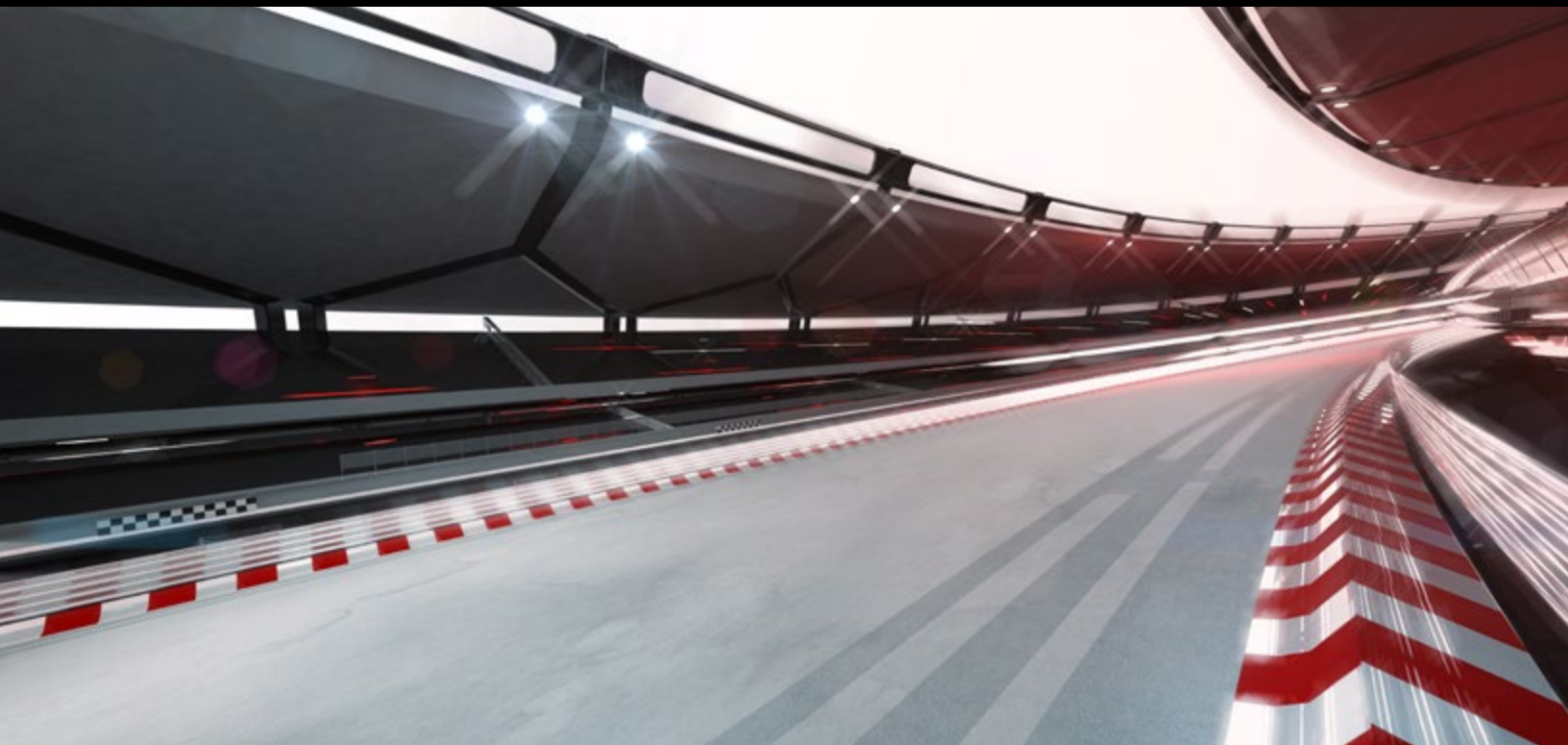
The Fast and the Frivolous

Pacing Remediation of Internet-Facing Vulnerabilities

a collaboration between

SecurityScorecard | Cyentia Institute



Introduction

"It don't matter if you win by an inch or a mile. Winning is winning."
- Dom Toretto, *The Fast and the Furious*

In many ways, cybersecurity is a race. We race against the actions of malicious adversaries. We race to shore up defenses after the latest headlines of impending cyber doom. We race to fill staffing gaps, streamline processes, and keep up with the latest technologies. We race to assess an ever-growing array of third parties on which we're increasingly dependent.

But are we winning that race?

That's the question we seek to answer in this study using a massive dataset from SecurityScorecard that spans 1.6 million organizations. We analyze billions of internet-exposed assets to measure the speed of vulnerability remediation over a three-year period. Below you'll find a sampling of the lessons we learned from the data and expand upon in this report.

CONTENTS

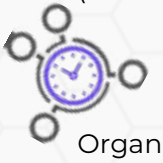
Key Findings

All told, **53%** of the 1,623,118 organizations assessed have at least one open vulnerability exposed to the internet. **22%** of those organizations amass over 1,000 vulnerabilities each.

It typically takes organizations about a year to remediate half of the vulnerabilities in the internet-facing infrastructure.

Firms with **10 or fewer** open vulnerabilities take about a month to close half of them. But when that list grows into the hundreds, it takes a year to reach that same halfway point.

In an unusual twist, the Finance sector has one of the slowest remediation rates (median=426 days), while Utilities rank among the fastest (median=270 days).



Despite a **15-fold** increase in exploitation activity for vulnerabilities with published exploit code, we see little evidence that organizations fix exploited flaws faster.

Organizations typically fix about **10%** of vulnerabilities each month, regardless of how many total vulnerabilities exist across their domain(s).

Even so, about **60%** of organizations are managing to drive down vulnerabilities across their external assets over time. That **60%** is a slimmer majority than we'd like to see, but we'll take Dom's suggestion and consider it a win.

Read on for all the related details and insights to set your organization up for gaining victory over vulnerabilities.

Methods & Firmographics

SecurityScorecard continuously scans the entire IPv4 space to identify vulnerable and misconfigured digital assets. Additionally, SecurityScorecard monitors signals across the Internet, relying on a global network of sensors that spans the Americas, Asia, and Europe. The company operates one of the world's largest networks of sinkholes and honeypots to capture malware signals and further enrich its data set by leveraging commercial and open-source intelligence sources. SecurityScorecard continuously monitors the security posture of over 12 million organizations globally, detecting over 60 billion vulnerabilities each week that are surfaced through its platform.

A subset of data collected by SecurityScorecard on vulnerability remediation was sanitized of all identifying information and provided to the Cyentia Institute for analysis in this report. The dataset encompasses 1,623,118 organizations, scanned over a three-year period, from early 2019 to early 2022. As you might expect, these organizations represent a wide variety of industries and sizes. Figure 1 provides more details around the sample.

Small and Medium Businesses (SMBs) form the majority of the dataset, which is reflective of the broader corporate environment that includes far more small firms than large enterprises.

The industries listed in Figure 1 are abbreviated versions of top-level sectors defined in the North American Industry Classification System (NAICS). You can find the definitions of those sectors, as well as their many subsectors on the NAICS website. While professional services and manufacturing firms claim the highest representation, the dataset contains tens of thousands of organizations from each sector. Thus, we feel confident saying that organizations like yours are represented.

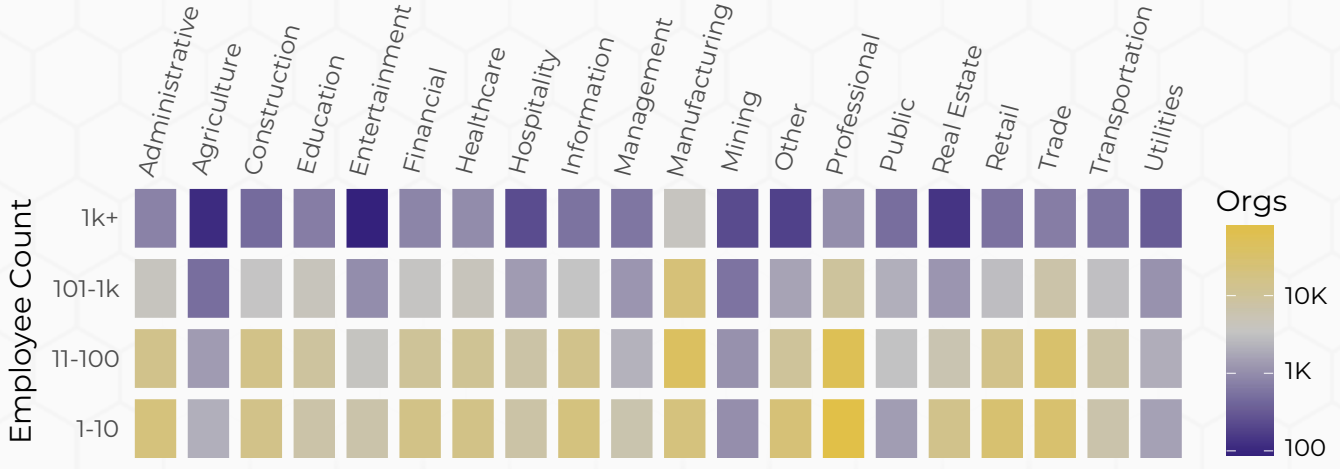


Figure 1: Organizations represented based on NAICS sector and employee count

While we chose not to include a geographic breakdown for organizations, we assure you that coverage is global. Europe (41%) is the leading region of operation, followed by North America (38%), and Asia (10%). These regional affiliations are supplied by Dun & Bradstreet and represent the geographic location for the firm's primary headquarters.

Vulnerability Prevalence

Before kicking off the main event centered on remediation, let's set the stage with information about the vulnerabilities that need remediating.

As part of its scanning regimen, SecurityScorecard identifies numerous vulnerabilities affecting internet-facing assets around the world. In this report, we focus on 2,429 of the 175,000+ total vulnerabilities published on the CVE List.

While not exhaustive, this is a subset of vulnerabilities that are prevalent and identifiable from external scanning. In other words, the same ones an attacker can readily find and exploit.

