censys

Think Like An Attacker

A Guide to Financial Services Cloud Security with Attack Surface Management

So Your Cloud Is Growing. How Are You Protecting It?

Here's a business tech reality you've no doubt observed within your own organization: more and more company assets are moving from static IP addresses to the cloud. And usually for good reason: the cloud is typically viewed as more flexible, scalable, and cost-efficient compared to traditional on-premise solutions. In fact, today 94% of enterprises now use some form of cloud services. Financial Services (FinServ) firms in particular have said that they expect to shift more than half of their workloads to the cloud by 2027, according to a report from McKinsey.

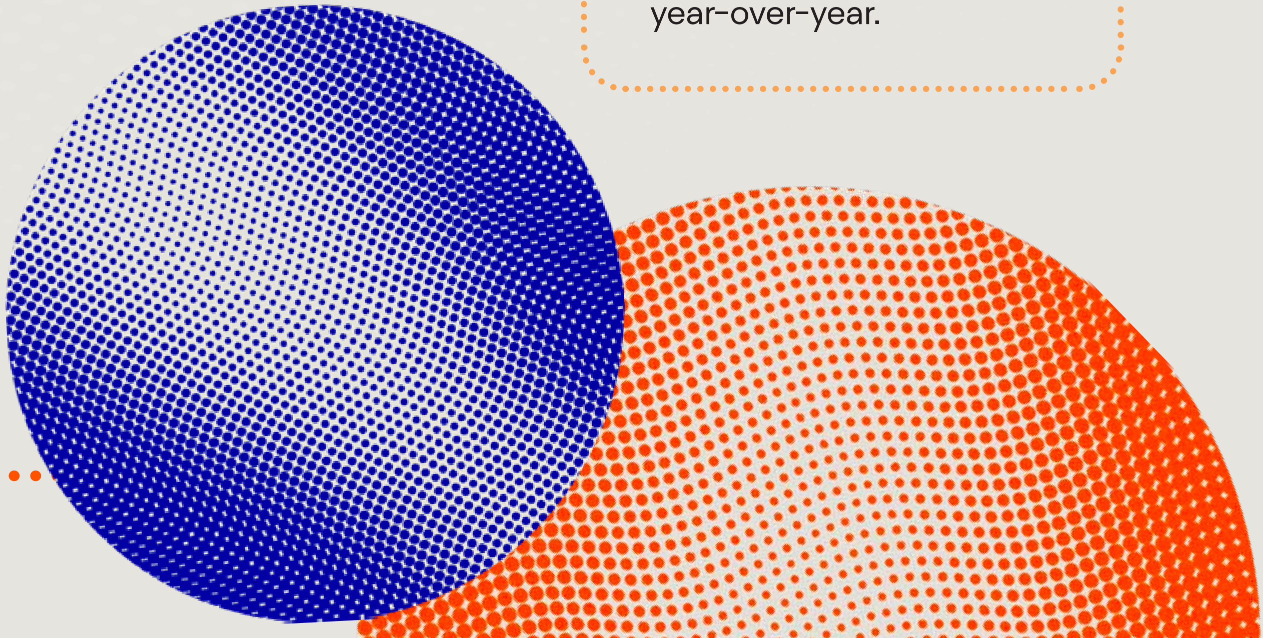
THE CHALLENGE FOR SECURITY TEAMS

While security professionals can acknowledge that moving to the cloud may benefit the organization, they also know that with these benefits comes reduced visibility into network operations, along with increased risk of misconfigurations and unintentionally exposed assets. It only takes one misconfigured asset — like a storage bucket or database — to create a catastrophic data breach. In fact, the reality is that the majority of breaches stem from these kinds of unglamorous cyber hygiene issues. Attackers are more likely to gain entry through forgotten assets, unpatched or misconfigured assets, or unknown assets than they are through advanced attacks.

