censys

How to Build a Business Case for Better Internet Intelligence

Cybersecurity Pros Need Good Internet Intelligence

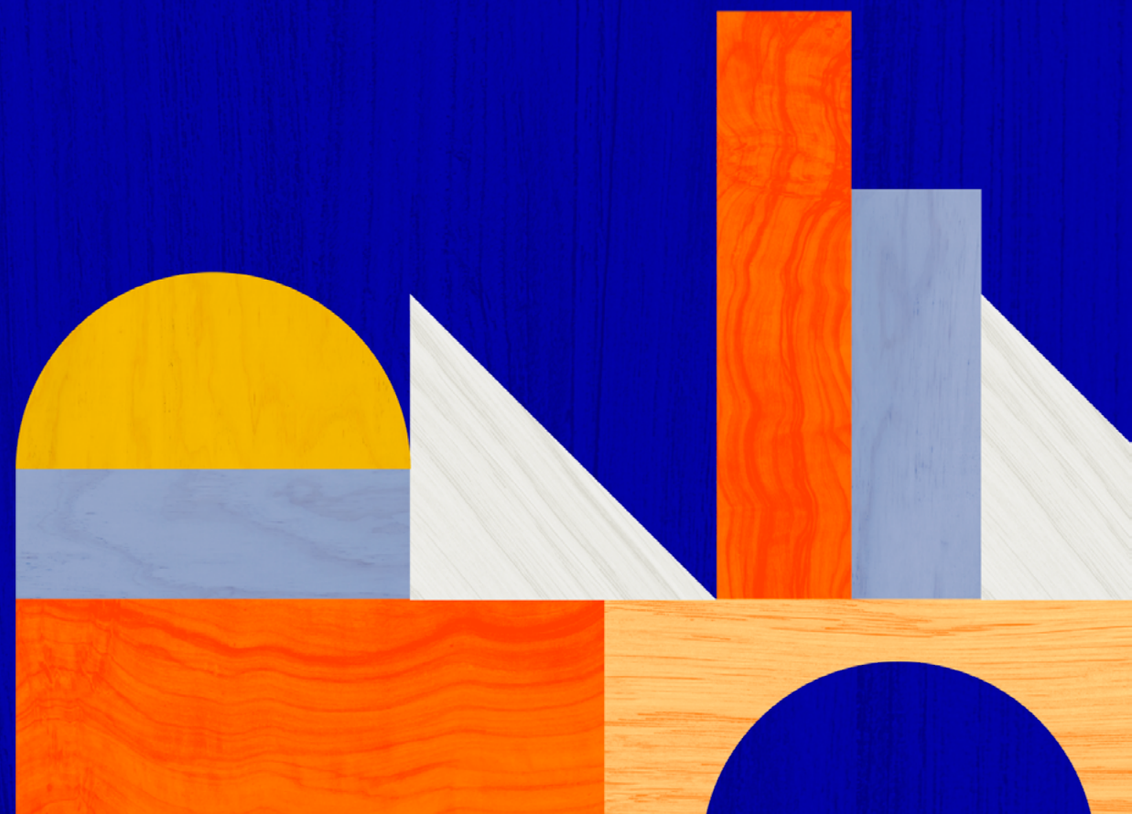
When it comes to protecting the org from cyber threats, it's all eyes on security pros like you. You have the awesome – and daunting – task of navigating a landscape that's becoming more and more complex every day.

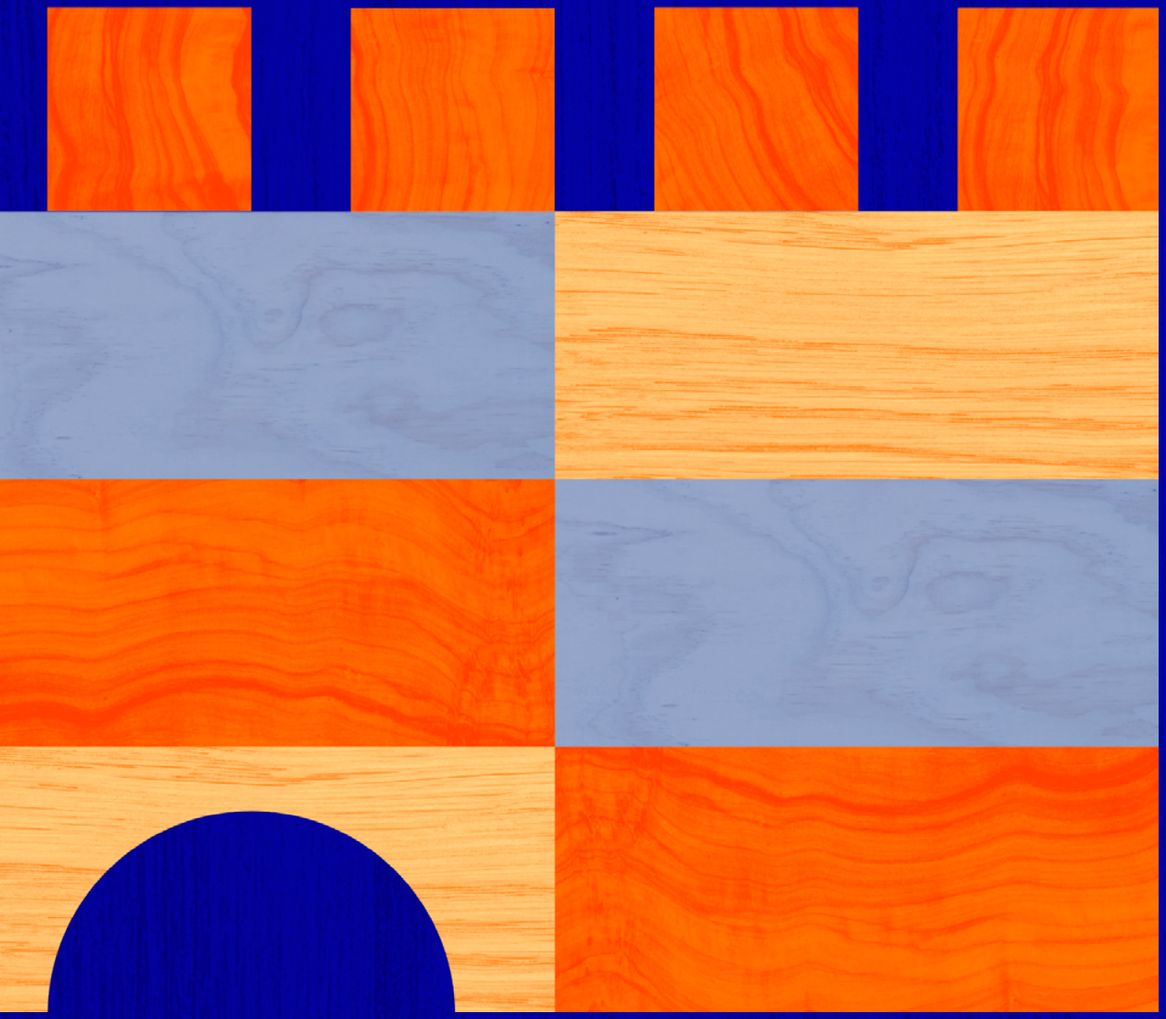
What's creating this complexity? Long gone are the days of lone actors deploying one-off phishing attacks; today's cyber threats are increasingly global, dynamic, and highly-sophisticated. Organizations in both the public and private sector now face the threat of hackers from all over the world, acting in groups to launch complex social engineering, ransomware, and malware attacks.