Of the 1,623,118 organizations assessed by SecurityScorecard, 53% had at least one exposed vulnerability. All of the organizations appearing in this dataset have had a vulnerability detected at some point within the past three years.

> *Of the 1,623,118 organizations assessed by SecurityScorecard, 53% had at least one exposed vulnerability.*

Among firms with open exposures, Figure 2 gives a breakdown of how many vulnerabilities exist across their digital footprint of internet-visible assets.

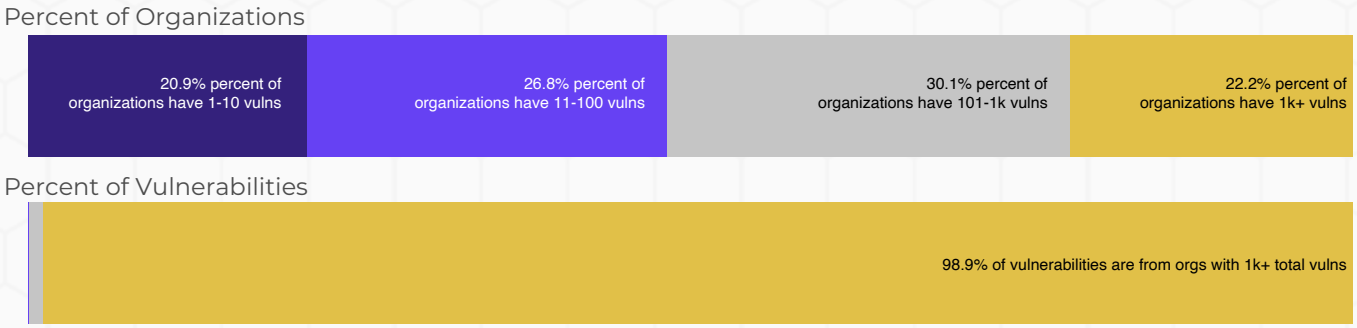


Figure 2: Distribution of open vulnerabilities at organizations

The top bar shows that about 20% of organizations have between 1 and 10 vulnerabilities, while about the same proportion exhibits over 1,000. So there's a wide and fairly balanced distribution in terms of vulnerability prevalence.

The bottom bar in Figure 2 upsets this apparent balance by clarifying that the largest firms with 1,000+ exposures claim the vast majority of total vulnerabilities detected.

Vulnerability Prevalence By Vendor

Figure 3 begins putting a face on detected vulnerabilities based on the vendor and platform associated with the CVE. Vendors toward the right account for a large number of vulnerable assets detected, while those toward the top were observed across numerous organizations. If you keep in mind these are internet-facing exposures, the list generally aligns with expectations. Web technologies, for example, are among the most prevalent exposures.

We feel compelled to caution readers about errant conclusions based on this chart. While it's tempting to say "look at those horribly insecure vendors/products in the upper right," this chart reveals much more about enterprise vulnerability management programs than vendors. The placement of these different technologies in the plot is primarily a factor of their install base and how organizations manage them. Sure, vendors can do things to make it easier for organizations to fix vulnerabilities in their products, and we'll discuss that when we look at remediation velocity.

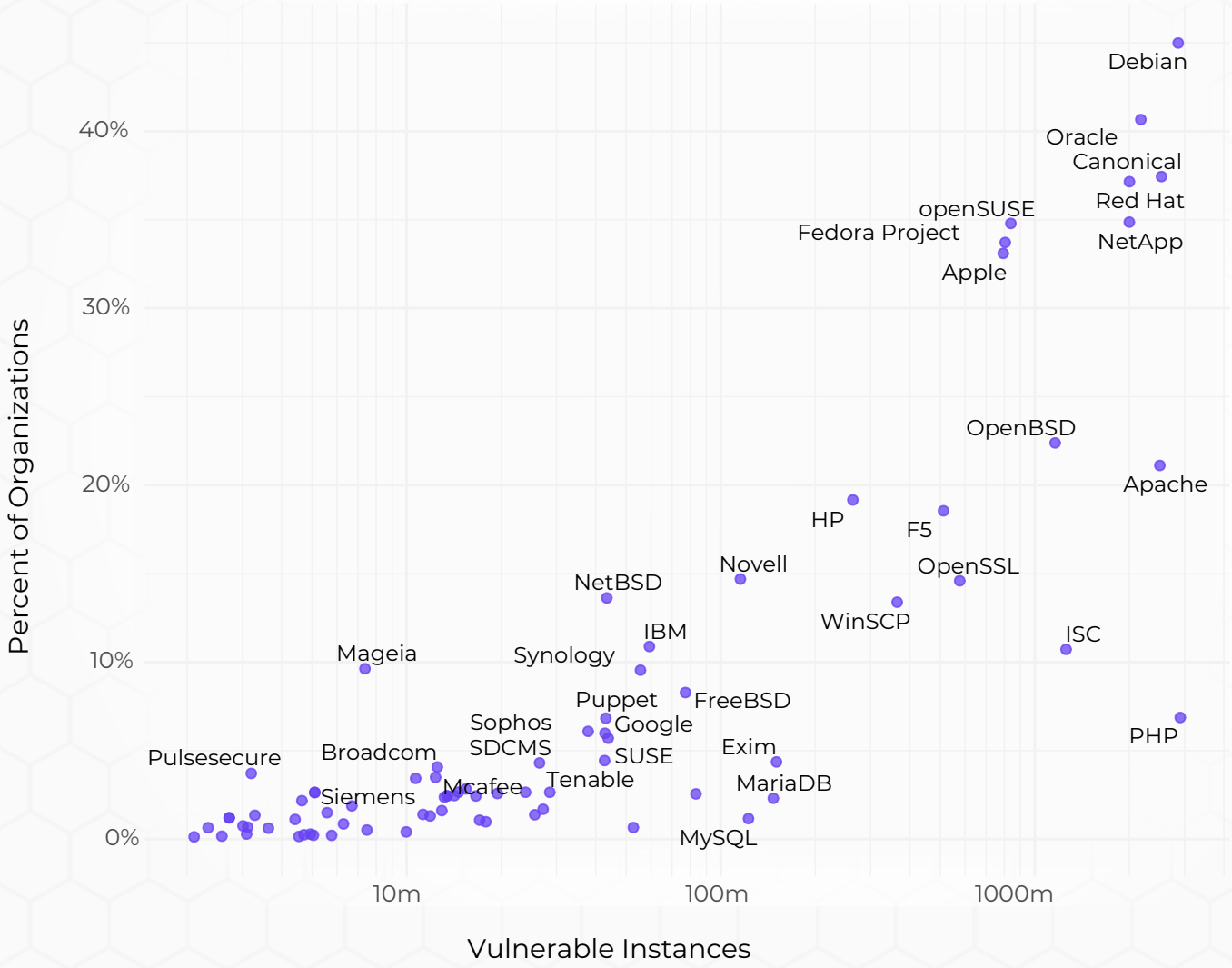


Figure 3: Total volume and prevalence of open vulnerabilities by vendor

Vulnerability Prevalence By Sector

Typically, a smaller digital footprint means fewer vulnerabilities; one thing we do find surprising is that the Hospitality sector exhibits the second-lowest vulnerability prevalence.

Industries often engage in different business activities and employ varied technologies to support those activities. As a result, it makes sense that such differences would impact the typical volume and variety of vulnerabilities present across the internet infrastructure of different types of organizations. Let's see if the data backs up that intuition.

We already learned that over half of all organizations in our dataset have open vulnerabilities, so let's see how sectors compare on that statistic.

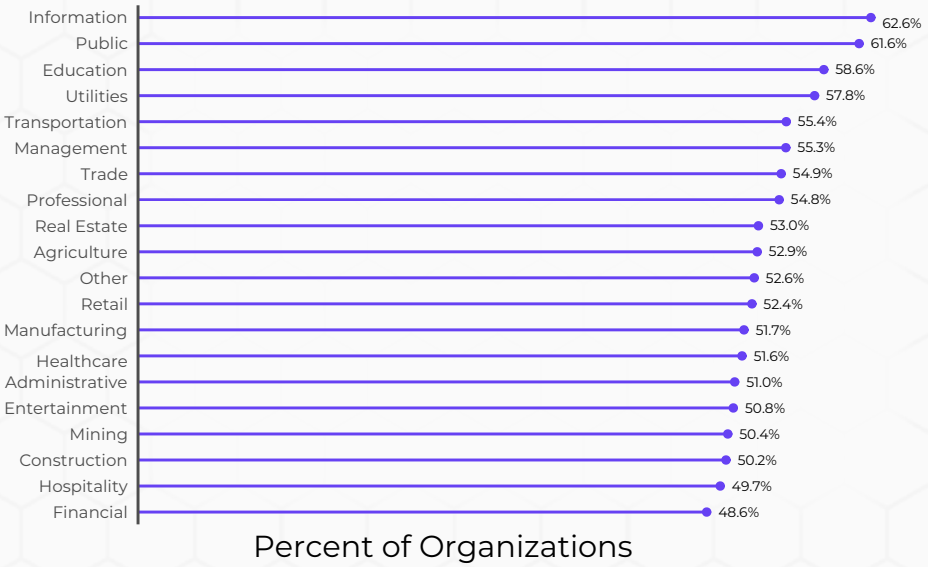


Figure 4: Proportion of organizations in each sector with open vulnerabilities

Figure 4 presents the percentage of firms in each sector with at least one open vulnerability detected in recent scan results.

Going back to our earlier statements about technologies and business activities, it's hardly surprising that the Information sector has the highest prevalence of open vulnerabilities. It should be noted that this does not mean they're the worst at managing them. That outcome is a byproduct of the tech-rich business models of such firms. Similar comments can be said of the Public and Education sectors, which land in the second and third spots in Figure 4's ranking. We'll see how they fare in fixing those vulnerabilities later.

Moving to the other end of Figure 4, it's also not surprising that the Financial sector exhibits the lowest proportion of open vulnerabilities. Financial services firms are highly-regulated, have larger-than-normal security budgets, and traditionally have been conservative about their internet footprint.

