if compromised, presents a potential foothold for gaining access to many others.

While the prevalence of unsafe services at the host level is relatively low, 33% of organizations expose one or more unsafe services across hosts under their control. That may seem lower than expected, depending on your perspective. But look at it like this—a full third of firms risk landing on attackers' radar simply by virtue of exposing these services. In that light, it is well worth admins' time to eliminate direct Internet access or deploy compensating controls for when/if such services are required.

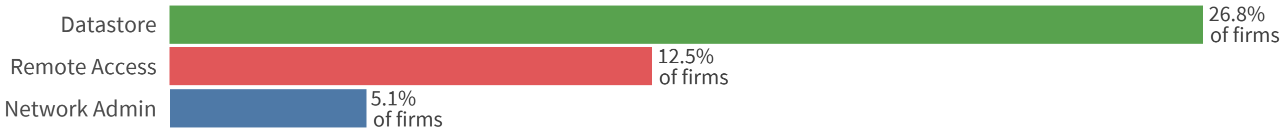
At this point, you might be curious as to which of the services listed at the beginning of this report are most commonly exposed. Per Figure 2, datastores lead by a large margin. If that brings to mind all the exposed S3 buckets, databases, and other events that frequent the headlines, it should. A simple web search will tell you why direct internet access to database services should be prohibited or secured.[2]

> Look at it like this–a full third of firms risk landing on an attacker's radar simply by virtue of exposing these services.

[3] Google "exposed s3 bucket"

Remote access and network admin services certainly have legitimate uses, but threat actors love to exploit them for illicit purposes. These services offer ne'er-do-wells direct paths to system consoles and datastores, which they can directly pilfer and use as staging points for tunneling deeper into their victim's network. Thus restricting accessibility of those services to legitimate users (i.e., limiting to internal or partner IP space) is an essential practice.

