REPORT

McAfee
Together is power.

Cloud-Native: The Infrastructure-as-a-Service (IaaS) Adoption and Risk Report

Table of Contents

REPORT

Cloud-Native: The Infrastructure-as-a-Service (IaaS) Adoption and Risk Report

Executive Summary

Infrastructure-as-a-Service (IaaS) is used by organizations of all sizes as the new default IT environment to build and host internal and customer-facing applications. In the rush toward IaaS adoption, many organizations overlook the cloud shared-responsibility model and assume that security is taken care of completely by the cloud provider. At the end of the day, the security of what cloud customers put in the cloud, most importantly sensitive data, is their responsibility.

The Rise of Cloud-Native Breaches

Numerous "breaches" have occurred in IaaS environments, but they don't look like your typical infiltrate-with-malware type of scheme. In most cases, the Cloud-Native Breach (CNB) is an opportunistic attack on data left open by errors in how the cloud environment was configured. Adversaries can exploit misconfigurations to escalate their privileges and access data using native functions of the cloud, instead of malware. In this study we asked 1,000 enterprises across 11 countries and multiple industries about misconfigurations, which have left millions of customer records, intellectual property, and the like open to theft.

We also analyzed our own customer use of IaaS through anonymized, aggregated event data across millions of cloud users and billions of events. Unfortunately for the state of cloud computing at this moment, we found that about 99% of misconfigurations go unnoticed by companies using IaaS. The enterprise companies we spoke to told us that they were aware of, on average, 37 misconfiguration incidents per month. Yet our real-world data shows that companies actually experience closer to 3,500 such incidents.

Connect With Us

Practitioner-Leadership Disconnect

Awareness of misconfigurations is clearly an issue. But only 26% of our enterprise survey respondents said their current security tools could audit configurations in IaaS. We hypothesize that there is a practitioner-leadership disconnect at work here. Ninety percent of companies told us they'd experienced some security issue in IaaS, misconfiguration or otherwise. But twice as many manager-level IT personnel—those closest to the IaaS environment—thought they'd never experienced an issue compared to what their CISO, CTO, and CIO leadership claimed. It's possible the speed of cloud adoption is putting some practitioners behind. Infrastructure changes rapidly in the cloud, opening the door for mistakes as code is released in continuous integration/continuous delivery (CI/CD) practices. Security leaders should consider enabling their staff with the tools they need to keep up with security issues, especially the ability to audit their IaaS deployments for misconfiguration before they enter a production environment.

IaaS: The New "Shadow IT"

Keeping track of security incidents in IaaS is increasingly difficult when you operate in multiple cloud service provider (CSP) environments. There's an interesting awareness trend here as well, similar to the "Shadow IT" we've seen for years with Software-as-a-Service (SaaS) applications being brought into the enterprise. Seventy-six percent of our survey respondents told us they use multiple IaaS providers. Yet in our real-world data, we found that 92% actually do, up 18% year over year. Security incidents are almost guaranteed to go under the radar if companies don't even know where all of their infrastructure lives.

The Rise of Cloud-Native Breaches

Let's begin by exploring the nature of a Cloud-Native Breach (CNB), which does not follow the traditional malware-infiltration and defense strategy we're accustomed to within network borders and on managed devices. We'll define a CNB as "*a series of actions by an adversarial actor in which they 'Land' their attack by exploiting errors or vulnerabilities in a cloud deployment without using malware, 'Expand' their access through weakly configured or protected interfaces to locate valuable data, and 'Exfiltrate' that data to their own storage location.*"

In Figure 1, you can see several examples of how the attack pattern of a CNB will progress. To further detail this structure, consider the following examples at each stage:

1. **Land** by gaining a foothold into the IaaS/Platform-as-a-Service (PaaS) environment.
   a. Leverage compromised/weak credentials to gain access as a legitimate user.
   b. Exploit a vulnerability, such as server-side request forgery (SSRF), in deployed software.
   c. Capitalize on misconfigurations of ingress/egress security groups.
2. **Expand** by finding ways to move beyond the landing node.
   a. Leverage privileges associated with a compromised node to access remote nodes.
   b. Probe for and exploit weakly protected applications or databases.
   c. Capitalize on weak network controls.
3. **Exfiltrate** data while staying under the radar.
   a. Copy data from the storage account to anonymous nodes on the internet.
   b. Create a storage gateway to gain access to the data from a remote location.
   c. Copy data from the storage accounts to a remote location outside the virtual private cloud (VPC).

