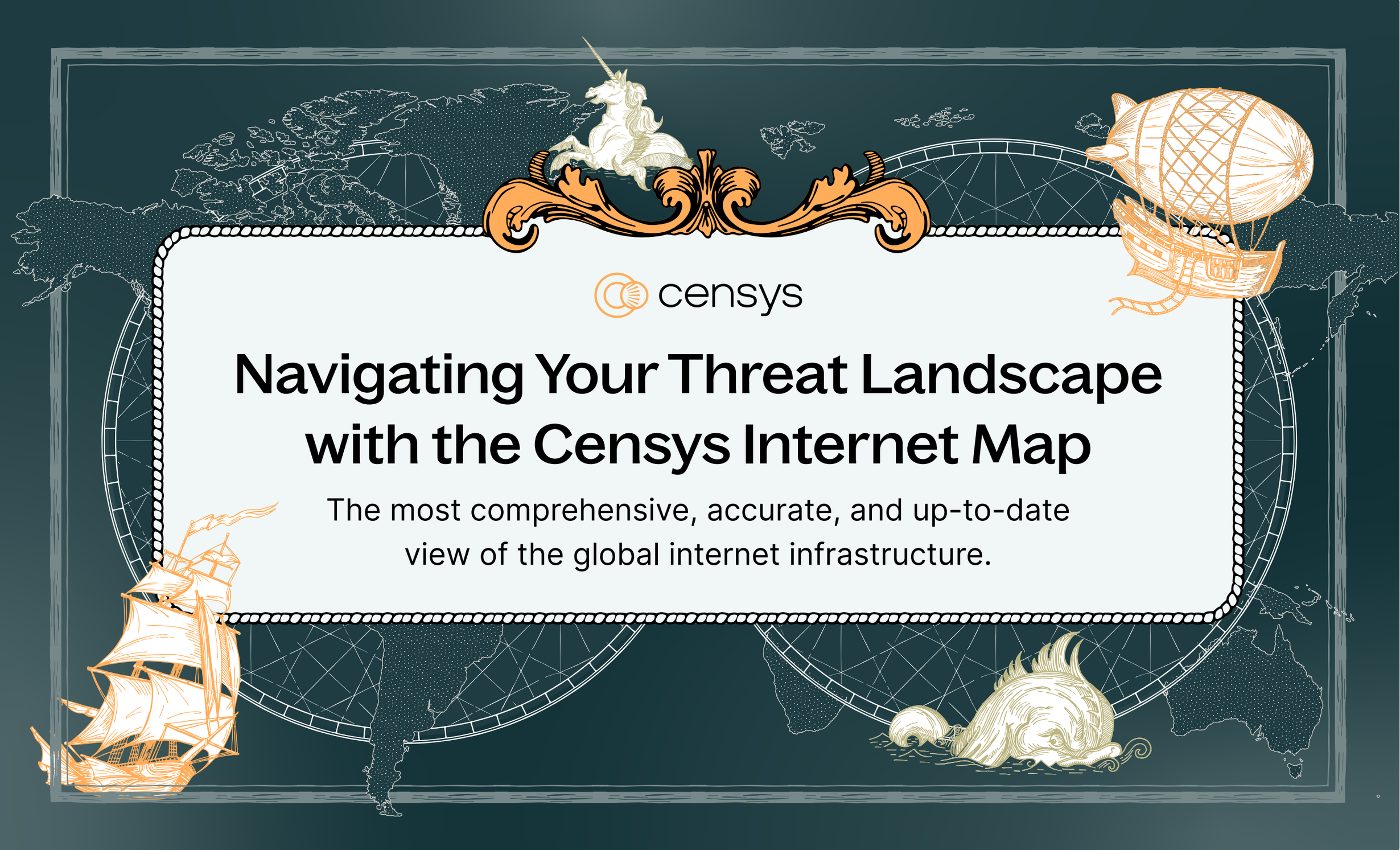


censys

Navigating Your Threat Landscape with the Censys Internet Map

The most comprehensive, accurate, and up-to-date view of the global internet infrastructure.

The Need for a Single Source of Ground Truth

Your cybersecurity strategy is only as good as the data that drives it. Complete, accurate, and real-time visibility of hosts and services on the global internet is essential for navigating an increasingly complex threat landscape. Anything less puts you at a disadvantage against threat actors.

Cybersecurity Teams Struggle with Subpar Internet Intelligence... and It Shows.

Internet intelligence guides almost every decision that cybersecurity teams make. Which risks should we prioritize first? Where should we look for threats? How is our attack surface changing over time? How well teams answer these questions depends on the quality of internet intelligence they have at hand. The better the intel, the faster and more successfully they can defend against current and future threats.