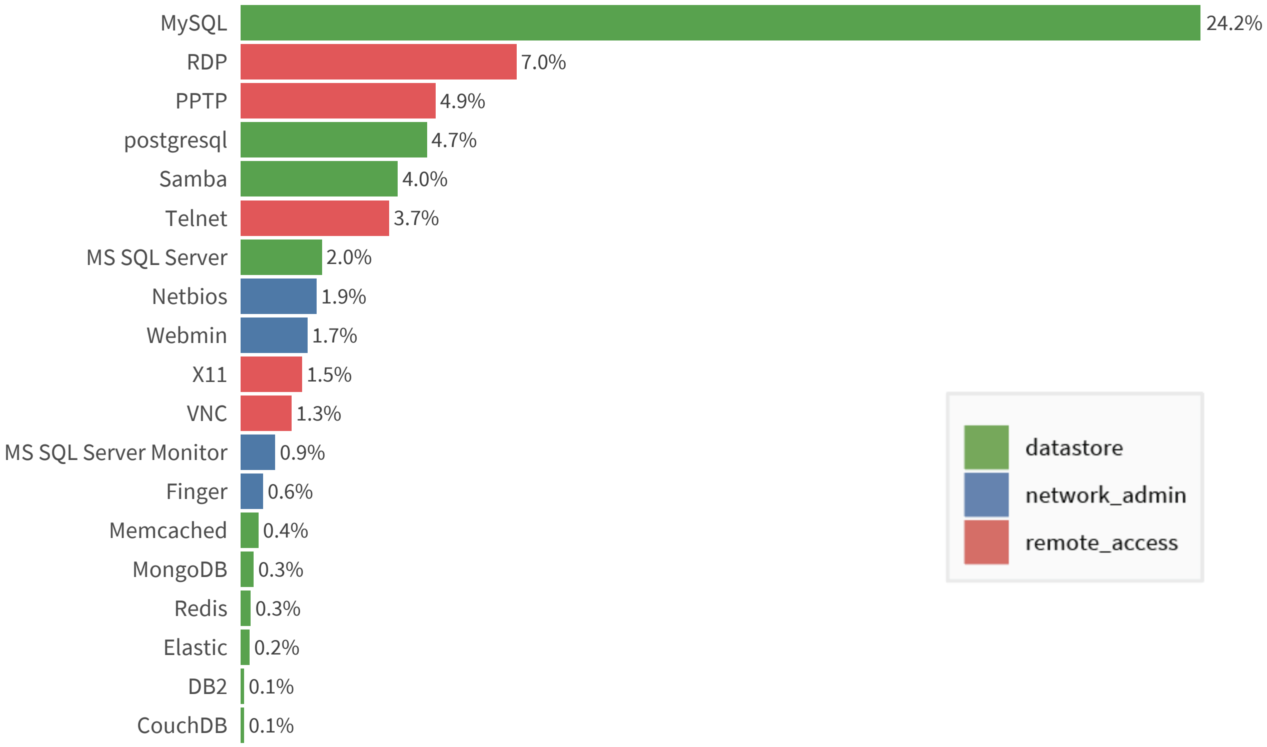
FIGURE 2: PREVALENCE OF UNSAFE SERVICES CATEGORIES EXPOSED BY FIRMS



Examining which specific services are most frequently exposed in Figure 3, MySQL is clearly the biggest offender. Let's just pause for a moment here to consider the seriousness of this. MySQL databases store data. Over 24% of companies expose one or more MySQL databases directly to the Internet. The only thing standing between a hacker and the data in the MySQL database is an authentication credential or a database vulnerability. So much for defense-in-depth...

And while we saw that 27% of unsafe services are datastores, two out of the top three fall in the remote access category. If exploited, RDP or PPTP (or any of the others) could provide easy entrance into an organization's internal network. Needless to say, such doorways shouldn't be advertised and open to the broader population of Internet users.

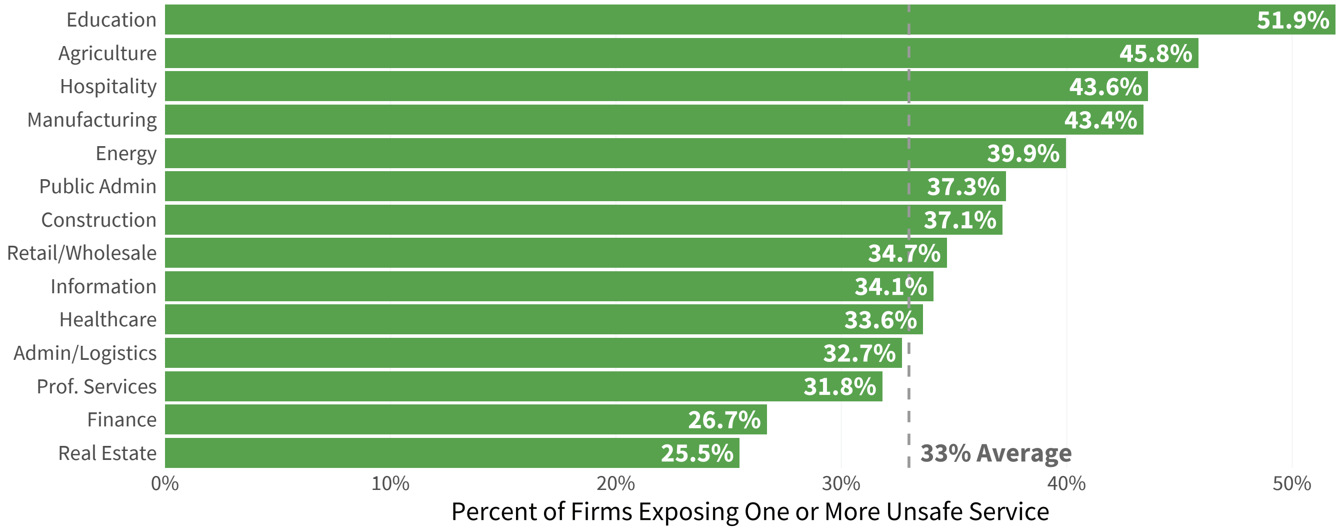
FIGURE 3: PREVALENCE OF UNSAFE SERVICES CATEGORIES EXPOSED BY FIRMS



Unsafe Services Across Sectors

What kinds of companies are more likely to expose sensitive services than others? As you might expect, our data shows that certain industries have greater tendency to expose services. Looking at Figure 4, the education sector has double the number of non-student hosts running unsafe services than finance or real estate. This isn't too surprising considering the culture of educational institutions, emphasizing open access to information and collaboration. And managing networks that can handle large numbers of staff, faculty, and students who are not full-time employees and may therefore not be subject to security awareness training can be challenging for operations teams, thus creating competing priority lists.