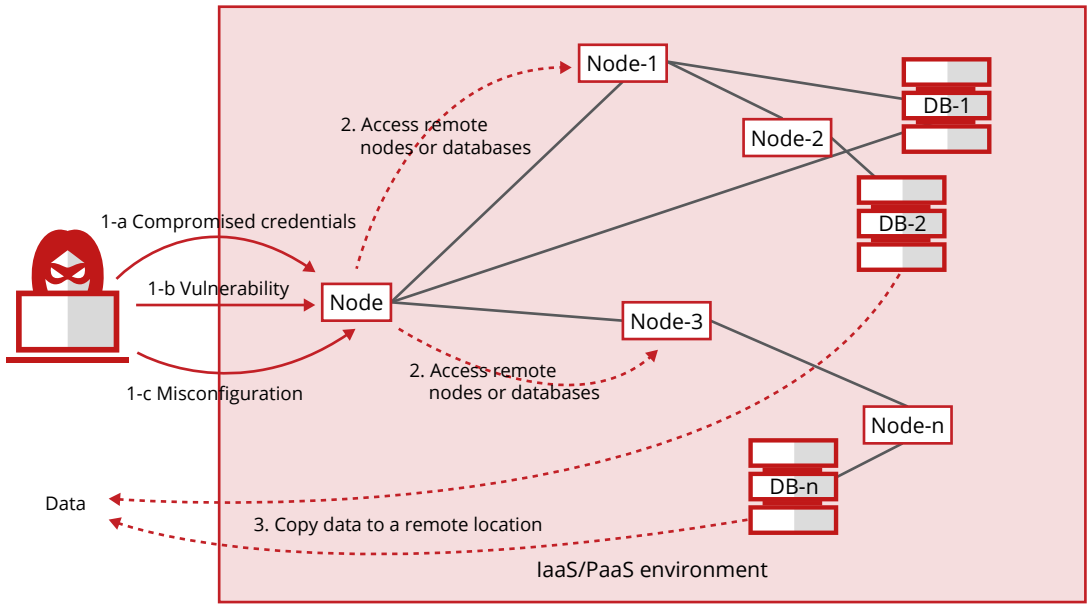

Figure 1. Cloud-Native Breach (CNB) attack chain.

We'll come back to these examples in more detail later. In our research we wanted to uncover the prevalence of these breaches and the impact they're having on companies worldwide. The most common point of leverage for a "Land" action is a misconfiguration in an IaaS resource, which is wholly the responsibility of the cloud customer but often overlooked. Through our own view of hundreds of thousands of misconfiguration events, we've extracted the following top 10 most commonly misconfigured settings, using Amazon Web Services (AWS) for a practical perspective:

The Top 10 Most Commonly Misconfigured Settings in AWS

1. EBS Data Encryption
2. Unrestricted Outbound Access
3. EC2 Security Group Port Configuration
4. Provisioning Access to Resources Using IAM Roles
5. Unrestricted Access to Non-Http/Https ports
6. Unrestricted Inbound Access on Uncommon Ports
7. Unused Security Groups
8. Unrestricted ICMP Access
9. EC2 Security Group Inbound Access Configuration
10. EC2 Instance Belongs to a VPC

When we asked our survey group of 1,000 enterprises across 11 countries how many misconfiguration incidents they experience every month, the answer was 37. Yet, when we look at our real-world data, we see that companies average 3,500 misconfiguration incidents per month, up 54% year-over-year. That means 99% of the misconfigurations in enterprise IaaS environments are going unnoticed, leaving the doors open for the "Land" stage of a CNB.

Known versus Actual IaaS Misconfiguration Incidents per Month

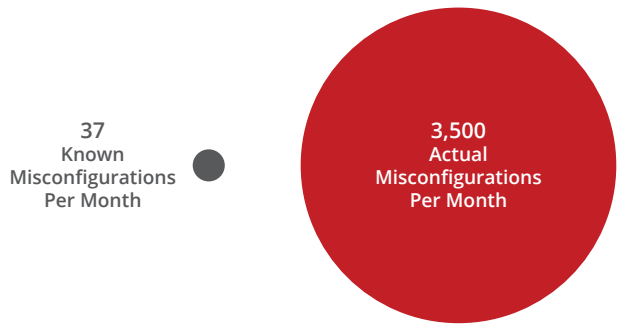

Figure 2. Please estimate how many IaaS misconfiguration incidents occur per month at your organization; occurrence of actual misconfiguration incidents.

...99% of the misconfigurations in enterprise IaaS environments are going unnoticed.

The velocity of cloud deployments means that misconfigurations are introduced, removed, or resolved on a constant basis as new infrastructure is rolled out. Much of this is automated by DevOps teams in the practice of CI/CD, which unfortunately automates misconfigurations along with all the rest. Our analysis of the 3,500 real-world misconfiguration incidents shows that 73% are eventually resolved, leaving 27% potentially vulnerable to attack. In our survey, we also asked how long it takes for companies to correct misconfigurations. Here is a summary of the responses:

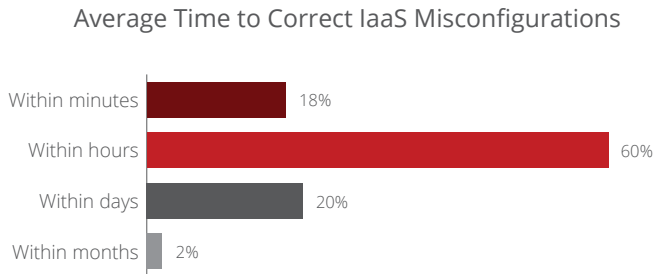

Figure 3. How long, on average, does it take for your organization to correct IaaS misconfigurations?