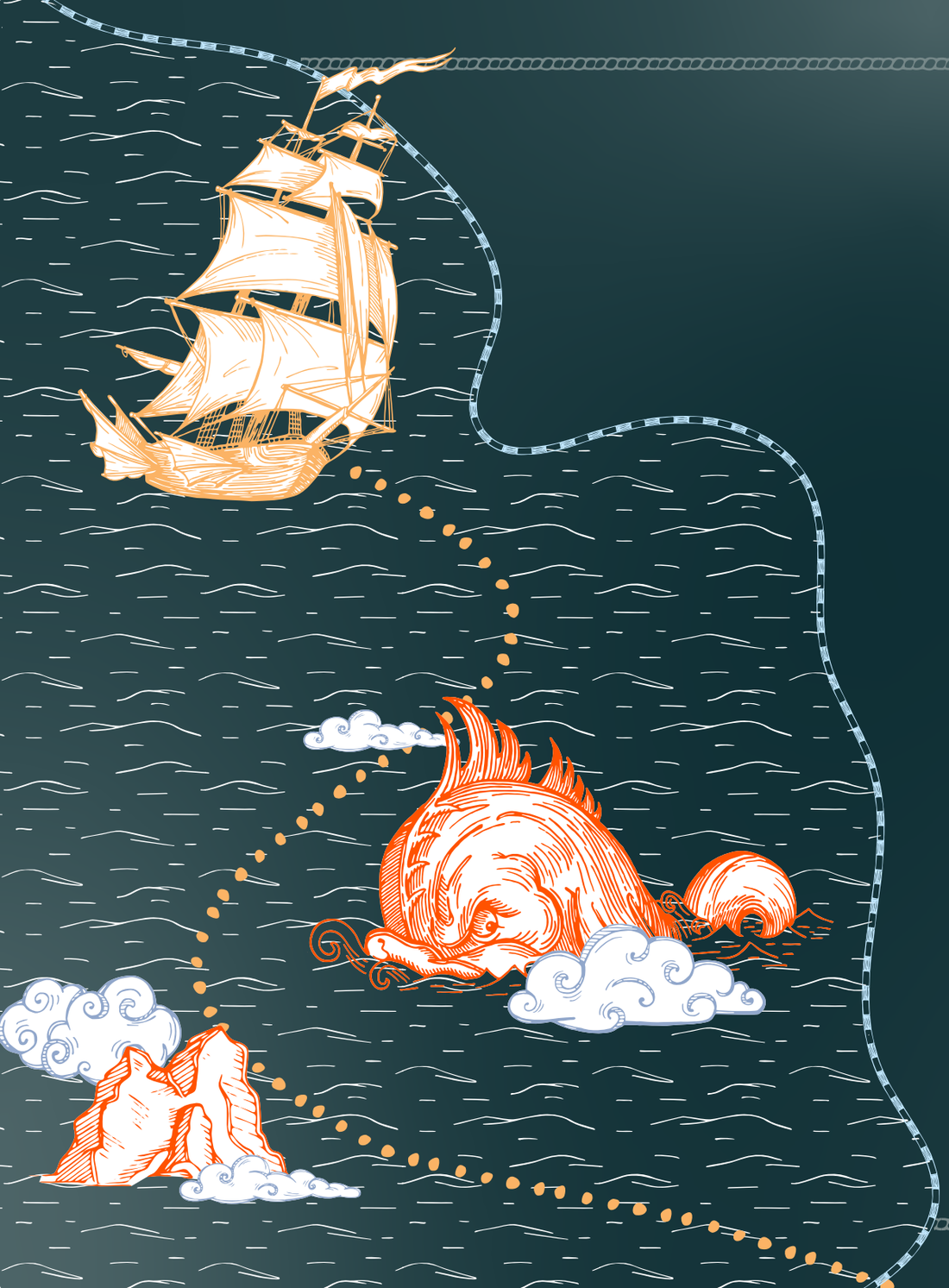
So how good is the internet intelligence that informs your team's decisions? If your answer sounds something like "good enough," consider this: the *2023 State of Security Leadership Report* found that **93% of surveyed security leaders said they had been successfully breached by a cyberattack within the last 12 months. Of those, 53% said they'd been successfully attacked 2-5 times**. Cybersecurity leaders and their teams are clearly struggling to identify and understand threats before adversaries take action. Without a trusted source of internet intelligence to act upon, teams are often left with too little, too late.

Though there are countless sources of internet intelligence on the market, not all are created equal. In fact, **the visibility these sources offer into internet infrastructure and threat intelligence almost always misses the mark**. Incomplete and outdated data streams offer only a partial view of the global internet. In today's aggressive threat landscape, data that's refreshed on a weekly or intermittent basis, with coverage that doesn't extend across all 65K ports with no context or enrichment, simply doesn't cut it.

Why “Good Enough” Data Isn’t Good Enough

Cybersecurity teams that hope to get by with incomplete, inaccurate data sign themselves up for extra time, effort, and frustration – along with significant security gaps.

- **Valuable resources are spent filling in the blanks:**
  What data streams can’t provide, teams have to source for themselves. This often means additional hours spent every week compiling, sifting, filtering, analyzing, and verifying disparate data streams for accuracy. This increases fatigue on already strapped teams and leaves blind spots open for exposure.
- **Noisy alerts and false positives waste time:**
  False positives are an inevitable byproduct of inferior data. That “malicious” alert you received about supposed malware? Turns out it wasn’t malware after all. But while you were digging into that false positive, an actual critical vulnerability to your network was lost in the noise. Poor data makes it difficult to understand and prioritize risks. Out of 500 DevSocOps professionals surveyed in 2022, 94% report false positives in vulnerability reports, while 67% find them often or all the time, according to InfoSecurity Magazine.



- **Exposures and vulnerabilities are missed:**
  If you don't have a full picture of your assets, you can't address the exposures and vulnerabilities to which they may be susceptible. Security leaders know they have work to do on this front. Those surveyed in the Censys *2023 State of Security Leadership Report* say understanding the entirety of their attack surface is their number one priority for the next 12 months. Comprehensive, global internet intelligence makes it possible to uncover everything that's associated with your attack surface, including assets your team doesn't know about.
- **Threat actors are simply working faster:**
  Cyber adversaries are scanning the internet about once an hour to find vulnerabilities on enterprise networks. That means hunting down emerging threats and quickly detecting compromise hinges on a near real-time view of the threat landscape. If you're looking at data that was pulled last night, last week, or worse yet, last month, you're missing the threats you're at risk for right now.
- **Activity on non-standard ports is overlooked:**
  More than 60% of all services now run on non-standard ports. Without intelligent scanning across 65,000 ports and visibility into these services, you're ignoring significant terrain that could be home to advanced threat activity.