That said, it's worth noting that there's less than a 10% difference between the Financial sector and most others in terms of industries with open vulnerabilities.

One thing we *do* find surprising is that the Hospitality sector exhibits the second-lowest vulnerability prevalence. This is where it's helpful to remember the source of the data that we're examining. It's very common for restaurants and hotels to outsource all or most of their booking, billing, and point-of-sale systems to an information services provider.

Thus, it's possible that many vulnerabilities in such systems would get filtered into the Information sector's tab. The construction and mining industries also fall into the "smaller digital footprint; fewer vulnerabilities" category.

We include Figure 5 because it helps explain a lot of what we see in Figure 4. Namely (and logically), industries where organizations must contend with a high volume of vulnerabilities will generally have a higher proportion of open vulnerabilities.

> *There is a less than a 10% difference between the Financial sector and most other sectors.*

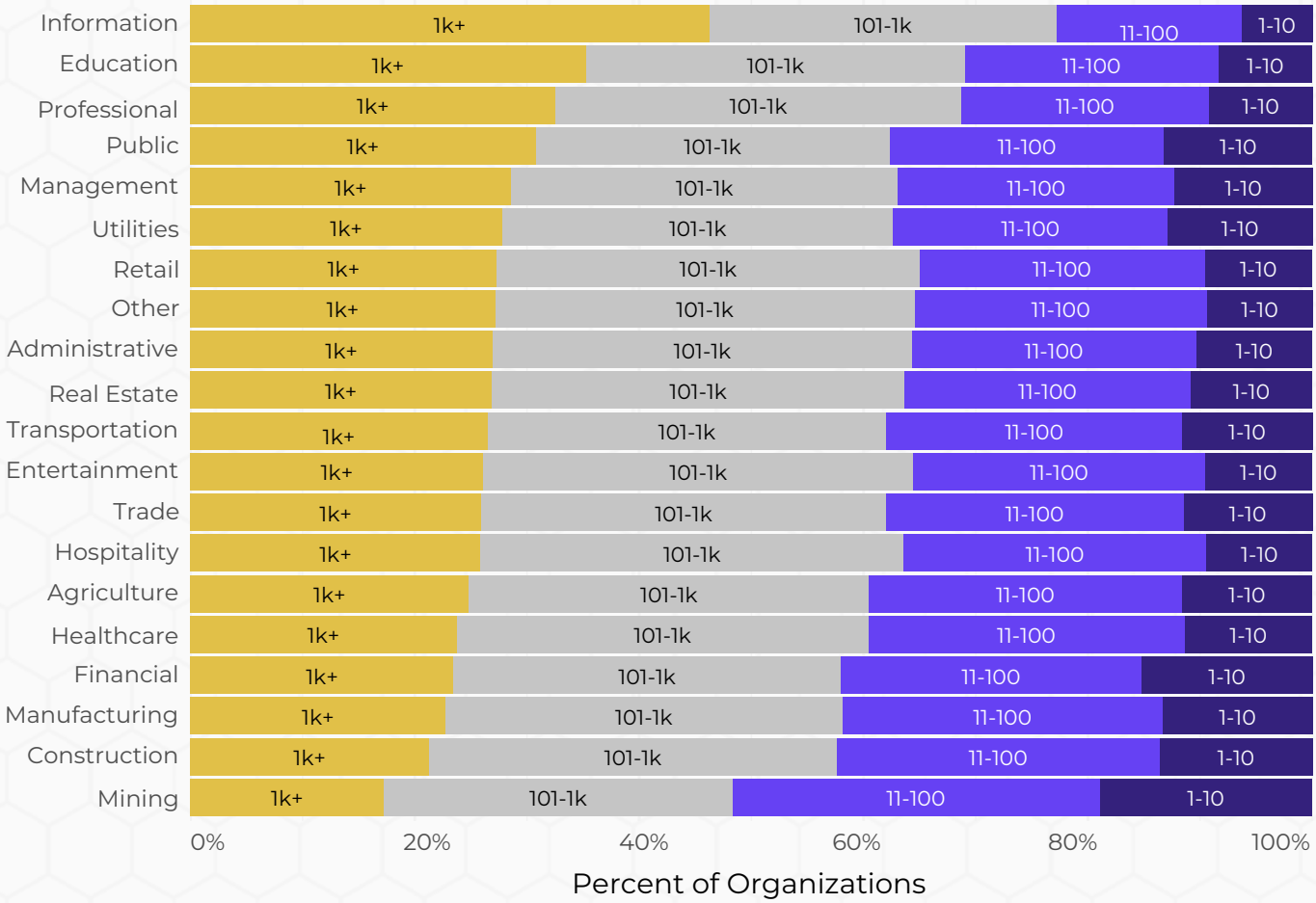


Figure 5: Count of open vulnerabilities observed across organizations in each sector

Vulnerability Prevalence By Employee Count

This talk of digital footprints may lead one to infer that larger organizations have more vulnerabilities. Figure 6 does indeed support that inference, but not to the extent one might expect.

Large enterprises may have more resources to find and fix vulnerabilities, but they also have more assets, more locations, and more complexity. SMBs might have less technical debt, but fewer hands to manage it.

Thus, organizations both large and small contend with different manifestations of the same challenge. That's probably why the differences in vulnerability prevalence by organization size in Figure 6 isn't huge.

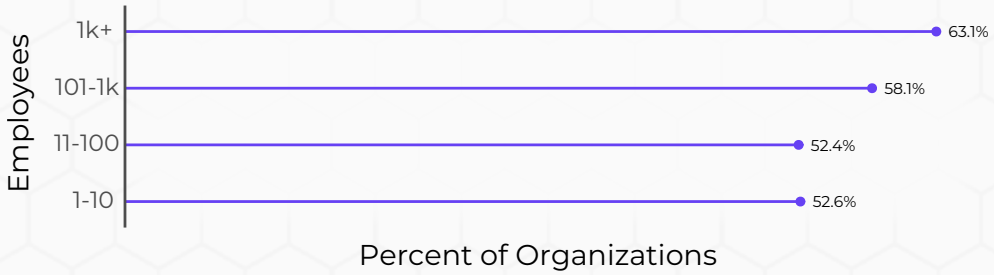


Figure 6: Proportion of organizations in each size category with open vulnerabilities

Vulnerability Prevalence By Region

When it comes to the percentage of organizations with exposed vulnerabilities, the region of operation carries about the same weight as industry or size. Per Figure 7, there's only a 12% difference in the prevalence of open vulnerabilities between the region with the lowest (North America) and highest (Africa).

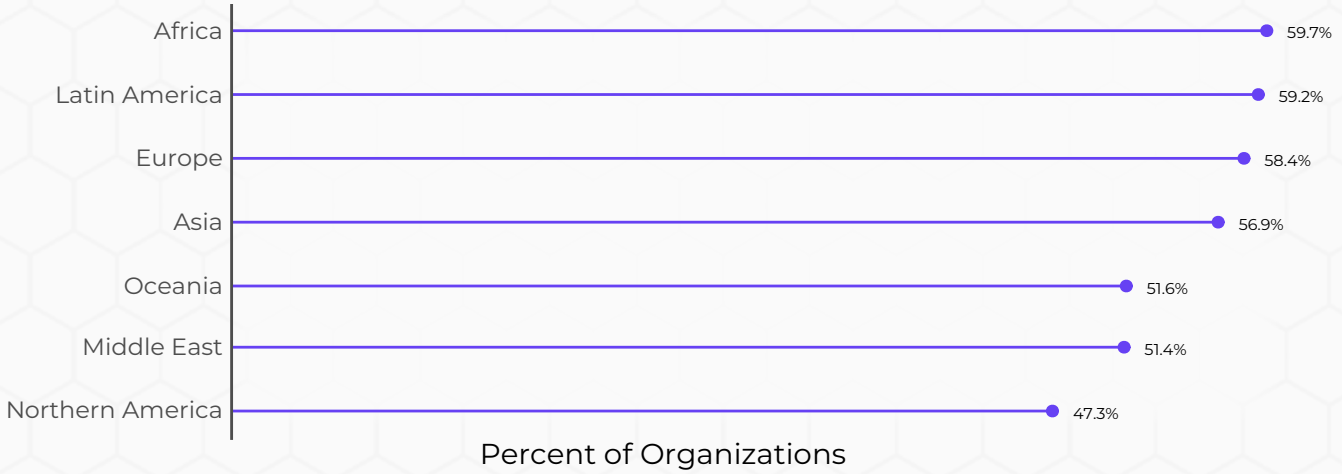


Figure 7: Proportion of organizations in each region with open vulnerabilities

All in all, firmographics don't seem to be a huge differentiating factor for how organizations manage vulnerabilities on the internet. Over half of organizations have exposures, and those organizations span all types, sizes, and regions. From a third party risk management perspective, this limits the assumptions we can make about an organization's capabilities based on those factors (i.e., we can't assume SMBs have poor security or that Fortune 1000s are impervious).

Remediation Velocity

IN THE LAST SECTION, WE SAW THAT ORGANIZATIONS OF MANY SIZES HAVE A WIDE RANGE OF OPEN VULNERABILITIES. IT WAS NECESSARY TO ESTABLISH THE UNDERPINNINGS OF THAT SEEMINGLY SIMPLE FACT IN ORDER TO GET TO THE REAL GOAL OF THIS STUDY—MEASURING THE SPEED AT WHICH THOSE VULNERABILITIES ARE REMEDIATED.

Survival Analysis of Internet Vulnerabilities

To measure the speed at which those vulnerabilities are remediated, we'll use a statistical technique known as survival analysis. In a nutshell, it measures the duration of time to some event of interest. In our case, that's the time required to remediate vulnerabilities.

For example, if an organization has 100 open vulnerabilities across its systems and manages to fix 15 of them today, that means 85 vulnerabilities remain open—an 85% survival rate. If they fix 10 the next day, survivability drops to 75%, and so on over time.

Survival analysis measures the duration of time to some event.

