CLOUD RISK SURFACE REPORT

Navigating safely in cloudy conditions

A collaborative research project between RiskRecon and the Cyentia Institute

riskrecon™

119 Cyentia INSTITUTE

This research was commissioned by RiskRecon.

RiskRecon collected the dataset and provided it to the Cyentia Institute for independent analysis and drafting of this report.

Table of Contents

DATA COLLECTION This report (re)uses the same data set behind the Internet Risk Surface Report. It is derived from RiskRecon's work in providing companies objective visibility into their third-party cybersecurity risk. For each organization analyzed, RiskRecon trains machine learning algorithms to discover internet facing systems, domains, and networks. For every asset discovered, RiskRecon analyzes the publicly accessible content, code, and configurations to assess system security and the inherent risk value of the system based on attributes such as observable data types collected and transaction capabilities. RiskRecon provided Cyentia a large anonymized sample of their production data set for this research. It contains sanitized information on 18,000 organizations and more than 5 million hosts located in 200+ countries. Across those hosts, RiskRecon identified over 32 million security findings of varying severity.

INTRODUCTION

An Important Question

"Are we safer on-prem or in the cloud?"

Who hasn't asked this question? And with good reason—all organizations want to ensure that their data and applications remain secure, even when outside their direct control. Business partners want to know if they're placing too much trust in any weak 3rd and 4th party links across the value chain, and the Insurance community needs to understand the potential points of systemic risk within their portfolio.

The question is only becoming more critical with time. According to Deloitte's Chief Cloud Strategy Officer, "[2019] is the year when workloads on cloud-based systems surpass 25 percent, and when most enterprises are likely to hit the tipping point in terms of dealing with the resulting complexity."

RiskRecon and the Cyentia Institute published the Internet Risk Surface Report in April, 2019. The goal of that exploratory research was to map and measure key risk factors associated with this growing complexity of the modern organization's digital footprint. Among the many lessons from that research, we discovered the rate of severe security findings in high-value assets hosted externally is 3X that of on-prem systems.

Having studied several broad aspects of the Internet risk surface, we now seek to narrow the focus to consider how the cloud shapes that surface. The benefits of migrating data, workloads, applications, and business processes to the cloud are incredibly compelling. But as a steady string of headlines reporting large data exposures from cloud environments suggest, those benefits don't come risk-free. Is the risk worth it? To help you answer that for your organization, we leverage a massive dataset supplied by RiskRecon spanning 18,000 organizations and over 5 million hosts yielding 32 million security findings. Read on for a preview of the fascinating facts and figures we share in this report.

[1] https://www2.deloitte.com/us/en/pages/consulting/articles/cloud-complexity-management-a-new-year-a-new-problem.html

75%

The top 5 clouds host assets from 75% of firms

2X

Firms are twice as likely to have high-risk exposures in the cloud vs. on-prem

12X

Average difference between clouds with highest vs. lowest exposure rates

Key Findings

1. Cloud consolidation is a thing; the top 5 clouds alone host assets from 75% of organizations.
2. Heavy consolidation may impact security; the rate of severe findings are highest when cloud diversity is lowest. Firms with 4 clouds exhibit one-quarter the exposure rate of those with just one cloud provider. Having 8 clouds drops that rate in half again.
3. Overall, organizations are over twice as likely to have high or critical exposures in high-value assets hosted in the cloud vs. on-prem. BUT clouds with the lowest exposure rates do twice as well as on-prem.
4. Some industries appear less cloud-ready than others; the prevalence of cloud-based exposures in the Healthcare sector jumps 4X to 5X compared to on-prem.
5. Size matters; Midsize firms appear a bit better off in the cloud, but larger enterprises tend to manage their internal hosts better.
6. Fresh Prince's mom was **wrong**—you DO have a rep yet. From the perspective of threat intel, hosts on your own network may have a worse reputation than your cloud provider.
7. Smokey the Bear was **right**—only you can prevent cloud fires. Even though we discovered an average 12X difference between clouds with highest and lowest exposure rates, this says more about users than providers. Security in the cloud isn't on the cloud; it's on you.

RECAP: THE INTERNET RISK SURFACE REPORT

1. An organization's internet surface area is larger and more complex than you might think. Most firms host assets across multiple countries and 3rd/4th party infrastructures.

2. Organizations place a huge amount of trust and value in the hands of 3rd parties. 84% of firms host critical assets externally.

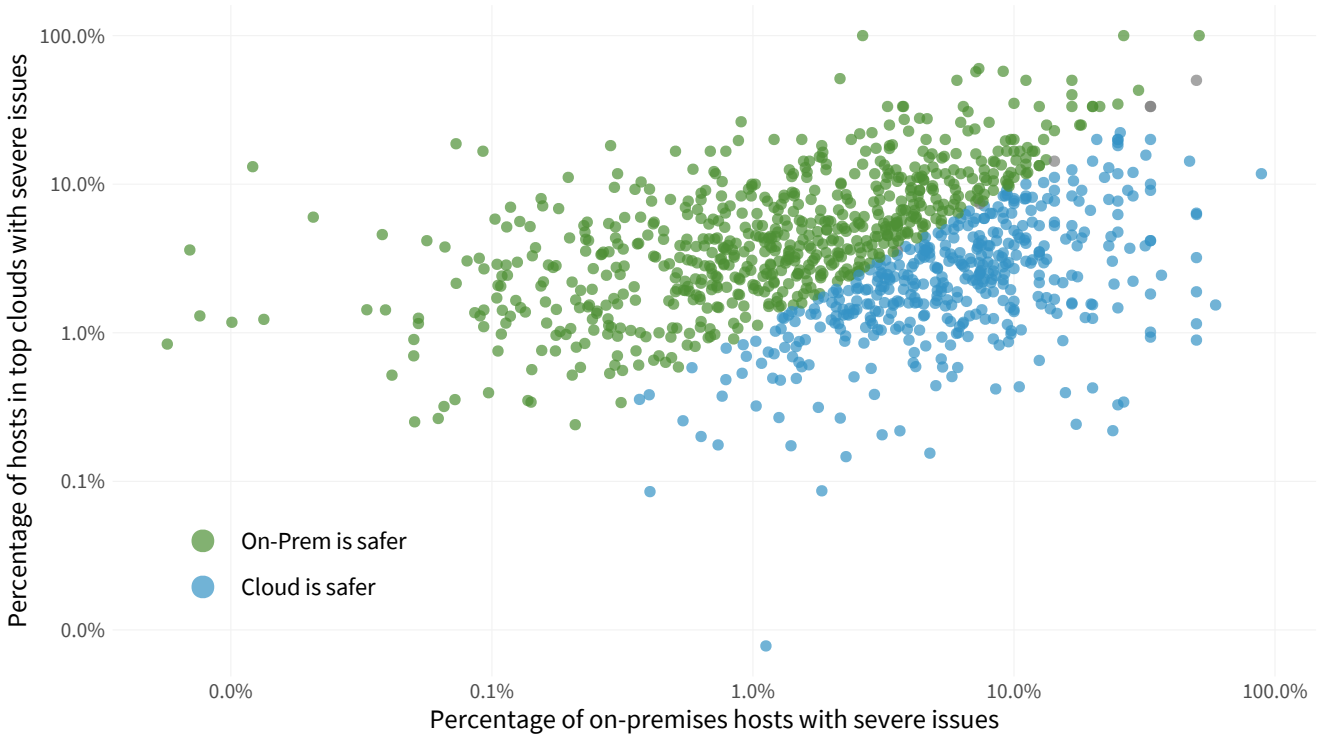
3. Exposures exist in all areas of the internet risk surface, but appear to aggregate in 3rd party networks. 35% of firms have severe security exposures in assets hosted with external service providers.

