

The Top 5 Risks of Not Investing in Exposure Management



What Every Security Leader Should Know



Your Attack Surface Is Evolving – Do You Have Visibility Into These Exposed Assets?

Welcome to the Golden Age of Cybercrime. There has arguably never been a better time to be a threat actor looking to cash in on the control of sensitive systems and data. The annual number of cyberattacks is the highest it has ever been – increasing 38% from 2021 to 2022 – and the average cost of a single attack has risen to a staggering \$4.35 million. Cybercrime is so pervasive across both public and private sectors that it's become a pressing matter of national security, resulting in the rollout of new federal cybersecurity strategies and mandates.

A key reason cybercriminals are gaining success?
Publicly exposed and unmanaged assets on the internet are easy targets.





Before we get into what this means for organizations, let's take a look at what we'll be covering in this piece:

- How Are Attack Surfaces Changing?
- What Is Exposure Management?
- EASM: A Use Case for Exposure Management
- Why Exposure Management Belongs in Your Tech Stack
- Waiting to Invest in Exposure Management? Delaying the Decision is Risky Business
 - Risk #1: Paying the price tag of a massive breach
 - Risk #2: Loss of brand reputation and customers
 - Risk #3: Lack of visibility into critical assets
 - Risk #4: Increased spend due to cloud sprawl and Shadow IT
 - Risk #5: Inefficient use of security resources
- Making the Right Investment with Censys Exposure Management

Let's dive in!

How Are External Attack Surfaces Changing?

First things first: what is an external attack surface and why is it so important? An external attack surface refers to all of an organization's external-facing assets that live on the internet and represent a potential point of entry for a hacker. Think about your organization's servers, hosts, websites, cloud-based collaboration tools, and more. All of these assets, both on-premises and in the cloud, make up your external attack surface.

Security teams have always needed to protect attack surfaces, and your team likely has a combination of different legacy tools and manual processes to help do just that. The challenge today, however, is how fast attack surfaces are expanding.



At Censys, our research finds that the average attack surface is growing at about 110% YoY.

This isn't surprising considering the rise of remote workforces, the increasing number of business project migrations, and the proliferation of IoT devices, among many other factors. Your business is probably more online than ever before, and will likely continue to expand its digital footprint. Plus, the majority of this expansion is happening in the cloud, which poses its own unique security challenges, particularly in multi-cloud environments. 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.



Security teams are therefore challenged to continuously and effectively discover, monitor, and protect all they own online.

This is an even bigger challenge for companies with subsidiaries, and for those involved in mergers and acquisitions (M&A). These companies not only need to know about what makes up their own attack surface, but they also need to understand the assets that are tied to their partners' as well. The last thing any potential parent company wants is to inherit unknown cyber risk.




So what can security leaders do to better defend these sprawling, complex attack surfaces against advanced threats? Enter Exposure Management.


What Is Exposure Management?

Exposure Management is defined by Gartner as “a set of processes and capabilities that allow enterprises to continually and consistently evaluate the visibility, accessibility, and vulnerability of an enterprise’s digital assets”. Attack Surface Management is a foundational part of the larger exposure management story and is the source of truth for organizations to identify and manage all of their assets that are exposed publicly. An Exposure Management platform, like Censys, takes the attacker’s point of view, looking outside-in at organizations and the entire internet.

A platform, like Censys, is continuously refreshed and provides a real-time, contextualized view of all internet and cloud assets, helping organizations identify risks across their attack surface, so that they can better prevent and defend against cyber attacks.

With Exposure Management, security teams are empowered to:

 **Act fast with confidence:** Time-to-detection is central to guarding against malicious attacks; acting fast enables you to take the critical steps needed to reinforce and remediate exposure. With an Exposure Management solution, like Censys, you have access to the most up-to-date data on the internet today, so that you can accelerate your response time.

 **More efficiently leverage security budget and resources:** Manually discovering and assessing online assets is incredibly time consuming for security teams. Without an automated system to detect new assets on a regular basis, teams are relying on sifting through endless streams of data ad hoc. With Censys Exposure Management, the discovery of assets is automated, resulting in a 30% gain in efficiency according to [Forrester Consulting's Total Economic Impact of Censys EASM™ report](#).



