Strategic Viability Assessment: Automated Security Configuration Management (ASCM) in the Era of Digital Resilience

1. Executive Strategic Assessment

The global cybersecurity market is currently navigating a profound structural transition, moving away from a decade-long focus on reactive threat detection and vulnerability patching toward a new paradigm centered on proactive digital resilience and verifiable configuration management. This report serves as an exhaustive viability assessment for a proposed software Minimum Viable Product (MVP) situated within the Automated Security Configuration Management (ASCM) domain. The analysis synthesizes market dynamics, regulatory pressures, competitive intelligence, and technological trends to determine not only the necessity of such a solution in the current market but also the precise strategic vectors required for its success.

The central thesis of this assessment is that the market viability for a new ASCM solution is currently at an optimal peak, driven by a convergence of legislative mandates—specifically the European Union's NIS2 Directive and the Digital Operational Resilience Act (DORA)—and the operational failure of legacy tools to address the complexity of hybrid infrastructure. While the market is populated with established players such as CalCom, Gytpol, and Senteon, there remains a significant, unaddressed gap for a solution that seamlessly bridges the divide between strict security compliance and operational stability through context-aware automation.

1.1 The Shift from Protection to Resilience

For years, the industry's primary obsession was "protection"—preventing the breach. However, the inevitability of cyber incidents has shifted the strategic focus of Chief Information Security Officers (CISOs) and Boards of Directors toward "resilience"—the ability to withstand, respond to, and recover from disruptions.[1] This shift is not merely philosophical; it is now codified in law. Regulations like DORA explicitly mandate that financial entities must ensure the continuity of critical functions, placing the stability of IT configurations at the center of compliance strategies.[2] In this context, a software MVP that automates system hardening is no longer just a security tool; it is a business continuity instrument. The market is demanding tools that can prove, with cryptographic certainty, that a system was hardened to a specific baseline at a specific point in time, shifting the value proposition from "best effort"

to "verifiable evidence".[3]

1.2 The "Fear of Outage" Barrier

The primary inhibitor to the adoption of hardening tools has historically been the "Fear of Outage." IT Operations teams act as gatekeepers, often rejecting security policies (such as disabling legacy protocols like NTLM or SMBv1) due to the risk of disrupting legacy applications.[4] The viability of the proposed MVP hinges entirely on its ability to solve this operational deadlock. The analysis indicates that competitors like CalCom have built their entire business model around "Impact Analysis"—the ability to simulate a policy change before enforcing it.[4] Therefore, for the MVP to be viable, it must prioritize "operational safety" features—simulation, rollback, and usage analysis—above pure security enforcement features. A tool that breaks production will be uninstalled immediately, regardless of its security benefits.

1.3 The Data-Driven Opportunity

A critical finding of this research is the potential for the MVP to disrupt the market by integrating Third-Party Risk Management (TPRM) data and business intelligence—exemplified by the capabilities of companies like Veridion—into the hardening workflow.[6] Current hardening tools operate in a vacuum, treating every server as a generic technical asset. A "Context-Aware" hardening platform that creates security policies based on the business function, location, and third-party risk profile of an asset represents a "Blue Ocean" strategy. This approach aligns with the growing demand for supply chain security mandated by NIS2, allowing the MVP to offer a unique value proposition that legacy incumbents cannot easily replicate.[7]

1.4 Viability Verdict

The proposed MVP is highly viable, provided it positions itself not as a "better vulnerability scanner," but as an "automated resilience platform" that guarantees compliance with DORA and NIS2 without disrupting business operations. The following report details the specific regulatory mechanisms driving demand, the weaknesses of current competitors, and the exact feature set required to capture market share in 2025 and beyond.

---

2. The Macro-Regulatory Environment: Compliance as the Primary Market Driver

The viability of enterprise security software is inextricably linked to the regulatory landscape. In 2025, the enforcement of stringent EU regulations creates a "compulsory consumption" dynamic, where organizations are legally obligated to purchase solutions that provide

automated hardening and configuration management.