Whereas server infrastructure was once protected behind a network perimeter or firewall, organizations now have hundreds to thousands of cloud accounts, each of which can have internet-facing points of entry. Merger and acquisition activity further expands the number of cloud assets connected to the organization, with each partnering entity or acquisition adding new cloud infrastructure and instances to the shared attack surface.

110%

The public-facing internet and cloud assets that Censys customers own have increased about 110% year-over-year.



FinServ firms can be particularly challenged to identify and manage their robust collection of cloud assets. The FinServ industry has undergone a rapid transformation in recent years, moving away from traditional brick-and-mortar operations toward digital-first infrastructure. We see this with the rise of online banking, mobile payment apps, IoT devices, and cloud computing.

As this digital infrastructure expands, the number of internet-facing assets that FinServ security teams are responsible for protecting grows, too, and teams must keep up with how they track and monitor these assets across various entities. To heighten the stakes further, FinServ security teams are also up against highly-motivated threat actors eager to breach networks to access exceptionally sensitive personal and financial consumer data.

80%

According to McAfee, 80% of workers have admitted to using SaaS applications without IT approval.

THE NEED FOR A NEW APPROACH

The reality for most organizations is that despite their security teams' best efforts, unknown, unsecured assets in the cloud often remain. In fact, 43% of all assets in Censys customer attack surfaces were initially unknown to the organization.

That's a lot left unprotected.

So how can FinServ security teams more effectively manage and protect their assets as their cloud presence grows?

It requires ***thinking like an attacker***.

What Do We Mean, "Think Like An Attacker?"

A "think like an attacker" mentality invites security practitioners to take an outside-in approach. If you were an attacker, how would you try to breach your company'? It's a unique but essential point of view because it's important for organizations to secure not only the assets they know about, but to secure the unknown ones as well, as those are some of the most vulnerable.

A study from Enterprise Strategy Group found that 69% of organizations have experienced at least one cyberattack that started by exploiting an unknown, unmanaged, or poorly managed internet-facing asset. These exposed, public-facing assets are low-hanging fruit for bad actors, particularly those looking to deploy ransomware attacks, as cited in a recent CISA-sponsored report from the Cyentia Institute.

HOW ATTACKERS CAN BREACH THE CLOUD

We know that nefarious actors are continually crawling the cloud, looking for vulnerabilities to exploit as pathways to sensitive company data. Censys research finds that attackers will often begin full scans for vulnerable systems within hours of a public vulnerability disclosure. And the more these attackers have crawled, the more effective and creative their methods have become (i.e.: the rise of social engineering and sophisticated credential hacking).

We can think about the cloud as a large apartment building: any external threat will be scoping out the building looking for open doors or windows. But as a building owner, it's almost impossible to ensure that all doors and windows remain locked shut, since so many people inside our metaphorical apartment building have access to opening or closing them. This leaves a lot of unknown gaps for an attacker to perform a successful intrusion.

In the cloud, attackers are similarly relentless in their search for vulnerabilities to be exploited to gain access to your company's data. And, just like all the individuals with the ability to open and close doors and windows, your company has numerous employees with the ability to create or resolve vulnerabilities, making it very difficult for security teams to be completely aware of every asset and those who access it.

THE BIG IDEA

By thinking like an attacker, FinServ firms can leverage cloud data protection solutions that not only secure known vulnerabilities, but identify the unknown vulnerabilities that are most susceptible to attacks.