ATTENTION:

**BREACHES
ARE QUITE
DANGEROUS**



Reduce the likelihood of a breach: Publicly exposed or unmanaged assets on the internet are low-hanging fruit for attackers. [Forrester's Total Economic Impact™ of Censys EASM report](#) finds that with Censys Exposure Management security teams gain a comprehensive view into all of their exposures, with full context into remediating and securing risks, reducing the likelihood of a breach by 50%.



Report security posture to executive leaders and decision makers: Executive reporting in cybersecurity is essential to keeping business leaders and decision makers informed about security initiatives, and ensuring that there's alignment between cybersecurity priorities and company goals. Censys provides meaningful insights to simplify communicating cybersecurity program effectiveness and provide a peace of mind to security teams.

Exposure Management Use Cases:

- External Attack Surface Management (EASM)
- Cloud Asset Discovery
- Exposure and Risk Management
- Security Framework & Compliance
- M&A Risk Monitoring and Subsidiary Management

Censys Exposure Management

Censys Exposure Management leverages our powerful, industry-leading internet scanning data so that your security team can quickly identify, prioritize, and remediate advanced threats and exposures across your attack surface.

Access to the best data is critical to ensuring you have complete visibility into both your known and unknown assets, whether they are in the cloud or on-prem. No other vendor on the market scans as frequently, with the same breadth, depth, or accuracy as Censys. Our foundational internet data, alongside our powerful attribution engine, empowers teams to respond to and mitigate exposures in as close to real-time as possible.



EASM: A Key Use Case for Exposure Management

An External Attack Surface Management (EASM) solution – sometimes referred to as ASM – is a core piece of Exposure Management. EASM leverages automated internet scanning to continuously identify and manage exposures in an attack surface, and empowers teams to automate the management of their entire attack surface, **including of assets that were previously unknown to them.**

In this way, EASM enables teams to see their attack surfaces from an attacker's point of view. You see everything that a potential attacker attempting to breach your security perimeter would see. That includes old microsite pages that were never decommissioned, cloud instances that remote employees spun up without IT's knowledge, subdomains that were hidden from view, and more.



The list goes on. Your security team may not know about the existence of these assets – but attackers will.

As we talk about the importance of adopting Exposure Management, you'll see that EASM solutions are central to a broader Exposure Management strategy.

Why an Exposure Management Solution Belongs in Your Tech Stack

Your organization may currently be using tools like cloud security posture management and vulnerability management to help manage your digital assets. Maybe they've done a fair job of monitoring the assets you already know belong to your organization. You tell these tools what to monitor, and they conduct scans on a semi-regular basis. However, **it's the assets you don't know about that are most vulnerable to attacks and which pose the biggest risks to your company's security.**

That's because unknown assets are where threat actors go first. Threat actors suss out which assets tied to an organization have been left unmanaged and unprotected, like expired certificates or misconfigured storage buckets.



In fact, **69% of organizations** have experienced an attack targeting “unknown, unmanaged, or poorly managed internet-facing assets”.

If you think your organization couldn't possibly have any unknown assets beyond its purview, consider this:

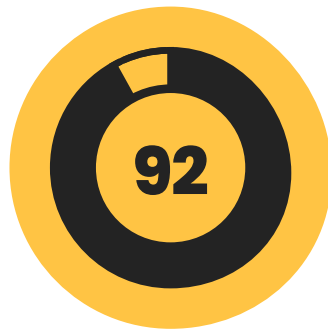


Censys has found that on average, 43% of assets in customers' attack surfaces are unknown.

An Exposure Management solution, like [Censys Exposure Management](#), provides the essential, automated visibility into all of your assets, known or unknown, and in this way offers a unique benefit that other solutions in your tech stack lack. While other tools and techniques on the market offer visibility into exposed assets, many of them only provide visibility into known assets, scan the internet intermittently, provide inaccurate data, and do not offer visibility into the cloud. In turn, they leave teams with an outdated and limited view of their exposed assets.

Don't Just Take Our Word for It

CISOs, cybersecurity analysts, and even the federal government recognize Exposure Management as increasingly critical to modern security strategy.



Of security leaders surveyed by Paradoxes Inc, **92% reported that they either had a fully deployed EASM solution, are implementing an EASM solution soon, or are shopping for one in the next 12 months.**

Analyst firms like Forrester and Gartner further recognize the importance of an Exposure Management solution. In their 2022 EASM Landscape report, Forrester explains why “External attack surface management (EASM) helps security and risk pros better assess third parties and M&A targets, uncover and reduce cloud sprawl, and bring IT and security into agreement about risk prioritization.”