FIGURE 4: PERCENTAGE OF FIRMS IN EACH INDUSTRY EXPOSING UNSAFE SERVICES



Hospitality, an industry known to be prone to cyber attacks, likewise rises to the top of risky industries in our dataset. Exploitation of remote access to point of sale and booking systems has long been a common threat vector plaguing hospitality, and the data here on unsafe services may indicate a systemic problem with configuration.

On the other side of the coin is healthcare, which falls to the bottom third of industries with one or more unsafe services. This is notable because, like hospitality, healthcare has been a main target of cyber criminal activity based on sensitivity of systems and information. Healthcare has made headlines many times for failing to properly protect access, so it's good to see that, at least, healthcare admins are more attentive to securing services than two-thirds of industries' admins.

It's not surprising to see financial services and professional services toward the bottom of this list, but finding real estate at the bottom is. According to the North American Industry Classification System (NAICS), the type of companies that fall into this classification are diverse and not the type of companies that would need many of the aforementioned internet services running to support them.

Unsafe Services Around the World

Following the sector-based view of unsafe services from the previous section, let's see if there's a geographic trend as well. Figure 5 color codes countries based on the percentage of domestically-hosted systems running unsafe services. Some countries don't offer much room for labels, so a quick recap is in order. The top five countries with the highest rates are Ukraine, Indonesia, Bulgaria, Mexico, and Poland. Countries shaded gray did not meet our minimum threshold for number of hosts.

FIGURE 5: PERCENTAGE OF HOSTS IN EACH COUNTRY EXPOSING UNSAFE SERVICES

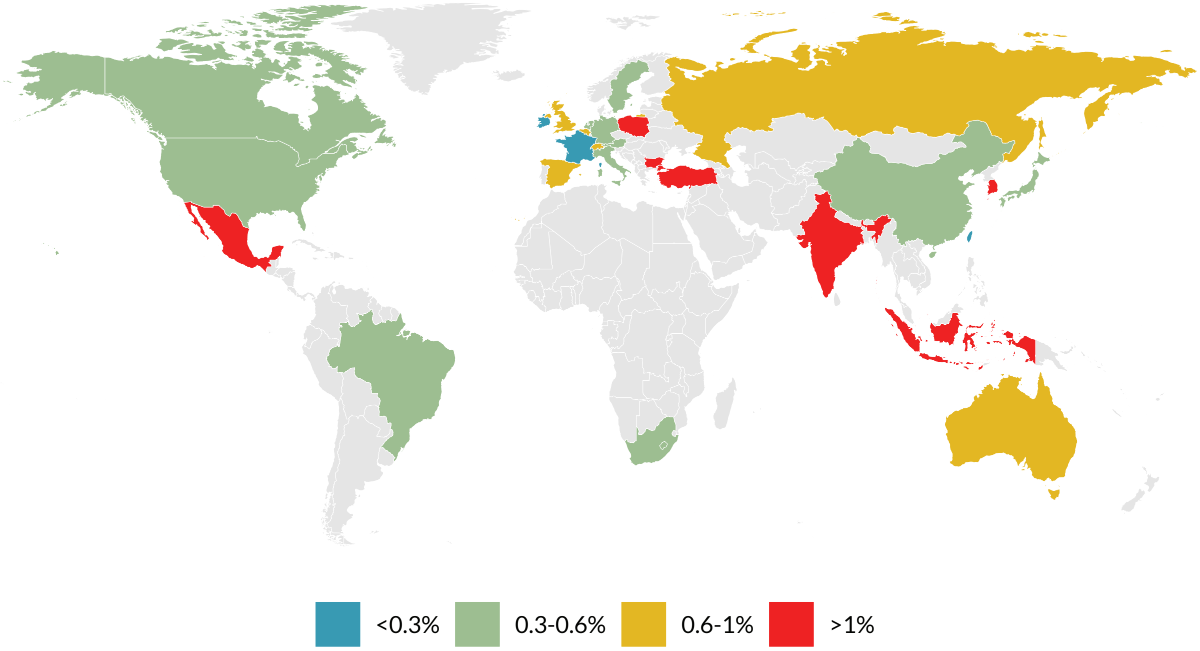


Figure 5 color codes countries based on the percentage of hosts running unsafe services. The top five countries with the highest rates are Ukraine, Indonesia, Bulgaria, Mexico, and Poland.

But what do we take from Figure 5? Similar to Figure 4, information like this is best used in considering where risk hotspot may exist across a portfolio of third parties. That does not mean, for example, that every educational institution in Ukraine flagrantly exposes unsafe network services to the Internet. But if your organization is looking to share sensitive information with such institutions, it might be wise to put some effort into assessing security posture and establishing appropriate controls.