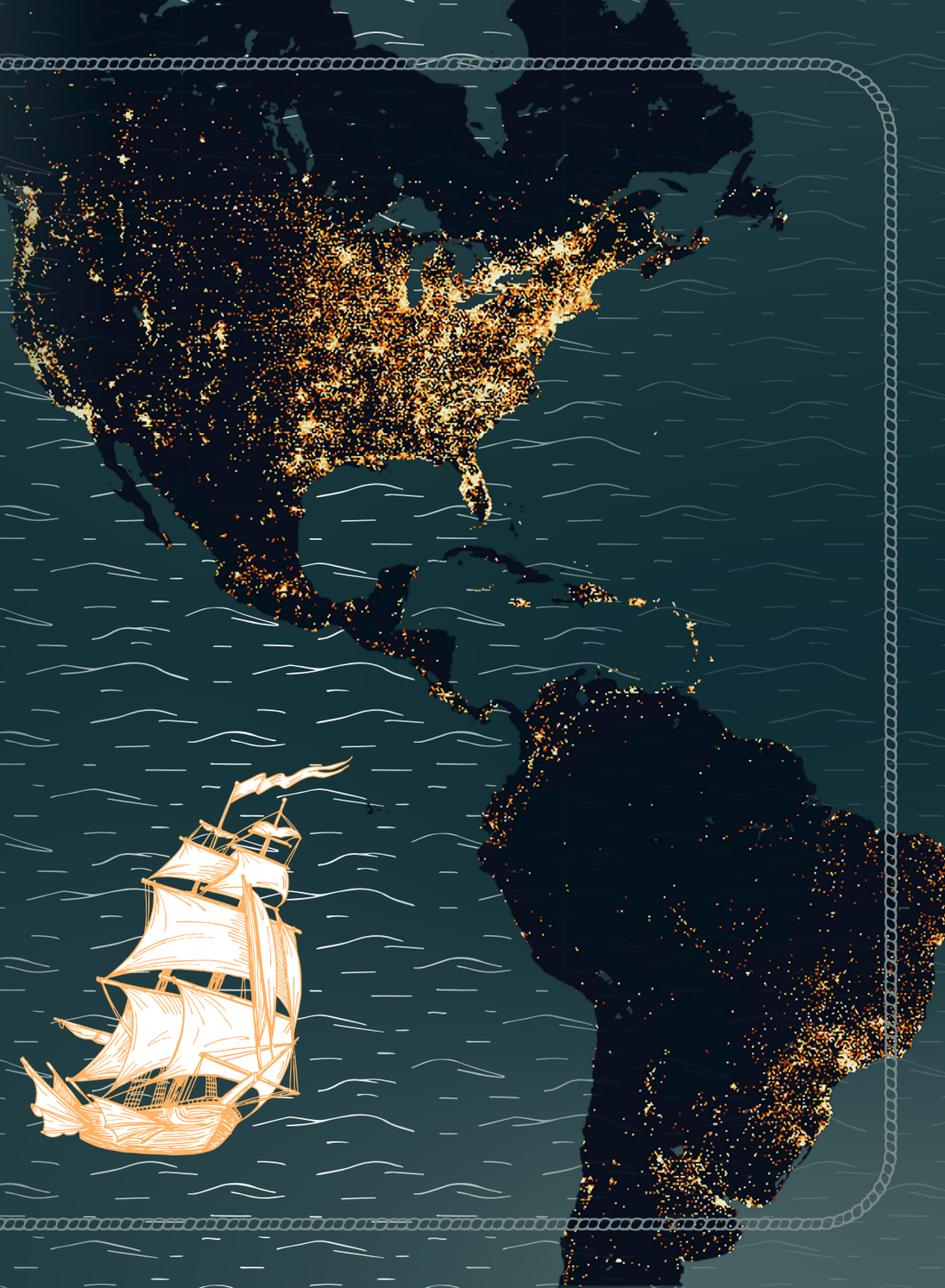
Superior Internet Intelligence Is an Indispensable Tool

To avoid these challenges, effectively secure complex digital environments, and understand emerging threats, **organizations need a single source of accurate internet intelligence**. They need advanced internet intel that provides visibility into all public hosts and services on the internet, enriched with context to identify both internal risks and external threats. This kind of robust, ground truth internet intelligence can not only separate essential alerts from the noise and reduce false positives, but enable security teams to intelligently prioritize and act on threats before it's too late.

And that's exactly why, at Censys, we've raised the bar to provide enterprises, governments, and researchers with **the best source of global internet infrastructure available, period**.

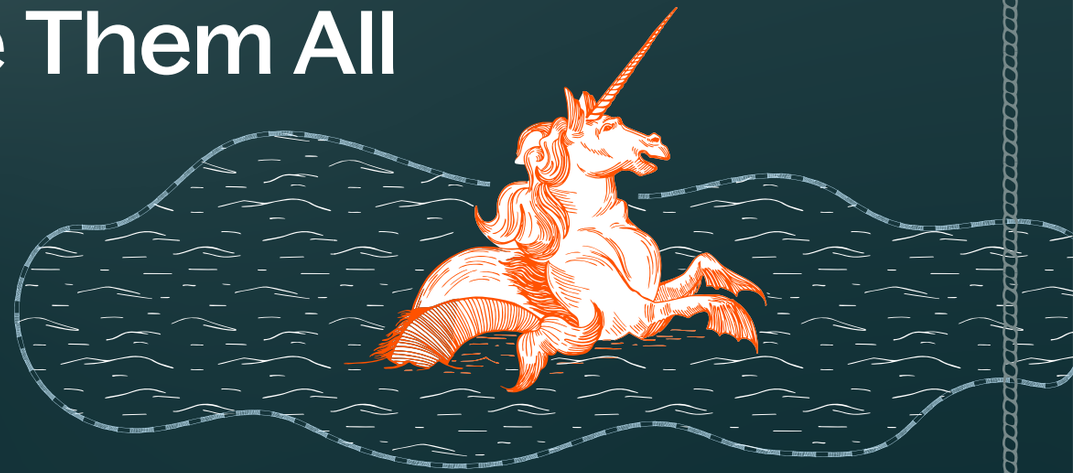
Meet: The Censys Internet Map.

Let's talk about what it is, how it works, and why you can't stay ahead of threats without it.



NAVIGATING YOUR THREAT LANDSCAPE WITH THE CENSYS INTERNET MAP

The One Internet Map to Rule Them All



The Censys Internet Map is the most comprehensive, accurate, and up-to-date collection of global internet infrastructure available, enriched with critical context to empower your security and intelligence teams.

Founded by the creators of ZMap, our proprietary Internet Map offers the fastest discovery and best coverage of internet hosts and services, as well as the deepest insights available about the infrastructure on the internet. Censys' Internet Map powers both our Exposure Management and Search products.

There's simply no better view of the global internet available. When independently compared to other internet intelligence sources, Censys data is identified as superior (keep reading for more on this).

It's More Than Just Internet Scan Data

Unlike other data sources, the Censys Internet Map offers a **deep, contextualized, attributed internet infrastructure map that supports multiple use cases**. We don't just collect banners or detect service presence, we create a structured snapshot of every host and running service down to the protocol level. We enrich the dataset with running software, TLS configurations, and so much more. Through our comprehensive scanning and multiple layers of enrichment, our Internet Map is the most powerful source of internet infrastructure available to support your intelligence-driven workflows.

How It Works

Three layers create a global internet map capable of powering any downstream use case. These layers are:

1. A comprehensive collection of ground truth internet scan data
2. Enriched metadata to make sense of every host and service on the internet
3. High-fidelity attribution provides intelligence about the organization and threats

To build out these layers, we focus on superior functionality in terms of both coverage and context.