Nearly a quarter of our respondents said they take longer than a day to correct misconfigurations in IaaS. This leaves plenty of time for an adversary to scan for open ports or other vulnerable resources to land their attack. Ideally, misconfigurations should be reduced prior to deployment, shifting the task of auditing configurations left in the deployment lifecycle. Some countries are further along in addressing configuration errors quickly, while others are much slower:

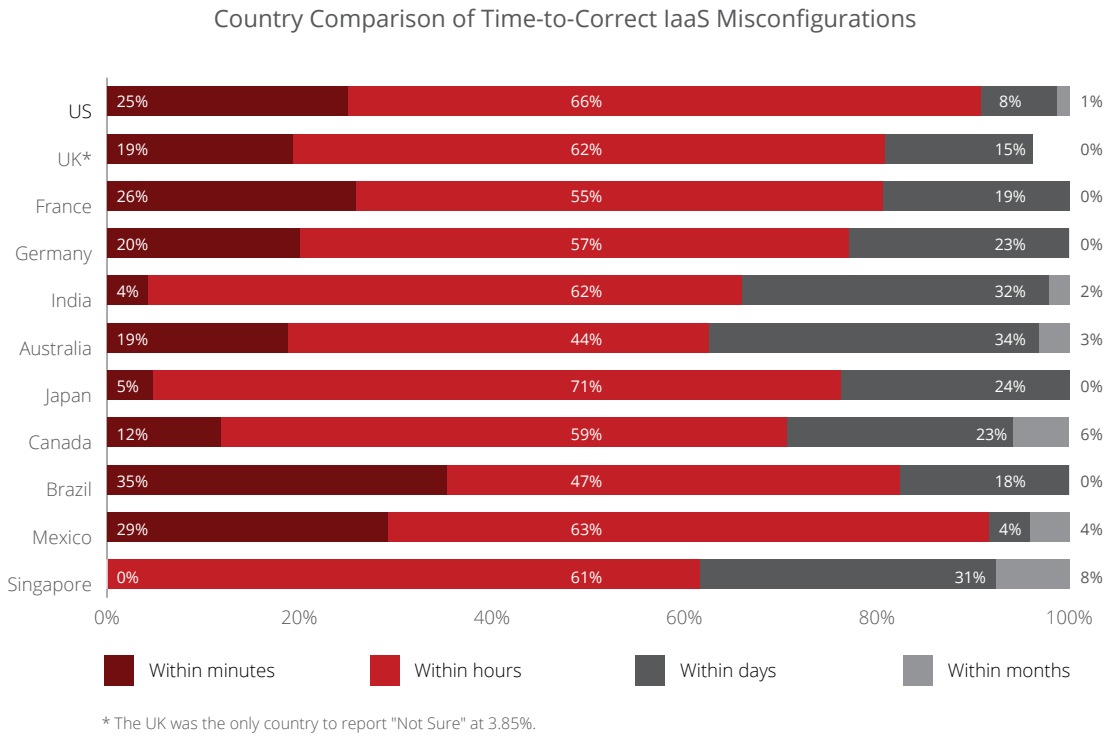

Figure 4. How long, on average, does it take for your organization to correct IaaS misconfigurations? (Shown by country.)

Reducing misconfigurations and vulnerabilities will mitigate the risk of an adversary landing an attack in an IaaS environment. However, that is just the entry point. Once the attacker has gained a foothold, their next step is to "Expand," seeking valuable data in storage objects and databases.

As we laid out above, moving laterally to locate valuable data is often accomplished by capitalizing on weak network controls, exploiting weakly protected applications or databases, or leveraging the privileges of the initially compromised node from the "Land" stage to access remote nodes. This activity occurs completely within the confines of a virtual private cloud (VPC), outside of the target company's network, making visibility difficult. The lateral movement, however, will appear anomalous to normal patterns of behavior if the cloud environment is monitored with some form of behavioral analysis, often User and Entity Behavior Analytics (UEBA). From our assessment of real-world cloud usage from enterprise companies using UEBA, we are able to see the prevalence of lateral movement events indicative of the "Expand" stage of an attack.