Revisiting What's at Stake

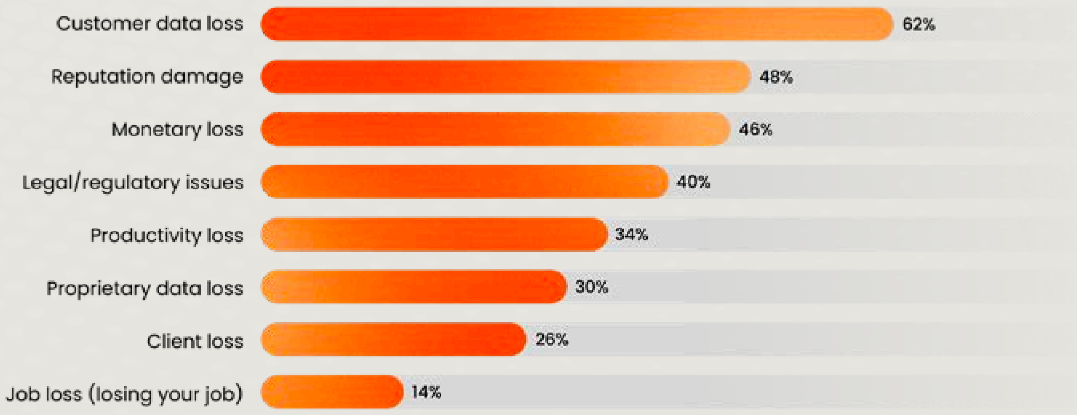
When it comes to cloud security, there's a lot on the line for FinServ security teams, their leaders, and the organization as a whole. The number of successful data compromises in the U.S. FinServ industry increased 177% from 2022 to 2023, with 61 million victims affected just last year. These breaches come at significant cost - the average successful cyberattack to a FinServ organization costs $3.6 million, the highest average expense for any industry. Beyond monetary loss from theft, disrupted operations, and customer attrition, FinServ firms affected by cyberattacks can also be confronted by hefty regulatory fines for failing to safeguard consumer data.

Additionally, FinServ firms are up against growing risk from their expansive ecosystems of third-party partners, including SaaS banking platforms, mobile money apps, payment processors. FinServ firms are the most popular targets for supply chain attacks, and within the last year alone, the industry has seen a 63% increase in cyber attacks that originated through their supply chains.

WHAT KEEPS SECURITY LEADERS UP AT NIGHT

These potentially catastrophic consequences are already keeping many CISOs and their security teams up at night. They recognize loss of customer data, reputation damage, monetary loss, and legal repercussions as outcomes that could have the most degree of damage to their organizations.

Please rank the below list of potential outcomes for your organization of a cyberattack based on the degree of damage to your organization

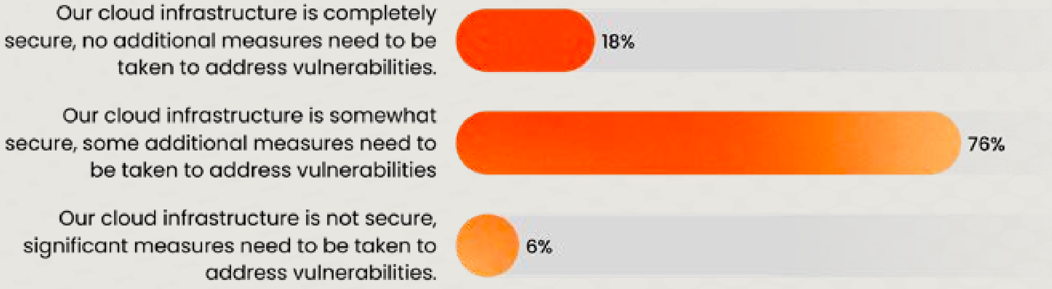


Source: Censys, The 2022 State of Risk & Remediation Report

CLOUD SECURITY STRATEGIES STILL FALL SHORT

Despite these worries, the majority of CISOs surveyed say their current cloud security strategy isn't measuring up. Over three-quarters of security professionals surveyed agree with the statement, "Our cloud infrastructure is somewhat secure, some additional measures need to be taken to address vulnerabilities."

Which best reflects your organization's current cloud state?



Source: *Censys, The 2022 State of Risk & Remediation Report*

That's why we're exploring why it's so important for FinServ firms to add the right cloud data protection solutions to their security stacks, and how Attack Surface Management (ASM) solutions can help organizations think like an attacker to secure their assets.