CHAPTER 1

Bottom Line Up Front

In the interest of getting the bottom line up front, we'll lead with a chart that leaks the answer to the core question guiding this analysis that we asked in the introduction of this report:

Figure 1: Comparison of hosts with severe findings in on-prem vs. cloud environments



Each dot in Figure 1 represents an organizations in our dataset with hosts that have high or critical findings both in the cloud and on-premises. Their position on the grid portrays the percentage of internal (horizontal axis) and cloud-based (vertical axis) hosts that have high or critical security findings. Blue dots indicate firms that have comparatively fewer security issues in the cloud. Green dots, conversely, appear better off on-prem.

You may think this falls short of laying our question to rest in your mind, and it's not just you. It shows a fairly similar split between organizations that operate more safely on-prem (60%) vs. in the cloud (40%). In which group of dots does your organization belong? Well, obviously we can't tell you that. But we can tell you what we learned about those organizations represented in Figure 1 and the factors that drive them to one side of the line or the other. Before we do, let's back up and start with the basics.

CHAPTER 2

Cloud Adoption Trends

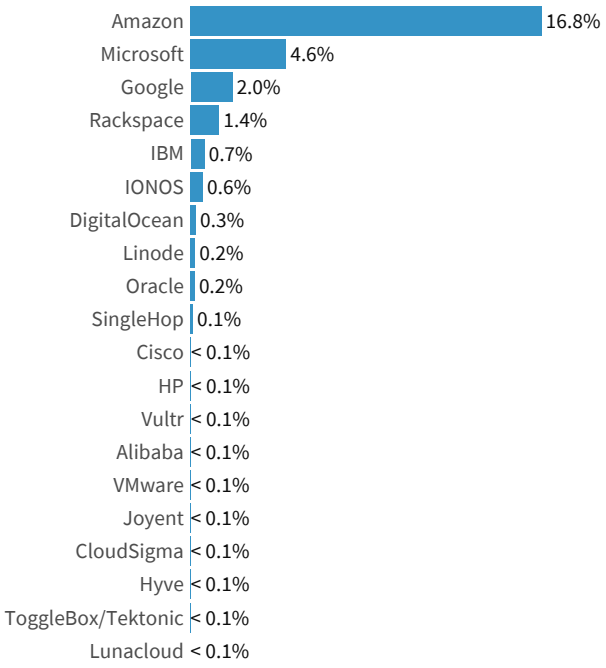
Top Cloud Providers

Readers of the Internet Risk Surface Report may recall a chart listing the top external service providers. That chart included a mix of cloud providers, content delivery networks, DNS, telecommunications services, etc. To narrow the focus on cloud services, we compiled a list of the top 20 cloud providers specializing in various 'aaS's using several external lists and cross-referencing those with our dataset. Figure 2 is the result of those efforts.

Taken together, the cloud providers listed in Figure 2 host nearly 30% of assets in our dataset and 77% of organizations use these clouds! Clearly, there's something to this cloud trend we keep hearing about. It's also clear that market share drops pretty quickly as you move down the list; none of the bottom 10 clouds account for more than 0.1% of hosts. In fact, the stats shared above barely change if we reduce scope to just the top 5 cloud providers (i.e., it's still ~17% of assets and 75% of organizations).

But Figure 3 on the next page proves that the reign of these top providers does not extend equally around the globe. Amazon retains the crown in all regions but two, and other leaders shuffle around somewhat after that. Even though Figure 3 omits minor clouds that may punch above their weight in a certain country, the overall point remains. Cloud availability and adoption varies regionally, and this is something global enterprises must consider, especially when partnering with vendors outside your current locale.

Figure 2: Top 20 cloud providers by percentage of hosts

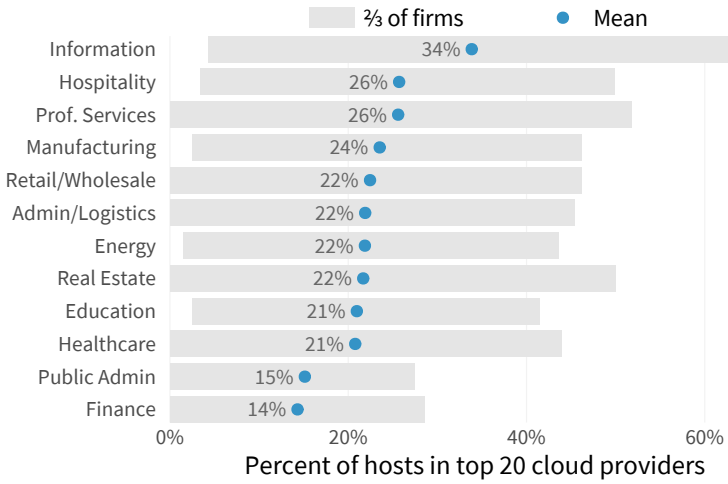


We identified the clouds in Figure 2 using several external lists cross-referenced with our dataset. You'll notice a lot of the charts in this report use "top X" cloud providers. Refer back here if you need a refresher on which clouds that includes.

Figure 3: Comparison of top cloud providers among organizations by region.

Cloud adoption rates for industries are compared in Figure 4, and it seems fitting that the Information sector leads the pack. After all, the cloud providers themselves fall under that designation according to NAICS. It also meets expectations that Finance and Public Administration bring up the rear. Those sectors have heavy existing investments in internal infrastructure and historically have a lower risk tolerance for moving it to the cloud. As we will demonstrate later, evidence is mixed as to whether such reticence is founded on the basis of security exposures.

Figure 4: Cloud adoption rates by industry



Figures 4 and 5 share a similar format. The blue dot marks the mean and the gray bars encompass the middle 2/3rds of firms in each segment. We do this to give a sense of what's "typical" (the mean) for the organizations represented as well as the amount of variation (gray bars) among them.

Figure 4 is a great example of where this is helpful. The mean adoption rate for the Information sector is high, but the gray bar is unusually wide too. This indicates many companies in that sector vary substantially from the mean. Cloud usage among financial firms, on the other hand, varies much less.

