

SMALL BUSINESSES, BIG RISKS:

Securing Your Digital Frontier with ASM

Small and medium-sized businesses (SMBs) are increasingly prime targets for cybercriminals. In 2023, 43% of U.S. SMBs experienced cyberattacks—a stark rise from 2021.¹ SMBs must tackle these growing threats despite limited budgets, smaller teams, and tight resources. To stay ahead, a proactive approach to security is essential.

Proactive Defense with Attack Surface Management

Your first line of defense is understanding what you need to protect. Without clear visibility into all of your internet- and cloud-facing assets, safeguarding your business is just guesswork. Attack Surface Management (ASM) offers the clarity and control SMBs need to manage their security posture effectively.

ASM is a critical security solution that identifies, inventories, and monitors all assets on an attack surface.

Here's how you can better protect your business with ASM.

43% of U.S. small and medium-sized businesses experienced cyberattacks in 2023¹

¹ [Accenture Cybercrime Study, 2023](#)

Proactive Defense with ASM

01



THE RISK

Blind Spots from Lack of Continuous Monitoring

As your business expands, so does your digital footprint. Payment systems, customer portals, and cloud services—each new connection represents a potential point of attack. Unfortunately, smaller security teams rarely have the resources to continuously monitor all assets, creating dangerous blind spots.



HOW ASM CAN HELP

Automated Asset Discovery and Continuous Coverage

ASM automates asset discovery, eliminating the need for manual checks and spotty coverage. It continuously inventories everything on your attack surface, **including S3 storage buckets, software, certificates, and other cloud and internet-facing assets you didn't even know existed.** Censys ASM's SMB offering refreshes your attack surface weekly, uncovering up to 65% more assets than competitors, giving your team the visibility they need to prioritize exposures.

65% more assets uncovered by Censys ASM's attack surface refresh compared to competitors

Proactive Defense with ASM

02



THE RISK

Unpatched Vulnerabilities Leave You Exposed

Threat actors are exploiting critical CVEs faster than ever; **the average time to exploit was 43% faster in H2 2023 than H1 2023.**² This means security teams need to act fast. However, with limited visibility, it's hard to know which vulnerabilities are relevant to your specific environment, or how impactful they are. This delay can be costly: exposed, public-facing assets are the *number one points of entry* for ransomware groups, who are increasingly targeting small businesses.³



HOW ASM CAN HELP

Instant Alerts and Risk Context

ASM takes the guesswork out of risk assessment, so that you can take immediate action. Censys ASM automatically assesses your attack surface for new vulnerabilities, and when assets are affected by a vulnerability, you'll be notified about the risk and its priority level. This means your team can close security gaps, and focus on the most critical vulnerabilities first.

Did You Know? The Censys Rapid Response program notifies you directly when a new CVE hits that affects your attack surface, and provides actionable insights powered by the Censys Research Team.

² [Fortinet Global Threat Landscape Report, 2024](#)

³ [Cyentia Ransomware Information Risks Insights Study 2024](#)

Proactive Defense with ASM

03



THE RISK

Difficulty Securing Budget Without Measurable Impact

With cybersecurity often comprising less than 6% of the average IT budget, demonstrating ROI is crucial to securing funds.⁴ But for many security teams, proving their value is a challenge without the right data.



HOW ASM CAN HELP

Built-In Reporting to Showcase Results

ASM automatically tracks and reports on the KPIs that showcase your impact. With Censys ASM's SMB offering, Quarterly Trends and Benchmarks Reports showcase **metrics like attack surface size, total active risks, and average remediation times**. The critical vulnerabilities your team addressed in record time? Let your quarterly report showcase the hard work. Historical trend analysis can provide further insight into progress over time.

6% or less of the average IT budget is typically allocated to cybersecurity

⁴ [Forrester 2024 Cybersecurity Benchmarks, Global](#)

Proactive Defense with ASM

04



THE RISK

Missed Opportunities Due to Integration Complexity

Small security teams can realize significant efficiencies and better position themselves to ward off attackers when their security tools work together. However, for teams who are already overwhelmed and understaffed, figuring out how to get tools to talk to each other can seem daunting.



HOW ASM CAN HELP

Seamless Integrations for Enhanced Efficiency

You can easily integrate Censys ASM with your existing security tools and workflows, including SIEM, SOAR, and ticketing systems. **Integrations can be deployed in 15 minutes or less**, making it simple to close data gaps and improve security operations without a heavy lift.

Get Started Today

Attackers won't wait for you to catch up. With the right tools, you can stay ahead of threats and focus on running your business. Censys ASM can empower you with the visibility, automation, and actionable intelligence you need to secure your digital assets—without overwhelming your team. Take control of your attack surface today, and turn your small business into a tough target for threat actors.



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.