



# Censys



## Attack Surface Management: The Problem With Cloud

Morgan Princing of Censys on Securing  
the Broader Attack Surface



## MORGAN PRINCING

*Pringing leads the Customer Success team at Censys. She helps customers derive value and build meaningful workflows around Censys' Attack Surface Management platform and Internet-Wide Scan Data. Her career in cybersecurity began in botnet detection, where she worked to protect websites, APIs and mobile apps from bots by detecting and blocking anomalies in web traffic. She is a 2019 World IT Award Winner for Women in Security.*

Morgan Pringing of Censys recently studied service exposure across cloud providers, and she was surprised by some of the findings related to data breaches and remote administration. She shares insight on how to improve attack surface management.

In a video interview with Information Security Media Group, Pringing, who is customer success lead at Censys, discusses:

- Key findings from her study;
- Biggest business impacts of exposed services;
- How to get a better handle on attack surface management – especially in the cloud.

### Number of Database Exposures

**TOM FIELD:** Morgan, you recently studied service exposure across cloud providers. What most surprised you?

**MORGAN PRINCING:** Our Censys labs team conducted this study to look at services exposed related to data loss and ransomware attacks across different cloud providers, and the number of database exposures they found across the board was surprising. The study found 1.15 million MySQL services that had an exposed external IP, and these were only on assets that were found in the cloud.

**“Almost every customer that I interact with has an exposed database. Databases are easy to misconfigure and there’s a lot of risk associated with them. Often, they are unknown assets that maybe were not part of the customer’s primary cloud account.”**

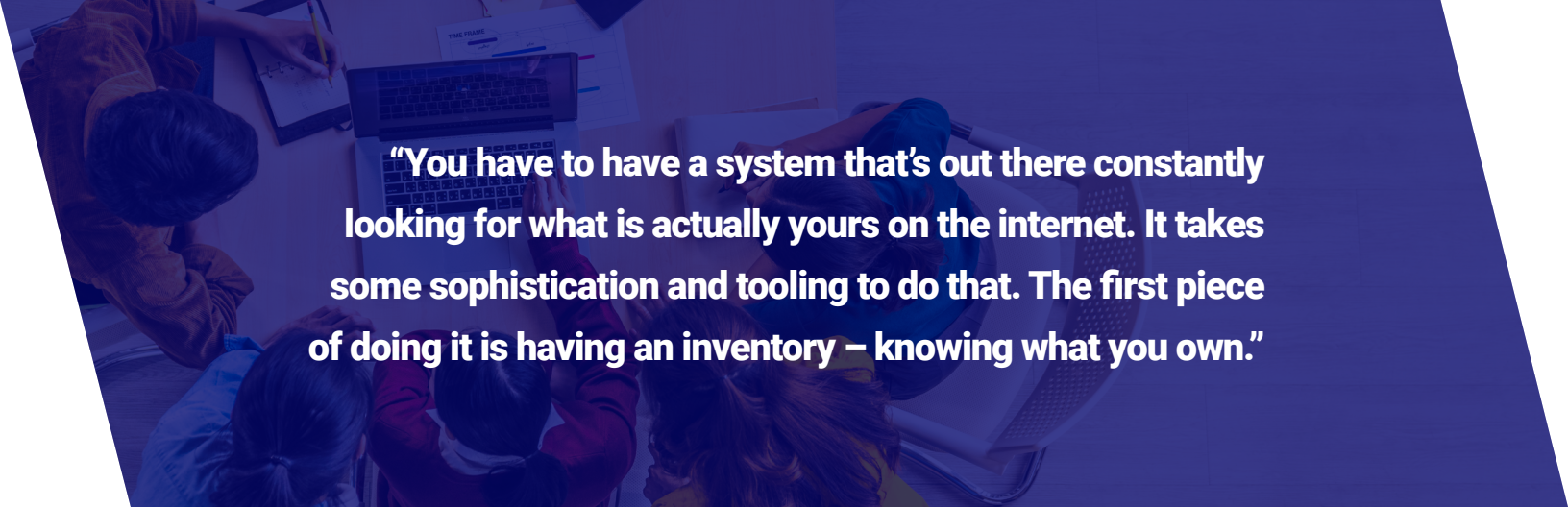
Some of the reasons for the exposures were fascinating and interesting. Our team zoned in on some of the services and even normalized them across 100,000 IPs per provider. Since a lot of people use Amazon, we normalized that so that it didn’t skew the numbers, and it helped us find some anomalies. For example, we looked at PostgreSQL services and saw patterns of heightened exposure on GCP and AWS. To try to figure out why, the team stood up PostgreSQL database instances on AWS and Google Cloud services to review how that setup went and to put themselves in the feeds of some security practitioners. They found that the pre-setup options defaulted to giving and assigning a public IP address to that database.