2X

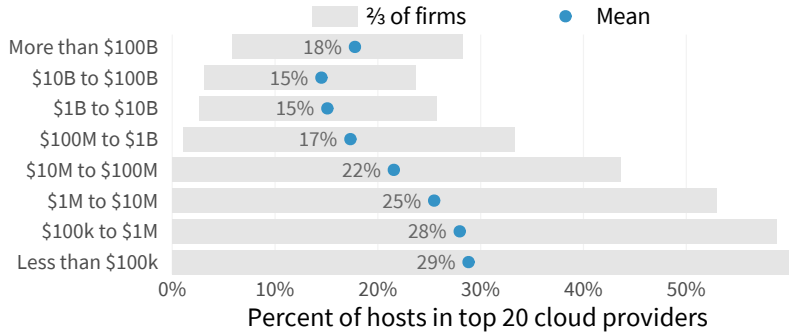
Cloud adoption in SMBs roughly doubles larger enterprises

70%

of firms rely on 4 or fewer cloud providers

Cloud usage by organization size (measured here in annual revenue) is quite fascinating. Figure 5 clearly portrays heavy adoption by smaller firms, which lessens steadily with growth. The story here is one we're well familiar with: SMBs place a high priority on reducing cost, maintaining flexibility, and focusing on their core business, and moving to the cloud serves those needs well. As organizations grow, their goals and requirements change, often triggering a desire to keep/bring assets on-prem. Note, however, the wide variation within each revenue range, especially among smaller companies. Those grey bars remind us that the mean doesn't represent every organization.

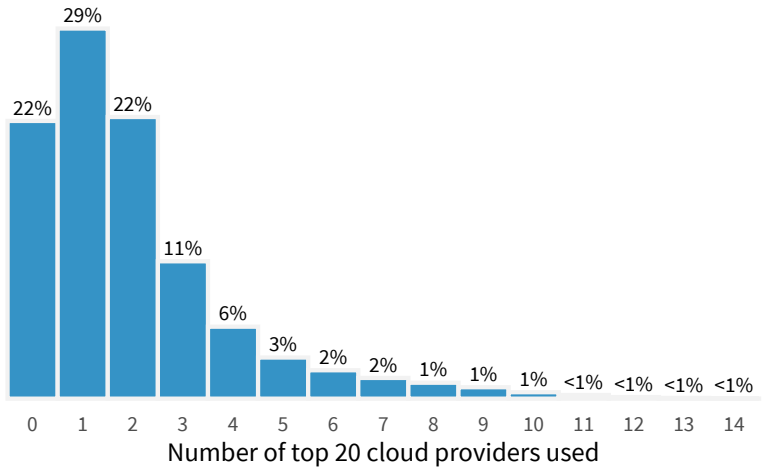
Figure 5: Cloud adoption rates by annual revenue



Aggregation in the Cloud

The previous section established extensive cloud adoption but didn't quite convey whether organizations consolidate into a few providers or diversify across many. There are some exceptions to the rule, but the general pattern revealed in Figure 6 tends toward consolidation. A full 70% of firms rely on 4 or fewer major cloud providers.

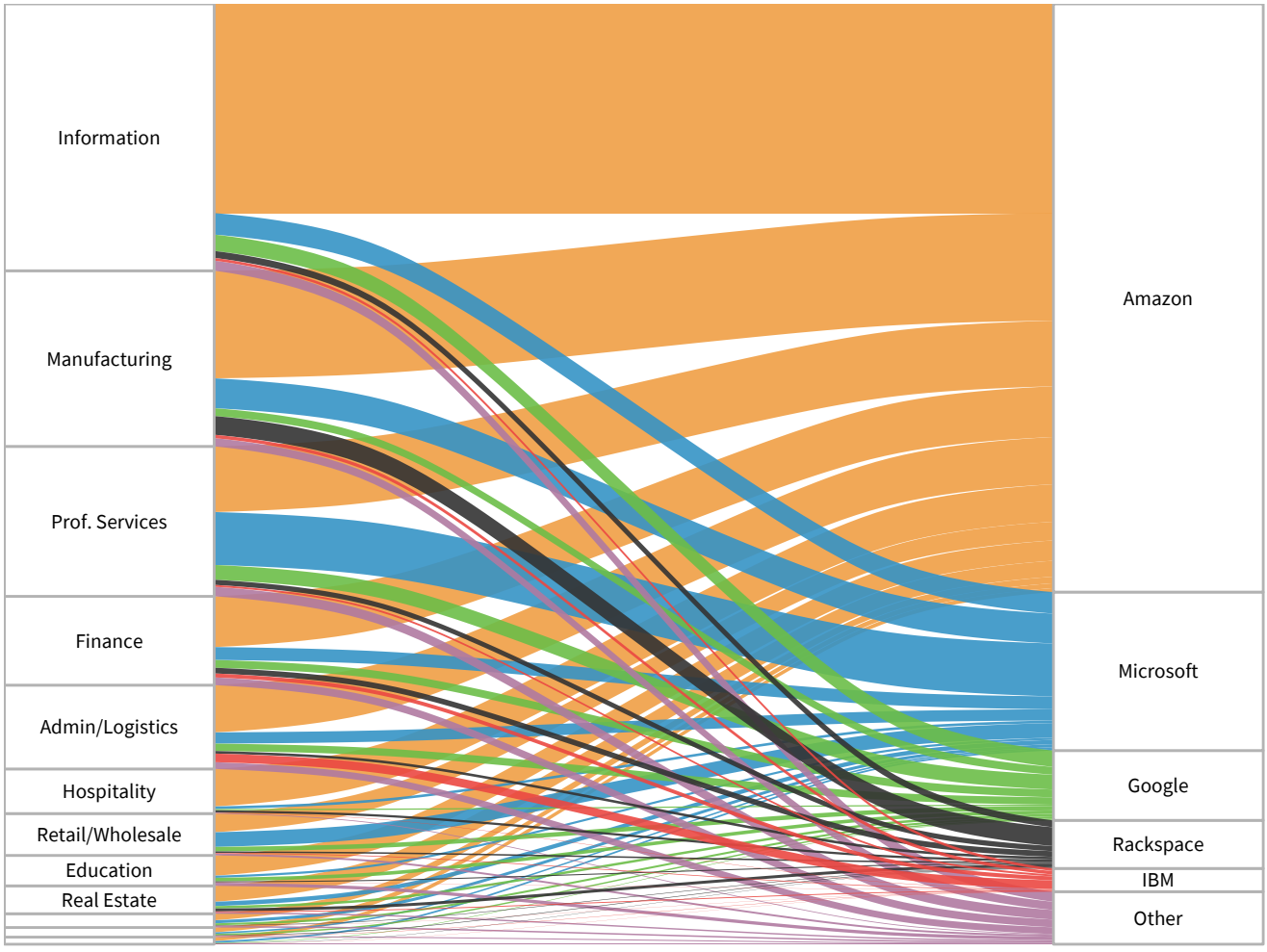
Figure 6: Distribution for the number of cloud providers per organization



We're likely seeing the result of organizations asking something akin to this question: "Do we streamline our infrastructure by putting all our hosts in one cloud basket or do we expend extra resources maintaining different features, frameworks, and APIs to better diversify across multiple providers?" As Figure 6 attests, organizations arrive at different answers to that question, but few appear to pursue maximum cloud diversity.

Figure 7 offers another illustration of this consolidation trend, tracing all cloud-based hosts to their respective providers. Since market share drops quickly after the top 5 cloud (see Figure 2), we collapsed all of those into the "Other" category). In it we see heavy aggregation into Amazon Web Services across all industries. But we also find some interesting differences. For instance, Professional Services appear to have a soft spot for Microsoft, Rackspace racks up hosts from the Manufacturing sector, and Admin/Logistics navigate to IBM (see what we did there?).