With advanced hacking tools at their disposal – the number of which increased by 65% from 2020 to 2021 – these hackers are also targeting infrastructure from multiple points of entry. To add to the challenge, the pandemic-fueled migration to the cloud has given hackers an even broader playground to infiltrate. Then there's the rise of Initial Access Brokers: groups who sell exposure access to other hackers for repeat offense.

These new tactics and opportunities for breach resulted in a 38% increase in global cyberattacks in 2022.

As cyber attacks increase in frequency, so too does the price we pay. The global cost of cybercrime is expected to jump from 8.44 trillion in 2022 to 23.84 trillion by 2027, with the global average cost of a data breach at 4.35 million dollars (in the United States, the average cost of a single data breach is a whopping nine million). But there's more for companies to consider beyond a hit to their bottom lines – cyber attacks can also erode organizations' customer trust, brand reputation, and legal standing.





Which brings companies and their security teams to the question: what is preventing a cyber attack worth? What do we need – and what should we invest in – to stay a step ahead of threat actors and protect our assets?

As a security pro in the trenches, you already know what's at the heart of this answer: best-in-class intelligence, plain and simple. Internet intel that's fresh, comprehensive, contextualized, and easy to explore. Intel that offers you the widest, most accurate view of the internet in near real-time, so that you can base your security strategy on truly reliable information. The kind of intel that in today's landscape isn't just a nice-to-have – it's a must. The better your intel, the more you can see.And the more you can see, the more successfully you can defend your organization.

The challenge, however, lies in convincing other folks in your org – whether it be your director, CISO, or CEO – that investing in access to the right internet intelligence treally is a prerequisite for successful security.

If you are reading this ebook, you have likely already made the decision to purchase a solution, like Censys, to help provide visibility into your attack surface and threat landscape by leveraging best-in-class internet intelligence data. Read on for insight into how to make a business case for your investment.

Do I Really Need a Business Case to Get Buy-In?

Companies increasingly recognize cybersecurity as vital to business, but not all understand what their security teams need to do their jobs well. Nor should we always expect them to. You and your team are the domain experts here, which means you're in the best position to advocate for the resources you need.

And anytime you're making a request that involves bringing on new resources, a little stakeholder education is going to be necessary.

A business case helps organize that education into a coherent, compelling narrative about why your request is justified. The business case format also helps you hedge objections, streamline vendor comparisons, drive urgency, and **ultimately get an answer from decision makers sooner.**

As a provider of best-in-class internet intelligence, at Censys, we know a thing or two about making a business case for better intel – and we've seen where stakeholder buy-in efforts succeed, and where they can fall short.

Why Companies Choose Censys for Better Internet Intelligence

Why does Censys win over stakeholders at organizations around the world? **We deliver the very best internet intelligence available, period.**

Whether you are looking for data to enhance your threat hunting capabilities or looking to gain visibility into your attack surface, Censys provides access to best-in-class internet intelligence you can use to proactively protect your organization against advanced threat actors. We lead the industry in scanning capabilities to provide the largest, most comprehensive dataset of internet intelligence available.

This best-in-class intel makes Censys the solution of choice for companies looking to:

1. Gain visibility into your attack surfaces and exposed assets
2. Protect the organization against emerging threats
3. Stay ahead of an evolving threat landscape
4. Empower security teams to take action fast
5. More efficiently leverage your security resources

What Makes Our Internet Intelligence Unique?

We can make these claims with confidence because of the key capabilities that set us apart. As you build out your own business case for Censys, you can draw stakeholder attention to some of the things we uniquely deliver: The bottom line is in order to ensure you are fully protected and informed, you need access to the very best data. If you settle for "good enough" you open yourself up to increased risk by not gaining full visibility.

Comprehensive, accurate, and up-to-date internet intelligence

Censys provides the most complete and accurate set of internet intel, with:

- Multi-perspective scanning from 5 unique global perspectives with Tier 1 ISPs
- 45x more services scanned than the nearest competitor*
- 2x more ports scanned than the nearest competitor
- Daily scans on top 137 ports and top 1440 ports in the cloud
- Deep scanning from non-standard ports
- >95% attribution accuracy
- A powerful layer of context and enables pivoting across related infrastructure

* GreyNoise Research, Oct. 2022: A Week in the Life of a GreyNoise Sensor

Context-aware search capabilities

Each asset we discover is enriched with data from multiple third-party sources to provide the most complete multi-perspective picture of every asset and its connections. Censys Search unlocks all of this information with a simple query language that allows you to easily search through mountains of data and find exactly what you're looking for.

Detailed access to historical data

We store all of the information we collect on the internet for up to two years, which means security teams can "look back in time" at how assets or groups of assets behaved in the past. This historical look back on any asset can be used for forensic analysis, breach investigations, or simply learning from past mistakes.

These differentiators are just the tip of the iceberg. You can learn more about our features and capabilities, and how our best-in-class data can empower your security efforts, at: https://censys.io/data-and-search/.

Why a Cybersecurity Company Chose Censys Over Competitors

A cybersecurity services company needed an internet intelligence provider to provide a state of systems check and to monitor for risks. After holding a competitive vendor process, their Chief Technology Officer said they chose Censys for its "speed of scanning, the depth of scanning, and the relative ease of ingesting the data."

Read the Case Study

Now that we've covered the value of good internet intel, why building a business case is important, and what Censys Search brings to the table, let's talk about how to build your own business case.

Define the Challenge You're Trying to Solve

Why is access to better internet intelligence a necessity for the business? What do you lose without it? As you begin to think about the message of your business case, focus on framing access to better internet intel as a solution to your organization's most pressing cybersecurity challenges.

In setting up your business case in this way, you'll help stakeholders see why better internet intel is a need-to-have rather than a nice-to-have.

Why Poor Cybersecurity Intelligence Is a Problem

As you think about the challenges you face dealing with subpar intel, consider some of these common consequences:

- Failing to discover a critical vulnerability that leaves your organization exposed
- Failing to take action on a potential threat due to lack of actionable insight and context
- Inability to understand the root cause of a threat
- Inability to identify emerging and real-time attacks
- Dealing with tools that are cumbersome and difficult to use
- Delaying response to risk incidents
- Spending more time on manual, redundant tasks and less time on strategy
- Difficulty communicating real threats to executives due to disjointed tools and data that's too granular
- Difficulty making sense of an evolving threat landscape

How Do These Challenges Affect the Business?

Now connect your challenges to their impact on the business. For example, let's say one of your top challenges is lack of up-to-date information. Speak to how this outdated intel hinders specific tasks, like risk remediation.

Identifying a critical exposure is all about timing. The makeup of internet assets are constantly evolving and today's threat actors are highly sophisticated and are always looking for vulnerabilities. If your data is outdated, even by a single day, you might miss a critical vulnerability or information about a CVE that was just identified.

This creates a knowledge gap that leaves the company vulnerable to being breached – and that is why access to fresh, near real-time data is needed.

TIP: Don't be shy about pointing to specific times the team already experienced a miss because of inadequate data. The more context you can give around challenges, the more urgency you create for a new solution.

Beware the Benefits

It can be tempting to frame your case around benefits, but a benefits-driven approach, on its own, can have drawbacks. Let's say you lead with how best-in-class internet intel from Censys will be faster and more comprehensive than what you're currently working with, and you'll be able to dissect data with more filters and parsing fields to gain deeper insights. Those are all great points that you'll want to include in your case, no doubt, but by leading with them, your stakeholders may wonder: *"So is this just a nice-to-have? Why do we really need this?"*

Identify Your Stakeholders

Next step is to identify and understand the needs of your audience. Who in your organization needs to approve the purchase, and what do they care about? Whose "yes" do you need? Your manager may come to mind first, but getting buy-in for new tech solutions rarely means a thumbs up from one person. In fact, the average tech purchase (across all tech types) involves between 14-23 people.