But things rarely run that smoothly in the real world of vulnerability remediation, as Figure 8 attests. Instead of a couple days to remediate 25% of vulnerabilities, our data shows it typically takes organizations 180 days to reach that milestone.

The half-life of vulnerabilities in internet-facing infrastructure is just shy of a year. And even after two years, there's still work to do.

The half-life of vulnerabilities is just shy of a year.

Depending on your professional experience, these findings may inspire reactions from "OMG; the internet is burning!!" to "Mm-hmm; seems about right."

Regardless of where you are on that reactionary spectrum, Figure 8 contains some important lessons about remediation velocities that are worth drawing out.

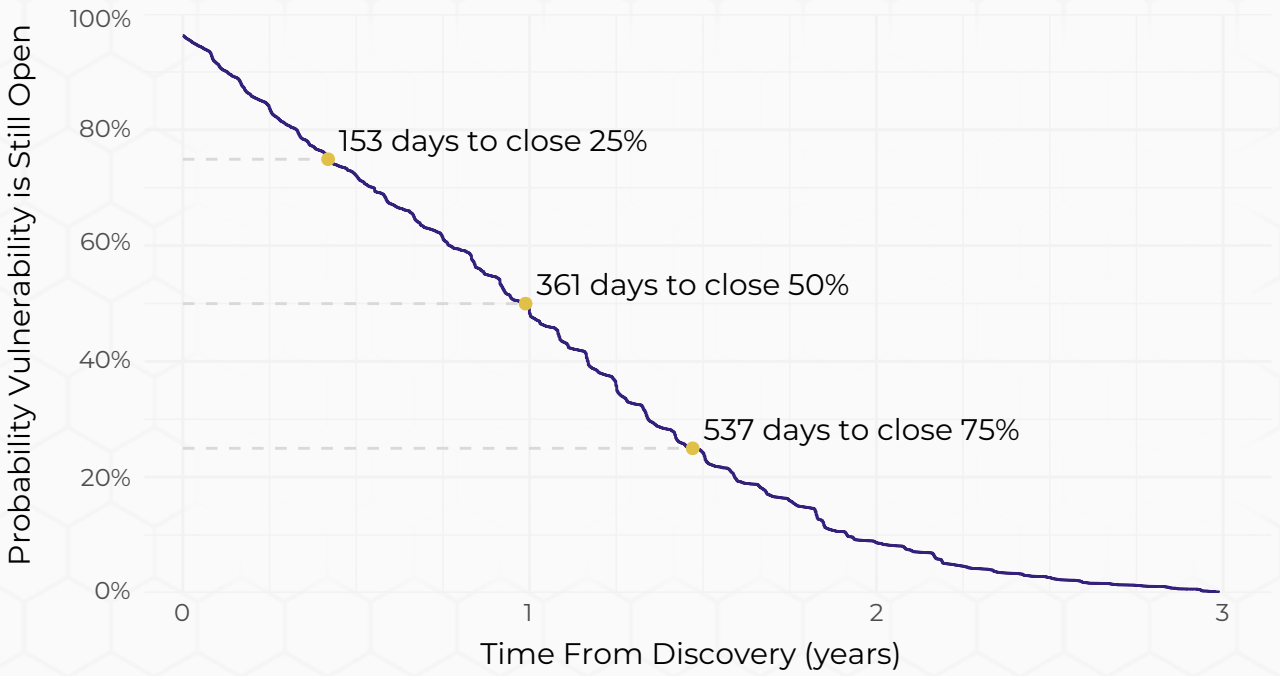


Figure 8: Overall remediation velocity across all vulnerabilities in all organizations

Some remediation velocity variance may be caused by the frequency in which vulnerabilities are scanned and fixed; a tighter, find-fix process may lead to faster remediation.

This survival curve looks considerably slower than others we've produced for security flaws discovered through code scanning in software development or found via vulnerability scans of mostly internal production assets. Part of the difference results directly from the variance in scanning cadence in these different domains of security.

Some differences may also relate to feedback. For example, if a firm runs a scanner internally, they tend to review the results and start fixing things. However, many of the organizations passively scanned by SecurityScorecard aren't immediately aware of their exposures. It also may be more difficult to patch internet-facing assets, because they support critical revenue-generating functions that can't be interrupted.

We could go on, and you probably have thoughts of your own. Bottom line: survival rates of vulnerabilities offer important baseline behavioral insights, and we're thrilled to be able to study them in these different contexts.

Survival curves are complicated, so we're going to adopt the KISS (Keep It Simple, Stupid) principle for visualizing remediation velocity from here on out.

Figure 9 shows a simpler view of the same basic information portrayed in Figure 8. The duration for the three key milestones are marked, which makes things much easier as we begin comparing remediation velocity among various categories in the following sections.

Figure 9: Simplified view of overall remediation velocity across all vulnerabilities

These differences speak to the efficacy of vulnerability management capabilities within those organizations.

We're going to do one more depiction of remediation velocity to make an important point. The timelines in the previous figures span all vulnerabilities across all organizations. However, it's possible to calculate remediation velocity for individual organizations too.

Figure 10 illustrates how long it takes organizations to remediate 50% of the vulnerabilities across their domain(s). Ten percent of firms reach the halfway point in fewer than three months. Another 13% of them take 18-21 months to hit the same milestone, and there's a fairly even spread between those timeframes. The tail trailing out over three years indicates a small minority of organizations that really take their time. The variation shown here should hammer home the point we wanted to make—remediation velocity differs dramatically among organizations.

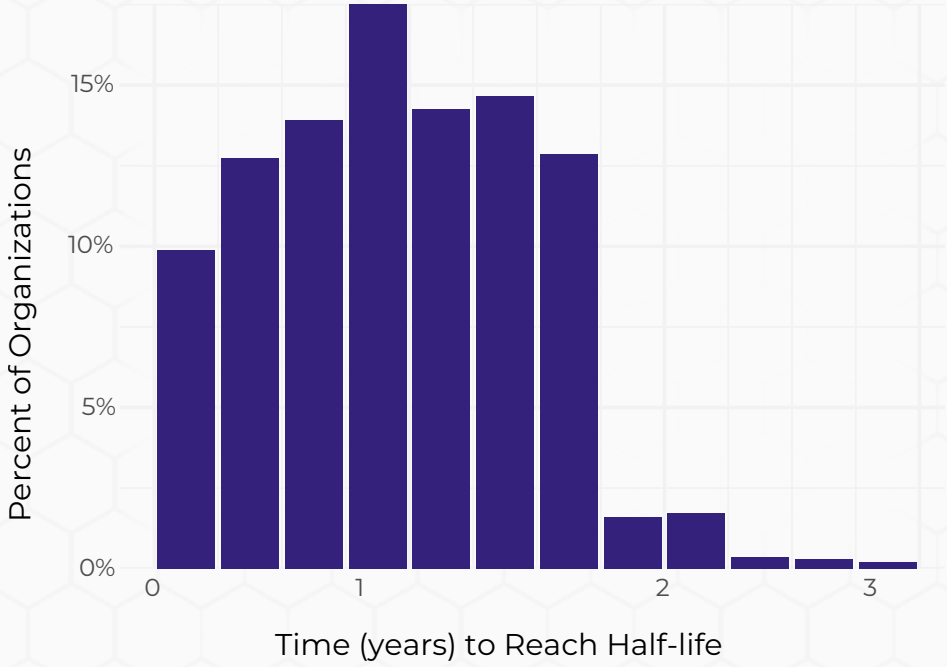


Figure 10: Variation among organizations in time to close 50% of open vulnerabilities

These differences are more than just pedantry. They speak to the efficacy of vulnerability management capabilities in those organizations. From a third-party risk management perspective, who would you want to partner with—firms hugging the zero remediation event horizon on the left or those struggling way out in the long tail to the right?

Remediation Velocity

Measures the speed and progress of remediation.

How quickly are issues addressed?

How long do they persist across assets?

Remediation Velocity by Organization Size

THE HYPOTHSIS IS THAT SMBS HAVE FEWER ASSETS WITH FEWER VULNERABILITIES, AND THEREFORE COULD FIX THEM FASTER. ALTERNATIVELY, LARGER ORGANIZATIONS HAVE MORE RESOURCES AT THEIR DISPOSAL, WHICH MAY HELP THEM STAY ON TOP OF THINGS.

Does remediation velocity correlate with size? As with prevalence, one could hypothesize that SMBs have fewer assets with fewer vulnerabilities, and therefore could fix them faster. Alternatively, larger organizations have more resources at their disposal, which may help them stay on top of things.

Based on Figure 11, larger organizations tend to have an advantage when it comes to remediation velocity. That said, the high degree of overlap exhibited means that we definitely can't assume or predict performance based on employee count alone.

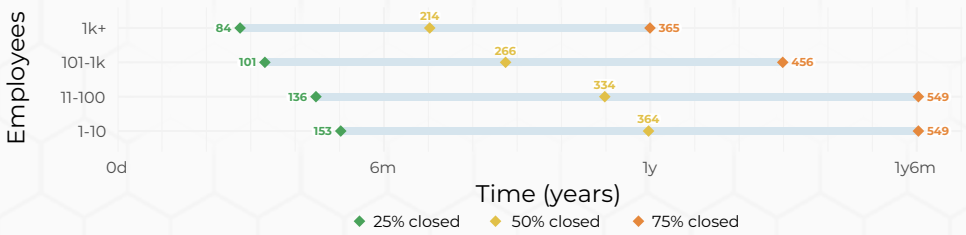


Figure 11: Comparison of remediation velocity by organization size

Another size-related view that we can examine is the total number of vulnerabilities observed for each organization. This doesn't necessarily indicate the size of the firm, but it does relate to the size and scope of exposures across their digital footprint. Figure 12 reveals a huge difference in remediation velocity between organizations with a handful of open vulnerabilities compared to those with hundreds or thousands.