Figure 7: Distributions of hosts among top cloud providers by industry



If you suspect the cloud aggregation conveyed by the previous figures suggests a massive transfer of trust and value to cloud providers, you would be correct. Figure 8 reveals the value allocation across millions of cloud-hosted assets owned by the organizations in our dataset.

Asset values depicted here are assessed and assigned by RiskRecon. In general, high-value assets collect sensitive data, authenticate users, run critical services, etc. Hosts assigned a medium value don't perform such functions, but are network neighbors to those that do, making them ideal pivot points into higher-security environments. Static assets that aren't connected to higher-value systems fall in the low range.

It's clear from the figure that any lingering notions that only lower-value assets belong in the cloud are antiquated. A full 80% of firms have high-value assets hosted externally, and 42% use one of the top 5 cloud providers from Figure 8. Also clear is that the value of assets across these clouds is not evenly distributed. Amazon appears to have the majority of high-value assets, Microsoft and Rackspace lean heavy in the medium category, and low-value assets gobble up much of Google's share. Between Figures 7 and 8, a rather startling picture of risk aggregation across industries and assets in the cloud begins to emerge.

Figure 8: Distribution of hosts among top cloud providers based on asset value ratings

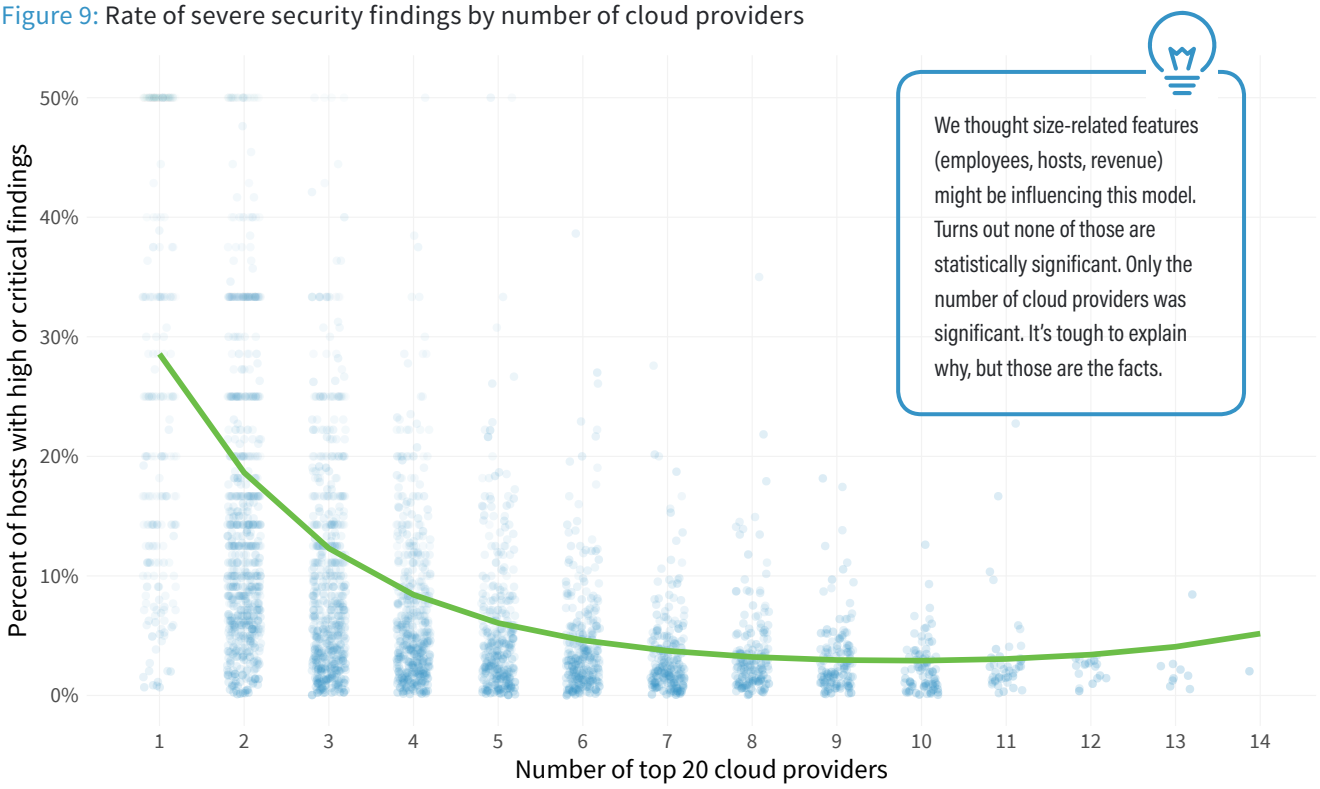
Consolidate or Diversify?

But does any of this matter? Does cloud adoption and/or consolidation negatively or positively impact the risk surface of an organization? Intuitively, it seems economic forces are conspiring to aggregate risk within a few cloud providers (heaven help us if AWS has a terrible, horrible, no good, very bad day[3]). On the other hand, internal networks aren't always the bastions of security we like to think they are; perhaps moving hosts out of that environment is a net positive.

[3] Essential reading for all risk managers and their kids: https://en.wikipedia.org/wiki/Alexander_and_the_Terrible,_Horrible,_No_Good,_Very_Bad_Day.

Being data people, we're not very comfortable with the "intuitively" and "perhaps" language used here. Let's see if we make that more concrete by adding a dimension of security findings to this analysis. Figure 9 tests the effect of provider diversification on the prevalence of findings among cloud-based hosts. The dots mark where various organizations in our sample stand with respect to those two measures and the line fits a regression model to the data to better visualize the overall trend.

Figure 9: Rate of severe security findings by number of cloud providers



That trendline in Figure 9 turns out to be quite interesting. It suggests that the rate of severe findings is at its highest when cloud diversity is at its lowest. As organizations use more cloud providers, that rate drops steadily...to a certain point. Firms with 4 clouds exhibit one-quarter the exposure rate of those with just one cloud provider. Having 8 clouds drops that rate in half again. Beyond that, security issues level off and even begin to rise among hyper-diversified cloud users. We can't help but see a kind of "Goldilocks Zone" here: there's a point where consolidation and diversification are "just right" for life in the cloud, and that point varies from firm to firm.

One bit of caution here. Keep in mind that all kinds of factors are at play here that we cannot consider in our analysis (yet). For instance, perhaps many of the firms with only one cloud provider are simply experimenting. This may reflect various stages of cloud maturity from left to right rather than the effects of consolidation vs. diversification. One hypothesis we find no evidence for is that size-related features (employees, hosts, revenue) affect what we see in Figure 9. We included them in our analysis, but the number of cloud providers was the only significant variable. Whatever the reasons, these results are noteworthy and we look forward to investigating this more fully in later research.

CHAPTER 3

Seeking Clarity on some Cloudy Questions

Are We Safer On-Prem or in the Cloud?

We're now ready to return to this central question that led off our analysis. From Figure 1, we already know there's a 60/40 split overall between organizations that operate more safely on-prem vs. in the cloud. Let's add more variables into that equation.