“““

“The risk of not having an ASM product, at a company of a certain size, is that it becomes untenable to know everything about what your company is deploying and exposing to the internet. Having tools that give you the information to consolidate and make decisions on what is occurring is essential.”

Senior Engineering, Technology Firm

The Censys 2022 State of Risk and Remediation Report

There's also a growing push from the federal government for agencies and corporations across sectors to bolster their security efforts through more proactive asset discovery and monitoring. In a Fall 2022 binding operational directive, CISA stated that "continuous and comprehensive asset visibility is a basic precondition for any organization to effectively manage cybersecurity risk."



The question isn't if Exposure Management can provide value, it's whether or not leaders will invest in Exposure Management and realize that value before it's too late.

Invest in Exposure Management



Delay the Decision to Invest

Avoid Consequential Risks





Waiting to Invest in Exposure Management? Delaying the Decision Is Risky Business

We recognize that your security team has a finite budget for new solutions and an endless list of priorities. However, delaying the decision to invest in an Exposure Management solution that is continuously monitoring your external attack surface comes at a huge risk.

When CISOs and other stakeholders make the mistake of thinking that an investment in Exposure Management is a “nice-to-have” rather than a “need-to-have,” they can put the very health of their business on the line. **Consider five of the most consequential risks security leaders face by not investing in Exposure Management.**

Risk #1

Paying the massive price tag of a breach



One of the most direct risks of failing to protect your attack surface is the financial fallout of a successful breach. The majority of risks observed on the internet are misconfigurations and exposures – which are exactly the kinds of risks that Exposure Management can easily detect before threat actors discover them.

When threat actors are able to take advantage of these oversights and successfully launch an attack, they can leave companies on the hook for millions of dollars in direct and associated recovery costs. The average global cost of a breach is \$4.35 million dollars and in the United States, that average more than doubles to \$9.44 million, the highest average cost of any country. And these numbers aren't projected to wane anytime soon. As threat actors and hacker groups become more sophisticated and expand their reach, the global cost of cybercrime is expected to rise from 8.44 trillion in 2022 to 23.84 trillion in 2027. In 2022 alone, cyber attack costs for U.S. businesses were up 80%.



The price tags that organizations face can be multifaceted and accumulate over time. Consider the varied costs of:

- Additional investments in people and systems needed to remediate a breach
- Revenue lost from affected customers who churn after a breach
- Revenue lost from disruption to business operations and product output
- Potential fines upon discovery that cybersecurity regulations weren't followed (ex: HIPAA, GDPR violations)
- Legal fees and payouts if customers whose personal data was compromised choose to take legal action
- Increase in cybersecurity insurance premiums

Then there's the potential added costs of ransomware payouts. Ransomware attacks have increased in recent years, accounting for approximately 20% of all cybercrime in 2022.



At Censys, our research team frequently uses our internet map data to uncover and track incidents of ransomware activity, like 2023's ESXiArgs ransomware attacks on hosts around the world.

While ransomware victims will do all they can to avoid making a payout to hackers, the reality is that the majority feel they're left with no choice. In a survey of IT decision makers who said their organizations had been victims of ransomware attacks, 83% ultimately paid the demand. The average cost of these payouts? \$1 million.





How Exposure Management Can Help:

By leveraging an Exposure Management platform, like Censys, you can increase your likelihood of preventing a breach and paying the associated price tag with the ability to continuously identify when routine security hygiene measures fall short. By automating the discovery, monitoring, and inventory of assets, those common internet risks that hackers most often use to compromise networks are readily highlighted and prioritized for your team to address. Continuous asset discovery also increases the likelihood that you'll find unknown, unmanaged assets associated with your organization before threat actors do.

By leveraging an Exposure Management platform, like Censys, you can increase your likelihood of preventing a breach and paying the associated price tag with the ability to continuously identify when routine security hygiene measures fall short. By automating



Risk #2

Loss of brand reputation and customers



Companies that fall victim to cybersecurity attacks can pay in more than just lost dollars. They also risk losing brand reputation and the trust of both current and future customers. Brand reputation is an invaluable asset to risk in any context; the World Economic Forum estimates that **25% of a company's market value can be directly related to its reputation.**

In this age of prevalent cyber risk, upholding your brand’s reputation is even more important. Customers, partners, shareholders, and the broader public expect that companies are proactively doing all that they can to thwart attacks. This is especially imperative given the extent of consumers’ Personal Identifiable Information – including medical information and financial records – that companies are responsible for protecting. When headlines reveal corporate security leaders weren’t enforcing routine security hygiene and left points of entry exposed, consumer confidence in the brand takes a serious hit – and customers go elsewhere as a result.

