censys

Your Healthcare Cyber Hygiene Checklist

Essential Steps to Strengthen Your Immunity to Cyberattacks

As cyber threats against healthcare organizations grow more frequent and advanced, staying ahead of attacks has never been more critical. Ensuring your digital infrastructure's "cyber health" remains robust is paramount to protecting patient data, critical systems, and sensitive medical devices.

Achieving complete visibility into both your network and the broader threat landscape is the cornerstone of a resilient cyber defense.

This checklist will guide your assessment of visibility and monitoring efforts, so that you can better protect your healthcare organization against a wide range of potential cyber threats.

↗ 2x

Cyberattacks on healthcare networks in the United States **more than doubled** between 2022 and 2023.[1]

Do You Have the Visibility You Need to Defend Against Cyberattacks?

KEY CAPABILITIES FOR HEALTHCARE SECURITY TEAMS

Evaluate your security posture with these critical capabilities to identify, monitor, and protect your digital assets – and prevent costly breaches.

Comprehensive Asset Discovery and Inventory

Knowing what's on your network is the first step to protecting it. Do you have a complete view of your assets?

- [ ] **I can discover all of my internet-facing assets**

  Make sure you have visibility into all public-facing assets, including cloud environments, on-prem systems, IoT devices, and shadow IT. These internet-facing assets represent potential points of entry, and most organizations have more unknown assets on their attack surface than they think. (Censys finds up to 80% of attack surfaces are unknown.)

- [ ] **I can monitor for new asset types**

  An asset discovery process should include cloud storage buckets, dynamic IPs, subdomains, and certificates. You should also be able to receive continuous updates on cloud assets across AWS, Azure, and GCP. As healthcare systems increasingly move from legacy systems to the cloud, visibility into dynamic cloud environments is imperative.

- [ ] **I have a view of all IoT devices on my attack surface**

  Internet-connected medical devices can serve as additional points of entry for attackers - yet many are left exposed and vulnerable. Make sure they're included in your attack surface discovery and management processes.

Real-Time Monitoring

You know that in cybersecurity, time is of the essence. Real-time visibility into the attack surface is crucial for staying ahead of threat actors looking to launch attacks.

- [ ] **I'm able to maintain an up-to-date asset inventory**
  Use automated discovery tools like Attack Surface Management that automatically update your asset inventory to reflect assets that have been added to or removed from your attack surface.

- [ ] **My attack surface is updated daily**
  Check that your attack surface inventory is refreshed daily, including with new domains, IPs, and services. Outdated views of your asset inventory - even just one day old - create consequential visibility gaps for your security team.

- [ ] **I have a current view of exposures on my attack surface**
  Identify exposed assets in real-time so that you can prioritize remediation efforts based on risk, particularly vulnerabilities commonly exploited by ransomware groups.

14,004

Number of **unique IP addresses** recently discovered by Censys exposing healthcare devices and data systems connected to potentially sensitive medical information on the public internet.

Supply Chain Security

Attackers increasingly target third-party healthcare ecosystems to launch attacks. The cyberattack on United Health's Change Healthcare unit, which handles a significant portion of payment processing for U.S. healthcare systems, highlighted the impact supply chain attacks can have on the broader industry.

- [ ] **I can map third-party dependencies**

  Identify and monitor all external vendors, cloud providers, and services you work with to mitigate potential supply chain risks.

- [ ] **I can track changes in vendor assets**

  Automatically update your attack surface for any changes related to mergers, acquisitions, or infrastructure updates.

- [ ] **I can monitor individual vendor risk and compliance**

  An internet intelligence source like Censys Search makes it possible to proactively observe exposures like misconfigured or outdated certificates associated with a specific vendor.

58% of individuals affected by data breaches in 2023 had data compromised after an attack was carried out on a **healthcare business associate.**[2]

Threat Detection

The ability to detect threats before attackers take action is crucial. Prevent ransomware, phishing, DDOS, and other frequent attack types on healthcare systems with enhanced threat detection efforts.

- [ ] **I can stay ahead of ransomware threats**

  Monitor your attack surface for weak points like unencrypted login pages, outdated software, default settings on critical systems, and other exposures that ransomware groups love to target.

- [ ] **I can monitor critical IT systems and relevant protocols**

  Ensure you're keeping track of the critical systems and protocols attackers will exploit, such as HL7, RIS, FHIR, and DICOM. Security teams can run queries against Censys' leading internet intelligence set to monitor systems and protocols on an ongoing basis.

Learn More →

- [ ] **I can easily utilize CVE context for risk prioritization**

  Use Common Vulnerabilities and Exposures (CVE) data to prioritize risks based on real-time exploitation information. Security tools that integrate CVE context into their datasets can help you understand relevant risk even faster.

- [ ] **I can receive immediate zero-day vulnerability alerts**

  Make sure your team receives timely notifications of zero-day vulnerabilities that affect your attack surface so you can quickly validate and patch them before an attack.

↗ **1,000**

The critical RCE vulnerability in NextGen Healthcare's MIRTH Connect platform allowed unauthorized access to sensitive patient data. Censys identified more than 1,000 exposed systems shortly after the CVE was announced.

Improve Your Cyber Hygiene with Censys

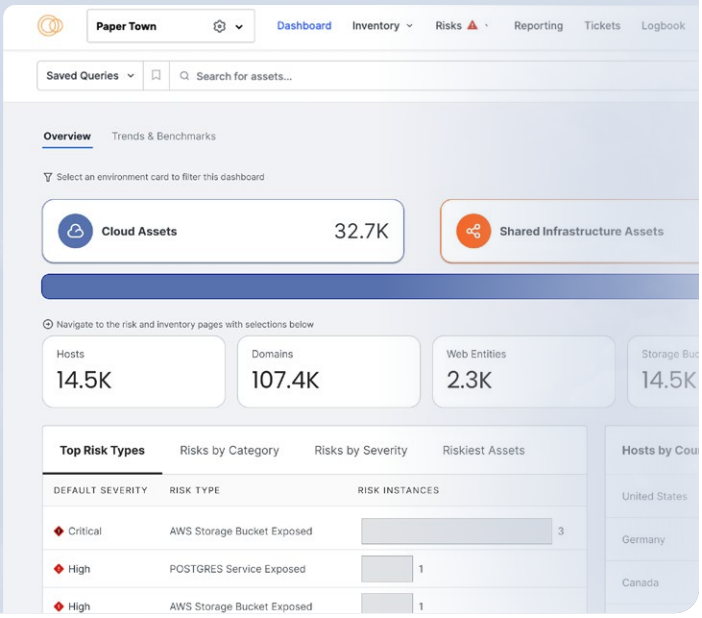
Achieving complete visibility into your attack surface and the broader threat landscape starts with access to unmatched internet intelligence.

Censys provides healthcare organizations with the most comprehensive, accurate, and up-to-date view of global internet infrastructure available, discovering new services six times faster than the nearest competitor. This intelligence is what powers our leading Attack Surface Management platform and Censys Search tool.

Comprehensive Visibility for Healthcare

Healthcare organizations of all sizes leverage Censys to continuously monitor attack surfaces and proactively investigate threats.

Learn More



[1] Cyber Threat Intelligence Integration Center
[2] Modern Healthcare

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.