Figure 10 features 4 of the 5 key measures we presented in the Internet Risk Surface Report: proportion of hosts (square size), asset value (columns), hosting location (rows), and the rate of severe security findings (color scale). This view facilitates a range of comparisons, including the relative proportion of assets hosted on-prem vs. in the cloud, how asset value distributes across hosting locales, and where high-severity issues accumulate. Let's unpack it.

Figure 10: View combining several risk surface measures for an organization

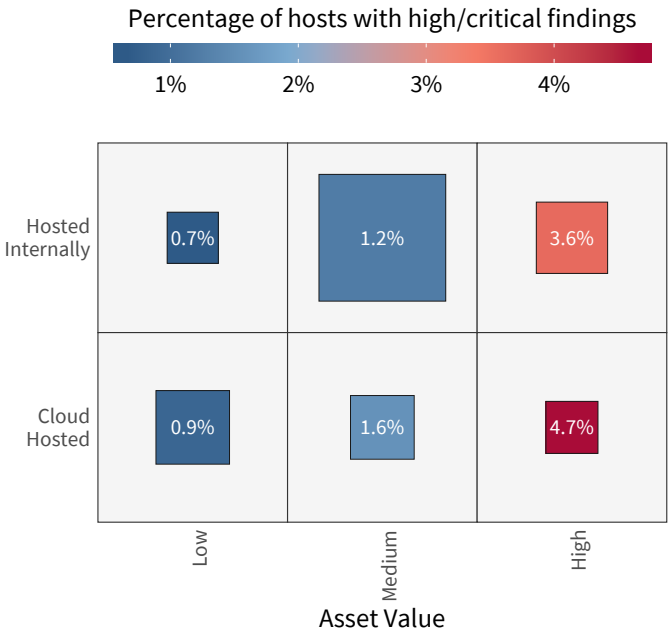


Figure 9 features 4 key risk surface measures: number of hosts (square size), asset value (columns), hosting location (rows), and the rate of severe security findings (color scale). So, the largest number of hosts are on-prem and of medium value. But high-value assets in the cloud exhibit the highest rate of findings.

In general, Figure 10 depicts high-value assets as having a higher rate of severe security findings, regardless of whether they're hosted on-prem or in the cloud. This admittedly has a lot to do with the valuation algorithm; more functionality means more complex software which leads to more potential issues. With respect to the internal vs. cloud distinction, cloud-based hosts appear somewhat more prone to severe findings in high-value assets (4.7% vs. 3.6% for internal hosts). Overall, organizations are over twice as likely to have severe findings in **at least one** high-value asset hosted in the cloud vs. on-prem.

Figure 11 proves the outcome differs significantly when comparing across industry and size segments. We're not labeling exposure rates in this chart (or the next one) because a) spacing issues and b) that's not the point. The goal here is to aid general visual comparisons across the segments and dimensions.

Notice how the Hospitality industry hosts the majority of low and medium-value assets in the cloud with few issues and yet their high-value assets appear beset with severe exposures. Educational institutions show almost the opposite trend; they host most assets internally and that's where the worst issues live too. This seems intuitive given the balkanized state of many university networks. Manufacturing and a few other sectors seem to be managing their risk surface relatively consistently regardless of where assets are hosted. We cannot conclusively determine whether these differences reflect sector-specific business models, digital transformation strategies, or security capabilities, but we suspect it's a mix of all these and more.

Figure 11: Comparison of internal and cloud hosting risk factors by industry

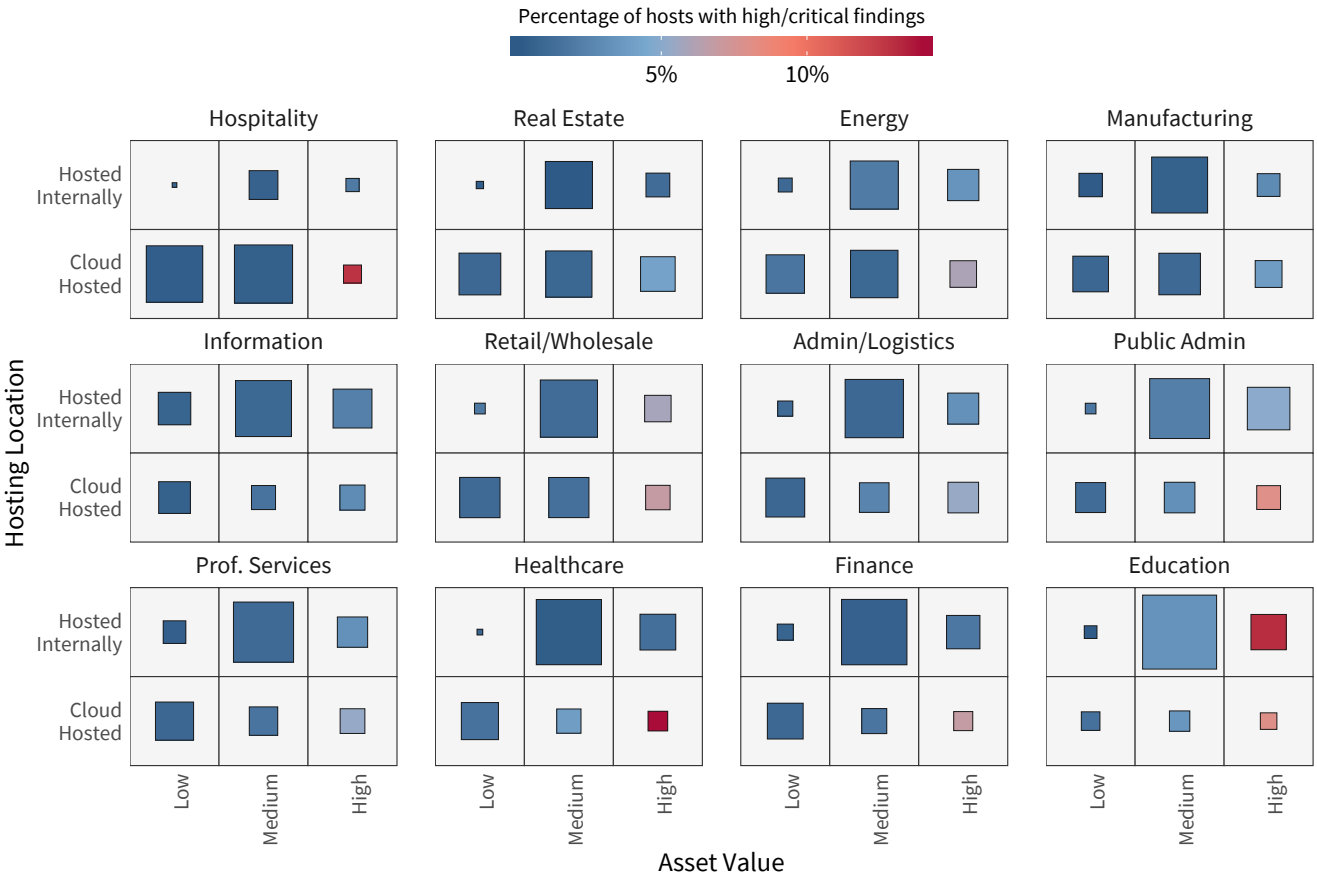


Figure 12 offers a similar view comparing organizational size categories. From our perspective, the most noteworthy finding here concerns the prevalence of severe findings in high-value and cloud-based assets. Both rate quite high among SMBs and comparably less among larger enterprises. When paired with what we learned earlier about heavier cloud adoption among smaller firms, these results stoke concerns about a dangerous concoction of convenience and complacency in the cloud. The (somewhat) good news is this "out of sight, out of mind" tendency appears to lessen (somewhat) with growth and maturity.