Privileged user threats are one example of how lateral movement can occur in an IaaS environment, where a compromised account or malicious insider uses their account-based privileges to directly access or change the configuration of connected resources, such as a data store, to allow for external access and exfiltration. Our research found that 58% of companies experience privileged user threats every month, averaging seven per month in IaaS. With access to the target's data, the next and final step is to "Exfiltrate."

The ultimate goal of a CNB is most frequently to steal data. There are several methods of executing this, which we touched on above. The adversary can sync data from one IaaS storage object to their own in a separate virtual private cloud (VPC), create a storage gateway connected to the desired data so it can be accessed from a remote location, or copy the data to a location hidden in Tor (open source software enabling private communication), making it relatively untraceable. Each rely on the freedom of data in motion to accomplish the task, which can be prevented. Data Loss Prevention (DLP) is often used to classify data as sensitive to an organization and block it from leaving to an unapproved location or simply block movement altogether. From the real-world cloud usage data we analyzed for this research, we took a subset of companies who currently run DLP in IaaS to see how many incidents they were experiencing:

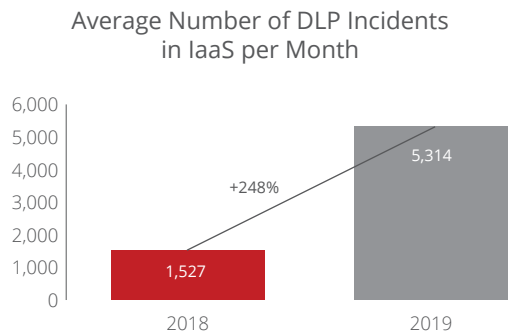

Figure 5. Prevalence of DLP incidents in IaaS for companies running DLP in the cloud.

...58% of companies experience privileged user threats every month, averaging seven per month in IaaS.

Companies actively assessing their data exfiltration attempts in IaaS currently see an average of 5,314 events each month. This increased 248% over last year, when companies experienced an average of 1,527. Since these companies have DLP in place, the incidents represent attempts to exfiltrate and not successful theft. From our survey, we learned that 36% of companies have the capability to run DLP in the cloud. The remaining 64% are subject to the 5,314 incidents they aren't currently blocking—all occurring in the cloud provider's environment— and most likely outside of their current visibility. Forty-two percent of the storage objects involved in these DLP incidents were misconfigured.

Misconfigurations make it easy to "Land." Lack of cloud-native visibility lets an attack "Expand" unnoticed. The ability to "Exfiltrate" is possible through multiple methods when DLP is not present. CNBs are happening regularly, sometimes making headlines, and more often going under the radar.

In figure 6, we have a real-world example where the attacker followed the pattern of "Land-Expand-Exfiltrate" to ultimately steal over 100 million customer records. Let's walk through what happened to close out our discussion on the rise of the CNB.

1. The adversary "landed" by exploiting a vulnerability using SSRF on a customer-deployed web application firewall (WAF).
2. They then "expanded" by leveraging the exploit in the compromised node to query a metadata service to obtain sensitive keys and tokens. This allowed the adversary to obtain broad privileges, including the ability to query and read storage objects.
3. Lastly, over 100 million customer records were "exfiltrated" from the storage object to anonymous nodes on the internet, and/or used tokens/keys from above step to invoke a custom script to copy storage object data to another storage object in another IaaS account.

Companies actively assessing their data exfiltration attempts in IaaS currently see an average of 5,314 events each month.