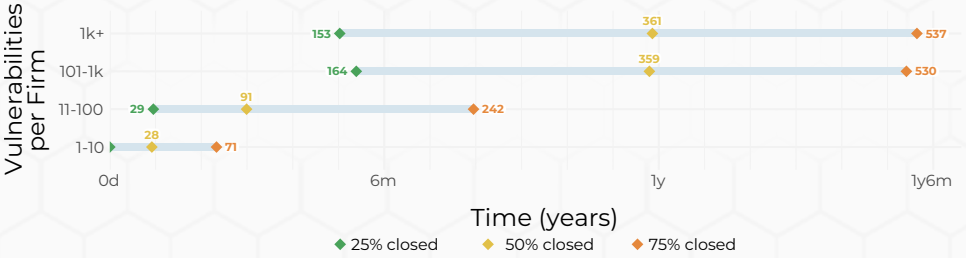


Figure 12: Comparison of remediation velocity by number of open vulnerabilities per firm

When the to-do list includes 10 or fewer issues, it takes about a month to close half of them. When that list grows into the hundreds, it takes a year to reach that same halfway point. The fact that a bigger task list requires more time to work through isn't shocking. But a 13-fold difference in remediation velocity makes a compelling case for including unmitigated vulnerability counts in third-party risk assessments.

Remediation Velocity by Sector

When examining the disparate survival curves in Figure 10, you may have surmised that certain types of organizations would be inherently faster or slower than others. To a certain extent, that would be correct. Figure 13 compares remediation velocity among sectors, and significant differences do exist. The Entertainment industry reaches vulnerability remediation half-life in about 8 months vs. 15 months for Healthcare.

It's important to note, however, that the overlapping intervals indicate there's more variation *within* industries than between them. In other words, there are many individual healthcare institutions that fix vulnerabilities at a faster rate than many entertainment companies. So take these sector-level rates for what they are — generalities.

> *The overlapping intervals indicate there's more variation within industries than between them.*

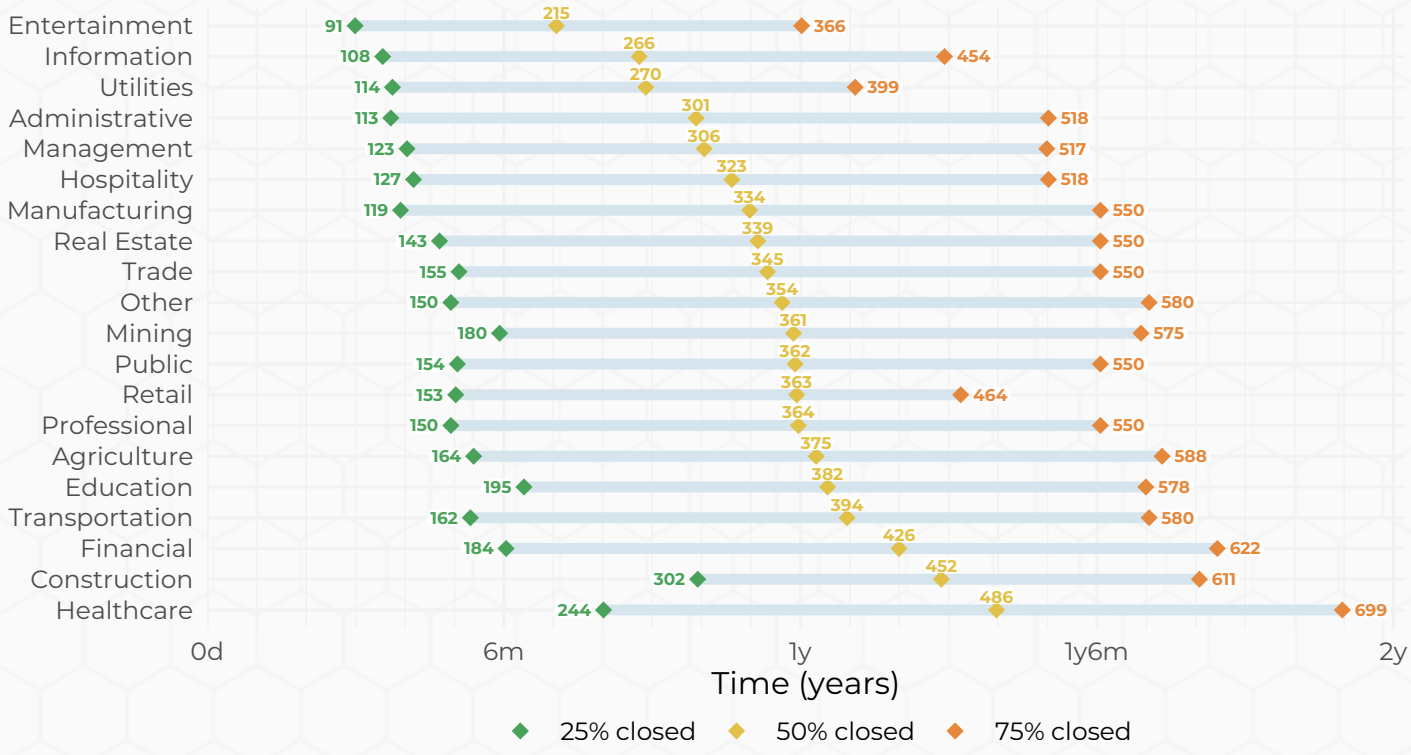


Figure 13: Comparison of remediation velocity among sectors

There are many observations one could draw from Figure 13, but we'll highlight some we found surprising. First and foremost, the Finance sector exhibits the third slowest remediation velocity. Being so accustomed to seeing financial firms on the better end of whatever security dimension we're measuring, this seems almost unbelievable. But that's why having access to insightful data such as this is so valuable; it keeps our assumptions in check and and shapes our understanding.

Figure 14 shows remediation velocity for defined subsectors within the Financial industry. Here we see that banks are quick to remediate, while insurance carriers are much less so. This backs up earlier comments about the high amount of variation within sectors.

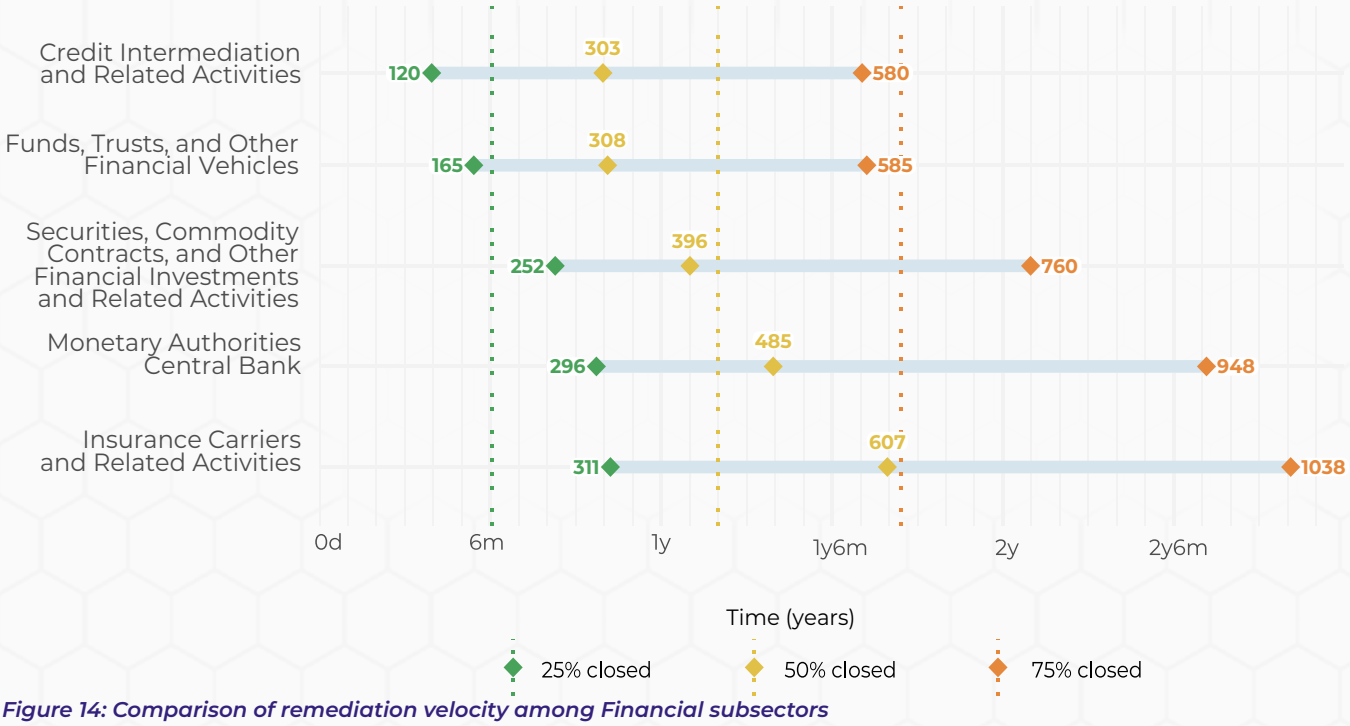


Figure 14: Comparison of remediation velocity among Financial subsectors

Having access to insightful data such as this is so valuable; it keeps our assumptions in check and and shapes our understanding.

Going back to surprises from Figure 13, it's rare, based on analysis of many other security datasets, to see Utilities so high up the rankings. Speed isn't exactly what comes to mind when thinking about the challenges of patching vulnerabilities in operational technologies (OT) and other infrastructure common to that industry. It's good to see that the critical infrastructure sector is staying on top of vulnerability remediation.

Peering into the Utilities subsectors in Figure 15, nuclear power *surges* ahead of the other energy generators for fixing security flaws. It completely *blows away* wind power generation by hitting the halfway mark about a year sooner. Sewage is also slow as you-know-what. In all seriousness, it's not clear exactly why certain types of utilities take longer than others. It likely a lot to do with the age and types of infrastructure inherent to different subsectors, as well as who's responsible for them (i.e., federal vs. municipal entities).