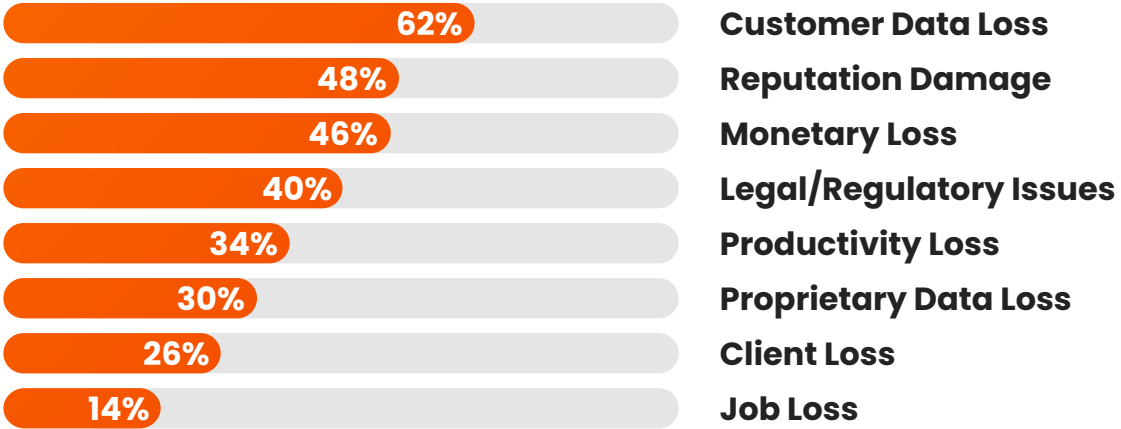


In fact, **“62% of Americans report that they will stop spending with a brand** for several months following a hack or breach”.



A similar study from PricewaterhouseCoopers found that **87% of consumers are willing to take their business elsewhere** after learning that a company has been breached.

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



Many security leaders already recognize the importance of protecting customer trust and loyalty. In a study from Censys, loss of customer data and reputation damage were seen as the two outcomes that would have the highest degree of damage to their organizations.

Though security leaders may recognize the importance of maintaining brand reputation and customer trust, it ultimately comes down to understanding what it takes to reduce the likelihood of an attack.



How Exposure Management Can Help:

In addition to reducing the likelihood of a breach with continuous attack surface visibility, the use of an Exposure Management solution can bolster stakeholder confidence. Your security team can communicate to its customers, partners, and others that you're relying on advanced, proactive security solutions that allow you to stay a step ahead of threat actors – and not just looking for unknown assets when your security team has extra time. Showing that you're doing all you can to prevent a breach will grow trust and confidence in your brand.



Risk #3

Lack of visibility into critical assets



Organizations that don't invest in Exposure Management don't have visibility into their critical assets, thus creating opportunities for breach and theft.

As defined by [CISA](#), critical assets are “the organizational resources essential to maintaining operations and achieving the organization’s mission.” Think about the servers that power your organization’s proprietary software product, or the certificates that protect your financial data. A breach of these critical assets due to gaps in monitoring could mean business comes to a sudden halt. **These assets therefore demand more than monthly, bi-weekly, or even weekly monitoring to be completely secure from cyberattacks.**

For companies in industries like energy, utilities, and other critical infrastructure sectors, continuous, automated detection and management can be essential for protecting systems integral to a functional economy and national security. The importance of Exposure Management in these sectors has been increasingly highlighted by the federal government, which recently mandated that all federal agencies and systems perform an automated asset discovery every 7 days across all of their IPv4-based assets.



How Exposure Management Can Help:

Automated solutions, like Censys Exposure Management, provide continuous monitoring of critical assets to an extent that manual efforts and other tools can't match. Censys serves as a system of constant vigilance that automatically notifies security teams when a risk is detected, while providing context into the risk's level of severity and recommendations for remediation.