Figure 12: Comparison of internal and cloud hosting risk factors by number of employees

The previous figures work well for visual comparisons, but fall short of supplying a statistically valid answer to the question of "where are we safer?" Constructing some statistical models[4] will help us add more rigor to this important question (but be prepared for an answer that's still less than definitive). Figure 13 contrasts exposure rates between on-prem (left side) vs. cloud-based (right side) assets among firms within the industries shown.

Of all sectors, Education is the only one that exhibits lower rates of high or critical findings in the cloud. The jury's still out, however, on whether it's actually "safer" or merely less unsafe than their industry-leading exposure rate among internal hosts. Healthcare is the big mover in the opposite direction. The proportion of cloud-based exposures in that sector jumps 4X to 5X compared to on-prem levels. Finance, Real Estate, and Admin/Logistics each show about 2X more severe findings in the cloud. On-prem vs. cloud looks to be a wash for the Public, Energy, Retail, and Hospitality sectors.

Lest you feel like your destiny in the cloud is merely a function of your industry, we feel compelled to reiterate that variation was very high, even among organizations in the same industry. Your actions undoubtedly have a greater effect on your security in the cloud than your NAICS code.

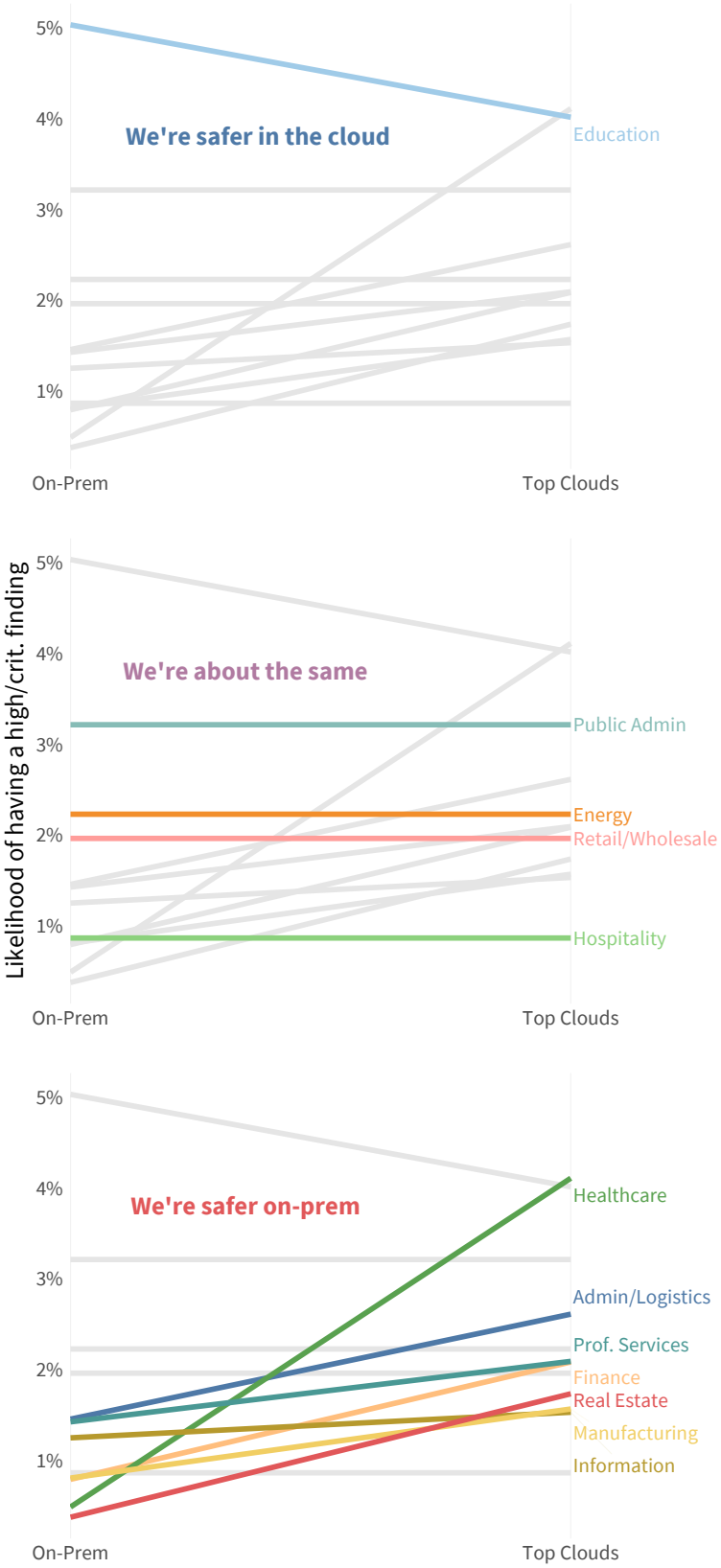
[4] It's easy to see why a firm's exposure rate in the cloud vs. on-prem could be influenced by many interrelated factors. We only care about one factor in Figure 13, and so we can build models for each industry that enable us to ask "all else being equal, do findings differ by industry?" These are also fully 'unpooled' models, meaning each industry gets the freedom to stretch its legs and find its own coefficients. We found this model type to provide the best explanation for the data. Other modeling approaches (random effects models, mixed effect models, partially pooled models, we could go on and on…) are also reasonable, but this approach balances simplicity with explainability. We use a similar approach for Figure 14 (revenue), even though it looks different.

Education is the only sector that exhibits lower rates of severe findings in the cloud

4X

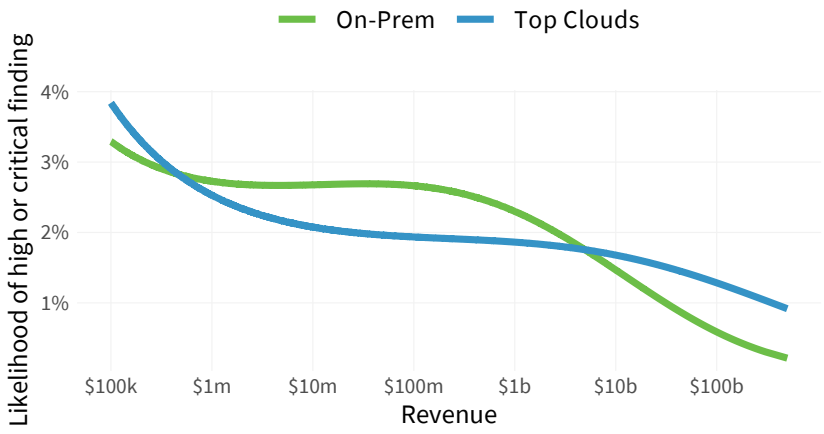
Cloud-based exposures in Heathcare jump 4X to 5X compared to on-prem levels

Figure 13: Models comparing exposure rates on-prem vs. cloud by industry



This presents a good opportunity for us to caution against jumping to conclusions. We could interpret these results to assert that the cloud is inherently unfit for Healthcare applications. But another interpretation could suggest that it's more about fitness for the cloud than fitness of the cloud. Said differently, perhaps certain industries or institutions simply aren't prepared for the paradigm shift of managing security in the cloud. With that in mind, let's create another model that examines this question from the perspective of organization size. Enter Figure 14, which compares the likelihood of exposure in on-prem and cloud hosts by revenue.