In addition to your department head, or CISO, you also need the buy-in from people in related departments who would be impacted by the purchase. This usually means departments like legal, IT, and finance, as well as your CEO. Anticipating the questions or concerns that these cross-functional groups may raise can make your path to buy-in more seamless.

If you're unclear who will have influence or be involved in a purchasing decision, look into how previous solutions at your company were brought in.

To hone in on what is important to each role, take a look at our stakeholder audience breakout:

Security Team Lead

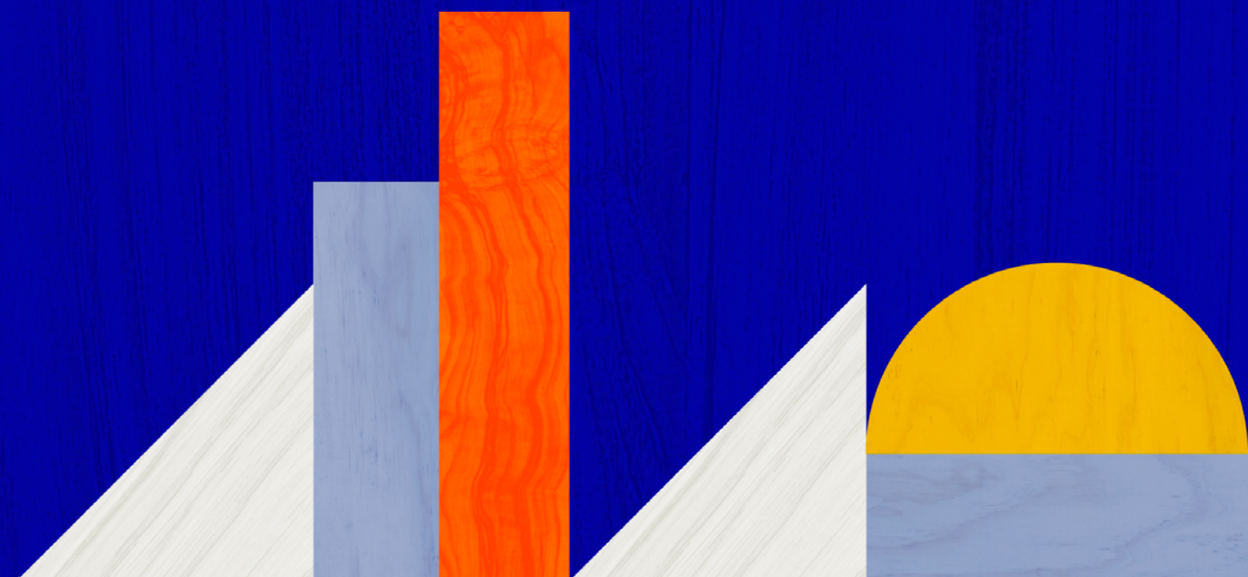
- **What They Care About**
  - Effectively managing exposures to prevent a breach and quickly remediating risks
  - Meeting the department's KPIs and objectives, to demonstrate that the security processes and protocols are effective
  - Ensuring that the company is not affected by the same vulnerabilities or breaches more than once (such as by failing to patch or upgrade a known vulnerability)
  - Ensuring that security personnel and resources are being efficiently used
  - Address how access to comprehensive, contextualized internet intelligence will increase the security team's threat hunting efficiency and effectiveness, and empower them to meet more internal KPIs
- **What It Means for Your Business Case**
  - Address how access to comprehensive, contextualized internet intelligence will increase the security team's threat hunting efficiency and effectiveness, and empower them to meet more internal KPIs.

VP/CISO

- **What They Care About**
  - Protecting the company from lost revenue and brand reputation damage as a result of a cyberattack
  - Maintaining regulatory and legal compliance
  - Maximizing security team resources efficiently (both human resources and tech stack resources)
  - Meeting and exceeding the company's KPIs and objectives for cybersecurity
  - Meeting and exceeding CEO and Board of Director expectations for protecting the business from cyberattacks and implementing effective security protocols for teams across the org
- **What It Means for Your Business Case**
  - Emphasize how outdated, incomplete internet intel doesn't give your security team a full picture of current vulnerabilities and potential threats, hindering proactive threat hunting and leaving the org at risk of a breach that could compromise sensitive data.
  - Additionally, with Censys, security teams save time and money through the automation or previously manual and time consuming tasks, like threat intelligence research.

Finance

- **What They Care About**
  - Making and approving strategic financial investments that deliver long-term ROI
  - Providing oversight and guidance to keep all company divisions within budget
  - Identifying new ways to minimize cash burn
  - Increasing revenue YoY
  - Identifying opportunities to grow the company's profit margin
- **What It Means for Your Business Case**
  - Position best-in-class data as a preventative, long-term cost-saving measure. Emphasize how access to good internet intel is essential to preventing even costlier cyberattacks (recall, the average cost of an attack is ~$4M).
  - Additionally, your CFO will be interested in increasing the productivity and effectiveness of current assets.

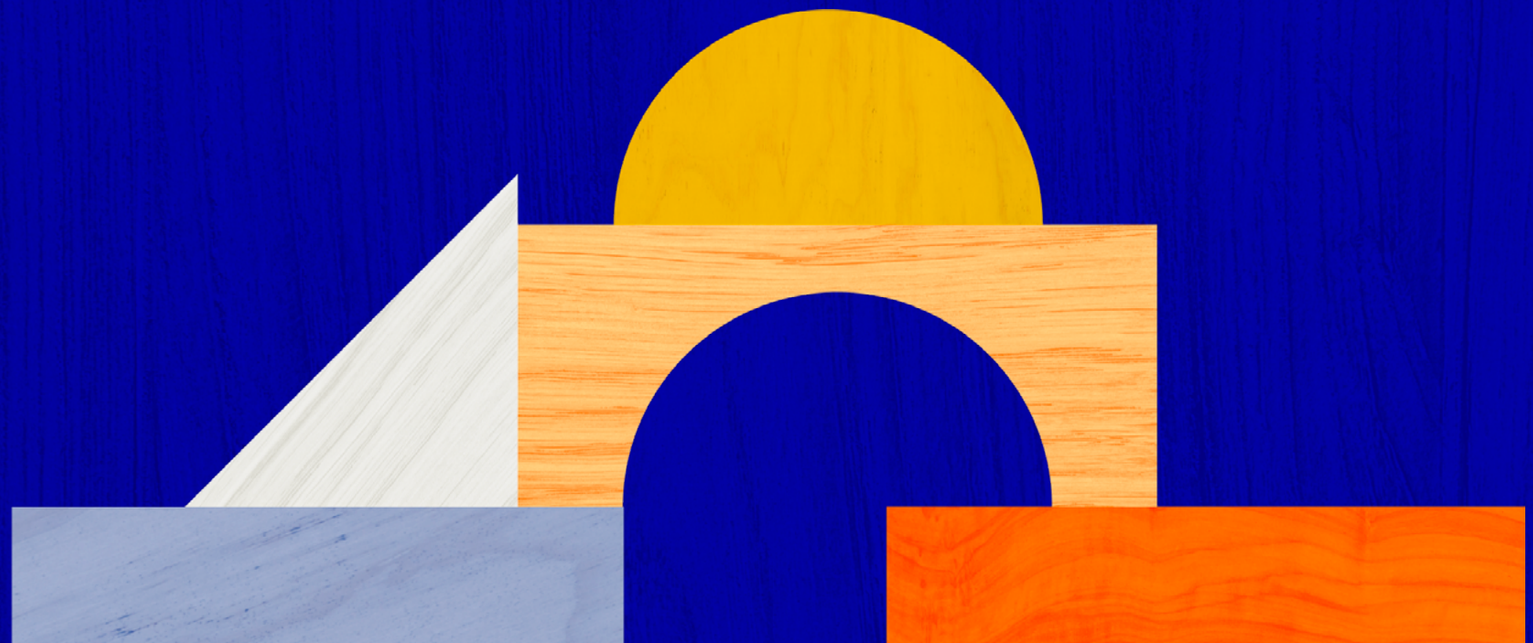


IT/Procurement

- **What They Care About**
  - Understanding the implementation complexity involved with procuring new systems and effectively managing required IT resources
  - Determining if a new solution will require integrations
  - Understanding the security implications of new solutions
- **What It Means for Your Business Case**
  - Include specific details in your business case about how your company will work with a solutions provider to gain access to better internet intel. Include detail on the setup process and provide an estimate of the internal technical resources that will be required.
  - Censys provides access to a variety of critical integrations, including cloud connectors, to ensure that systems are connected. Additionally, because Censys is a web-based platform, there is very little or no deployment or configuration.