Let's start with some preliminary cloud security best practices.

Best Practices for Protecting Your Cloud Data

Every company and security team is different, with intricate nuances within each of their cloud environments dictated by company priority and resources. There are some cloud data protection best practices, however, that are important for every organization. These best practices, when implemented with the right tools, can help your team adopt a more proactive approach to cloud security and instill a culture of security across the organization.

#1 BEST PRACTICE #1:

Know your current state of cloud security

Understanding the existing state of cloud environments will help create future controls or policies for the organization, reducing rogue cloud assets or misconfigurations. Conduct ongoing asset discovery to better understand your cloud data and network in sanctioned or unsanctioned environments.

Questions to consider when evaluating your current state of cloud security can include:

- Where do my internal and external assets live?
- Who within the organization has access to them?
- How am I managing inventory as assets are spun up or decommissioned from the cloud?
- How am I communicating security expectations to members of the organization outside of IT?

#2 BEST PRACTICE #2:

Establish data protection policies

It's essential for FinServ organizations of all sizes to establish cloud data protection policies and procedures that are not only followed by security teams, but every department throughout the company. This goes back to the goal of creating a proactive culture. Developing and distributing these policies will help foster a culture of data security company-wide, increasing the responsibility of the numerous individuals with access to cloud environments. **An important consideration**: *find ways to make the secure option the easy option for employees*. Despite best intentions, most employees will ultimately be focused on optimizing performance within their own functions. Complicated protocols are less likely to incentivize proper security behavior.

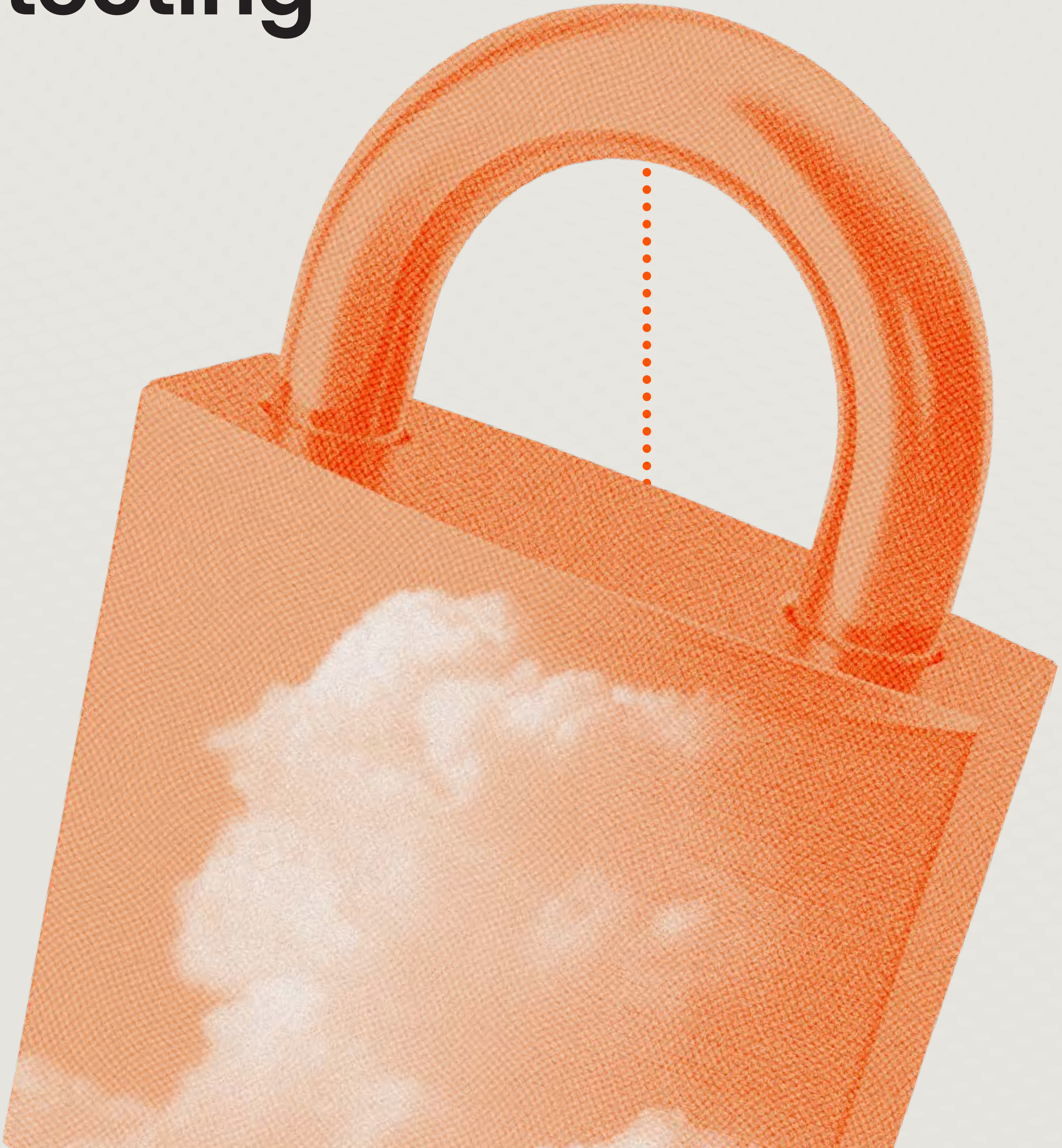
Best Practices for Protecting Your Cloud Data