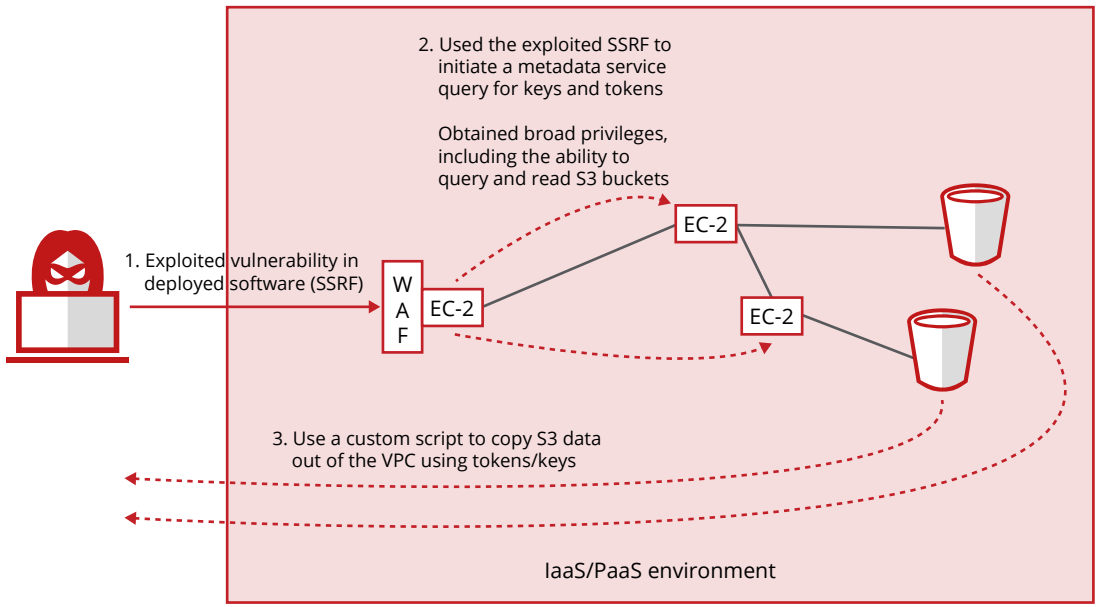

Figure 6. Sample real-world CNB, anonymized.

Practitioner-Leadership Disconnect

Why are the doors so often left open in a CNB? In the "Land" stage of the attack, misconfiguration of IaaS resources is the most prominent culprit. Yet from our survey respondents, we learned that only 26% of companies can currently audit for IaaS misconfigurations with their security tools. During this study we hypothesized that there may be a disconnect between security leaders and the practitioners closest to IaaS environments. Do security practitioners have the right tools to keep up with misconfigurations in IaaS? Is leadership too slow to adapt to the rapid changes in cloud technology? Let's explore.

Taking a step back for a moment, we can look at the overall landscape of security issues in IaaS for a high-level comparison between leaders and practitioners. We asked the companies in our survey to identify which security issues they had experienced in IaaS:

...only 26% of companies can currently audit for IaaS misconfigurations with their security tools.

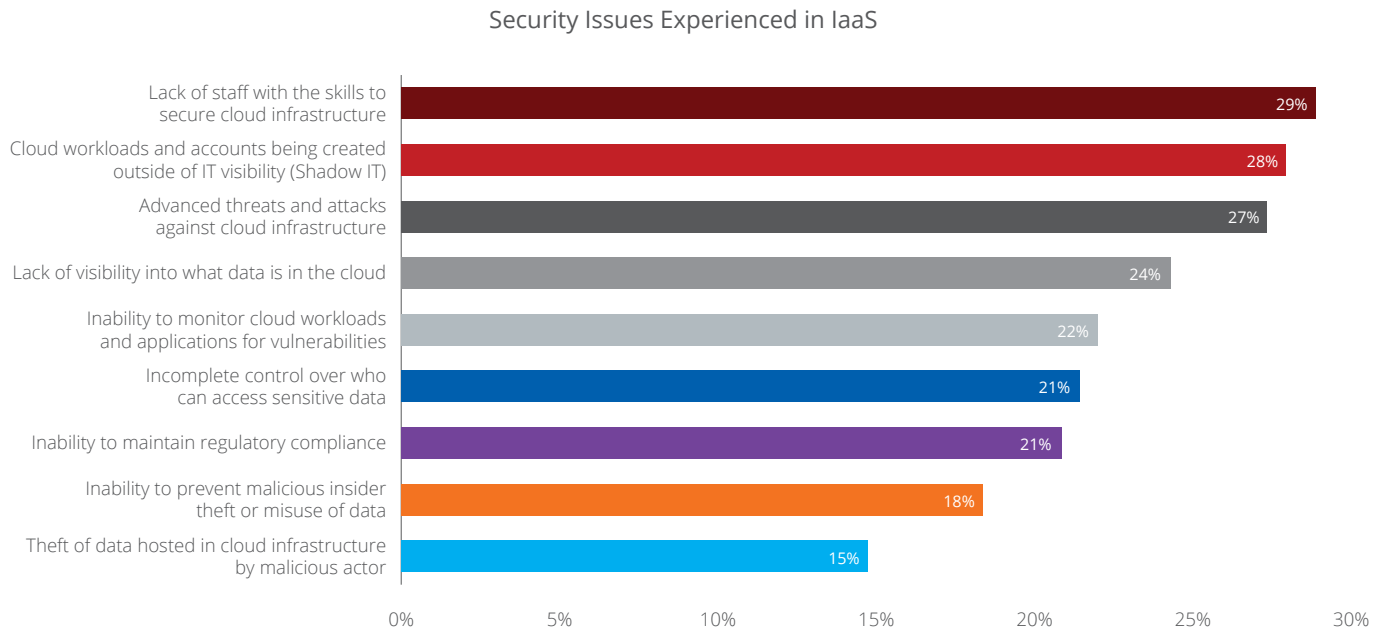

Figure 7. Has your organization experienced any of the below issues when it comes to using IaaS?