CEO

- **What They Care About**
  - Growing the business YoY through customer acquisition, customer retention, and new revenue streams
  - Exceeding customer, shareholder, and partner expectations for quality of product/service delivered
  - Upholding and improving the integrity of the brand to advance customer loyalty, new customer acquisition, and competitive positioning.
- **What It Means for Your Business Case**
  - Underscore the connection between a strong cybersecurity posture – which requires good internet intel – and the overall health of the business. Just one cybersecurity breach can result in significant loss of money, customers, and brand reputation, as well as introduce legal complications. Help your CEO understand the complexity of today's evolving threat landscape by leveraging third-party data and insights that shed light on the risks that orgs who do not modernize their cybersecurity strategy face.



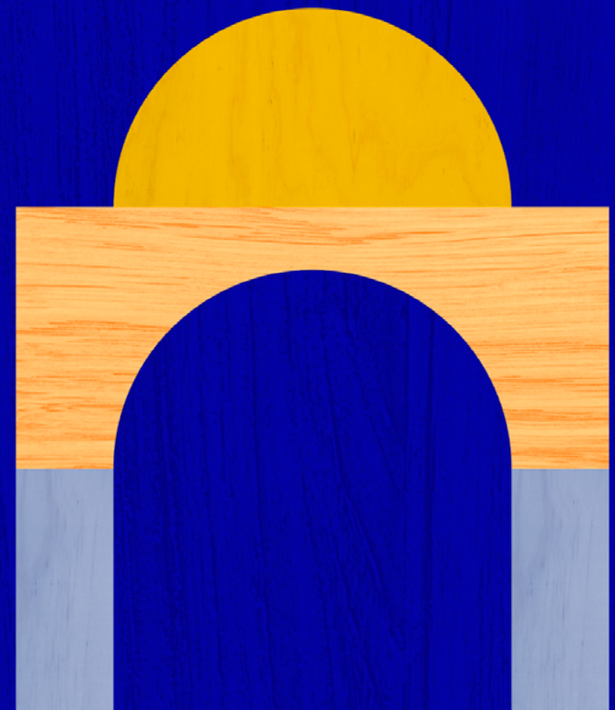
Further Understanding Your Audience

In your own company, what other specific objectives might these leaders have? Do certain roles tend to have more influence than others? Maybe your CFO has been with the company for 20+ and has the most dominant personality in the C-suite.

Another question to consider as you think about your audience: are there any company-wide shifts on the horizon or in the recent past that might be relevant to a procurement decision?

For example:

- **Recent layoffs or budget cuts?**
  - If workforce reduction is at play, focus on how access to better internet intelligence will help remaining team members work more efficiently (such as by faster threat discovery and investigation) and how better internet intelligence is a strategic, long-term investment that advances the org's cybersecurity position.
- **An upcoming merger or acquisition?**
  - Whether your org has been acquired, is looking to acquire, or is planning to merge with another, it's key that all parties have a full understanding of each others' security postures. Advanced internet intelligence can give partners greater visibility into owned assets and potential risk factors, as well as make it easier to share reporting.
- **A major security breach?**
  - Even more reason to invest in better internet intelligence! Speak to how best-in-class intel can support more comprehensive threat hunting and risk remediation to prevent another breach.
- **Uptick or downtick in customer acquisition, retention or satisfaction scores?**
  - Enhancing your organization's cybersecurity measures signals the value you place on customers' data and privacy. Leveraging best-in-class internet intel shows that you're committed to protecting their information.
- **An increase in remote workers?**
  - Every organization has seen an explosion of remote work since 2020, and this cultural change in the workplace is here to stay. However, remote work opens up your organization to more potential security exposures through an increase in internet-connected assets, poor employee security practices, and shadow IT.



Do Your Vendor Homework

You've defined your challenges and identified your stakeholders; now it's time to get familiar with different vendors who can help. Even if you have a preferred solution in mind, you'll want to demonstrate to stakeholders that multiple options have been considered, and that there's clear rationale for your recommendation. Being informed about different vendors can also help you better handle stakeholder objections, which we'll get to shortly.

Vendor Evaluation: What to Look For

- **Is data refreshed continuously?**
  - **Censys:** Yes. Censys provides access to the freshest, most accurate internet dataset of any solution available. Censys continuously scans IPv4 hosts on over 3,500 ports. In contrast, most competitive vendors only refresh data on a weekly or even monthly basis, impacting your ability to see threats in real-time.
- **How many ports does the data solution scan compared to other vendors?**
  - **Censys:** Censys scans the top 137 ports and top 1440 ports in the cloud, and continuously scans IPv4 hosts on over 3,500 ports. That's 45x more services scanned than the nearest competitor and 2x more ports scanned than the nearest competitor, including detecting services on non-standard ports. Many competitors in the space simply do not have the scanning infrastructure that Censys has built in-house. Instead, many vendors rely on third-party scanning data that they do not own.
- **Do you have the ability to parse and filter data?**
  - **Censys:** Absolutely. Censys customers benefit from a user-friendly interface that includes a wide range of 1,400 fields for hosts and 1,100 fields for certs, which can be leveraged in an easy-to-use query language. This enables complex and custom searches that users can leverage to find advanced threats, IOCs, and understand trends across the Internet.
- **Do you have the ability to download the data?**
  - **Censys:** Yes. All users can access and ingest Censys data via the web UI, API, or through integrations. For Enterprise customers, we also have data snapshots and BigQuery setups available.
- **Will you have detailed access to historical data?**
  - **Censys:** We store our internet intelligence for up to two years, with access to seven years of historical data. The historical look back for any asset can be used for forensic analysis, breach investigations, or simply learning from past mistakes.

- **How many different users can access the data?**
  - **Censys:** All of our packages give customers an unlimited number of users.
- **How can I integrate this data into my existing tools?**
  - **Censys:** Censys gives you the flexibility to utilize Censys Search data in your existing workflows without sacrificing the amount of results you can find. Both Censys supported and third-party integrations with some of the most popular security tools helps this information fit seamlessly into your security program.
- **Will you have access to a Customer Success Team?**
  - **Censys:** Yes! All paying customers have access to a dedicated Customer Success Manager who is available to answer questions, collect feedback, assist with troubleshooting, and help you maximize your use of Censys Search.

Making Comparisons

In addition to collecting information about data vendors individually, look for resources that compare vendors against each other. This can provide a clearer view of strengths and weaknesses. Comparison charts can also be helpful visuals for your stakeholders. In this example on the right from GreyNoise Intelligence, a number of internet scanners, including Censys, are compared against each other to look at breadth of coverage.