Coverage

Users gain access to the most comprehensive and up-to-date visibility of hosts and services on the global internet. The Censys Internet Map:

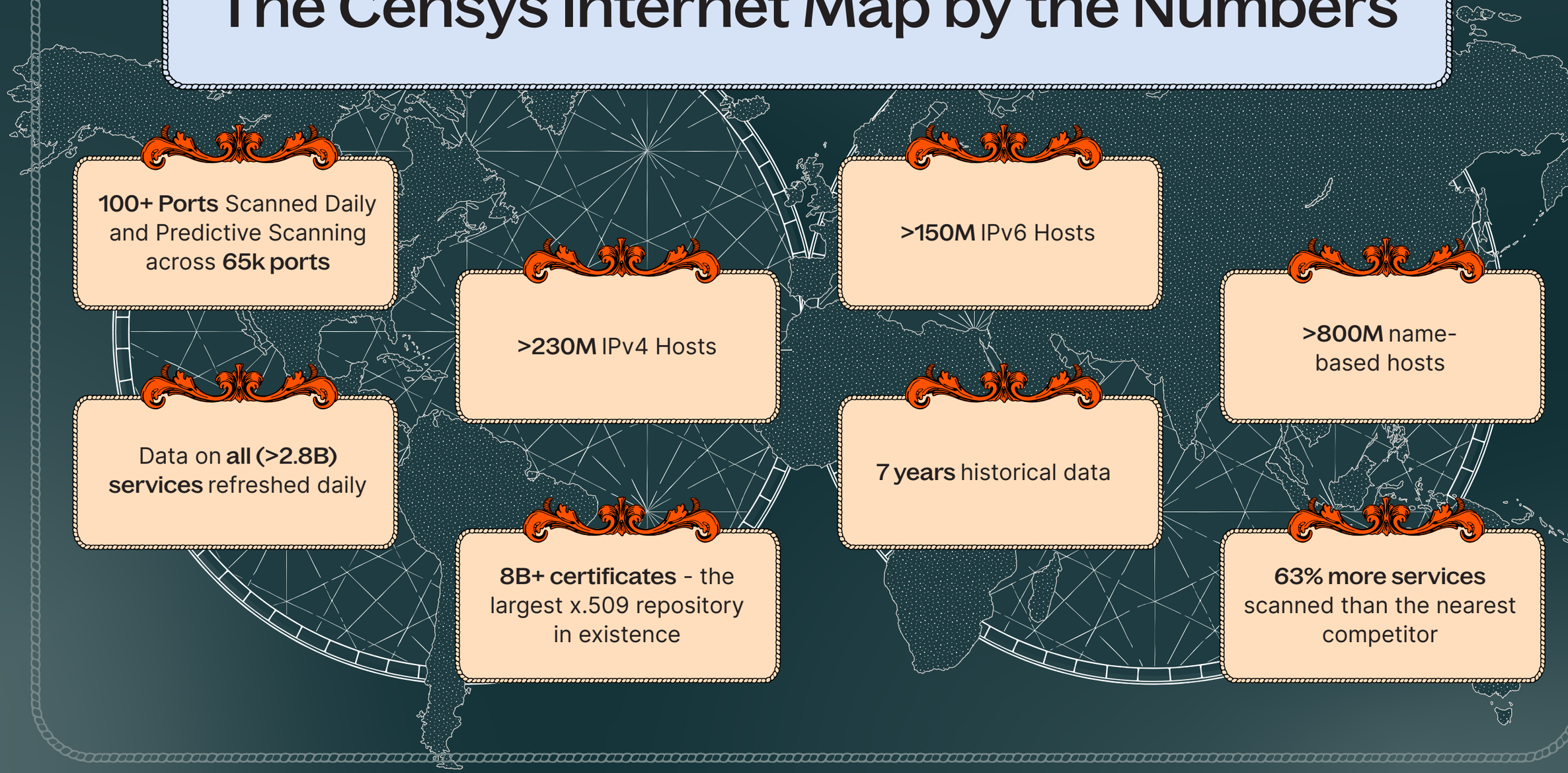
- Provides multi-perspective scanning from 7 Tier-1 ISPs
- Identifies and scans websites by name, providing complete visibility into HTTP-based exposure and vulnerability
- **Is the only vendor conducting daily comprehensive scans of the top 100+ ports and proprietary ML-based discovery of services across all 65k ports**
- Provides ~100 Deep Protocol Scanners and Automatic Protocol Detection to identify services running on unassigned ports
- Prioritizes cloud scanning to capture ephemeral cloud services

Context

Data is enriched with detailed context to identify host types and understand how assets are connected and configured. The Censys Internet Map provides:

- Detailed visibility into open ports and running protocols, regardless of standard port assignment, to understand host intent (**Censys is the only vendor to do this**)
- The **world's largest x.509 certificate database** to identify related infrastructure and suspicious hosts
- Geolocation data to understand where a host resides
- Configuration and registration data to understand and determine ownership
- Software detection to identify potential threats, risks, and vulnerabilities
- Device type labels to clearly identify host type (i.e. IoT, Database, VPN, etc.)

The Censys Internet Map by the Numbers



100+ Ports Scanned Daily and Predictive Scanning across **65k ports**

>230M IPv4 Hosts

>150M IPv6 Hosts

>800M name-based hosts

Data on **all (>2.8B) services** refreshed daily

7 years historical data

8B+ certificates - the largest x.509 repository in existence

63% more services scanned than the nearest competitor

Using the Censys Internet Map to Solve Your Security Challenges

The Censys Internet Map is designed to support a wide range of downstream use cases for enterprise organizations across industries, governments around the world, and researchers in academia. These users typically leverage our Internet Map data to address some of their most critical cybersecurity objectives, including:

1. Gaining full visibility into their attack surface
2. Protecting the organization against emerging threats
3. Understanding and staying ahead of an evolving threat landscape
4. Empowering security teams to act fast
5. Monitoring M&A risk and managing subsidiaries
6. More efficiently leveraging security resources

To support these objectives, our Internet Map data is made available through two Censys solutions: Censys Exposure Management and Censys Search. Our proprietary map data is the foundation upon which each is built.

Let's look at some of the most common ways Internet Map data is put to use through these two solutions.

Censys Exposure Management

Access the critical information your team needs to continuously discover, understand, communicate, and automate the management of its internet-exposed assets, so that you can better defend against advanced threats. Censys Exposure Management supports a number of specific use cases, including:

Top Use Cases

- **External Attack Surface Management (EASM):** Ensure your entire attack surface is always secure with a near real-time, attacker-centric view of all of your external-facing assets on the internet and cloud. Continuously discover, manage, and protect your rapidly-growing attack surface in today's evolving threat landscape. Benefit from complete visibility, >95% attribution accuracy, and 63% more services scanned than the nearest competitor.
- **Cloud Asset Discovery:** Gain a centralized and complete exposure inventory across your entire cloud environment. Vendor agnostic cloud connectors provide a centralized view of all assets, so that you can understand your total cloud footprint, identify and eliminate Shadow Cloud accounts, move cloud assets to managed environments, and monitor assets for vulnerabilities.
- **Exposure & Risk Management:** Discover known and unknown exposures to mitigate risks and reduce breaches by up to 50%. Teams can aggregate, prioritize, and remediate advanced threats and exposures with the most comprehensive dataset available.
- **Security Framework & Compliance:** Noncompliance can have devastating results for you and your customers. Stay ahead of the curve and up to date with evolving standards, such as NIST and the Biden Executive Order, with the complete visibility, context, and tools you need to be compliant.
- **Merger, Acquisition & Subsidiary Risk:** Inherited risk can hinder your growth strategy and expose your organization. Organizations use the visibility provided by Censys Exposure Management to instantly evaluate potential risks during the M&A due diligence process. In doing so, they eliminate the need for special asset discovery projects while shortening time spent on due diligence by 40%.