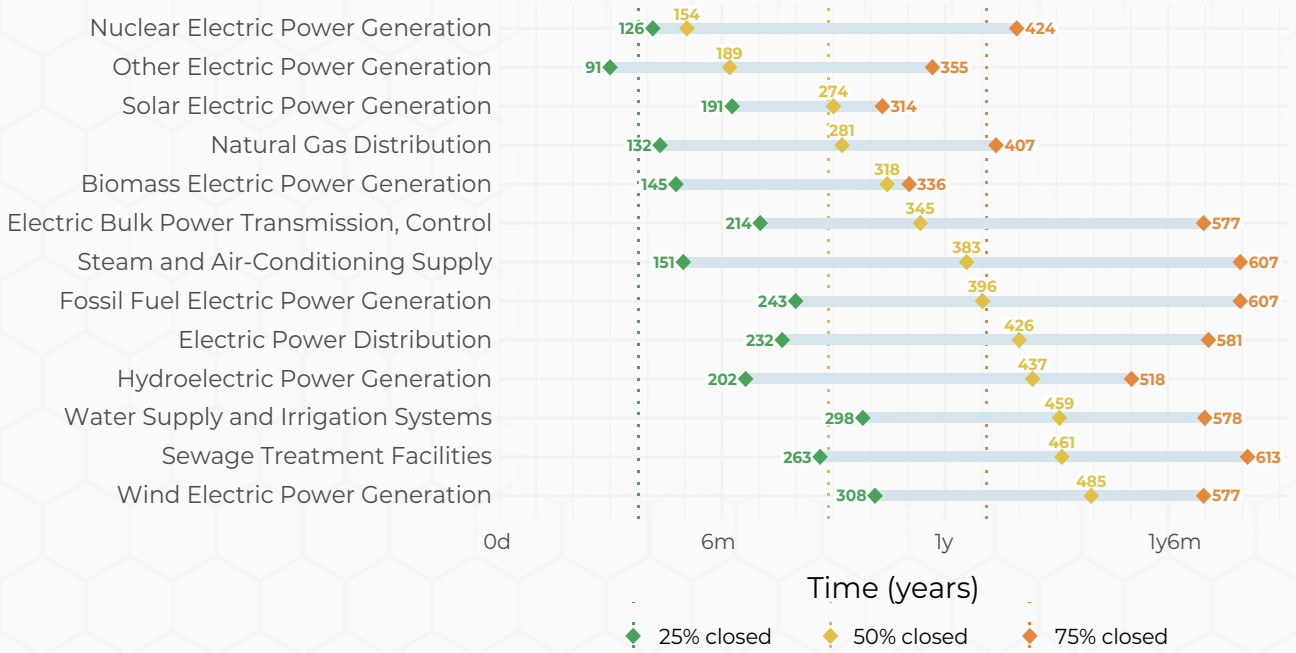


Figure 15: Comparison of remediation velocity among Utilities subsectors

For another example, let's break down the public sector. We see that the EPA is quick. and NASA—despite all its rockets—is slow. Ah well; they won the space race, so we can give them a little slack for overlooking ground-level challenges, like vulnerability management. Perhaps these results will provide some upward momentum to reach for new heights.

NAICS doesn't differentiate the public sector based on federal vs. municipal agencies, but if it did, we'd expect to see major differences. And it may well be that those differences shine through the subsectors shown here. Those toward the bottom with the slowest remediation velocity commonly operate at the state and local level.

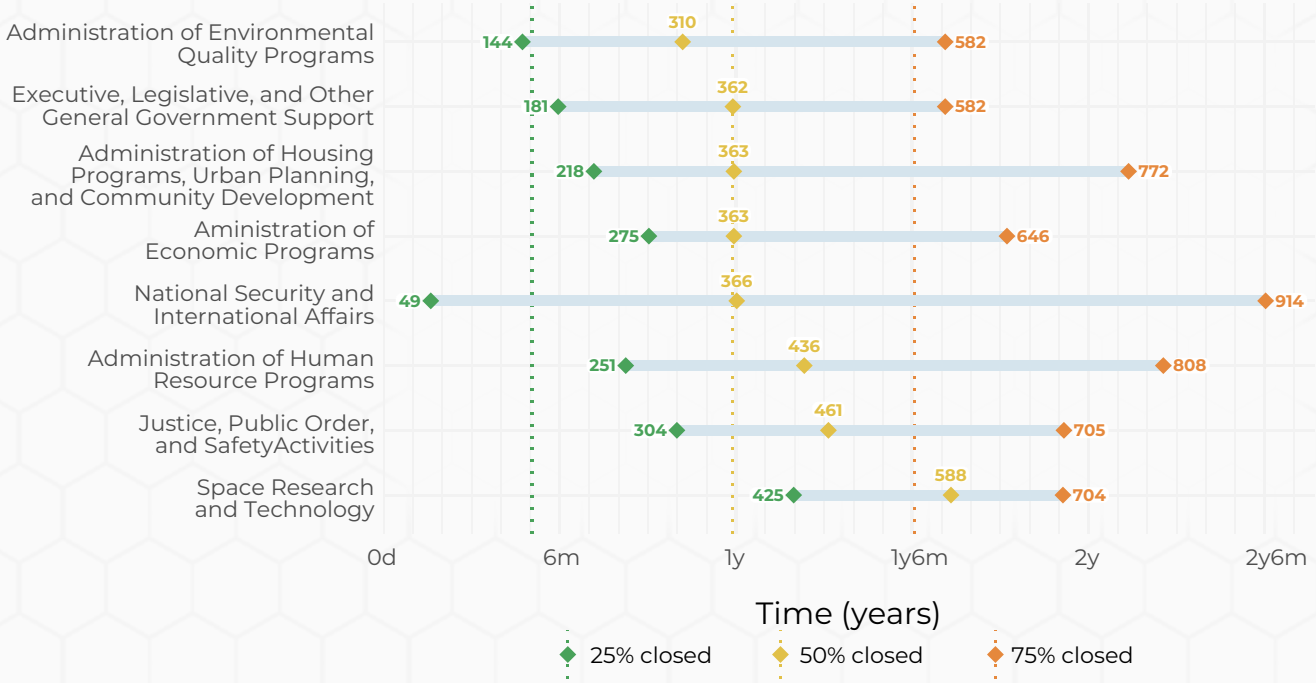


Figure 16: Comparison of remediation velocity among Public subsectors.

The regional comparisons shown likely run counter to prevailing wisdom, with organizations located in Europe and North America posting the slowest pace of remediation.

Remediation Velocity by Region

The regional comparisons shown in Figure 17 likely run counter to prevailing wisdom. Organizations located in Europe and North America post the slowest pace of remediation, with a one-year half-life, while Asia-based organizations clock the fastest times. That result is especially curious since North America has the lowest prevalence of open vulnerabilities (back in Figure 7).

A whole host of factors could be contributing to what we see here. Technologies differ around the globe, as does organizational culture. It's logical that regulatory pressures would play a role too, but we'd expect to see quicker action from traditionally more regulated regions, like Europe, and that's clearly not happening.

It's entirely possible that sample size is the main driver here. Together, Europe and North America claim nearly 80% of all organizations, so we may be seeing a fuller dose of reality in those regions.

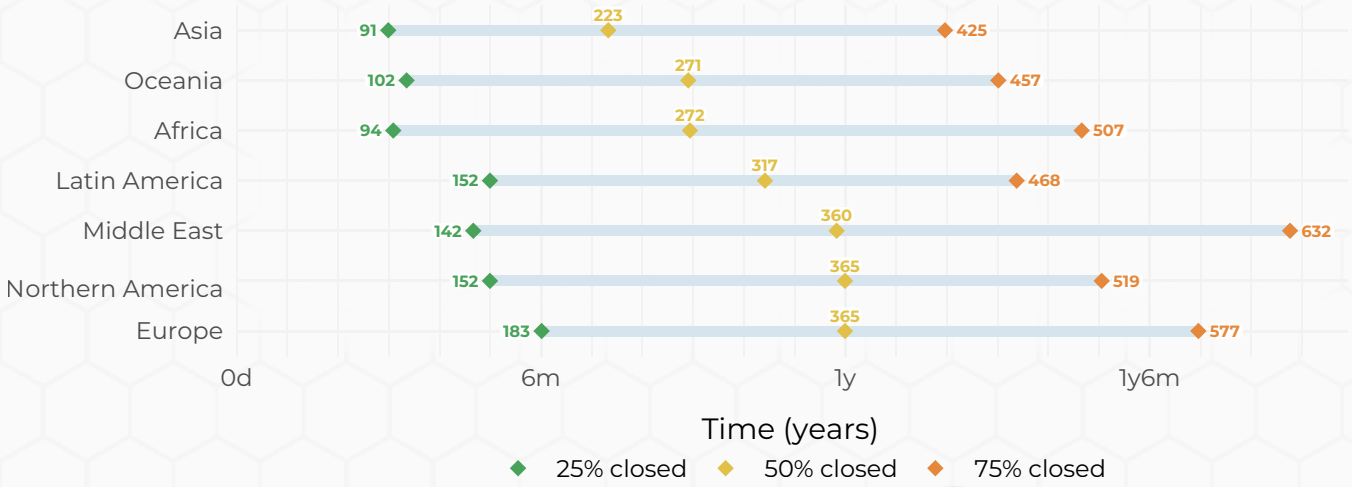


Figure 17: Comparison of remediation velocity among global regions

Remediation Velocity by Vendor

Earlier in this report we broke out software and hardware vendors based on the prevalence of detected vulnerabilities. Figure 18 picks up that thread, this time comparing vendors according to remediation velocity. Turns out the differences among them are quite substantial.

There's more than a six-fold difference between the vendor with the fastest (Dropbear) and slowest (PHP) fix rates. Keep in mind that we're not measuring how quickly vendors release a patch for vulnerabilities (though that may be a contributing factor), but rather how quickly organizations fix them across their domain(s). Certain technologies or assets may be easier to remediate, vary based on criticality or sensitivity, or offer support for automated updates.