BEST PRACTICE #3:

Apply strategies to unknown assets

Vulnerability management and cloud data protection policies are critical first steps, but they only achieve the maximum benefit if they are applied not only to the assets your team is aware of, but to unknown assets. As the cloud becomes increasingly complex and common cloud misconfiguration mistakes create more vulnerabilities, it's essential for security teams to turn their unknown assets into known assets to perform the highest level of protection. And if you doubt that your organization has any unknown assets, consider this: when Censys evaluated the attack surfaces of 37 large organizations, we found that on average, they had **44 different domain registrars and presence in 17 different hosting providers**. That's a lot of sprawl.

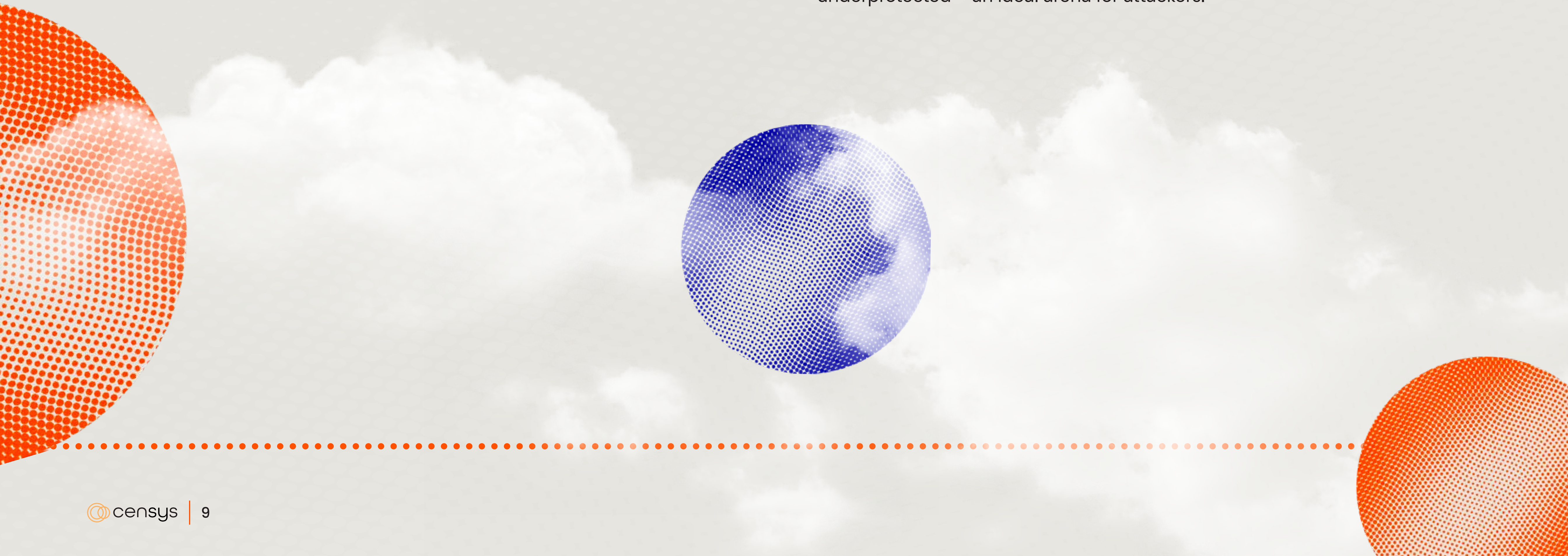
When it comes to pursuing these cloud security best practices, traditional security tools often don't measure up. Unsure if your existing tech stack is up for the challenge? Read on for an introduction to Attack Surface Management.