> "With Censys we found out that we had a lot more externally visible assets. We thought 'oh, it's probably under 5,000 assets' and it was double that. Since implementing Censys we closed over 5,000 high risk issues."
>
> – Senior Security Engineer, Cloud Communications

Censys Search

Proactively protect your organization against advanced threats with access to best-in-class data from the Censys Internet Map, made available through the query-based Censys Search tool. Censys Search enables security teams and threat hunters to more successfully pursue tasks like identifying malicious command and control infrastructure, locating vulnerabile or compromised hosts, remediating risks to prevent further compromise, and strengthening their overall security posture.

Top Use Cases

- **Threat Hunting:** Proactively identify, profile, and detect threats from today's most sophisticated cybercriminals with access to the most complete, accurate, and updated data about our global internet infrastructure. Use Censys Search to enrich internal threat feeds with host and certificate data, or to identify advanced persistent threats (APTs) with nation-state actors in order to gain insights on network infrastructure.
- **Security Operations:** Effectively prioritize and triage security events and mitigate threats to your network with ground-truth infrastructure data. Comprehensive, accurate, and near real-time data that can be contextualized with parsing and indexing gives users rich context about the threats and events teams need to address.
- **Incident Response:** Quickly and confidently investigate and mediate security incidents with an attacker's outside-in perspective. Use Censys to search for hosts vulnerable to a new or existing vulnerability across the entire internet. Many teams use Censys Search queries to learn more about CVEs and respond to zero-days.
- **Research and Reporting:** Analyze historical and emerging threats, patterns, and changes in the internet to improve your security and policies. Use the 7+ years of historical data available in Censys Search to create a timeline of adversary infrastructure or track the history of a compromised or suspicious host.
- **Pentesting:** Identify potential exposures, gather information for reconnaissance, and conduct vulnerability assessments to evaluate potential risks during the M&A due diligence process. In doing so, they eliminate the need for special asset discovery projects while shortening time spent on due diligence by 40%.

> **"The powerful search functionality and extensive historical data made Censys great to use for attribution. Censys is used in almost every investigation we do."**
>
> - Bill Marczak, Research Fellow at Citizen Lab

Unique Capabilities to Help You Stay Ahead of Threats

The Censys Internet Map's advanced functionality gives teams distinct advantages they can use to better defend against adversaries. With unique capabilities like machine learning-based predictive scanning and daily smart refreshes, security teams can gain an unparalleled view of the global internet that allows them to better understand the threat landscape.

ADVANTAGE #1

Machine Learning-Based Predictive Scanning

ADVANTAGE #2

Automatic Protocol Detection

ADVANTAGE #3

Parsed & Indexed Protocol Fields

ADVANTAGE #4

Daily Smart Refreshes

ADVANTAGE #1

Machine Learning-Based Predictive Scanning Allows You to See All Running Services

The Censys Internet Map's advanced Predictive Scanning capability provides intelligent targeting of running services across 65k possible ports on every host. Predictive Scanning is the only research-backed scanning technique used to discover services across 65k ports. In particular, this capability provides greater visibility into services that are increasingly being run on non-standard ports.

Why do we care about non-standard ports? Not only are they where the majority of services (60%+) now live, **non-standard port assignment is also a common tactic that threat actors use to obfuscate exposure**. According to 2021 research from Stanford University, services on non-standard ports are more likely to be insecure.

The Censys Internet Map's Predictive Scanning adds over 107M new services to the nearly 3B global internet services we continuously monitor. Security teams can use this powerful data to improve operational impact, reduce false positives, and provide a substantial return on investment and risk reduction.

With Predictive Scanning, security teams gain more visibility into services like:

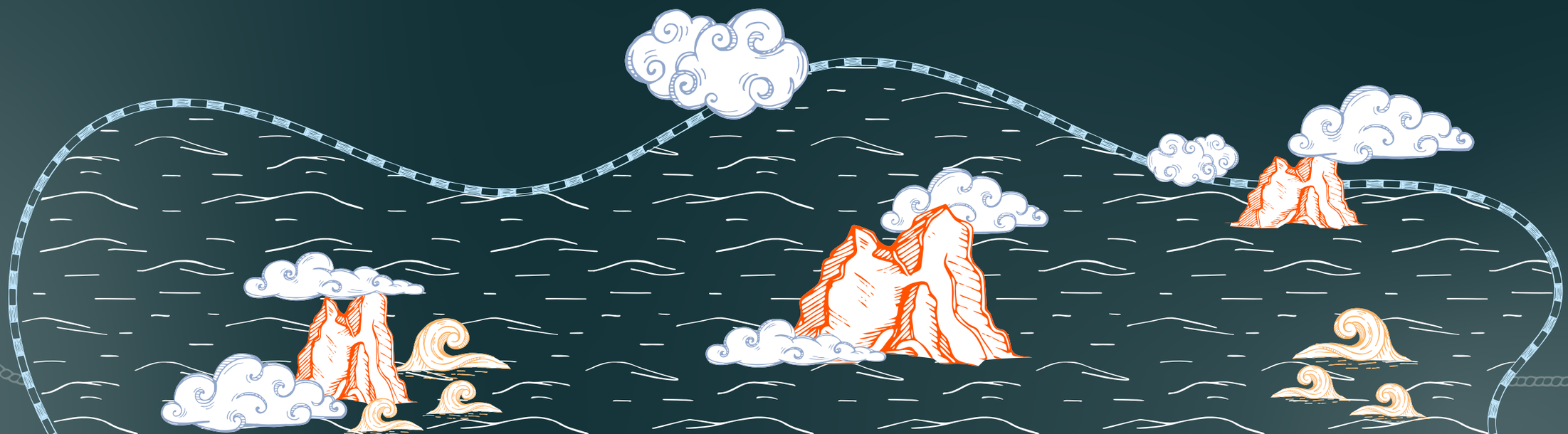
- **Services from Internet of Things (IoT)**, which businesses in industries like manufacturing, energy, and healthcare are leveraging for growth, but which also present high risk due to lagging security standards
- **Autonomous Systems** only running services on non-standard ports that attackers might utilize to host malicious infrastructure and hide from scanners
- **A massive proliferation of newer services** by vendors like online portals, data analysis tools, and business productivity enhancers that are especially popular in hybrid and remote environments that are typically run on high, non-standard ports

ADVANTAGE #2

Automatic Protocol Detection to Improve Visibility

Automatic Protocol Detection is a major differentiator that provides significant visibility into potential exposures by identifying the risky services run on non-standard ports that might not be visible through other tools. With Automatic Protocol Detection, **you can discover and mitigate risks with a more complete understanding of their external attack surface**, as well as gain a more comprehensive view of running services, regardless of port assignment, and in turn improve the quality of your threat investigations.