Ninety percent of our respondents said they had experienced at least one of these security issues in IaaS. Interestingly, if we look at the inverse—those who reported "we have not experienced any security issues in IaaS"—we find an interesting divide based on role in the organization:

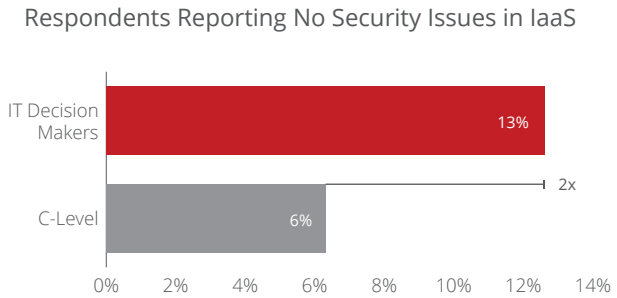

Figure 8. Has your organization experienced any of the below issues when it comes to using IaaS? Those reporting "My organization has not experienced any issues with using IaaS."

Twice as many IT decision makers reported having no security issues in IaaS. There could be several issues blocking visibility here. C-level leaders may have access to more information than their practitioner staff, increasing their scope of visibility. Practitioners may not have the tools they need to see these issues to begin with, which makes it harder to do their job. Let's look closer at misconfigurations specifically to see if we can uncover an answer. Sixty-seven percent of all respondents told us they were aware of misconfigurations in their IaaS environments.

Looking at the responses by role, we see the same disconnect:

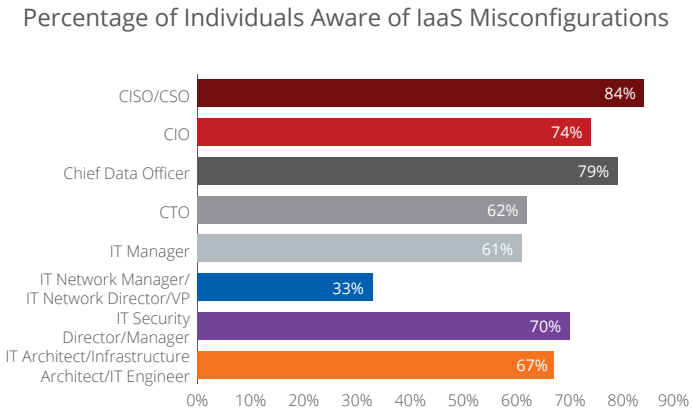

Figure 9. Please estimate how many IaaS misconfiguration incidents occur per month at your organization; showing the percentage of respondents reporting misconfigurations (by role).

The divide is clear again. Eighty-four percent of CISO respondents were aware of misconfigurations in their IaaS environment, while practitioners were at least 14% less aware, and network teams as much as 51% less aware than CISOs. The disconnect is present for a broad set of security issues in IaaS and for misconfiguration on its own. Looking at every security issue we asked about, you might expect that certain teams would have less awareness than others, and the ultimate roll-up to CISOs would result in more comprehensive visibility. But for misconfigurations alone, it is less convincing. Both practitioners and CISOs should have similar levels of visibility into a singular issue. That brings us back to one conclusion: security practitioners aren't equipped with the tools they need to keep up with security in IaaS.

Another answer could be the talent pool itself. You might have noticed the number one security issue in IaaS was a lack of staff with the skills to secure cloud infrastructure. More than one in four companies told us they had a skills shortage for IaaS security practitioners.

This may be the other half of the equation. However, we fundamentally believe that with security tools that integrate into the CI/CD tool chain and operate at the speed of cloud deployments, enough efficiency can be gained to make up for a perceived shortage of people to do the work. This challenge is more difficult for some countries than others:

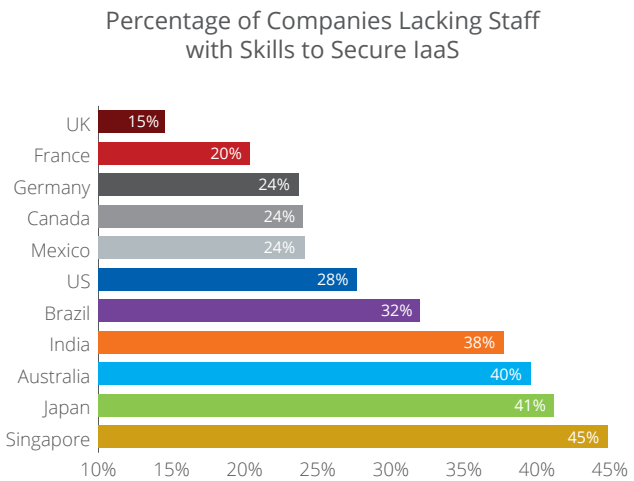

Figure 10. Has your organization experienced any of the below issues when it comes to using IaaS? Showing lack of staff with the skills to secure cloud infrastructure (by country).