Improving Cloud Security with Attack Surface Management

Many organizations utilize cloud-specific security tools such as Cloud Security Posture Management (CSPM) to accomplish their security goals. These solutions are often successful, but incomplete in terms of the breadth of what they have visibility into and what they protect.

To this point, Censys worked with Forrester Research to support a Fortune 100 prospect who felt confident that their company was only using nine different cloud accounts. After complementing the existing cloud security stack with Attack Surface Management, we revealed they had data in 23 different accounts. That's 14 additional accounts that were unknown and underprotected – an ideal arena for attackers.



Improving Cloud Security with Attack Surface Management

ENTER: ATTACK SURFACE MANAGEMENT

That brings us to Attack Surface Management, **a critical security technology that empowers security teams to transform their unknown assets into known assets**. Attack Surface Management is a sought-after cybersecurity tool that provides continuous, end-to-end discovery and monitoring of all of an organization's external-facing assets (not just the ones they already knew about). It gives security teams a view of their attack surface from an attacker's point of view, complete with context security teams can use to prioritize and remediate risks.

Attack Surface Management platforms are typically cloud-based SaaS products that continually find public-facing assets across all providers, networks, and accounts. Unlike most security products, these solutions don't require agents or complex integrations. Rather, they use proprietary algorithms fed by internet data sources (like passive DNS, WHOIS, internet-wide scans) to automatically identify assets that belong to an organization and, in turn, analyze those assets for security risks and compliance violations.

84%

84% of decision-makers reported that a solution that automates discovery and monitoring of their organizations' external-facing assets for better risk management is very important.

Forrester Research Consulting for Censys

In their Hype Cycle for Security for Operations Report, Gartner® states that:

"External Attack Surface Management (EASM) provides valuable risk context and actionable information to SRM leaders. EASM delivers visibility through four primary capabilities:

- Monitoring (continuously) for exposed assets (cloud services, IPs, domains, certificates and IoT devices)
- Asset discovery for external-facing assets and systems
- Analysis to assess and prioritize the risk and vulnerabilities discovered
- Remediation, mitigation and incident response through prebuilt integrations with ticketing systems and SOAR tools"

In other words, Attack Surface Management can be a security team's solution to proactive, effective cloud security management.

Ok, But How Do I Find the Right Attack Surface Management Solution?