Other internet intelligence providers rely on standard port assignments to natively identify protocols (i.e. 443 = HTTP or 22 = SSH). However, this approach overlooks the reality that threat actors and network administrators often run services on non-standard ports (as discussed above). Automatic Protocol Detection from the Censys Internet Map, on the other hand, inspects application layer data and observes service behavior to identify the running service, giving you critical visibility into otherwise obfuscated risks.



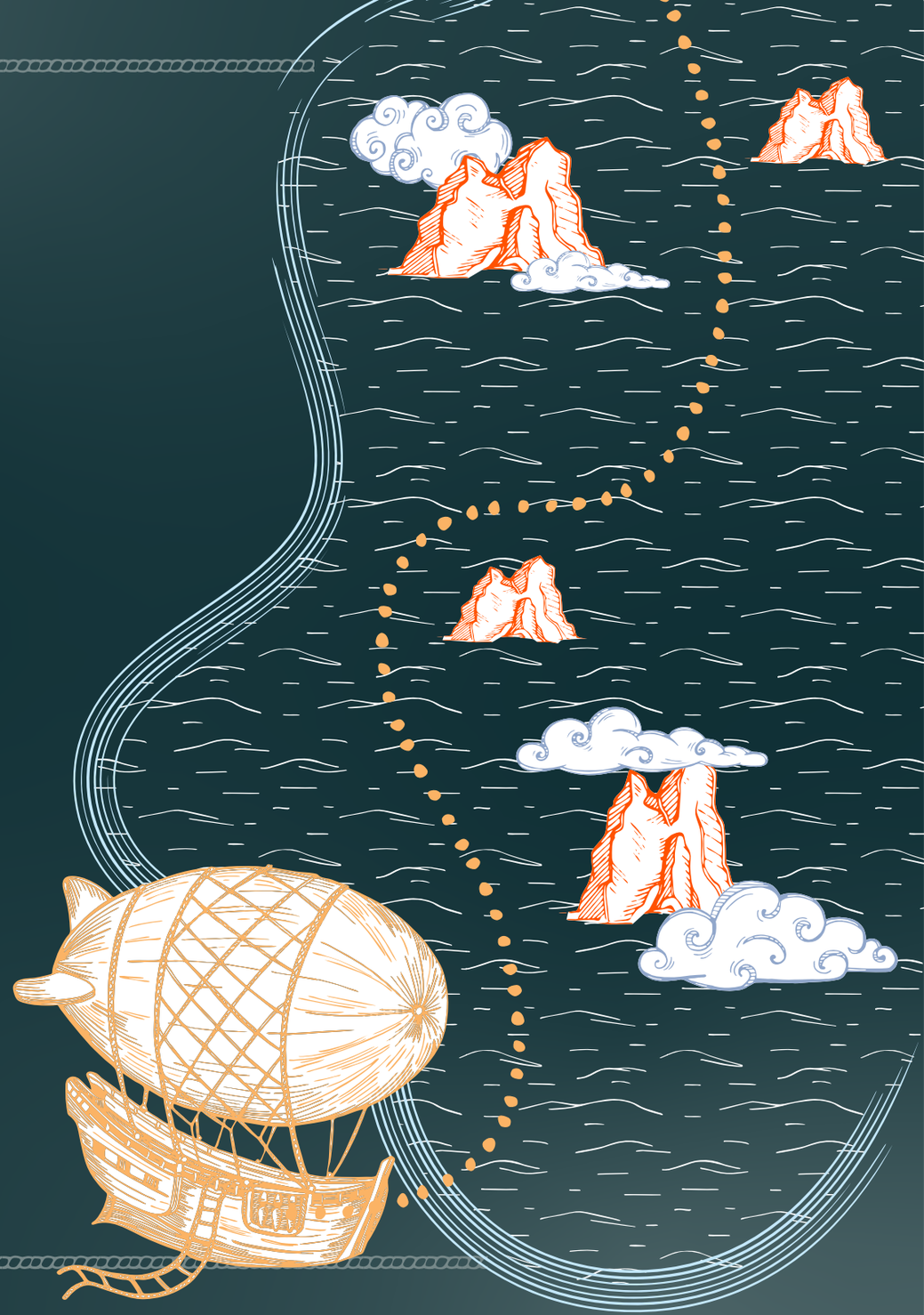
ADVANTAGE #3

Parsed and Indexed Protocol Fields Make It Easier to Respond to Incidents

The Censys Internet Map parses and indexes >2,000 fields in its scan results, providing detailed information about service configuration and vulnerability, as well as helpful metadata like DNS, Geolocation, and IP WHOIS.

Cybersecurity teams can use this data to "pivot" their investigations and understand asset relationships to more quickly conduct incident response. For example, a shared field value may reveal related infrastructure being used by attackers. These fields can also be used to understand who owns an asset and to more quickly remediate vulnerabilities or misconfigurations.