Correlation of Unsafe Services With Other Problems

Overall, the ease with which attackers can find and exploit unsafe services at scale across the Internet suggests that organizations should be more concerned with the consequences of unnecessarily exposing services versus the number or fraction of exposed hosts. This section seeks to explore whether such services correlate with unsound security practices more generally. For instance, are the firms that expose Telnet to the internet also likely to store sensitive data in the clear or allow simple authentication practices? In other words, if an organization exposes many of these services to the internet, do they also exhibit more critical security findings?

To answer that, let's get a quick look at how many unsafe services firms typically expose. Doing so narrows our sample to organizations with more than 100 Internet-facing hosts. What we see in Figure 6 is that 23% of firms expose one service, 13% expose two services, and just under 10% of organizations exposing five or more services. Interesting data, you say, but does that matter? Figure 7 on the next page says yes.

FIGURE 6: PROPORTION OF FIRMS EXPOSING MULTIPLE UNSAFE SERVICES

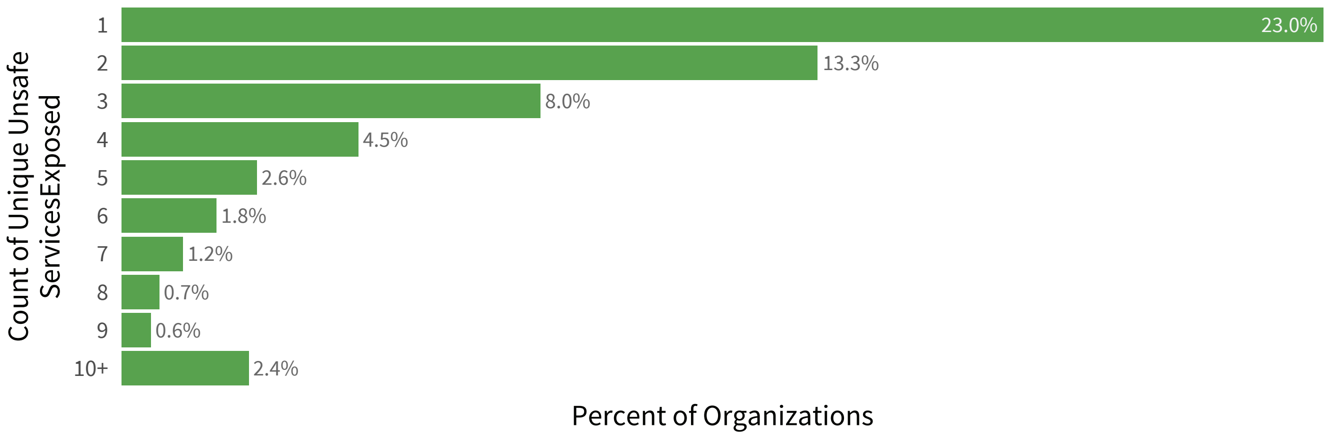
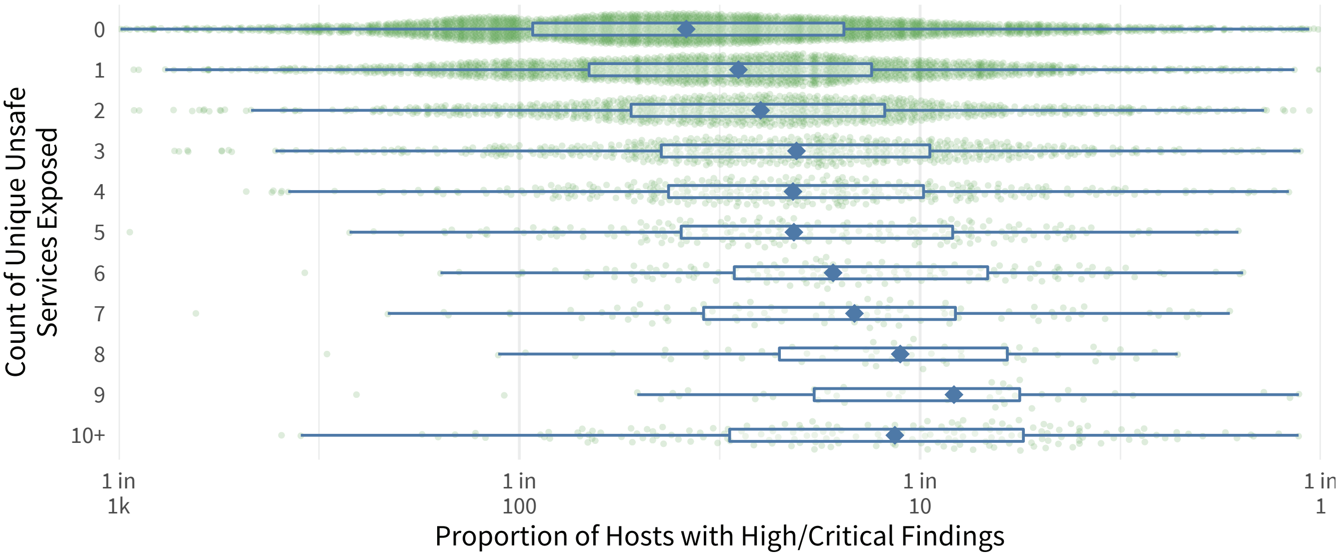