Clearly some countries are further ahead in their skills training than others, which should be a call to increase investment in the education needed to support the future of IT infrastructure in the cloud. Overall, we can surmise that companies will benefit from increased investment in security tools developed for CI/CD tool chains that deploy into IaaS and training for their staff to build skill sets in cloud-native security. While that should address the awareness disconnect between leadership and practitioners, it is not the only visibility issue companies are facing with IaaS.

More than one in four companies told us they had a skills shortage for IaaS security practitioners.

IaaS: The New "Shadow IT"

You can't secure what you can't see, right? We've been through this before. The first stage of cloud adoption was a slew of employee-acquired apps for file sharing and collaboration that IT never knew about, hence the term "Shadow IT." With SaaS, IT teams caught up and now sanction the most useful applications on the market, like Microsoft Office 365, so their users no longer have a need to go find their own "best pick" to solve a given business problem.

As IaaS adoption rapidly increases, we're seeing a similar trend occur with infrastructure services like AWS or Microsoft Azure. Each provider has unique services to offer, leading to valid business cases for establishing a "multicloud" environment, where multiple IaaS providers are used by design. If you're working on a project to migrate a large swath of Windows Server-based applications to the cloud, your first choice might just be Microsoft's own cloud infrastructure in Azure. Otherwise, most companies turn to AWS as their first choice by default.

So applications are going into the cloud and are being built in the cloud, but do most companies know where? Many don't have a complete grasp on the multicloud sprawl occurring today:

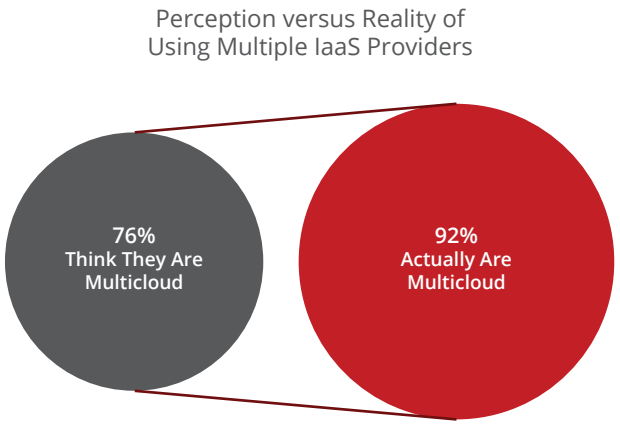

Figure 11. Which of the following IaaS providers does your organization use? Showing respondents with multiple selections; versus actual use of multiple IaaS providers.

When asked, 76% of the companies in our survey stated they use multiple IaaS providers. But when we look at our real-world data of actual cloud use, 92% actually do, up 18% year over year. That 16% spread between perception and reality is enough to cause concern, given the nature of data entering IaaS environments. Typically IaaS deployments are an extension or replacement for business-critical applications, often customer facing. Developers at a healthcare provider may solve the challenge of patient image sharing between doctors, but if they do it in Azure when the security team spends all of their time securing AWS, there is immediate potential for noncompliance. All it takes is a test environment configured with publicly readable storage to put an entire company at risk.

The risk is clear, so where does it most frequently occur? Our survey respondents gave us insight into the market share across the largest IaaS providers:

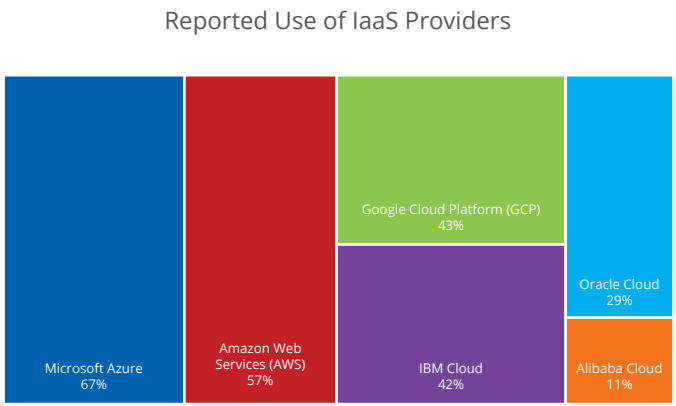

Figure 12. Which of the following IaaS providers does your organization use?

There's a fairly even spread across the top four, which backs up our multicloud finding. It is surprising to see Azure lead overall, but less so when you consider the orientation many global enterprises have towards Microsoft products, from Office 365 to Windows Server and Windows itself. Interestingly, while the share of providers is broad, actual usage within these environments tells a different story:

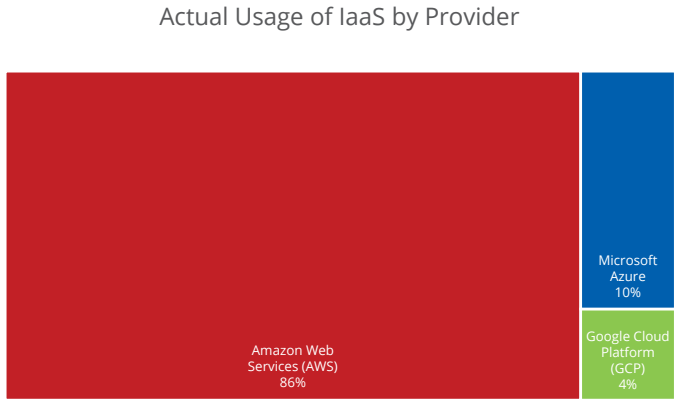

Figure 13. Actual usage share of leading IaaS providers (percentage of access events).