2.1 The Digital Operational Resilience Act (DORA)

The Digital Operational Resilience Act (DORA), fully applicable as of January 2025, is a game-changer for the financial sector and its ICT providers. Unlike previous guidelines, DORA is a regulation, meaning it applies directly and uniformly across all EU member states, eliminating the fragmentation of national laws.[2]

2.1.1 The Mandate for Configuration Management

DORA moves beyond simple data protection to mandate "operational resilience." Article 9(2) requires financial institutions to implement "sound monitoring of risks," which includes the management of ICT third-party risk and the continuous monitoring of system configurations.[1] The regulation explicitly targets the integrity of ICT systems, requiring firms to detect and prevent "configuration drift"—unauthorized or accidental changes that weaken security posture.[9] This legal requirement creates immediate demand for the proposed MVP. Manual hardening—the reliance on spreadsheets and sporadic scripts—is no longer sufficient to meet the "continuous" monitoring requirements of DORA. An automated platform that continuously enforces a "Golden Image" and reports on deviations becomes a necessary compliance artifact.[10]

2.1.2 ICT Risk Management and Liability

Under DORA, financial entities must maintain a "complete register of outsourced activities" and monitor the risks associated with third-party providers.[1] This connects directly to the MVP's potential integration with data enrichment sources like Veridion. By using external data to assess the risk profile of software vendors installed on hardened endpoints, the MVP can help customers satisfy DORA's Third-Party Risk Management (TPRM) requirements.[7] Furthermore, DORA introduces strict incident reporting timelines (e.g., 72 hours for full reports), necessitating tools that can instantly correlate a security incident with a specific configuration change or vulnerability.[11]

2.2 The NIS2 Directive

The NIS2 Directive significantly expands the scope of regulated entities to include "essential" and "important" sectors such as energy, transport, health, water, and digital infrastructure.[12]

2.2.1 Management Liability and Accountability

NIS2 introduces a powerful economic driver for the adoption of automated tools: personal liability for management bodies. Article 20 states that the management bodies of essential entities must approve cybersecurity measures and supervise their implementation, and they can be held personally liable for non-compliance.[13] This fundamentally changes the sales conversation for the MVP. The buyer is no longer just the IT Manager; it is the Board of

Directors seeking protection from liability. The MVP's reporting capabilities must therefore be designed to provide "Executive Assurance"—clear, non-technical metrics that prove compliance with NIS2 standards.[14]

2.2.2 The "Cyber Hygiene" Requirement

Article 21 of NIS2 outlines ten baseline cybersecurity measures that mandated entities must implement. Crucially, this list includes "basic computer hygiene practices," which encompasses software updates, password management, and—most relevant to the MVP—system hardening.[14] This elevates system hardening from a "best practice" to a statutory requirement. Organizations can no longer opt out of hardening because it is "too difficult." They must implement it to avoid fines of up to €10 million or 2% of global annual turnover.[14] The MVP provides the automation necessary to implement these hygiene practices at scale, making it a critical compliance tool.

2.2.3 Supply Chain Security

NIS2 mandates that organizations address the cybersecurity risks of their supply chains.[12] This creates a network effect: large regulated entities will force their smaller suppliers to demonstrate security compliance. The MVP can target these smaller suppliers (SMEs) with a "lite" version of the platform, helping them meet the security requirements demanded by their enterprise customers. This "trickle-down" compliance pressure significantly expands the Total Addressable Market (TAM) for the MVP beyond just large enterprises.[8]

2.3 Broader Global Standards (CIS, NIST)

Beyond EU regulations, the global standard for hardening remains the Center for Internet Security (CIS) Benchmarks and the NIST Cybersecurity Framework.

- **CIS Benchmarks:** These are prescriptive configuration guides (e.g., "Set 'Minimum Password Age' to 1"). The research indicates that leading competitors like Senteon and CalCom explicitly market their ability to align with CIS standards.[16] The MVP must natively support CIS Level 1 and Level 2 profiles to be competitive.
- **NIST SP 800-53/171:** For US markets, particularly defense contractors, adherence to NIST guidelines is mandatory (e.g., CMMC compliance). Partnerships between hardening firms like Coalfire and C3 Integrated Solutions demonstrate the high value placed on tools that accelerate NIST compliance.[18]

2.4 Market Sizing and Growth Trends

The market for Security Configuration Management is experiencing robust growth, driven by these regulatory tailwinds.

- **Market Growth:** The global configuration management market is projected to grow from approximately $2.8 billion in 2023 to over $9 billion by 2032, with a Compound Annual Growth Rate (CAGR) of around 13.9% to 15.6%.[19]

- **Security Automation:** The broader security automation market is also surging, expected to reach over $20 billion by 2034.[21]
- **Segment Dominance:** The "Server Infrastructure" segment currently dominates the market, but the "Security Devices" and "Cloud Resources" segments are growing rapidly, highlighting the need for tools that can harden hybrid environments.[20]

---

3. The Core Operational Problem: Why Incumbents Fail

Despite the availability of Vulnerability Management (VM) tools from giants like Tenable, Rapid7, and Qualys, the market for dedicated hardening solutions remains vibrant. This is because legacy VM tools fundamentally fail to address the operational realities of configuration management.