Something like that is built into the design of the systems and it’s meant to help teams get things done quickly. But holistically, as we’re looking at these problems and trying to fix them at scale, we need to think about how we can help security practitioners build in security correctly.

## **Business Impact of Service Exposures**

**FIELD:** What are some of the biggest business impacts of these exposed services?

**PRINCING:** There are a lot. With remote administration, which is a vector that our cloud study looked at, the business impact is huge. Ransomware increased 300% in 2020. Lots of our customers struggle day to day with ransomware attacks, and often those attacks are distributed across verticals like SMB and VNC. Customers are also being affected by compliance and fines. More penalties are being issued for companies that expose personal information from customers. In the Capital One breach, for example, the company was charged \$80 million in civil penalties. And that was for 100 million lines of customer data exposed. Those big fines have a big impact. If a customer has a vulnerability that gets exploited by an attacker, they should expect to end up paying fines too.



**“You have to have a system that’s out there constantly looking for what is actually yours on the internet. It takes some sophistication and tooling to do that. The first piece of doing it is having an inventory – knowing what you own.”**

## **Data Breaches**

**FIELD:** What are the key takeaways of your research regarding exposed services related specifically to data breaches?

**PRINCING:** The key takeaway for exposed services related to data breaches is their prolific nature. They’re more common than you think. Almost every customer that I interact with has an exposed database. And whether they know about it or not, it’s always a challenge. Databases are easy to misconfigure and there’s a lot of risk associated with them. Often, they are unknown assets that maybe were not part of the customer’s primary cloud account.

## **Remote Administration**

**FIELD:** What are your takeaways for exposed services that are related to remote administration?

**PRINCING:** Remote administration protocols – like SMB, SSH and VNC – are hot topics. If you’re a customer who is starting to think about tackling some of these issues, the biggest takeaway is that we see these services pop offline and online a lot. This wasn’t in the report; it comes from our personal knowledge. These things take a bit of work to fix permanently. You might close them once and then have a lot of them rebound and reopen. Having a pen test once a year might not capture that. You need a continuous system to help find some of the root causes of those exposures.



## The Broader Attack Surface

**FIELD:** Based on the study, what are your conclusions regarding how to secure this new broader attack surface that we all are dealing with today?

**PRINCING:** Securing the attack surface is always a challenge. By the nature of what it is, it's a growing space. We as vendors in the attack service management space have to keep up with new ways that attackers are infiltrating systems. And that takes more than just a point-in-time analysis. You have to have a system that's out there constantly looking for what is actually yours on the internet. It takes some sophistication and tooling to do that. The first piece of doing it is having an inventory – knowing what you own. From there, you can start to do things like manage the risks that you find.

## The Censys Approach

**FIELD:** How is Censys helping its customers to get a better handle on attack surface management, particularly when it comes to the cloud?

**PRINCING:** Censys started by scanning the full IP before internet space. We scan all of the IPs multiple times a week, so we have a great inventory of everything that's exposed on the internet. Security researchers use it all the time. It allows us to write these reports, like the one that we did on the cloud, to be able to paint a picture of the internet. And our inventory powers our Attack Surface Management platform as well; we have data that can help us point to all of these assets. And we do analysis to help us say, "Hey, this might be something that belongs to your company."

A lot of the breaches that occur happen on assets that companies didn't know about and that were not getting regularly scanned and updated by the company's tools. We can help companies get a full picture of their assets and show them the risks of those assets. We can bring those assets into a managed state, particularly with a cloud lens.



## Internet Visibility Is Our Vision

Censys was founded by security researchers who are passionate about developing technology that provides anyone the power to fully understand their digital risk and exposure. Individuals and enterprises – and anyone in between – can harness this power to discover new information and insight as the internet, IoT and cloud evolve. This evolution fuels the Censys team to work tirelessly to broaden our world-renowned visibility and think innovatively about how our outside-in approach can help our customers mitigate every vulnerability.

## About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to information security and risk management. Each of our 28 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment and fraud. Our annual global summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

(800) 944-0401 • [sales@ismg.io](mailto:sales@ismg.io)

 BANK INFO SECURITY®  Just for Credit Unions CU INFO SECURITY®  GOV INFO SECURITY®  HEALTHCARE INFO SECURITY®

 infoRisk  
TODAY®

 CAREERS INFO SECURITY®

 Data Breach  
Prevention, Response, Notification. TODAY

 CyberEd.io

**iSMG**  
INFORMATION SECURITY  
MEDIA GROUP

902 Carnegie Center • Princeton, NJ • 08540 • [www.ismg.io](http://www.ismg.io)