...76% of the companies in our survey stated they use multiple IaaS providers. But when we look at our real-world data of actual cloud use, 92% actually do.

When we look at our real-world cloud data, the share of actual use within leading IaaS providers shifts dramatically toward AWS. This is important to note for two reasons. First, this tells us where to prioritize security, since most data will likely be going into AWS. Second, it shows the increasingly fragmented, multicloud reality of IaaS in the enterprise, especially when we look at the share-shift year over year.

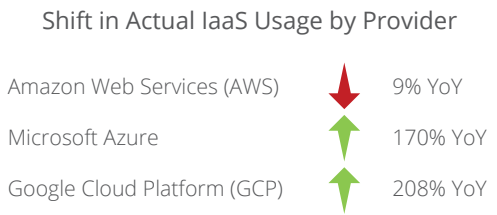

Figure 14. The shifting landscape of IaaS usage (percentage of access events).

Enterprise companies are moving past test and experiment phases of Azure and GCP into increasing production use. While AWS is still the most used cloud infrastructure provider, Azure and GCP are quickly ramping up. For security, the trend points to a more even split of risk across providers. This may be positive for resiliency and failover when these providers have an outage, but setbacks could occur trying to manage each provider individually. Security teams and their tooling must both be multicloud.

Recommendations

We've entered a new reality for enterprise infrastructure, and we should expect it to change more rapidly than ever before. The capacity of infrastructure teams to upgrade, innovate, and deploy new technology is no longer a constraint. Instead we all have access to the global teams at AWS, Microsoft, Google, and others who are rapidly upgrading, innovating, and making it easier and faster to deploy infrastructure than ever before. As we've explored in this paper, our first and most critical step is to establish holistic methods for maintaining visibility over how teams are using these providers, and then move to applying best practices for risk mitigation and governance. Here are a set of recommendations to get you there:

1. **Build IaaS configuration auditing into your CI/CD process:** Do it early—preferably at code check-in—to minimize the amount of misconfigurations that make it into production. Look for security tools that integrate with Jenkins, Kubernetes, and others to automate the audit and correction process.
2. **Evaluate your IaaS security practice using a framework like "Land-Expand-Exfiltrate":** This helps you check controls against the entire attack chain, increasing your likelihood of stopping a breach.
3. **Invest in cloud-native security tools and training for security teams:** Cloud tools and training help security teams understand cloud infrastructure at the same level as their DevOps counterparts. Security tools, like cloud access security brokers (CASBs), cloud security posture management (CSPM), and cloud workload protection platforms (CWPP) are built to work within DevOps and CI/CD processes but are not replications of on-premises data center security. They require new knowledge that goes hand in hand with cloud transformation.

As we've explored in previous research, companies that actively secure their cloud infrastructure with cloud-native security tools increase their use of the cloud and the benefits they gain from it. Companies using a CASB with IaaS, for example, deployed 71% more applications. Not only are these companies doing a better job of keeping up with the speed of IaaS, they are accelerating it. That means they can grow their business faster—by addressing security with tools built for the cloud.

Methodology

To bring you these findings, we surveyed 1,000 IT professionals in 11 countries selected to represent a diverse set of industries and organization sizes. These results were used in comparison to aggregated, anonymized cloud usage data for more than 30 million McAfee® MVISION Cloud users worldwide, who collectively generate billions of unique transactions and policy events in the cloud each day. Both of the data sets represent companies across all major industries, including financial services, healthcare, public sector, education, retail, technology, manufacturing, energy, utilities, legal, real estate, transportation, and business services.

About McAfee

McAfee is the device-to-cloud cybersecurity company. Inspired by the power of working together, McAfee creates business and consumer solutions that make our world a safer place. By building solutions that work with other companies' products, McAfee helps businesses orchestrate cyber environments that are truly integrated, where protection, detection, and correction of threats happen simultaneously and collaboratively. By protecting consumers across all their devices, McAfee secures their digital lifestyle at home and away. By working with other security players, McAfee is leading the effort to unite against cybercriminals for the benefit of all.

www.mcafee.com.

McAfee™
Together is power.

2821 Mission College Blvd.
Santa Clara, CA 95054
888.847.8766
www.mcafee.com