3.1 The "Fear of Outage" and Operational Deadlock

The single most significant barrier to hardening is the fear that changing a configuration will disrupt production services.

- **The Scenario:** A security scan identifies that "SMBv1" is enabled on a critical server. The security team demands it be disabled to prevent ransomware. The IT Operations team refuses, fearing that an old printer or legacy application relies on SMBv1 and will stop working.
- **The Deadlock:** Without a way to know for sure, the setting is left insecure. This "Fear of Outage" paralysis is ubiquitous in enterprise IT.[4]
- **Incumbent Failure:** Standard VM scanners identify the risk ("SMBv1 is On") but offer no insight into the *impact* of fixing it ("Will disabling it break anything?"). They act as auditors, not engineers. This leaves the Operations team with the burden of testing, which often leads to inaction.[22]

3.2 Vulnerability Management vs. Configuration Management

It is crucial to distinguish between software vulnerabilities (CVEs) and configuration vulnerabilities.

- **CVEs:** These are bugs in code (e.g., Log4Shell) that require a patch. VM tools excel here.
- **Misconfigurations:** These are "features" left in an insecure state (e.g., Default Passwords, Permissive RDP, Unencrypted Backups). These require a *policy change*, not a patch.
- **The Gap:** VM tools often treat misconfigurations as low-priority "informational" findings. They lack the granular control to remediate them safely. For example, a VM tool might tell you to "Disable RDP," but it won't help you create the complex firewall rule exception needed to keep the administrator's access while blocking the internet.[22]
- **The Opportunity:** The MVP can position itself as a "Configuration Assurance" platform that picks up where VM tools leave off. It handles the "last mile" of security—the complex,

context-dependent settings that scanners ignore.

3.3 The Problem of "Configuration Drift"

Systems do not stay hardened. Administrators make temporary changes for troubleshooting (e.g., "I'll just disable the firewall for 5 minutes") and forget to revert them. Updates and patches can reset configurations to insecure defaults.

- **Continuous Enforcement:** DORA and NIS2 require *continuous* monitoring. Periodic scans (weekly/monthly) are insufficient to detect drift in real-time. The MVP must offer real-time drift detection and automated remediation (or "self-healing") to maintain the compliant state.[9]
- **Legacy Tool Weakness:** Many legacy tools are "scan-and-report" engines. They take a snapshot in time. They do not maintain a continuous state of enforcement, leaving a window of vulnerability between scans.[24]

---

4. Technological Paradigms and Architecture

To successfully compete in the modern market, the MVP must leverage contemporary technological architectures. The research highlights several key trends that differentiate modern solutions from legacy software.

4.1 Agent vs. Agentless vs. Semi-Agent

The architecture of the endpoint collector is a critical strategic decision.

- **Heavy Agents (Legacy):** Competitors like CalCom often rely on persistent agents. While powerful, these are disliked by IT teams due to performance overhead and the complexity of management.[24]
- **Agentless (Cloud-Native):** Solutions like Orca Security use "SideScanning" to assess cloud workloads without touching the OS. This is low-friction but often lacks the depth to change OS-level registry settings or manage on-premise hardware effectively.[25]
- **Semi-Agent (The Gytpol Model):** Gytpol uses a "semi-agent" or non-persistent executable triggered by the Task Scheduler. It runs, checks/remediates, and then terminates. This "lightweight" approach reduces the performance footprint and friction with IT, making it a highly attractive model for the MVP to emulate.[22]

4.2 The "Simulation Engine" (Learning Mode)

To overcome the "Fear of Outage," the MVP must implement a Simulation or Learning Mode.

- **Mechanism:** This feature monitors system logs and traffic to predict the impact of a policy. For example, before enforcing "NLA Only for RDP," the system checks the security logs for any successful RDP connections that *didn't* use NLA.
- **Value:** It produces a report: "If you enforce this policy, Users A and B will be locked out."

This empowers the admin to fix the users' clients *before* enforcing the server policy, guaranteeing zero downtime. This capability is the primary differentiator for market leaders like CalCom and must be a core feature of the MVP.[4]

4.3 Security Knowledge Graphs

The complexity of modern infrastructure requires a sophisticated data model. Linear databases (SQL tables of assets) are insufficient to capture the interdependencies of security risks.