Risk #4

Increased spend due to cloud sprawl & Shadow IT

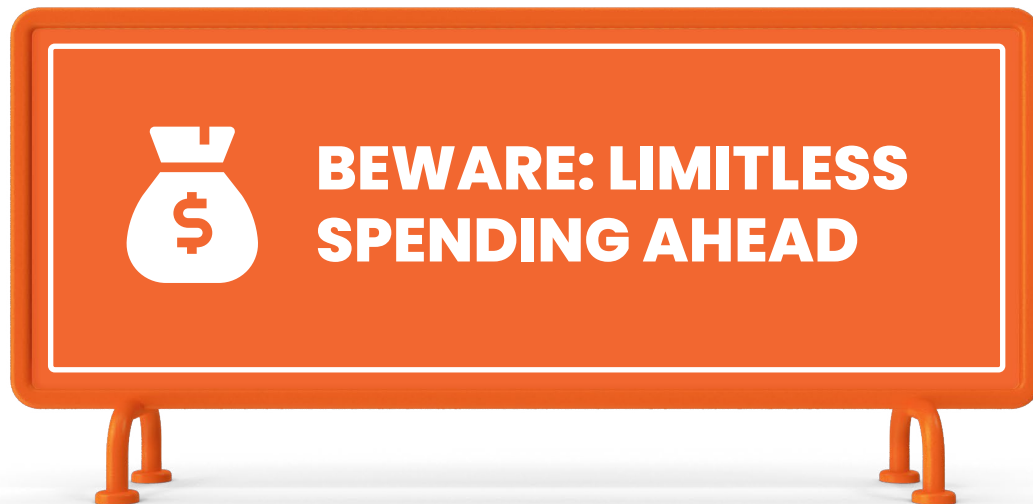


Lack of visibility into all of your assets also means you might be paying for services you aren't aware of and don't need. These hidden assets often live in the cloud or fall into the category of "Shadow IT" – digital assets created without the knowledge of IT or security.



Cloud Sprawl

Cloud sprawl is a particularly relevant issue for companies to address given that recent studies show enterprises waste one-third of their budgets on under-used or unused cloud resources. Consider: where else your organization could invest that misappropriated 30%?



Multi-cloud environments can make it challenging for security teams to track and manage everything they own across all of their cloud instances. We see evidence of just how expansive companies' hosting footprints can be in our own research. When examining attack surfaces for a sample of 37 large organizations, **Censys discovered these organizations have, on average, presence in 17 different hosting providers** (including cloud, datacenter, and on-premises equipment). In addition to multiple hosting providers, other research has found that the average company has more than 900 unknown cloud services. Discovering and monitoring an organization's presence across this many cloud services is a near impossible task for teams relying on traditional approaches.

Shadow IT

Shadow IT poses similar challenges and costs. More than 80% of employees surveyed by McAfee admit to using unapproved SaaS resources while on the job, and a [study from Gartner](#) found that 38% of technology purchases are managed, defined, and controlled by business leaders rather than IT. Even the most well-intentioned team members in the org will occasionally forget to let IT know that they've logged into a new SaaS app from their work account, or are accessing company sites on a personal computer. Be that as it may, getting a handle on Shadow IT can save significant expense. **Gartner found that Shadow IT comprises 30-40% of IT spending in large enterprises.**



How Exposure Management Can Help:

Continuous asset discovery brings the scope of your cloud sprawl into a single perspective and shines a light on Shadow IT hidden from view. With a full picture of what your organization owns, you can take action to eliminate or decommission these unneeded assets, and save significant operational expenses in the process. Uncovering cloud sprawl and Shadow IT also creates opportunities to reinforce proper security protocols to team members across the organization.



Risk #5

Inefficient use of security resources



Your security team is made up of talented professionals with the expertise to focus on strategic security initiatives. That means they provide the most value when they can work on higher-order tasks, like integrating threat intelligence into security processes or conducting complex root cause analyses. Yet, without an automated Exposure Management solution, these team members are likely still spending time on recurring, redundant asset discovery and threat monitoring efforts that underutilize their capabilities.

Consider that at 43% of organizations, manual asset discovery takes more than 80 hours, and is typically conducted weekly, bi-weekly, or on a monthly basis. That's two weeks of effort from a full-time security practitioner, with an outcome that still yields gaps in visibility.

At Censys, we often hear about these kinds of inefficiencies when speaking with customers. For example, [this European government agency](#) shared that prior to adopting Censys EASM, their security team relied on a variety of disparate traditional security tools and OSNIT techniques, and as a result, asset enumeration tasks took them nearly a full week to complete. After implementing automated EASM, **they reduced time spent on enumeration to just 20 minutes.**





"I have more time to keep on digging instead of doing the basics first. It's a timesaver in a way that is huge."