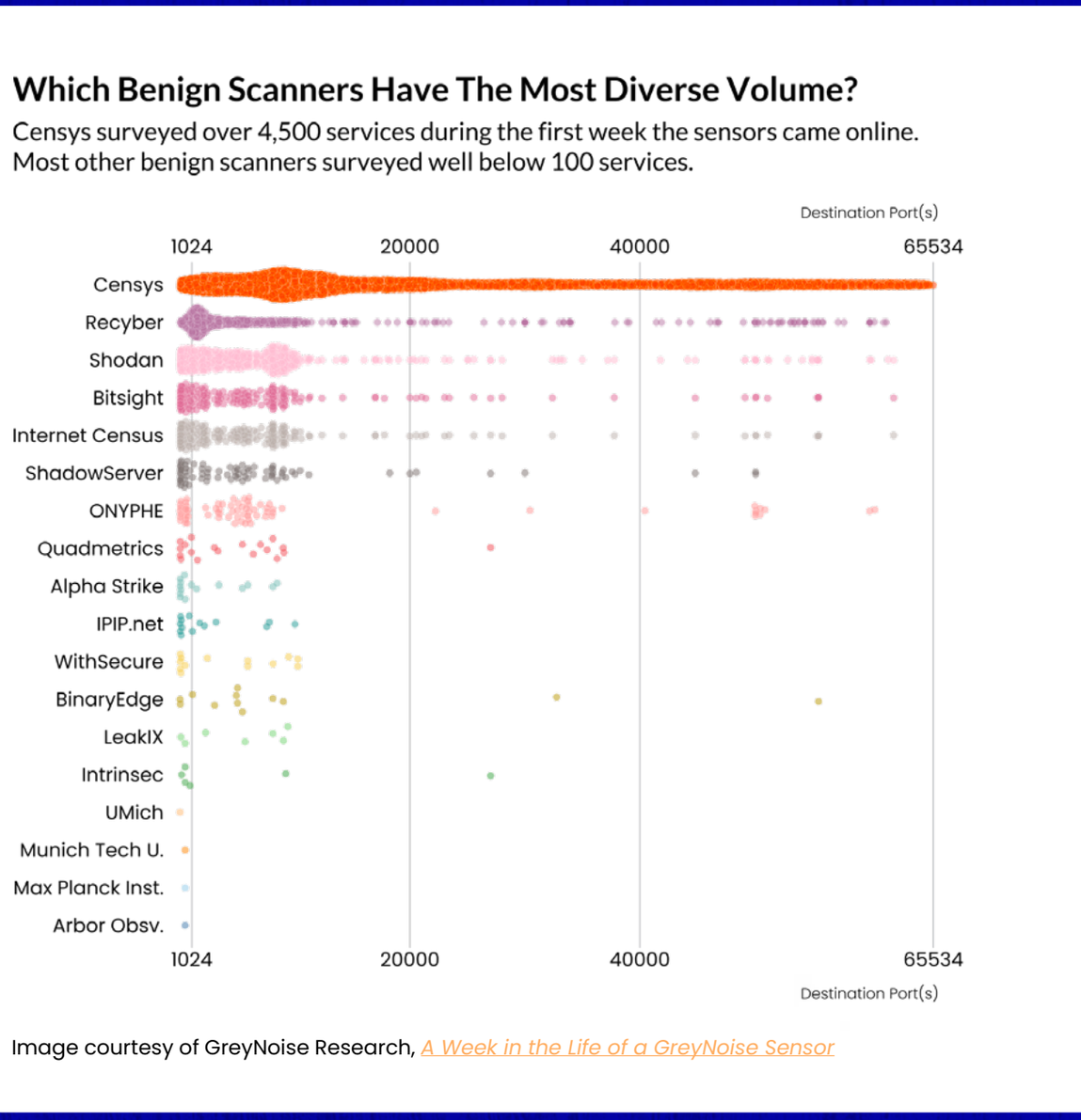


Image courtesy of GreyNoise Research, *A Week in the Life of a GreyNoise Sensor*

Understanding the Typical User

Another vendor consideration is customers served. Who primarily uses the vendor, and what do those customers have to say about the solution? A solution might be great for lone threat hunters or academic researchers, but fall short on supporting enterprise cybersecurity teams. Other solutions may be just fine for corporate security efforts but have little-to-no experience supporting the nuances of federal government data needs. **At Censys, our users represent a variety of use cases and industries, including government, healthcare, and tech.**

Customer Testimonials

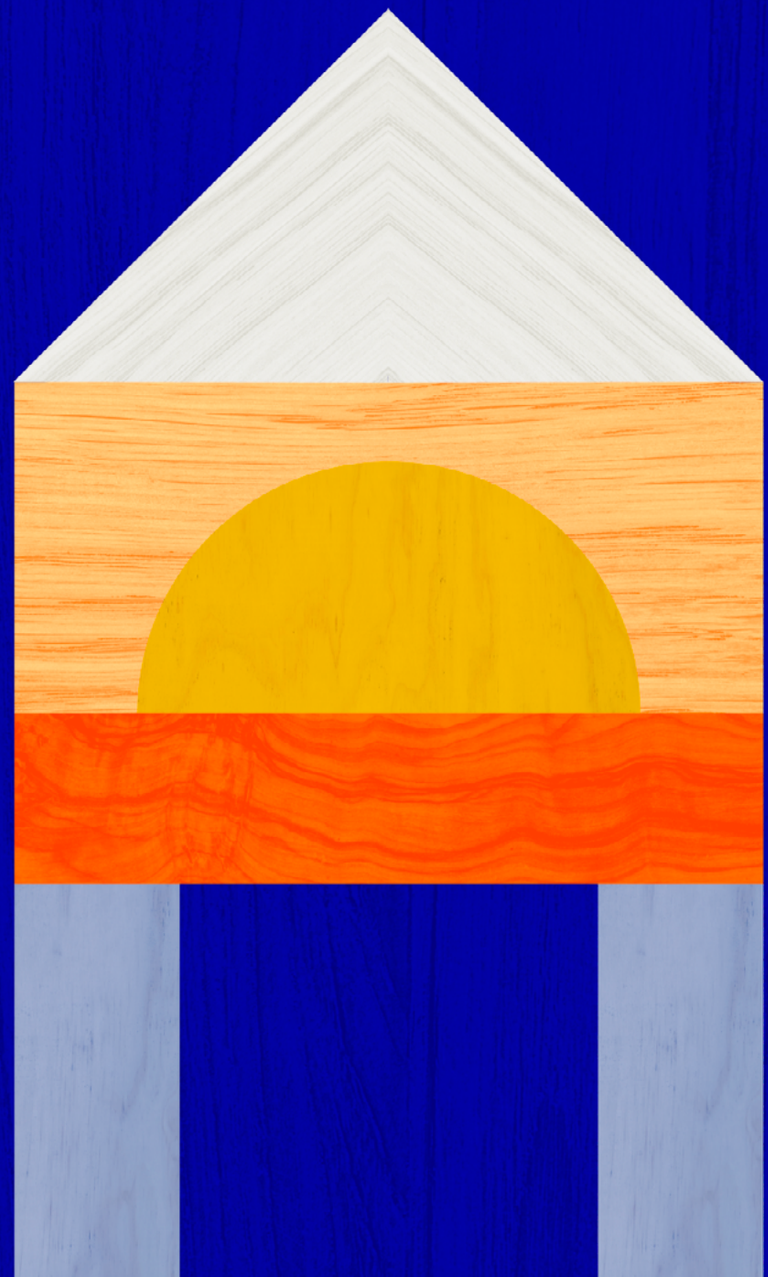
Look for customer testimonials to add color to your vendor evaluations.