- **Graph Theory:** Security Knowledge Graphs map the relationships between assets, identities, vulnerabilities, and configurations. For example, a graph can reveal that "Server A is critical not because of its data, but because it holds a stored credential that grants access to the Production Database."
- **Market Trend:** Startups like Cyscale and 7AI are leveraging graph technologies to provide context-aware security. The MVP should utilize a graph database (e.g., Neo4j) to model these relationships, allowing for advanced queries like "Show me all assets exposed to the internet that are also missing the latest CIS hardening patch".[26]

4.4 Agentic AI and Autonomous Remediation

The frontier of cybersecurity in 2025 is "Agentic AI"—autonomous agents capable of reasoning, planning, and executing complex tasks.

- **Beyond Chatbots:** Unlike simple LLM chatbots, agentic AI can take action. It can triage alerts, investigate root causes, and propose remediation plans.
- **Application to MVP:** The MVP can incorporate "AI Agents" that assist with the hardening process. An agent could analyze a simulation report and say, "I see 3 exceptions to this policy. I recommend creating a specific exclusion group for these 3 servers and enforcing the policy on the rest. Shall I proceed?" This lowers the skill barrier for junior administrators and accelerates remediation.[29]

---

5. Competitive Landscape Analysis

The market is segmented into distinct tiers of competitors: Specialized Hardening Vendors, Vulnerability Management Giants, and Emerging Startups.

5.1 Specialized Hardening Vendors (Direct Competitors)

5.1.1 CalCom (CalCom Hardening Suite - CHS)

CalCom is the established leader in the "Zero Outage" hardening space, particularly for large enterprises and critical infrastructure.

- **Core Value Proposition:** Their entire brand is built on the promise of preventing downtime through their "Learning Mode." They focus heavily on the "Impact Analysis"

phase of the workflow.[4]

- **Target Market:** High-end enterprise, healthcare, and finance. Their pricing reflects this, with subscription models estimated around **$240 per server/year** and minimum server counts (e.g., 100 servers).[31]
- **Strengths:** Deep expertise in OS hardening; strong reputation in regulated industries; proven "Learning Mode" technology.[5]
- **Weaknesses:** Legacy architecture (heavy reliance on SCOM/SCCM in older versions); high cost; opaque pricing; traditional sales motion (no self-service).[4]

5.1.2 Gytpol (The "Validator")

Gytpol positions itself as a validator of configuration health, focusing on the gap between intended policy and actual state.

- **Core Value Proposition:** "Validation" and "Remediation without disruption." They differentiate by analyzing "Usage"—checking if a vulnerable setting is actively used before disabling it.[32]
- **Architecture:** Lightweight "semi-agent" (task scheduler driven), which is easier to deploy than CalCom's persistent agents.[22]
- **Pricing:** Public sector pricing indicates ~£50 ($65) per unit/year, but enterprise deals are often sold in large blocks (e.g., $300k contracts), suggesting a high barrier to entry for smaller customers.[10]
- **Strengths:** Fast remediation; "Revert" capability; strong focus on "Usage" analytics to prevent breakage.[22]

5.1.3 Senteon

Senteon is a newer entrant focused on the MSP channel and CIS Benchmark alignment.

- **Core Value Proposition:** Simplifying CIS compliance for MSPs. They focus on "drift management" and maintaining the score over time.[33]
- **Target Market:** MSPs and mid-market organizations.
- **Strengths:** Modern interface; MSP-friendly multi-tenancy; strong alignment with CIS standards.[17]

5.2 Vulnerability Management Incumbents (Secondary Competitors)

5.2.1 Tenable, Qualys, Rapid7

These are the giants of the industry. They dominate the "Scan and Identify" market.

- **Relationship to MVP:** They are "frenemies." They identify the misconfigurations but rarely fix them effectively.
- **Weakness:** Their remediation capabilities are often limited to integrations (e.g., opening a Jira ticket) rather than direct, safe action on the endpoint. They lack the "Simulation" capabilities of CalCom/Gytpol, meaning their "Fix" buttons are viewed as dangerous by

Ops teams.[23]
- **Pricing:** Tenable.io starts around $3,000-$5,000 for small asset blocks but scales aggressively. Tenable One (unified exposure management) starts at $50,000+.[23]

5.3 Emerging Startups and Disruptors

5.3.1 Aikido Security

Aikido represents the "Developer-First" approach.