Senior Security Analyst

European Government Agency

Without Exposure Management, your team might also be wasting unnecessary effort attempting to understand assets, associated risks, and their levels of severity. Analysts might detect unfamiliar assets tied to the organization, but lack the level of data needed to determine where the assets came from and if they pose any significant risk. In turn, time is spent going down rabbit holes and making assumptions.



How Exposure Management Can Help:

Exposure Management solutions will automatically display multiple data points about a newly-discovered asset so that analysts don't have to spend time hunting for information on their own.

An Exposure Management solution will also automatically detect risks and alert security teams when risks are identified. Risk notifications include context about the risk's level of severity and recommendations for how to remediate.



Censys provides risk detection for over 120 different asset types, with actionable remediation recommendations to eliminate or mitigate each risk.

Let Exposure Management Reduce Your Risk

Though attack surfaces have become increasingly complex, it doesn't mean they can't be successfully defended from advanced threats. When security leaders invest in a leading Exposure Management solution, they not only reduce their organization's risk of an attack, they reduce the likelihood of a number of other downstream risks to the business – including financial instability, loss of brand reputation, lack of visibility into critical assets, money wasted on cloud sprawl and shadow IT, and inefficient use of team resources.

Exposure Management is the only cybersecurity solution that's designed to comprehensively and continuously discover, monitor, and inventory the assets that make up your attack surface. With Exposure Management, your security team can manage its evolving attack surface with confidence, and better defend against attacks as a result.




Making the Right Investment with Censys Exposure Management


Start your search for the right Exposure Management solution with Censys. Censys offers the leading Internet Intelligence Platform for Threat Hunting and Exposure Management. Our Exposure Management platform includes [Censys External Attack Surface Management](#), a best-in-class EASM solution which empowers security teams to gain full visibility into their attack surfaces.

Enterprise organizations across industries turn to Censys for automated asset discovery, monitoring, and understanding to identify and remediate advanced threats and exposures. An outside-in view, or attacker's perspective, of every asset and exposure is refreshed daily, hourly, or on-demand, giving your organization near-real time visibility and context so you can manage and communicate your cybersecurity posture. Your external attack surface is also assessed for risks and each is prioritized by what is important to you.




What Makes Censys the Leading Exposure Management Solution?


 **Total External Attack Surface Discovery:** Whether assets are known or unknown, leverage Censys's comprehensive dataset to discover critical exposures and mitigate risks, while embedding best practice monitoring into your security operations. Censys touches every device on the internet every 2-3 minutes.


 **Attribution Engine:** Get a complete and automated view of your organization's perimeter using the Censys Attribution engine. Seed data is used to establish high confidence connections to discover internet assets. Our attribution algorithm increases customers visibility up to 80%.




 **Risk Triage and Prioritization:** Each asset in the attack surface is updated daily and measured against 300+ different risk fingerprints to determine the severity of security weaknesses that are discovered. Severity is based on impact, exploitability, and likelihood, making priorities clear.



 **Risk Context and Remediation Guidance:** We focus on simplifying security decisions with rich and precise risk context to facilitate specific remediation guidance. Details of the type and potential security impacts of each discovered risk are provided, along with recommended steps for remediation.

 **Rapid Response:** Censys fingerprints and prioritizes putting emergency vulnerabilities into our platform as risks, often within 24 hours of the vulnerability disclosure.

 **Dashboards & Interactive Reporting:** Censys aggregates raw attack surface telemetry into easy-to-understand dashboards and trends that quickly enable security teams to determine and report on the overall state and security of your organization's attack surface.

 **Cloud Connectors:** Benefit from easy-to-use, vendor agnostic integrations with cloud providers.



The one place to understand everything on the internet.

Censys is the leading Internet Intelligence Platform for Threat Hunting and Exposure Management. We provide governments, enterprises, and researchers with the most comprehensive, accurate, and up-to-date map of the internet to defend attack surfaces and hunt for threats. Censys scans 45x more services than the nearest competitor across the world's largest certificate database (>10B), reducing the likelihood of a breach by 50%.

Founded by the creators of ZMap, trusted by the U.S. Government and over 50% of the Fortune 500, Censys' mission is to be the one place to understand everything on the Internet.

hello@censys.com

www.censys.com