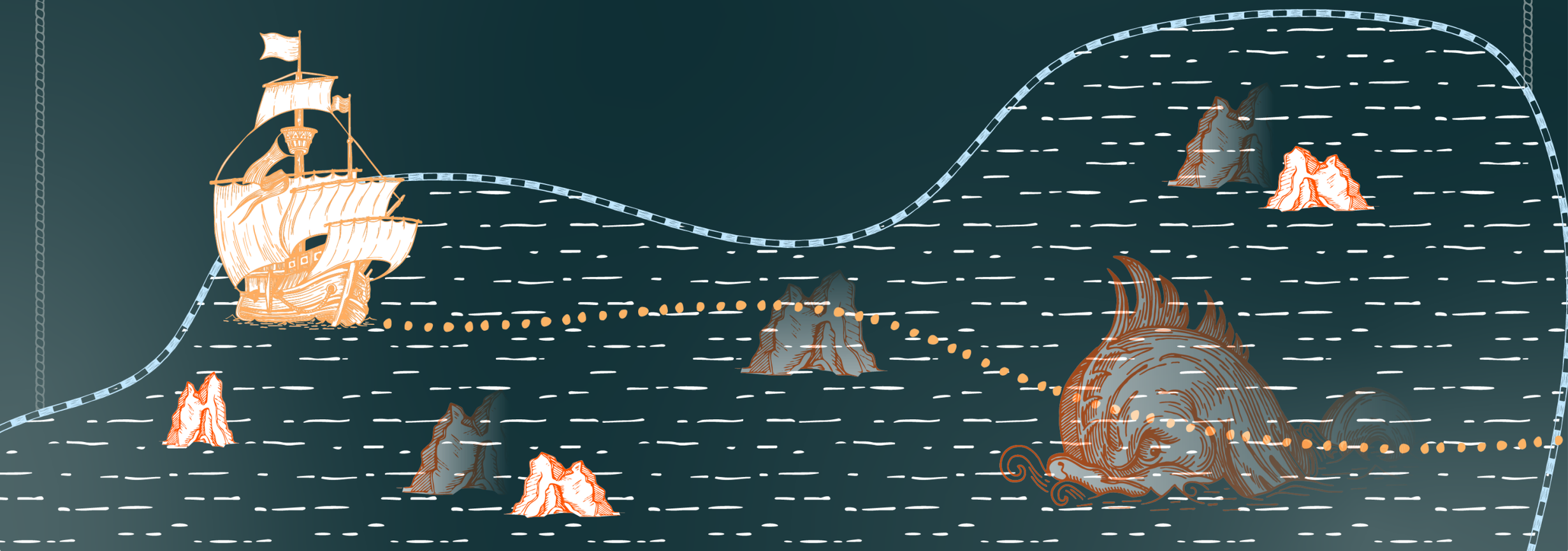
By parsing and indexing structured data (rather than simply providing raw banner data), Censys enables threat hunters to easily uncover patterns in attacker behavior and to track how services change over time. These changes are important to understand as they can highlight ownership updates, service reconfiguration, and compromise.



ADVANTAGE #4

Daily Smart Refreshes Reduce False Positives

False positives are one of the most prevalent and aggravating challenges that security teams with inferior data encounter. **More than 60% of security professionals estimate their security function spends over three hours per day validating false positives**, according to research from InfoSecurity Europe. The Censys Internet Map's Smart Refreshes capability conducts daily refreshes on all services in our dataset, to ensure that information about identified risks is accurate and up-to-date. This in turn significantly mitigates the likelihood of false positives. Research from Forrester Consulting found that the average Censys customer reduces their likelihood of false positives by 70%.



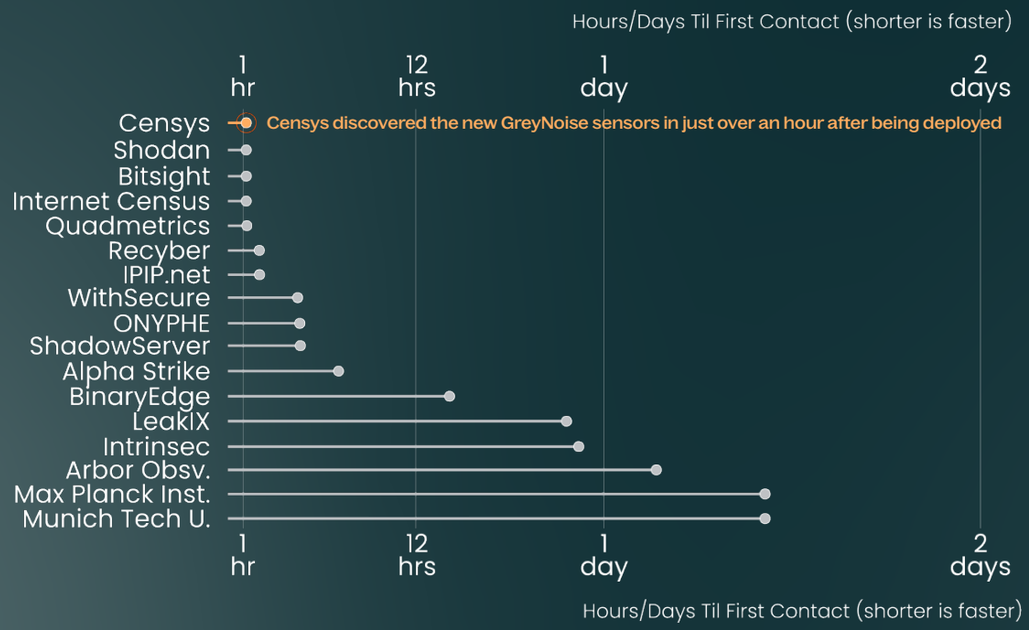
PROVEN SUPERIORITY FROM THIRD-PARTY RESEARCH

Don’t Just Take Our Word for It

The Censys Internet Map’s proprietary data has been independently verified to be the fastest, freshest, and most comprehensive when tested against other sources of internet data.

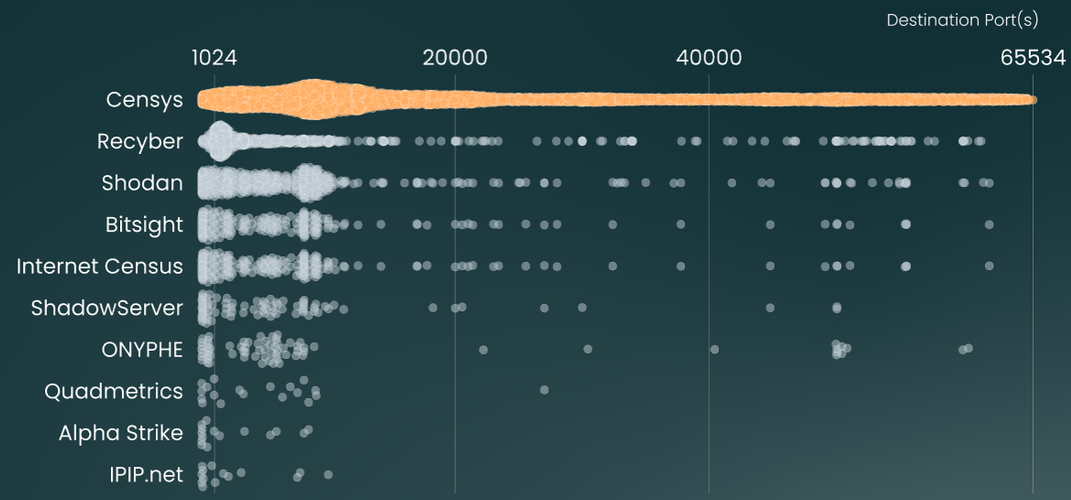
Faster Service Detection

In a study from GreyNoise Research, Censys was found to identify new nodes on the internet faster than any other source. When we consider just how quickly today’s adversaries are taking action, this kind of speed to detection is imperative.



More Comprehensive Coverage

In this same study, GreyNoise Research found that Censys surveyed significantly more internet services than others. Consider the scanning gaps observed from other providers – what nefarious activity might be present on these overlooked services? Censys’ Smart Refresh capability ensures that users are only notified of accurate, relevant activity.