- **Strategy:** It targets the software development lifecycle (SDLC), scanning code and containers before deployment. It uses a "Freemium" model and transparent pricing ($350/month) to capture the mid-market.
- **Relevance:** Aikido proves that a "bottom-up," transparently priced security product can disrupt the enterprise sales models of giants like Tenable.[35]

5.3.2 7AI and Agentic Startups

New startups like **7AI** are raising massive funding ($130M Series A) to build "Agentic Security" platforms that use AI agents to automate triage and response. This validates the investor appetite for AI-driven automation in security operations.[30]

---

6. The "Blue Ocean" Strategy: Context-Aware Hardening

The competitive analysis reveals that while the "technical hardening" space is contested, the "business-aware hardening" space is virtually empty. This is where the integration of **Veridion** (Business Data) creates a massive opportunity.

6.1 The Context Gap

Current tools (CalCom, Gytpol) operate on **Technical Context**: "This server has 4 CPUs and runs Windows 2019." They lack **Business Context**: "This server processes payments for the German subsidiary."

- **The Problem:** Hardening rules often need to be tailored to business risk. A server in a high-risk geopolitical region needs stricter hardening than an internal print server. Currently, this tagging is done manually, if at all.

6.2 The Solution: Data-Enriched Hardening

By integrating Veridion's data enrichment APIs, the MVP can automate the application of context.

- **TPRM Integration:** Veridion data can identify the business activities and risks associated

with third-party software vendors found on the endpoints.[6]

- **Use Case:** The MVP detects a niche accounting software installed on a workstation.
  - *Standard Tool:* Ignores it or checks for CVEs.
  - *MVP with Veridion:* Queries Veridion's database. Identifies the software vendor. Checks the vendor's ESG and Risk scores. If the vendor is flagged as "High Risk" (e.g., sanctions, poor security history), the MVP automatically applies a "Zero Trust" hardening policy to that workstation, restricting its network access.
- **Strategic Value:** This capability directly addresses DORA's requirement for **ICT Third-Party Risk Management**, turning the hardening tool into a comprehensive Risk Management Platform.[1]

---

7. Commercial Strategy and Pricing Models

To penetrate the market, the MVP must adopt a pricing model that disrupts the high-cost, high-friction models of the incumbents.

7.1 Competitor Pricing Benchmarks

The following table summarizes the estimated pricing landscape:

Competitor	Pricing Model	Estimated Cost	Segment Focus
Gytpol	Per Unit / Block	£50 ($65) per endpoint/year (High Minimums) [32]	Enterprise / Gov
CalCom	Per Server (Subscription)	~$240 per server/year (Min 100 servers) [31]	Enterprise (Critical Infra)
Tenable.io	Asset-based	~$38-$50 per asset/year [23]	General Market
Senteon	MSP / Per Endpoint	Custom (Likely $2-$5/endpoint/month)	MSP / Mid-Market
Aikido	Flat Rate / Tiered	~$350/month (Team) [37]	Dev / Mid-Market

7.2 Disruptive Pricing Strategy for the MVP

The MVP should utilize a **"Land and Expand"** model with transparent, tiered pricing to lower the barrier to entry.

7.2.1 Freemium Tier ("The Validator")

- **Offer:** Free "Audit Mode" agent. Scans endpoints and reports on misconfigurations and compliance gaps (CIS/DORA).
- **Goal:** Functions as a lead magnet. Demonstrates value immediately by showing the user their risk posture ("You are only 40% DORA compliant").
- **Psychology:** Once the user sees the "Red" dashboard, they are motivated to pay for the "Green Button" (Remediation).

7.2.2 Commercial Tier ("The Enforcer")

- **Pricing:**
  - **Workstations:** $25/year per device. (Aggressive pricing to undercut Gytpol and capture volume).
  - **Servers:** $120/year per device. (Undercuts CalCom by 50% while offering similar "No Outage" guarantees).
- **Features:** Includes Remediation, Simulation/Learning Mode, and Auto-Rollback.

7.2.3 Premium Tier ("The Compliance Suite")

- **Pricing:** +$5,000/year Platform Fee.
- **Features:** "Audit-Ready" Reporting Packs for DORA, NIS2, and HIPAA. Access to the **Veridion Data Integration** for Third-Party Risk Context.
- **Logic:** Enterprise customers are less price-sensitive regarding regulatory compliance. Charging a premium for the specific reports they need for auditors captures this value without raising the per-asset price for the operational teams.