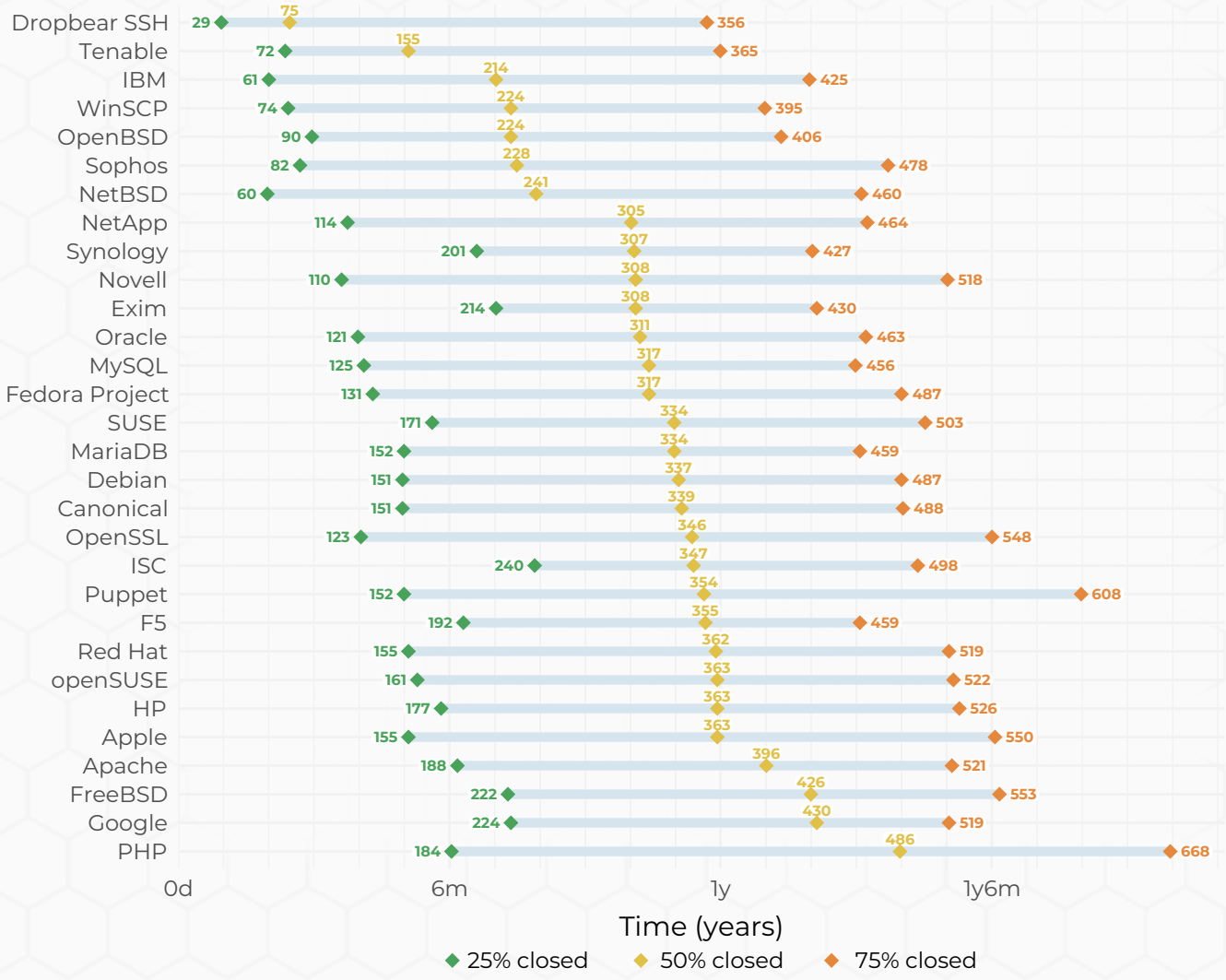


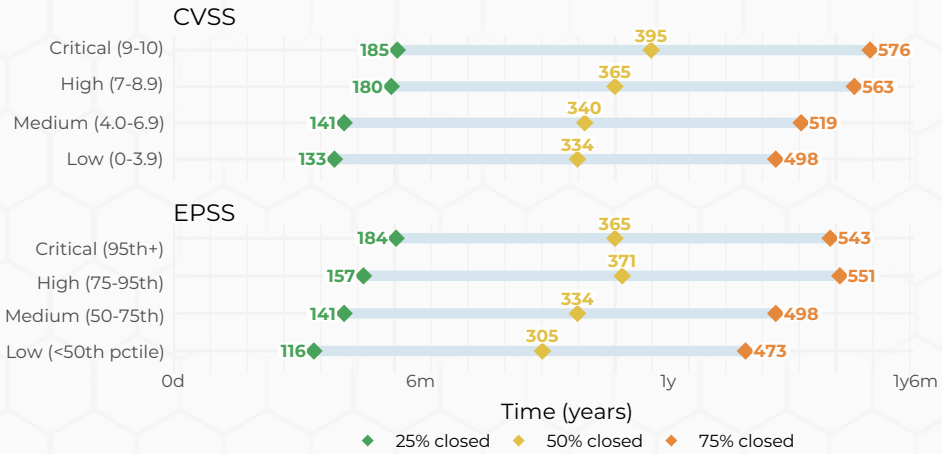
Figure 18: Comparison of remediation velocity among technology vendors

From a risk management perspective, Figure 18 suggests that it may be wise to consider duration of exposure for various web-based technologies. Those that tend toward longer fix times may need to be monitored more closely and/or protected more diligently to minimize exploitation over their remediation lifecycle. These results also broach the topic of vulnerability severity.

Remediation Velocity by Severity

There's been growing attention in recent years on risk-based vulnerability management. The general idea is that it's impossible to remediate all vulnerabilities at all times, so it becomes necessary to focus on the subset that represent the most risk to the organization.

While many use the Common Vulnerability Scoring System (CVSS) to prioritize vulnerabilities for remediation, a growing body of research demonstrates that that's not the most effective strategy. Another prioritization method gaining steam is the Exploit Prediction Scoring System (EPSS). Housed as a special interest group in FIRST.org, EPSS is an open, data-driven effort for estimating the probability that vulnerabilities will be exploited in the wild.



If organizations were prioritizing remediation efforts based on CVSS or EPSS, we'd expect to see faster fix times for vulnerabilities rated as critical. But Figure 19 illustrates that's not happening. There's essentially no meaningful difference in remediation velocity by CVSS or EPSS criticality levels.

Figure 19: Comparison of remediation velocity based on CVSS and EPSS scores

Given that recent research found a 15-fold increase in exploitation activity for vulnerabilities when exploit code is available, [1]another prioritization approach that is gaining steam is to focus on vulnerabilities with exploit code or kits available. Unfortunately, we see no evidence that organizations fix these vulnerabilities faster.

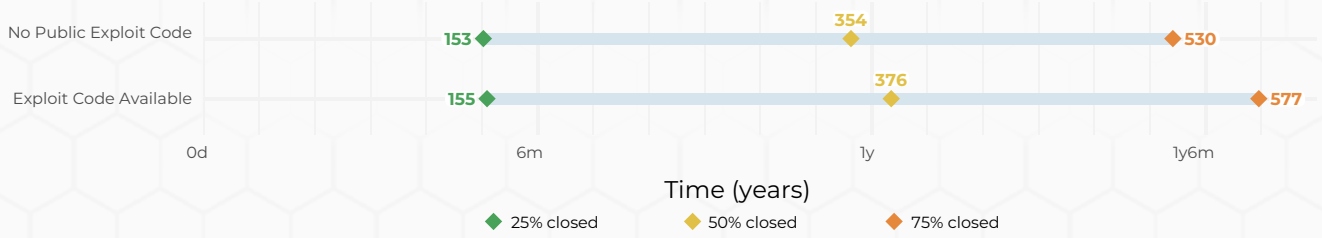


Figure 20: Comparison of remediation velocity for vulnerabilities with/without exploit code

It's clear that many organizations aren't taking a risk-based approach to managing exposure across their web-facing assets, and that can't be a good thing for the health of the digital ecosystem. From a third party risk management perspective, one could make a strong case for this as a major differentiator when assessing organizations.

One thing that might change this state of affairs is emerging regulations such as the Binding Operational Directive 22-01 from the Cybersecurity and Infrastructure Security Agency (CISA). The directive requires federal agencies to remediate a list of known exploited vulnerabilities within timeframes that are far more aggressive than what appears to be the norm from Figure 20.

[1] Cyentia Institute and Kenna Security. Prioritization to Prediction, Volume 7: Establishing Defender Advantage. Available at https://website.kennasecurity.com/wp-content/uploads/2021/05/Prioritization-to-Prediction-Volume-7-Establishing-Defender-Advantage.pdf

Remediation Capacity

Remediation velocity is certainly a key performance indicator for vulnerability management programs, but it doesn't quite get at the all-important question of "Is it enough?" Answering that question requires an understanding of what constitutes "enough," as well as how that's to be measured.

As a step toward that goal, we'll close this report by briefly examining the concept of remediation capacity. Remediation capacity measures the ratio of open vs. closed vulnerabilities in a given timeframe. Below capacity indicates that organizations can't keep up with newly discovered vulnerabilities over time. Above capacity means the program is generally able to close enough vulnerabilities to offset the new ones.

The left side of Figure 21 plots all 1.6 million organizations in our sample, based on the average number of observed vulnerabilities across their domain(s) each month, and the average number of those vulnerabilities that are closed each month. The result is, quite frankly, astounding. Regardless of how many total vulnerabilities exist across their domain(s), organizations typically fix about 10% of them each month. What's more, we've done similar analysis on a different dataset and found the same ~10% ratio for remediation capacity.

Of course, not every firm fixes exactly 10% of their vulnerabilities. That's why we see dots above and below the line. The chart on the bottom in Figure 21 depicts that variation, marking the 25th (7.7%), median (10%), and 75th (12.4%) percentiles for remediation capacity. This points to a ceiling on remediation capacity, and reinforces the points made earlier about the all-important need to prioritize vulnerabilities that represent the most risk.