"Censys structures internet data in a way that's easy to understand and query. Without regular expression queries and the ability to query specific fields, we wouldn't have been able to develop or search for other hosts that matched our signature."

- Citizen Lab Research Fellow

Read the Case Study

TIP: As you go along, take notes on vendor differences and package up in a simple matrix (like the one at the end of this guide) to include as part of your business case.



Showcasing Value & Handling Objections

You've done your prep work – now it's time to showcase what your recommended vendor will bring to the table. The idea here is to draw a connection between the challenges you identified at the outset to the specific value the vendor provides. You can see how we took this approach with our Censys Search solution.

- **Our Company's Security Challenge:**
  We lack full visibility into threats because of limited scanning, which creates gaps in our security strategy.

  How Censys Search Can Help:
  Multi-perspective scanning and daily coverage of the most popular ports ensures Censys data is as fresh and accurate as possible. Intelligently scanning each port to discover the underlying services, certificates, software, and configurations gives us the most comprehensive data set of Internet intelligence available.

- **Our Company's Security Challenge:**
  Our data isn't refreshed continuously, which means that when we try to learn if we're impacted by a zero-day, we're looking at outdated information.

  How Censys Search Can Help:
  Censys provides the most complete, accurate, and up-to-date set of internet data available. Censys conducts daily scans on the top 137 ports and the top 1440 ports in the cloud, which is twice as many ports scanned as the nearest competitor. Censys also continuously scans IPv4 hosts on over 3,500 ports from multiple perspectives, offering 99% visibility of the Internet. Additionally, maintains the largest X.509 certificate repository in the world containing 9.5 billion certificates.

- **Our Company's Security Challenge:**
  Our existing data doesn't enable us to understand the root cause of threats very well, which means we're susceptible to running into the same issues in the future.

  How Censys Search Can Help:
  With structured data and historical views, Censys makes it possible to pull a wealth of insight about threat activity and root cause. Users can explore 1400+ fields for hosts and 1100+ fields for certificates in an easy-to-use query language. Censys also maintains more than two years' worth of data; users can look at changes to an asset or group of assets at a specific point in time.

- **Our Company's Security Challenge:**
  We waste a lot of manual effort trying to understand the data we see, pulling data into our systems from disparate sources, and then reporting out to our executives in a way that makes sense.

  How Censys Search Can Help:
  With access to APIs and multiple integrations, Censys offers the flexibility to utilize Censys Search data in your existing workflows without sacrificing the amount of results you can find. Both Censys supported and third-party integrations with some of the most popular security tools helps this information fit seamlessly into your security program. This makes it easier for teams to import data findings to existing systems and share out information that's digestible for executives.

Handling Objections

Even the best thought-out business cases can face questions and objections from stakeholders. After pitching your ask for a solution, you might hear objections that sound like the following:

- **Objection:**
  PRICE: "This sounds great and all, but you know that we're tightening our budget this year. We need to focus our spend on the essentials."

  Response:
  Best-in-class data *is* essential to the org's overall health (helping to prevent a cyberattack with catastrophic consequences). This is a long-term investment that we should think of as a cost-prevention measure. If we don't keep up with today's complex and evolving threat landscape, we put ourselves at risk to lose much more than the cost of good internet intel.

- **Objection:**
  ALTERNATIVES: "Are there other ways we can address the challenges you brought up? What if we took a few things off your plate so you can spend more time digging into the data we do have?"

  Response:
  Strong intel is the foundation of any security strategy; we can only go so far with subpar intel, even if we increased headcount or dedicated more time to working with the data we do have. There is no substitute for maximum visibility.

- **Objection:**
  COMPETING PRIORITIES: "I hear where you're coming from, but other teams have already made purchase requests. I'm not sure if we can fit this in."

  Response:
  Can we discuss the business priorities of other purchase requests? Access to top-tier internet intel empowers our frontline efforts to protect the org, and gaps in our security ultimately undermine the efforts of other departments.

- **Objection:**
  ROI: "What's the return on investment for this kind of intel? By upgrading from what we currently have, are we really gaining value?"

  Response:
  Yes - while we can't know for sure if or when a security breach could occur, we do know that the average cost of a cyberattack for an enterprise org like ours is almost $4 million.

  Access to better intel:

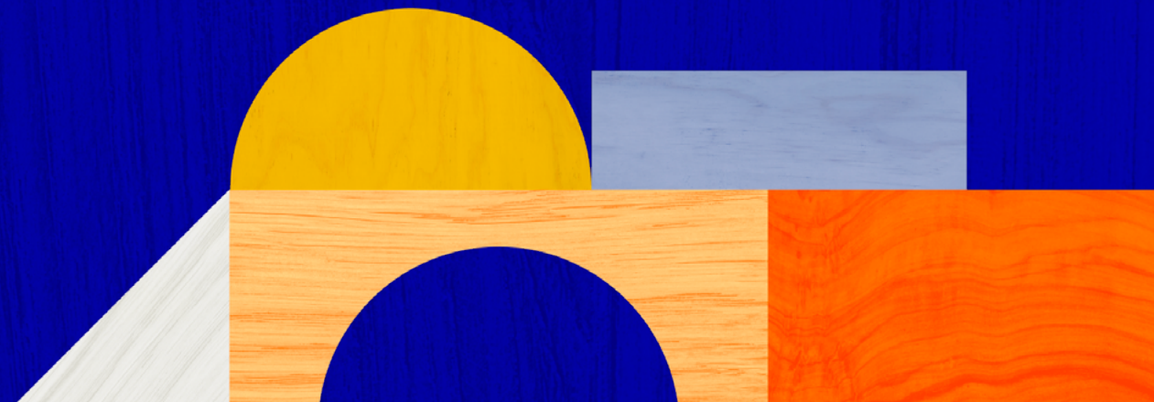
  - Eliminates time spent collecting disparate information about threats
  - Allows us to use our people resources more efficiently
  - Empowers us to respond to threats more quickly
  - Allows us to proactively search for unknown attack methods to prevent a breach

Address Implementation Complexity & Timelines

An inevitable follow-up to your pitch for better internet intelligence? Logistics. How would your team get access to the intel? When it comes to implementation and onboarding, win stakeholder trust by making sure your business case is transparent about potential complexities and timelines. Ideally, if you've done your vendor homework well, you're recommending a solution like Censys, concerns should be minimized.

Questions to consider might include:

- **Will the team need training to access and use the intel? If so, how much?**
  - **Censys:** Most security teams find the Censys Search tool intuitive and can get up and running in minimal time. There are a wide range of onboarding tutorials available to users on support.censys.io, and any self-guided training can be paired with dedicated support from a member of our Customer Success team as needed.
- **Are you able to add users on an as-needed basis?**
  - **Censys:** We offer three tiers of paid access to Censys data – Pro, Pro Plus, and Enterprise. While each package involves a different number of dedicated monthly searches and API lookups, all packages offer organizations an unlimited number of users.
- **What does the vendor's customer support service entail?**
  - **Censys:** Customers of Censys can expect to receive both technical support and a dedicated Customer Success Manager to assist with onboarding, implementation, and adoption. Whether it's providing live training/working sessions or providing insight into how other customers are leveraging our data, you can expect to receive white glove support from Censys.
- **Who would need to be involved in implementation?**
  - **Censys:** Typically we see titles such as 'Attack Surface Manager', 'Security Analyst', 'Security Researcher' or even CISOs involved in the implementation of Censys.
- **Are we able to integrate with our existing systems?**
  - **Censys:** We offer an easy-to-use REST API that allows users to quickly and easily develop integration workflows into nearly any platform. Additionally, official Censys integrations include: Splunk Core, Maltego, Google BigQuery, Recon-NG, Command Line, NMap, Postman, Python Library.