There's a lot to consider when evaluating Attack Surface Management providers. You want a solution that not only gives your security team the highest degree of confidence, but provides the efficiencies and operational advantages your organization's leadership can buy into. When exploring your options, it's helpful to consider the following capabilities:

ASSET DISCOVERY

Attack Surface Management solutions should uncover modern cloud assets like storage buckets. They should also find internet hosts, services, websites, and certificates. Questions to ask when thinking about asset discovery capabilities include:

- What data sources does the platform analyze to find unknown assets?
- How often does the platform uncover new assets?
- Does the platform correctly identify all of my assets, including assets I didn't already know about? Remember to not only consider the true positive cases, but also false positives and false negatives.

DISCOVERY EXPLANATION

Attack Surface Management solutions should explain how and why they attribute specific assets to your attack surface.

- Does the platform explain how it linked assets to my organization?
- Does the platform provide proof (e.g., specific DNS lookups) to back up attributions?

INVENTORY

Attack Surface Management solutions should let you explore and search your inventory as well as understand your external dependencies.

- Does the platform allow me to understand the assets that compose my attack surface and where they're located?
- Can I easily ask my own questions about my assets? ASM solutions should provide you a history of each asset to aid in investigation.
- Am I able to look up the history of a host or service to understand when it came online?

When exploring solutions, you'll also want to ask about features related to **Data Depth & Accuracy, Risks & Compliance, Reporting, Integrations, Tagging, and Security Controls**. For a full breakdown of capabilities to consider, check out The Attack Surface Management Buyer's Guide.

Get Actionable Intelligence with Censys Attack Surface Management

You can start your search for the right solution with the industry's leading platform: Censys Attack Surface Management. Censys shines a light on unknown and unmanaged cloud assets, and identifies possible misconfigurations across all cloud providers in near real-time, providing an attacker-centric view of your cloud environment and prioritizing the vulnerabilities that are most likely to be exploited. The total visibility Censys provides also helps FinServ security teams better manage sprawl and control the potential runaway costs of cloud adoption.

Censys is the only Attack Surface Management platform with native integrations into the three largest cloud providers. Easily maintain your cloud inventory across all providers with hourly updates, and understand what exists outside of your sanctioned cloud accounts.

THE CENSYS DIFFERENCE:

The Feature	Why it Matters
Integrations Marketplace	Onboard any integration, with any vendor, in 15 minutes or less to deliver a streamlined, automated, and integrated security ecosystem
Attribution Engine	Gain a complete and automated view of your organization's perimeter, establish connections with high confidence using seed data, and increase your visibility up to 80%
Cloud Connectors	Easy to use, flexible, and secure hosted cloud connectors with daily asset ingestion and major cloud service providers support
Rapid Response	Safeguard your business with lightning-fast identification and prioritization of zero-day vulnerabilities

CENSYS IN ACTION

Many cloud breaches occur because of customer misconfigurations rather than traditional software vulnerabilities. **Censys found 18 misconfigured, publicly-exposed S3 storage buckets, including a bucket with sensitive server configuration data, for an international enterprise**. Censys also helped a leading global banking institution improve visibility into its network of nearly 2,000 critical suppliers with accurate, real-time data about zero-day risks.

FINAL THOUGHTS

The security of your cloud environment is simply too important to leave to traditional, reactive approaches. Attack Surface Management provides complete visibility into the entirety of your cloud environment, empowering FinServ security teams to protect the organization to the fullest extent. Invest in a proactive security approach today, and expand your organization's cloud presence with confidence going forward.

Learn more about Censys Attack Surface Management for cloud security.

censys

The one place to understand everything on the internet.

Censys is the leading Internet Intelligence Platform for Threat Hunting and Attack Surface Management, known for discovering assets six times faster than its closest competitor. Censys offers the most comprehensive, accurate, and up-to-date map of the internet available with daily refreshes of billions of services and the world's largest certificate database empowering our customers to proactively discover, prioritize and remediate threats. Established by the creators of ZMap and trusted by the U.S. Government, along with over 50% of the Fortune 500, Censys' mission is to be the one place to understand everything on the internet.

hello@censys.com
censys.com