Figure 6 elaborates on how many unsafe network services organizations expose to the Internet. 67% expose none (Figure 1), 23% expose just one, 13% two, on up to the just over 2% that run 10 or more of these services. On the following page, Figure 5 tests whether running more services correlates with more security problems.

> If an organization exposes many of these services to the internet, do they also exhibit more critical security findings?
>
> (Spoiler: Yep)

Figure 7 acts as the "So What?" of Figure 6. The green dots in Figure 5 represent organizations, and their position along the horizontal axis shows the percent of their external hosts that exhibit high or critical security findings. The clusters of green dots show wide variation. Some organizations that expose few unsafe services have a higher density of security findings than those exposing many and vice versa. From this view, it's difficult to discern any concrete pattern or story.

FIGURE 7: PROPORTION OF FIRMS EXPOSING MULTIPLE UNSAFE SERVICES



The green dots in Figure 7 show the percent of each firm's external hosts that exhibit high or critical security findings. The blue dots mark the average for each group, making it clear that the rate of severe security problems increases consistently with the number of unsafe services.

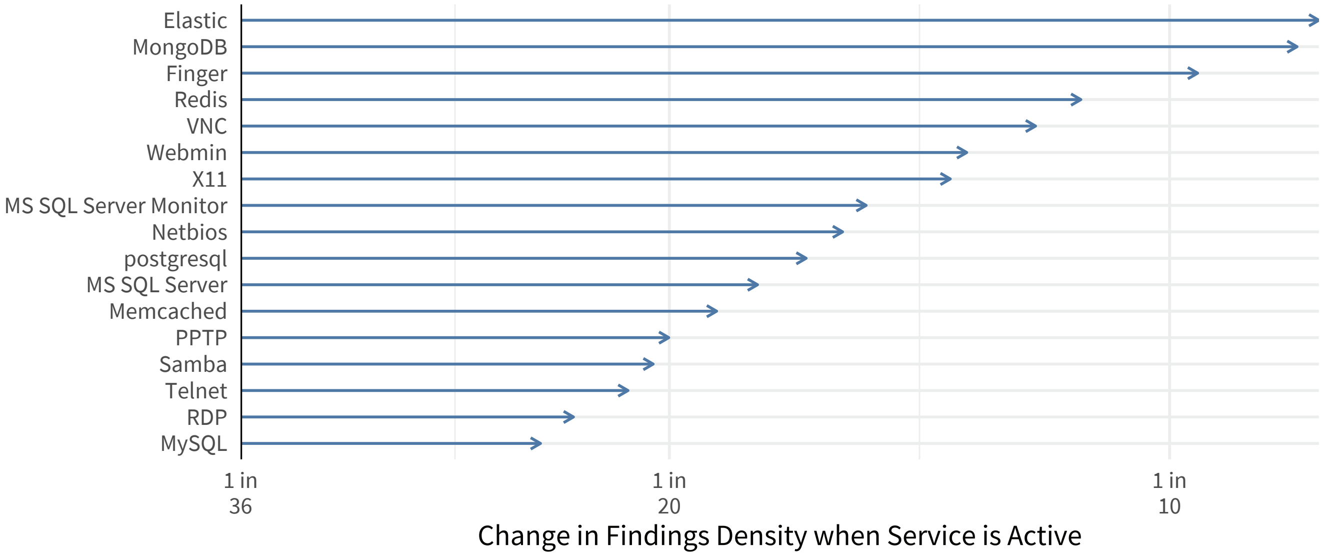
However, the blue boxplots and dots provide a better big-picture statistical view of what's happening. Here we clearly see that the average rate (blue dot) of findings increases consistently with the number of unsafe services. A typical firm exposing zero unsafe services to the Internet has about 1 high or critical security issue for every 38 hosts (2.6%). Comparatively, a firm running nine of such services exhibits a findings density that's nearly 5x higher (1 in 8 hosts, or 12%)! This is yet another example of the strong correlation between hygiene and health (or practice and posture, if you prefer) in cybersecurity.