Fresher Signals

Censys is the **only** vendor conducting daily comprehensive scans of the top 100+ ports and proprietary ML-based discovery of services across all 65k ports. This near real-time view is imperative for security teams considering that GreyNoise Research also found that unknown and possibly malicious entities on the internet are performing their own scans on a daily basis, probing for at best information and at worst opportunities to carry out exploits.

	Day 1	2	3	4	5	6	7
Censys	1,769	2,599	3,934	2,604	2,913	2,563	2,680
Shodan	127	171	143	122	1,816	225	318
Bitsight	178	275	265	220	211	221	217
Internet Census	178	275	244	220	210	221	217
Recyber	51	81	88	76	795	88	70
ShadowServer	30	68	43	52	56	37	42
BinaryEdge			40	4		82	9
IPIP.net	9	10	11	23	19	4	7
WithSecure	4	23	3	2	1	1	
Intrinsec			19	1	2	2	
ONYPHE	5	8	8	7	7	4	1

Delivering Real Value

Censys customers experience tangible benefits and concrete returns on investment. In a recent study on the Total Economic Impact™ of Censys, Forrester Consulting found that the average Censys customer experiences:

- 30% increase in security team efficiency
- 15% time savings through faster remediation
- 70% reduction in false positives on attack surfaces

When others independently evaluate Censys in action, they find what we've long known to be true: **our data really is the difference**.

Cybersecurity Teams Deserve World-Class Internet Intelligence

You can’t protect what you can’t see.

Or what you don’t understand, for that matter.

Yet, many cybersecurity teams have long been asked to do just that – and in their pursuit, have wasted countless hours sifting through disparate data streams, evaluating stale, inaccurate intel, and missing risks that traditional scanning sources can’t see.

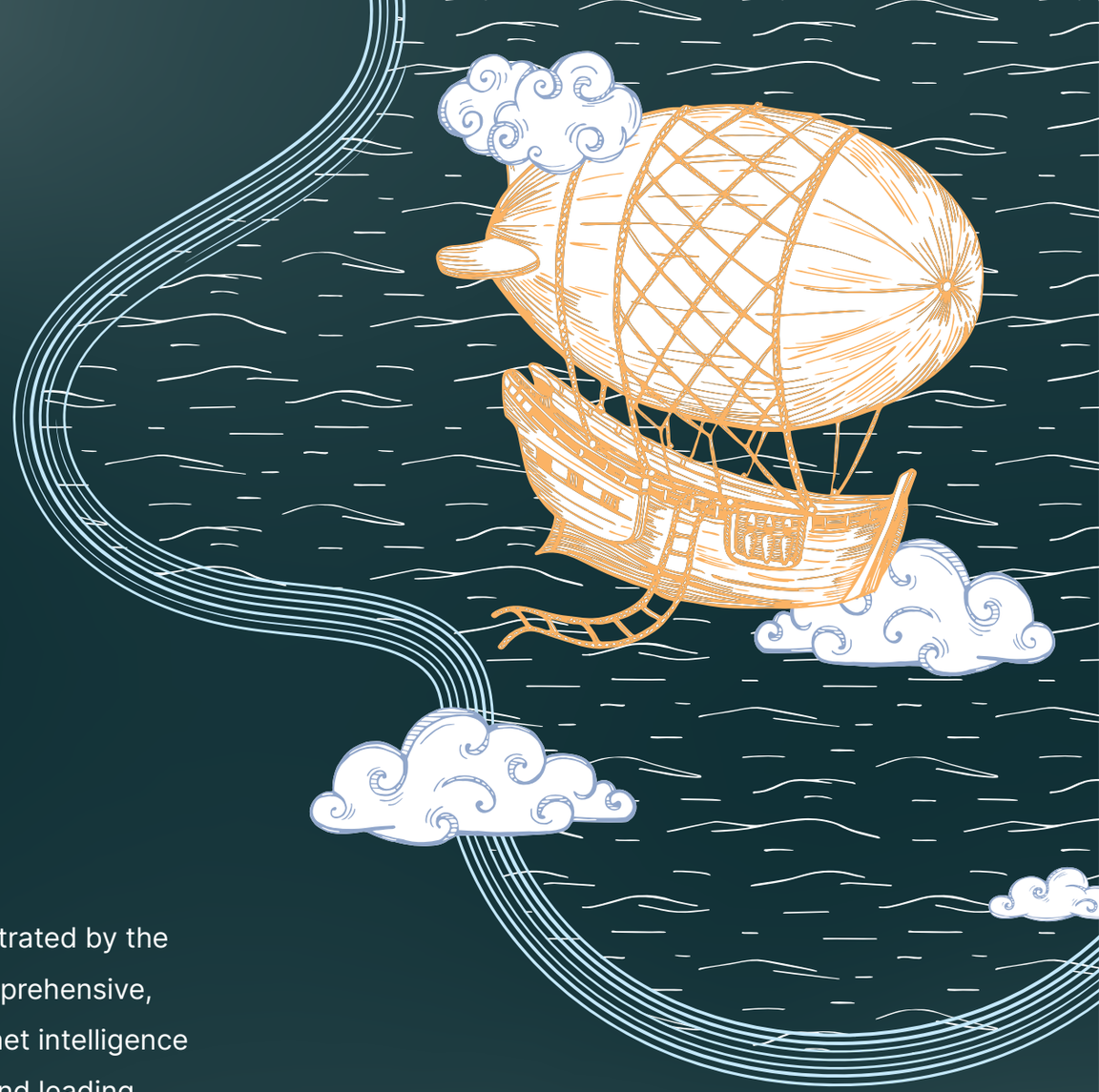
It’s time to do better. And we can.

As the best-in-class source of global internet infrastructure, the Censys Internet Map provides the most comprehensive, accurate, real-time, and contextualized view of the internet that is critical to cybersecurity teams’ defense against advanced threats. Our Internet Map is raising the bar on internet intelligence and revolutionizing how teams execute their cybersecurity strategies.

Join us - and say goodbye to time wasted on data that’s just “good enough.”

You can see Censys Internet Map data in action at search.censys.io.

To learn more about how the Censys Internet Map can advance your cybersecurity strategy, reach out to us at: www.censys.com/contact.



About Censys

Censys' mission is to be the one place to understand everything on the internet. Frustrated by the lack of trustworthy Internet intelligence, we set out to create the industry's most comprehensive, accurate, and up-to-date map of the Internet. Today, Censys delivers real-time Internet intelligence and actionable threat insights to global governments, over 50% of the Fortune 500, and leading threat intelligence providers worldwide.

hello@censys.com
www.censys.com