Figure 14: Models comparing exposure rates on-prem vs. cloud by organization size (annual revenue)



> First observe the general trend of decreasing likelihood of exposure as revenues grow for both on and off-prem hosts

Let's first observe the general trend of decreasing likelihood of exposure as revenues grow for both on and off-prem hosts. This is consistent with Figure 12 and likely the result of increased resources and maturity. Beyond that, we note some intriguing sub-trends. According to the model, organizations between $1M and ~$5B operate a little more safely in the cloud. The opposite holds true for those outside that range—the really small and the really big.

> Organizations between $1M and ~$5B operate a little more safely in the cloud

What do we do with this information? From Figures 13 and 14, it seems that the answer to our leading question depends on who you ask. Like so many things, what's "better" or "safer" for any given firm often comes down to some kind of SWOT analysis. And we'll be honest and say that we don't (yet) have all the factors collected to conduct that analysis. So, while we don't have the answer to life, the universe, and everything cloud,[5] we hope to have provided some data-driven perspective that helps you continue pursuing those answers.

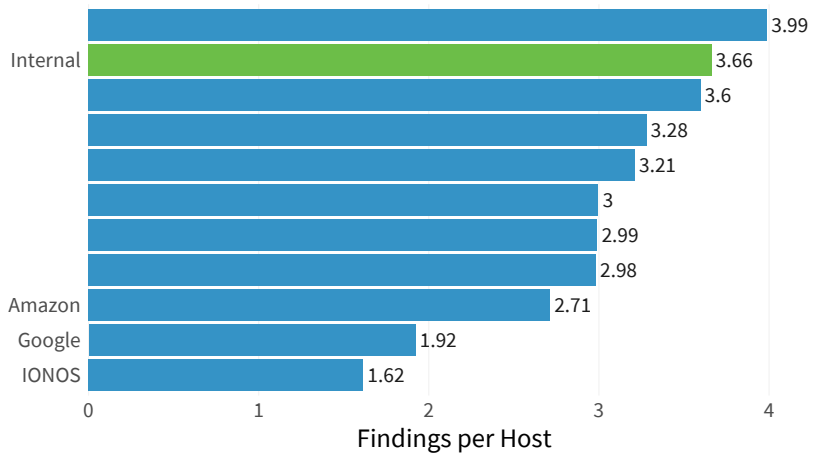
[5] But we're pretty sure it's 42.

Do Security Findings Differ Among Clouds?

We imagine most of you reading this report are already well established in the cloud or somewhere along the migration process. Given the information above, you're probably thinking "then we've got to find a safe port somewhere around here". So in which sector of Cloud City should you aim to Land(o)? We've seen that cloud-based hosts generally have a higher rate of severe findings than those on-prem, but does that rate differ among the major clouds? After all, nobody wants to chance their prized assets to a random hand of sabacc.[6] Our analysis in this section looks to even those odds.

Figures 15 and 16 offer two complementary views comparing the prevalence of security findings among cloud providers. Figure 35 uses the total number of findings per host (of any severity) and Figure 16 shows the proportion of hosts with high or critical findings. We've also included comparable rates for internal hosts in both charts (in blue). There are some rather shocking stats in this section that demand careful consideration and explanation.

Figure 15: Total number of findings per host (any severity) in top clouds



Let's start with Figure 15, where we see some measure of variation among clouds in terms of the number of findings per host. There's a 2.5X difference between the providers with the highest and lowest rates. Perhaps most interesting is that issues affecting internal hosts outnumber all clouds except one. From this perspective, pretty much any of these clouds offer equivalent or better "safety" than on-prem hosting. But there's a caveat to Figure 15—it includes findings of any severity level. This may indicate clouds are successfully deploying security tools to clean up the minor security bugaboos at a rate at least as good as your IT team.

[6] Thanks for indulging our need to include at least a few Empire Strikes Back references in this cloud report. May the Force be with you from Bespin to your own corner of the galaxy.

> There are some rather shocking stats in this section that demand careful consideration and explanation

> You'll notice right away that we're only labeling the 3 clouds with the lowest rates in Figures 15 - 17. We made that decision to avoid misleading and counter-productive reactions like "OMG - run for your lives from Cloud X now!"
>
> Instead, digest these figures with a clear and thoughtful head. Notice there are, in fact, differences. Consider why those differences exist. Think about how your actions affect security outcomes in the cloud, regardless of provider. To us, the main takeaway is that choosing a cloud that suits your needs and capabilities an important cyber risk decision.

> From this perspective, pretty much any of these clouds offer equivalent or better "safety" than on-prem

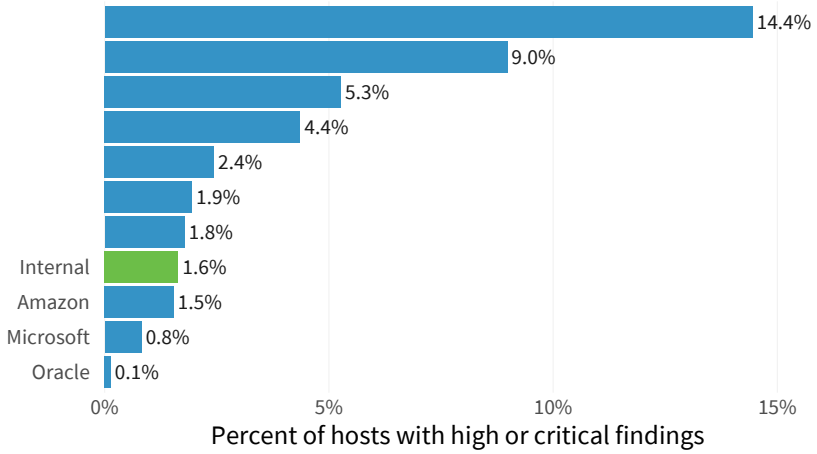
144X

difference between the min and max rate of severe exposures among cloud providers

> Security **in** the cloud is not **on** the cloud; it's **on you**.

Figure 16 filters out the lower-level noise and focuses on just high and critical security findings. Here we see a different story. Averaging host exposure rates for the top 3 and bottom 3 clouds yields a 12X difference. If we compare the absolute minimum and maximum values, we find a 144X disparity. Only 3 of the top 10 clouds exhibit a lower likelihood of severe exposures than the baseline for internal hosts. Referring back to Figure 2, however, reminds us that 2 of those 3 claim the highest adoption rates.