> " A firm exposing zero unsafe services to the Internet has about 1 high or critical security issue for every 38 hosts. Comparatively, a firm running nine of such services has a findings density that's nearly 5x higher!

What's Most Indicative of Insecurity?

As you might suspect, some of these unsafe services are better indicators of broader security problems than others. Figure 8 presents the details. The vertical line marks the base rate for severe security findings among organizations at about 1 in 36 hosts (2.8%). The blue lines indicate the change in that baseline rate when a firm runs any of the unsafe services listed on the left. Thus, ElasticSearch and MongoDB appear to be the biggest canaries in the coal mine. Organizations that expose those services to the Internet have a rate of severe findings that's 4x to 5x higher than the baseline!

FIGURE 8: UNSAFE SERVICES WITH ASSOCIATED HIGH/CRITICAL SECURITY FINDINGS



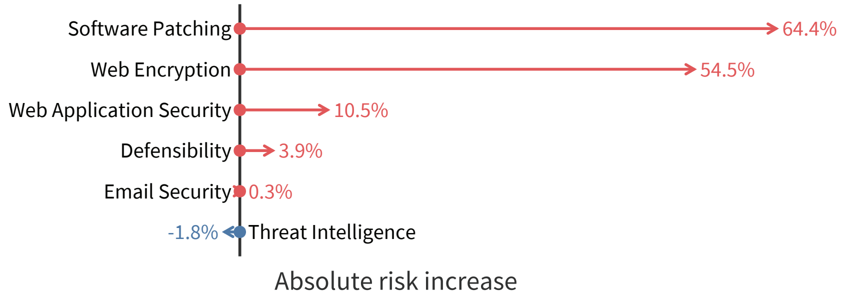
The arrows in Figure 8 indicate the change in the baseline findings density (1 in 36 hosts) when organizations run the unsafe services listed on the left. For instance, firms that expose ElasticSearch and MongoDB have 4x to 5x higher the rate of severe security findings than those that do not run those services on Internet-facing hosts.

You may recall from an earlier section that MySQL was found to be the most prevalent exposed service by a wide margin. However, MySQL is the least of all evils listed in Figure 8 in terms of presaging additional security issues. Similar things can be said of PPTP, Telnet, and RDP, which all fall near the bottom of the chart. But don't interpret that as a green light to spin up those services willy nilly; all of them indicate a significantly higher propensity for security problems. But Figure 8 does offer a reasonable prioritization mechanism if you're looking for a place to start in tidying up your Internet footprint. Take our word for it—none of these will spark joy.

> Paying attention to smoke signals like these services can be a warning of yet unseen fires endangering your organization and its third parties.

Now that we know which unsafe services correlate most strongly with other organizational security findings, let's see what types of findings that entails. Figure 9 makes it clear that failing to patch software is the most prevalent security finding associated with unsafe services. Read the chart like this: 64% of hosts that run unsafe services are also missing important patches. Co-occurring issues with web encryption are a close second. The point here isn't that unsafe services cause patching, encryption, or other problems, but rather lax security practices tend to occur in droves. And that's why paying attention to smoke signals like these services can be a warning of yet unseen fires endangering your organization and its third parties.