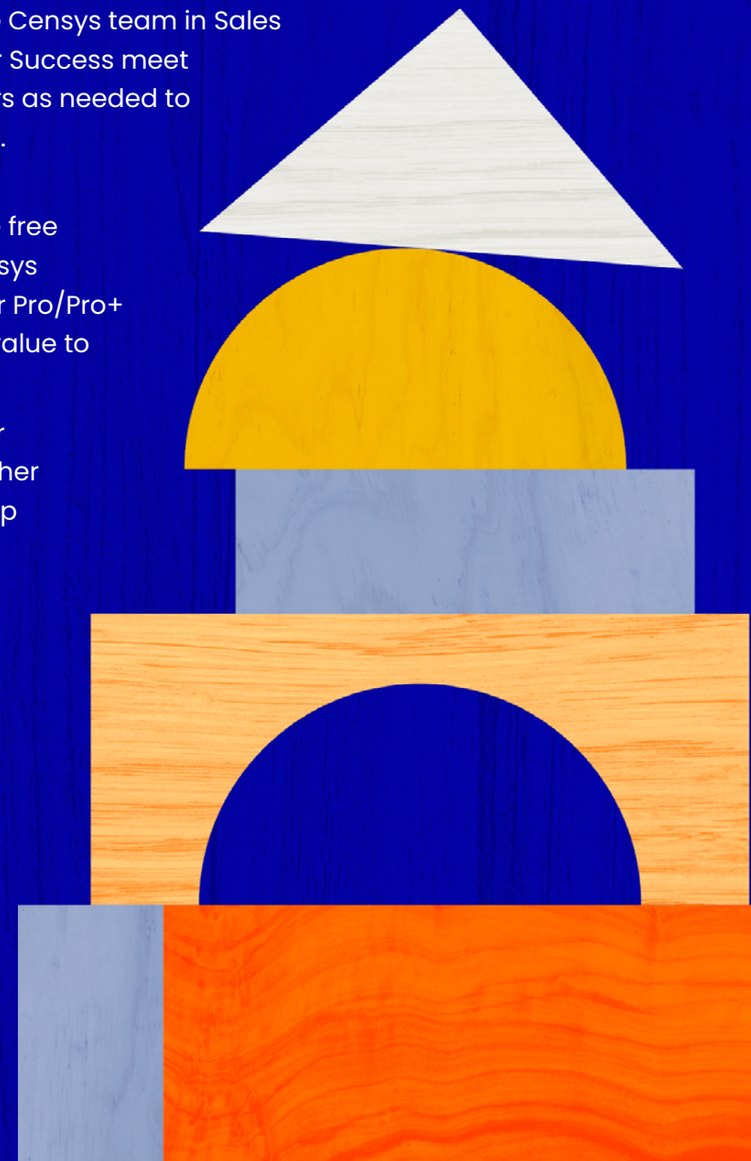
Be Patient, but Persistent

You may have pitched your case – but don't expect the greenlight after just one conversation. As with any new solution, convincing stakeholders to invest in best-in-class internet intel could take time and mean multiple touchpoints with a vendor. Think about the different ways to familiarize your stakeholders with the value of better intel. Maybe your ongoing efforts start with passing along vendor collateral, then progress to an in-depth demo, and then to a demonstration of what you've been able to accomplish with a free trial.

In our experience with prospective Censys customers, the stakeholder buy-in journey can look like:

1. An organization identifies a gap in their existing internet intel and needs to augment it with external scanning data from a third party, or build their own scanner.
2. A prospective power user reaches out with interest in the Censys Search solution, and has initial conversation with Censys Sales.
3. A member of the Censys Sales Team shares informational collateral including info sheets, analyst reports, demo videos, and sample data sets.
4. The prospective power user makes their business case for better internet intel to their internal stakeholders, and shares Censys collateral.
5. The prospective power user invites key stakeholders to an upcoming Censys webinar, or arranges for a personalized demo with the Censys team.
6. Additional members of the Censys team in Sales Engineering and Customer Success meet with individual stakeholders as needed to address specific questions.
7. Meanwhile, a prospective power user is exploring the free community version of Censys Search and/or a trial of our Pro/Pro+ package to demonstrate value to stakeholders.

Your journey to win stakeholder approval may take shape in other ways, but the key here is to keep engagement ongoing and to partner with a vendor like Censys that's equally invested in working with your stakeholders.



Make Your Case

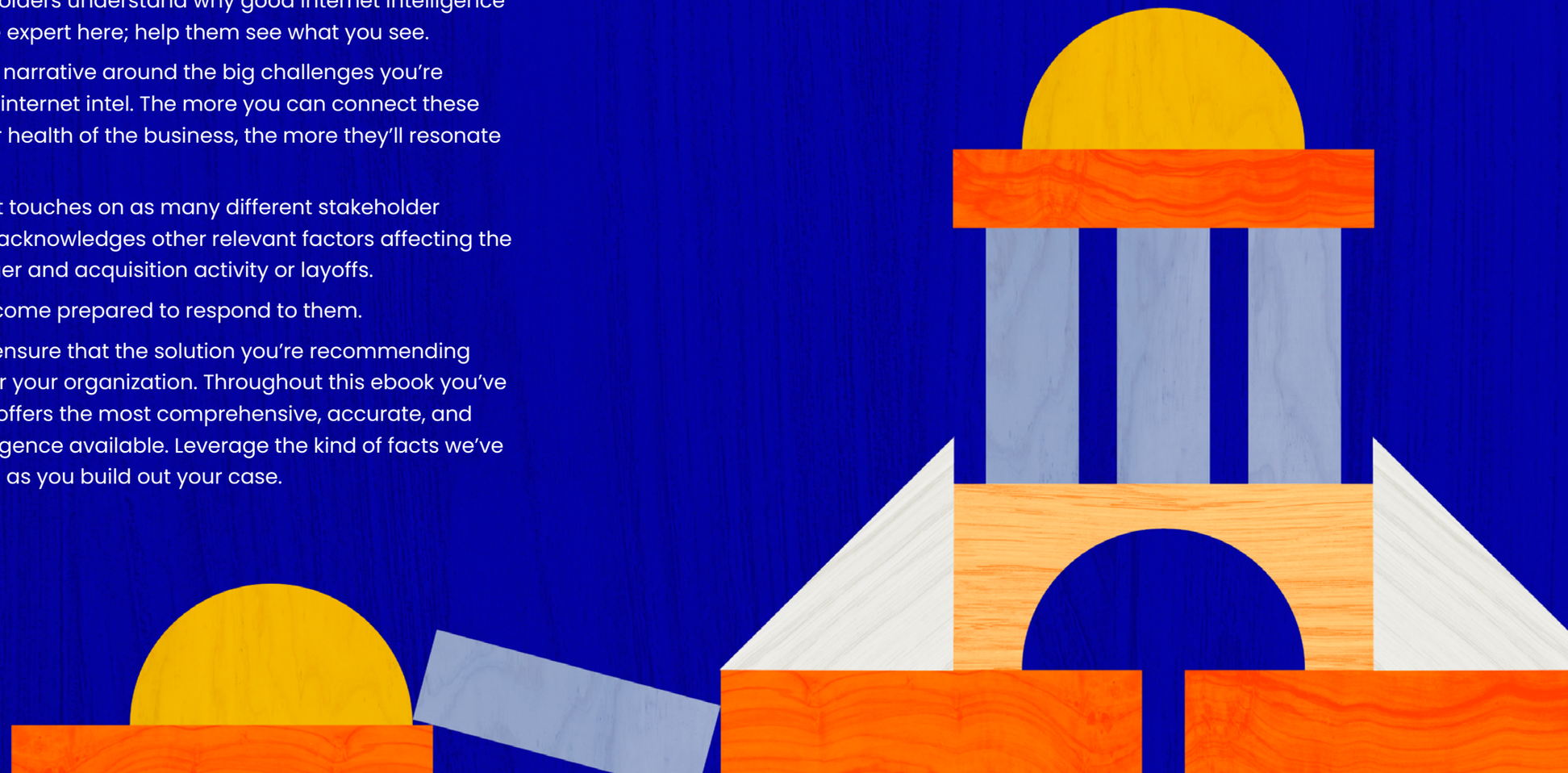
You have the framework and strategies needed to win buy-in for best-in-class internet intelligence; now it's time to deliver.