Figure 16: Percent of hosts with high or critical findings in top clouds



So should you hurriedly pull all of your precious hosts out of clouds not listed in Figure 16? Not so fast. Similar to what we said in the previous section, this very well may be more of an indication of who is using these clouds and how they're being used. For instance, we make no distinction here for PaaS, IaaS, SaaS, etc. On one end of the *aaS spectrum, security falls mainly on the provider; on the other end, the user. Some cloud providers allow more freedom to use dangerous configurations and software or provide less in the way of security monitoring and tools. Furthermore, some clouds cater mainly to enterprises and some to individuals, which undoubtedly affects these results.

The bottom line is that we cannot discern from the data at hand exactly why these security differences exist or who owns what portion of the responsibility. Ultimately, users are responsible for securing their hosts in the cloud, regardless of what provider owns the infrastructure. That said, we clearly see there are differences, and that was the main question we wanted to answer at present. And that means choosing a cloud provider that suits your needs and capabilities an important cyber risk decision.

> **Ultimately, users are responsible for securing their hosts in the cloud, regardless of what provider owns the infrastructure.**

13X

On-prem hosts are 13x more likely to be blacklisted than any of the top cloud providers

Before closing the book on cloud comparisons, let's examine one more potential differentiator—reputation. If the rate of security findings serves as a proxy for risk, threat intelligence related to hosts provides an indicator of reputation. For this reason, RiskRecon collects threat intel feeds from numerous open and commercial sources. In theory, hosts appearing on these so-called blacklists indicate infrastructure that may be compromised or otherwise engaging in suspicious activity. Threat data feeds are notoriously short-lived and prone to false-positives, but that doesn't really matter for our purposes here. Reputation is reputation, earned or not.

Figure 17: Percent of hosts with intel-based findings in top clouds.

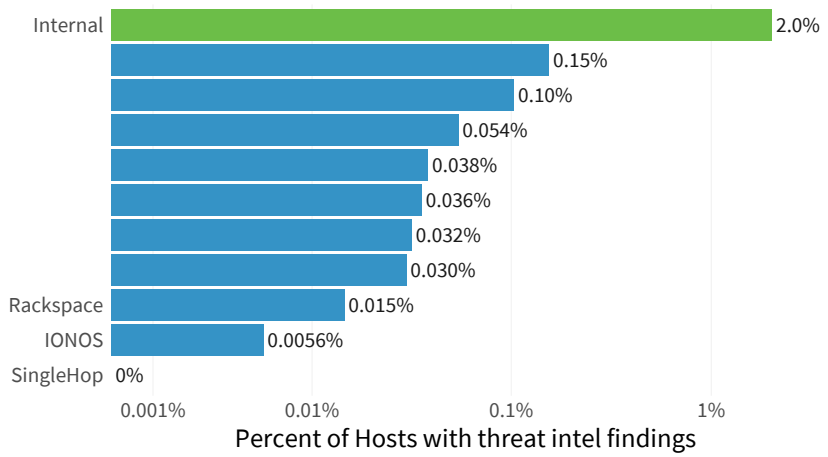


Figure 17 shows the percent of hosts that appear on in our threat intel lists and can be mapped back to a specific organization or cloud provider. It tells a completely different story than the findings-based figures above. On-prem hosts are 13x more likely to be blacklisted than any of the top cloud providers. In other words, your reputation is probably worse than your cloud provider's.

> "We can't determine exactly why these differences exist. But they do, and that means choosing a cloud provider that suits your needs and capabilities an important cyber risk decision.

In truth, though, this is not a fair comparison. Internal networks have user-generated traffic and clouds generally do not. Users click malicious email attachments, visit suspicious websites, many other things that make it more likely for hosts to land on someone's naughty list. We attempt to control for this by filtering the dataset to just web servers for both internal and cloud-based hosts, but this still probably isn't quite "apples to apples."

Even so, the results are thought-provoking. Cloud providers likely have strong incentives to monitor reputation lists closely and quickly remediate/block hosts that appear on them. Assuming your provider's reputation rubs off on you, these results suggest that cloud decisions have a reputational impact in addition to the risk impact established previously.

CHAPTER 4

Cautions & Recommendations

Normally, this section would be titled "Conclusions & Recommendations," but we're going to break with tradition. In an effort to avoid potential misinterpretation of findings, we feel compelled to offer some cautionary words at the conclusion of this report. We'll do that in the form of a brief Q&A and include some recommendations in the mix.

Q: You say hosts in the cloud are twice as likely to have severe security exposures. Should I avoid the cloud altogether?

A: That's neither our decision nor recommendation. Our findings show some organizations actually fare much better in the cloud and some fare worse. Without knowing a lot more about your organization and capabilities, it's impossible to predict where you fall in that spectrum. Our findings can support your cloud decision, but they should not be the sole criterion for making it.

Q: You say the rate of severe findings is highest when cloud diversity is lowest. Should I start spreading my hosts around a multiple clouds?

A: Not on the basis of these results alone. We suspect what's really going on here is more complicated than "more clouds = more secure." And we're confident that distributing hosts willy-nilly across cloud providers does not constitute a sound security strategy. That said, we do think there's a legitimate risk dimension to the question of cloud consolidation vs. diversification, and we plan to study this more in the future.

Q: You say some clouds have a MUCH higher rate of host-based exposures. If I'm using one of those, should I change providers ASAP?

A: Once again, this is not our call and not our recommendation. By and large, your actions have a greater effect on your security in the cloud than simply which provider you choose. But we do recommend evaluating cloud providers based on security features such as their own internal controls and tools and guidance they make available to assist users in securing their environments. Some clouds are undoubtedly a better match for your needs and capabilities than others.

Q: You say firms in my industry and size range are safer on prem. Does that mean I'm destined for major security failures in the cloud?

A: No it does not. We saw a huge amount of variation in cloud and on-prem exposure rates, even among organizations of the same industry and size. We'll reuse/reword what we said to the last question: by and large, your actions have a greater effect on your security in the cloud than simply what industry you're in or how many employees you have. At the same time, factors such as business models and security resources absolutely affect cloud readiness. An honest assessment of who you are, what you want, and where you're at should definitely factor into your decisions.

Beyond that, our general recommendation following on from this research is awareness. As with any business decision, jumping into something you don't understand, haven't prepared for, or cannot control is foolish and bound to fail. It is no different in the cloud. In the words of the Great OODA: orient and observe before you decide and act.

To kickstart your OODA-ing, the Cloud Security Alliance offers a wealth of resources on best practices for securing cloud environments. But as those environments evolve into "fiefdoms" with their own architectures, tools, and procedures, it becomes more and more necessary to supplement general best practices with more specific guidance from the cloud providers themselves. We highly suggest familiarizing yourself with these resources.

We wish you good luck and godspeed as you navigate safely through the clouds! Let us know if we can help in that journey.

riskrecon™

RiskRecon enables clients to control third-party risk by providing vendor security assessments that are comprehensive, actionable and available on demand.

www.riskrecon.com

119 Cyentia INSTITUTE

The Cyentia Institute produces rigorous, accessible research content that provides value to our partners' core audiences and the security community at large.

www.cyentia.com