FIGURE 9: TYPES OF FINDINGS CORRELATED WITH EXPOSURE OF UNSAFE SERVICES



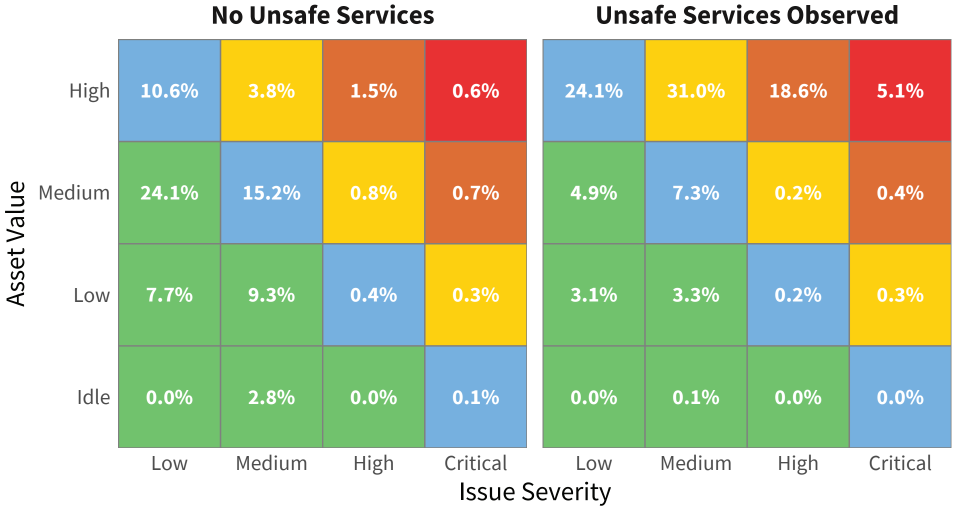
Read Figure 9 like "64% of hosts running unsafe services are also missing key software patches."

One More View on Risk Priorities

Services like those discussed in this report form the foundational fabric of network infrastructure in the modern era. It would be nigh impossible to maintain IT-dependent business operations without them. That said, such services pose a serious threat when exposed directly to the internet without security controls to shield them from unauthorized use. Furthermore, we've shown that the organizations that tend to be more lax in controlling these services also tend to exhibit wider security issues.

We leave you with one final figure presenting a view of this topic through the lens of RiskRecon's risk priority matrices. The upper right is where your eye should be drawn. Assets rated as high value support sensitive and/or critical business functions. That's why the nearly 9x jump in critical security issues among high-value servers running unsafe services is a major red flag that you don't want waving prominently across your infrastructure and third parties.

FIGURE 10: RISK PRIORITY MATRICES FOR SERVERS WITH TLS 1.2 ENABLED VS. NOT ENABLED



No Unsafe Services

Asset Value	Low	Medium	High	Critical
High	10.6%	3.8%	1.5%	0.6%
Medium	24.1%	15.2%	0.8%	0.7%
Low	7.7%	9.3%	0.4%	0.3%
Idle	0.0%	2.8%	0.0%	0.1%

Unsafe Services Observed

Asset Value	Low	Medium	High	Critical
High	24.1%	31.0%	18.6%	5.1%
Medium	4.9%	7.3%	0.2%	0.4%
Low	3.1%	3.3%	0.2%	0.3%
Idle	0.0%	0.1%	0.0%	0.0%

Assets rated as high value support sensitive and/or critical functions. That's why the nearly 9x jump in critical security issues among high-value servers exposing unsafe services is a major red flag.

How Can We Put This Into Practice?

Wondering how RiskRecon can help your organization take action on the findings from this report? Read this.

Enterprise Risk Management

RiskRecon's continuous IT profiling and security analytics give you intimate visibility into your Internet connected systems, where they're hosted, what their configuration is, and if it meets security requirements. RiskRecon's analytics discover the IT profile of every system and analyze each one against 41 security criteria like those examined in this report. Combined with RiskRecon's ability to automatically determine asset value at risk, your teams can easily identify issues, prioritize response, and act efficiently.

Third Party Risk Management

Performing third-party assessments without objective data puts you at a huge disadvantage, leaving you only the ability to review unsubstantiated questionnaire answers. Which of your third parties are exposing unsafe network services? Do your vendors really patch software vulnerabilities? RiskRecon objectively verifies vendor cybersecurity risk performance, enabling your analysts to see how well your vendors actually implement and operate their risk management program.

Mergers and Acquisitions

Know exactly what you're acquiring. RiskRecon delivers objectively gathered information about any company's information security program. You'll gain full knowledge of the environment and risks of an acquisition beforehand, enabling you to establish merger costs and potential liabilities with the Board and enter into the M&A process with greater peace of mind.

RiskRecon enables clients to easily understand and act on their third-party risk through cybersecurity ratings and continuous security control assessments.

www.riskrecon.com

The Cyentia Institute produces compelling, data-driven research with the aim of improving knowledge and practice in the cybersecurity industry.

www.cyentia.com