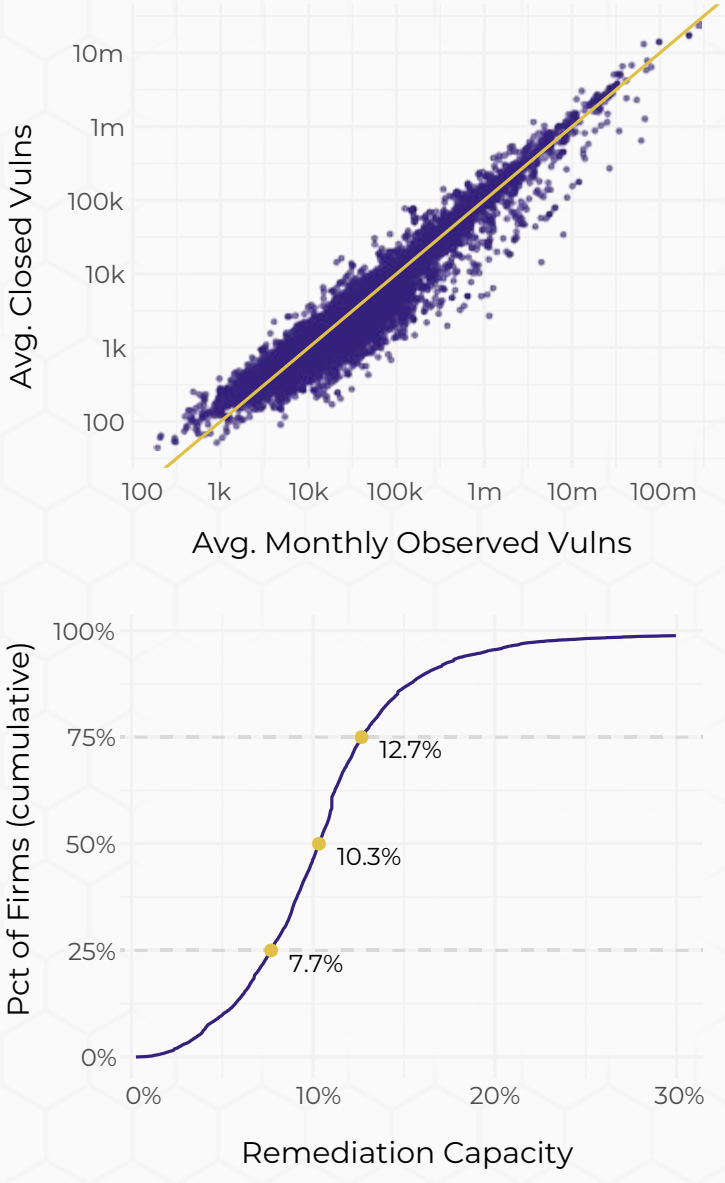


Figure 21 (right): Overall vulnerability remediation capacity across all organizations

Remediation Capacity

Measures the ratio of open vs. closed vulnerabilities over time.

Below capacity indicates that organizations can't keep up with newly discovered vulnerabilities over time.

Above capacity means the program is generally able to close enough vulnerabilities to offset the new ones.

Is It Enough?

So, we've established some limits on remediation capacity, but we still haven't addressed the "Is it enough?" question. One final chart will start us down that path, and we'll leave it to future research to continue the journey to its conclusion.

To create Figure 22, we measured the percent change in the number of open vulnerabilities each month for each firm. Taken together, these monthly measures reveal whether security exposures are piling up or trending down.

We were pleasantly surprised to learn that about 60% of organizations are driving down vulnerabilities across their external assets over time (and some at a pretty good clip!).

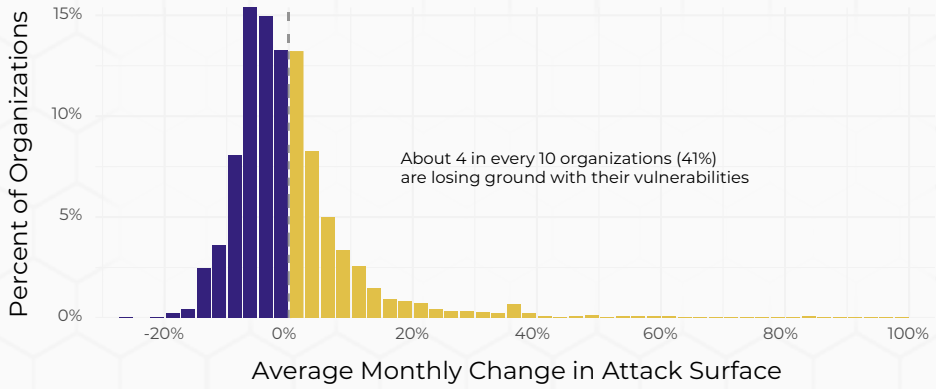


Figure 22: Organizations gaining vs. losing ground in vulnerability remediation over time

THE KEY TAKEAWAY FROM ALL OF THIS

Even though the velocity or capacity of vulnerability remediation might not be impressive in its own right, the majority of organizations still manage to reduce overall exposure over time. Thus, the challenge for third-party risk managers is to reliably identify which organizations across their portfolio are winning the race against vulnerabilities and which ones are losing it.

We hope this analysis helps you find the winners and avoid (or assist) the losers.

READY. SET. GO!

Conclusion & Recommendations

In this report, we've looked in some detail at vulnerabilities and patterns of remediation. There were some surprising bumps in the road; we found:

- Unexpected industry patterns
- Striking differences in remediation where we expected there to be little difference
- Smaller differences where we expected large differences.

The Fast & Furious movies recommended driving as fast as possible, and that's generally been the advice for remediating issues. But real life isn't a Hollywood movie, it's plain that firms are not remediating in top gear.

Although companies may feel the need for speed, the reality is not every vulnerability needs to be remediated, in fact companies may not have resources to do so - there are speed limits in place.

The results in this report show remediation is an issue for organizations of all sizes - no one has the resources to break records. The simplistic advice to focus on the most severe issues plainly isn't helpful, we need something better.

THE CONTINUOUS MONITORING PROVIDED BY SECURITY RATINGS SERVICES GIVES YOU THE ABILITY TO WORK WITH YOUR PARTNERS, PRIORITIZE VULNERABILITY REMEDIATION, AND BUILD A SAFER AND MORE RESILIENT ECOSYSTEM.

Final Reflections from SecurityScorecard

Prioritization is a superpower, and one that will help you focus on the most severe issues. To be scientific about risk management, however, your prioritization needs to be rooted in data that you can trust. SecurityScorecard's robust data collection infrastructure scans over 4.2 billion IPs every 3 days across more than 2,300 ports on each IP address. This allows us to track over 7,000 CVEs and add newly discovered ones within days, providing the most up-to-date and actionable security data that teams need to stay on top of their remediation efforts. Yet, this scanning capability can also potentially create a lot of noise. With over 60 billion security issues discovered by our scanning of all of IPv4 weekly, this volume of data needs to be prioritized to provide teams with the information they need to focus on the most critical vulnerabilities. This is where our ratings system and ability to search our data lake come in. This is how mere risk management evolves into risk intelligence.

Our Scorecards break down an organization's security posture into 10 key groups of risk factors - such as Network Security, DNS Health, Patching Cadence, and Endpoint Security. Within each group, issues are categorized into high, medium, and low severity based on the MITRE ATT&CK Framework, along with recommendations on how to remediate and prioritize issues on a Scorecard. We automatically provide you a path to improve your security posture through our Score Planner, enabling your team to cut through the noise and clearly prioritize with the confidence that comes with data-driven decision making. We also calibrate our scoring weights and measures every month in order to fine tune the risk calculations based on breach events and implied breaches published in disclosure notifications.

If you want even more detailed observations of risk, our Attack Surface Intelligence gives you the ability to search SecurityScorecard's rich data lake by domain name, IP address, IP range, CIDR Notation, CVE and malware hashes. Go beyond what you see on your and your vendors' Scorecards to uncover blindspots, react with focus through prioritization, and unite stakeholders to address on the most severe vulnerabilities.

But, we all know that security is a team sport and your organization's vendors and service providers, such as your third and fourth parties, are key team players that you rely on every day. Continuously monitoring your third and fourth party risk enables you to not only gain visibility into pressing security issues but also invite them to collaborate and remediate known issues on their Scorecard. Your security posture is never just your security posture. It's a combination of yours, your vendors, and their vendors that make up your entire ecosystem. The continuous monitoring provided by security ratings services gives you the ability to work with your partners, prioritize vulnerability remediation, and build a safer and more resilient ecosystem. We are not just protecting our businesses, we're also protecting our identities and our global economy when we each do a better job of managing cyber security risk.

SecurityScorecard

Funded by world-class investors including Evolution Equity Partners, Silver Lake Waterman, Sequoia Capital, GV, Riverwood Capital, and others, SecurityScorecard is the global leader in cybersecurity ratings with more than 12 million companies continuously rated. Founded in 2013 by security and risk experts Dr. Aleksandr Yampolskiy and Sam Kassoumeh, SecurityScorecard's patented rating technology is used by over 30,000 organizations for enterprise risk management, third-party risk management, board reporting, due diligence, cyber insurance underwriting, and regulatory oversight. SecurityScorecard is the first cybersecurity ratings company to offer digital forensics and incident response services, providing a 360-degree approach to security prevention and response for its worldwide customer and partner base.

SecurityScorecard continues to make the world a safer place by transforming the way companies understand, improve and communicate cybersecurity risk to their boards, employees and vendors. Every organization has the universal right to their trusted and transparent Instant SecurityScorecard rating. For more information, visit securityscorecard.com or connect with us on LinkedIn.

Gain continuous visibility into your digital footprint, vulnerabilities, and clear steps to remediate them with SecurityScorecard. Claim your free account now and take control of your cybersecurity risk.

Cyentia Institute

The Cyentia Institute is a research and data science firm working to advance cybersecurity knowledge and practice. Cyentia pursues this goal through data-driven research publications like this one and through a growing portfolio of analytic services. Learn more at www.cyentia.com.