censys

# How the Financial Services Industry Proactively Identifies Threats with Censys

The Financial Services industry is one of the most targeted sectors for malicious cyber attacks. With the expansion of digital infrastructure, proliferation of sensitive data, increased attacker sophistication, and stringent regulations, FinServ CISOs and their Cyber Threat Intelligence teams are under significant pressure to identify and respond to critical threats before adversaries take action.

To gain an upper hand, FinServ organizations are turning to the Censys Internet Intelligence Platform for access to unmatched global threat intelligence.

## 3 WAYS FINSERV ORGANIZATIONS ARE WINNING WITH CENSYS

## 1 Customizing Threat Intelligence Feeds

### THE CHALLENGE

Most major financial institutions rely on multiple threat intelligence feeds to gain visibility into the threat landscape and track attacker infrastructure. However, these various off-the-shelf intelligence feeds often don't provide the specific, contextualized data that CTI teams need for sophisticated operations. For example, feeds may be refreshed on an intermittent basis, can be plagued by a high rate of false positives, and lack the meta data needed to truly determine whether activity is benign or malicious.

### THE SOLUTION

This visibility gap is why a US-based global Fortune 500 bank sought out Censys to validate the accuracy and completeness of its existing threat intelligence feeds. Censys provides the most comprehensive, accurate, and up-to-date map of internet infrastructure available, identifying new services six times faster than the nearest competitor.

This global bank's CTI team also sought out Censys to augment their threat intelligence feeds with more customized intel that's targeted to their specific threat profiles. With Censys, the bank can access historical data about hosts and certificates to identify credible evidence of malicious activity, by identifying patterns or fingerprints of past threat actor infrastructure to understand their tactics and predict their next move.

# 2 Enhancing Brand Protection

### THE CHALLENGE

Threat actors are deploying increasingly sophisticated brand impersonation attacks against FinServ organizations, including socially engineered phishing attacks and domain spoofing campaigns. As a highly-regulated industry responsible for vast amounts of sensitive customer data, FinServ organizations must take increasingly proactive brand protection measures.

### THE SOLUTION

In the face of these challenges, a global Fortune 500 bank sought out Censys to bolster its brand protection efforts. The bank was able to use Censys threat intelligence to proactively identify an advanced persistent threat attempting to impersonate one of its regional entities. The APT likely sought to impersonate the bank's domain in an attempt to collect the user login information from customers.

With Censys, FinServ organizations can tap into the world's largest x.509 certificate repository to identify similar evidence of domain impersonation, phishing attempts, and related infrastructure from nefarious actors. For example, teams can run automated queries on certificate data that will identify any new certificates created within the last 24 hours that could be related to typosquatting, look-alike domains, and spoofing.

> “
>
> **Censys allows me and my team to proactively identify and research malicious infrastructure. I use it daily and it has become an integral part of my toolset.**
>
> - Censys Customer, Enterprise Financial Services Organization

# 3 Improving Visibility into Third-Party Risk

### THE CHALLENGE

Modern FinServ organizations depend on a robust network of fintech partners and other third-party vendors. Though security teams can use Third-Party Risk Management programs to monitor risk within third-party ecosystems, many TPRM programs are unable to provide accurate and timely data, especially when zero-day vulnerabilities hit.

### THE SOLUTION

A leading global banking institution uses Censys to improve visibility into its network of nearly 2,000 critical suppliers. Censys is uniquely positioned to help augment this bank's existing TPRM program by delivering the most up-to-date and accurate information on zero-days and other risks.

Censys' daily scanning cadences, contextualized attribution, and Rapid Response alert program, which notifies customers when they could be affected by new zero-days, give this bank and other FinServ organizations the visibility they need to effectively manage third-party risk.

## Empowering the FinServ Industry with Trusted Internet Intelligence

With Censys, FinServ organizations can adopt a proactive and versatile approach to threat hunting and defending their expanding attack surfaces. Learn more about how your team can leverage Censys' unmatched view of the threat landscape at censys.com.

censys

VISIT
censys.com

CONTACT
hello@censys.com

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