Final Thoughts to Keep in Mind

- Don't assume that stakeholders understand why good internet intelligence is so important. You're the expert here; help them see what you see.
- Focus your business case narrative around the big challenges you're trying to solve with better internet intel. The more you can connect these challenges to the broader health of the business, the more they'll resonate with stakeholders.
- Build a business case that touches on as many different stakeholder interests as possible and acknowledges other relevant factors affecting the business, like recent merger and acquisition activity or layoffs.
- You'll face objections, so come prepared to respond to them.
- Do your due diligence to ensure that the solution you're recommending really is the best option for your organization. Throughout this ebook you've seen why Censys Search offers the most comprehensive, accurate, and up-to-date internet intelligence available. Leverage the kind of facts we've shared about our solution as you build out your case.

Start Your Business Case

Fill in our business case template, found in the following pages of this ebook, as you collect information and build out your talking points.



Building Your Own Business Case

Ready to make your case for best-in-class internet intelligence? Use this template as you gather information and build out your talking points.

Stats to Get You Started

You may find that data points like these come in handy as you talk with stakeholders about the importance of investing in cybersecurity solutions.

- Cyber attacks increased 38% in 2022. - CheckPoint Research
- The average cost of a cyber attack is 4.35 million dollars. - IBM
- The cost of global cybercrime is expected to rise from 8.44 trillion in 2022 to 23.8 trillion in 2027. - Statista
- The number of hacking tools increased 65% from 2020 to 2021 alone. - HP Threat Insights Report
- The annual number of security breaches on enterprise organizations increased by 27.4% from 2021 to 2022. - PurpleSec

Step 1: Define Your Top Challenges

Rather than jump to the benefits of best-in-class internet intelligence, begin by orienting your case around the challenges you face. What is your security team struggling with? Why are these pain points important to address? This will help stakeholders see why better intel is a need, rather than a want.

	Potential Challenges				
	#1	#2	#3	#4	#5
Why We Need to Address					

Step 2: Identify Your Audience

Getting buy-in for any type of new solution usually requires input from multiple folks in the org. Though you may know who will ultimately sign on the dotted line, think about others who could have influence over the decision – finance, legal, IT/procurement, your CEO, etc.

	My Stakeholders				
What They Care About					
What I Should Focus On					

Step 3: Compare Vendors

	Vendors		
	Censys		
Global Coverage	Peering from 5 Tier-1 ISPs US and EMEA Scanning >99% of all internet hosts Visibility across 3,592+ ports 2.3B Observed Services 200M IPv4 Hosts 32m IPv6 Hosts 600M Virtual Hosts >3,500 Ports		
Certificates	~9B Certificates Worlds Largest Certificate Repository		
Speed	Daily Scanning on 137 top ports Weekly Scanning on 3,592 Ports		
Context	Daily Scanning on 137 top ports Weekly Scanning on 3,592 Ports		
Historical Lookback	More than two years of historical data are available for users to filter by in the Censys Search tool.		
Implementation	No on-prem implementation is required. Users login to their Censys Search account remotely.		
Price	Free, Pro, Pro-Plus, and Enterprise pricing models are available to fit an organization's specific needs. Models vary by query allotments, but all permit an unlimited number of users.		
Industry/Customers Served	Censys data is trusted by more than 100+ customers, including the U.S. government and 10%+ of the Fortune 500.		
Notes			

Step 4: Showcase Value & Handle Objections

	Security Challenges We Face				
	#1	#2	#3	#4	#5
How the Recommended Solution Can Help					
ROI Implications *Time saved?* *Efficiency gained?* *Customer data better protected?*					

Step 4: Showcase Value & Handle Objections

	Potential Stakeholder Objections				
	#1	#2	#3	#4	#5
Responses					

Step 5: Address Implementation

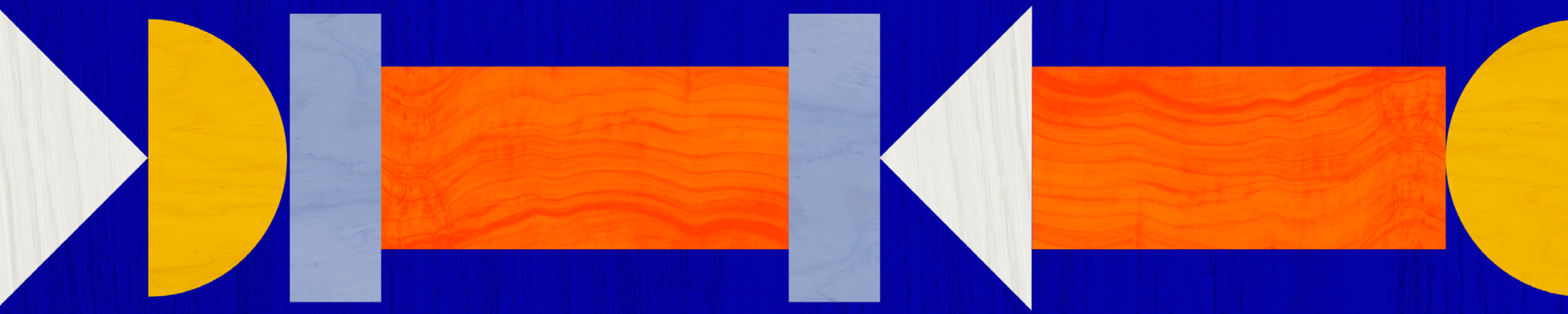
Let's talk logistics. How would your team access the new data solution? Learn as much as you can from a vendor about what happens after a contract is signed, and be transparent with stakeholders.

	Questions to Consider						
	Will the team need training to access and use the data? If so, how much?	Are you able to add users on an as-needed basis?	What does the vendor's customer support service entail?	How long does implementation take for a company of our size?	Who would need to be involved in implementation?	Are integrations with existing systems necessary?	Vendor's Customer Success Points of Contact
My Notes							

Step 5: Engage Stakeholders Over Time

Winning stakeholder approval can take time. After you present your business case, you may need to keep familiarizing stakeholders with a solution until you get that resounding yes. Plan out your engagement strategy: who will you follow-up with, and what will you share with them? Consider: vendor collateral, personalized demos, invitations to webinars, and meetings with sales and customer success.

	Stakeholder Engagement Schedule					
	Week 1	**Week 2**	**Week 3**	**Week 4**	**Week 5**	**Week 6**
Who						
How						
Links to Resources						



censys

The one place to understand everything on the internet.

For security pros who protect the organization, Censys is the best at finding exposures attackers will exploit. Our industry-leading Internet scanning platform and >9.1B certificate database (the world's largest) enable us to provide 63% more service coverage than our nearest competitors. Founded by the creators of ZMap, at Censys we've made it our mission to make the Internet a more secure place for everyone.

hello@censys.io
www.censys.io