7.3 The "Service to SaaS" Pivot

If the current "project" is born out of a consulting practice, the transition to SaaS must be managed carefully.

- **The Trend:** There is a strong market trend of "Service to SaaS" pivots, where consulting firms automate their manual processes into software products. This increases valuation multiples from ~3x (Services) to ~10x (SaaS).[38]
- **Strategy:** Use the software internally first to deliver "Tech-Enabled Services." Sell a hardening audit, use the MVP to deliver it in half the time, and then upsell the client on retaining the software for continuous monitoring. This "Trojan Horse" strategy builds a paid user base while validating the product.[39]

---

8. Technical Implementation Roadmap

To be considered a "Viable" competitor to CalCom and Gytpol, the MVP must meet specific technical requirements derived from hardening standards and competitor capabilities.

8.1 Core Hardening Capabilities

Based on the Cisco and General Hardening guides [16], the MVP must support:

- **Protocol Hardening:** Automated disabling of SMBv1, LLMNR, NTLM, and weak TLS ciphers.
- **Access Control:** Verification of local admin group membership (removing unauthorized users).
- **Logging & Auditing:** Ensuring that audit logs (Security Event Log) are configured to capture relevant events (e.g., Process Creation, Login Failures) as required by DORA incident reporting.[9]
- **Network Security:** Management of host-based firewalls (Windows Defender Firewall / iptables) to lock down ports like RDP (3389) and SSH (22) to authorized IPs only.

8.2 The "Simulation Engine" (Must-Have)

The MVP *must* implement a simulation capability.

- **How:** For Windows, this can be achieved by ingesting Event Logs. To simulate "Block NTLM," the agent queries the Microsoft-Windows-NTLM/Operational log for Event ID 8002/8003 (NTLM usage). If recent events exist, the simulation reports "Fail."
- **Why:** This is the only way to compete with CalCom's "Zero Outage" promise. Without this, the tool is just a dangerous script.[4]

8.3 Architecture Specifics

- **Graph Database:** Use a graph backend (Neo4j) to map asset relationships. This enables queries like "Find all servers managed by Admin X that have Vulnerability Y".[27]
- **API-First:** Unlike CalCom, the MVP should be API-first to allow integration with SIEMs (Splunk, Sentinel) and ITSM tools (ServiceNow), which is critical for enterprise workflows.[43]

---

9. Conclusion

The assessment of the software MVP confirms **High Market Viability**. The convergence of the DORA and NIS2 regulations in 2025 has transformed Security Configuration Management from a "nice-to-have" into a "must-have" for thousands of EU and global organizations. The "Fear of Outage" remains the primary barrier to adoption, creating a lucrative opportunity for a solution that can guarantee operational safety through simulation and impact analysis.

By positioning the MVP as a **"Resilience Platform"** that combines the "Zero Outage" safety of CalCom with the **"Context Awareness"** of data providers like Veridion, the project can carve

out a defensible niche against both legacy incumbents and generic vulnerability scanners.

Strategic Recommendations Summary

Strategic Pillar	Recommendation	Rationale
Product Positioning	**"Safe Compliance"**	Focus on DORA/NIS2 liability reduction + "Zero Outage" guarantee.
Key Feature	**Simulation/Impact Analysis**	Essential to overcome the "Fear of Outage" barrier (CalCom's moat).
Differentiation	**Context-Aware Hardening**	Integrate Veridion data to bring business/TPRM context to technical hardening.
Pricing	**Disruptive Tiered Model**	Free Audit tier + Aggressive per-endpoint pricing to undercut Enterprise tools.
Sales Channel	**MSP & Insurance**	Partner with MSPs (like Senteon) and Cyber Insurers who need proof of hardening.

The window of opportunity is open. The regulatory deadline of January 2025 for DORA and NIS2 creates a sense of urgency that the MVP must capitalize on immediately.

Works cited

1. Digital Operational Resilience Act (DORA) - PwC, accessed December 10, 2025, https://www.pwc.com/mt/en/services/pwc-digital-services/cyber-security-and-privacy/cyber-security-services/dora.html
2. DORA & Authentication Master Guide - Secfense, accessed December 10, 2025, https://secfense.com/blog/dora-and-authentication-master-guide
3. Key Security Trends VARs and ISVs Should Prioritize in 2026 - - RSPA, accessed December 10, 2025, https://www.gorspa.org/commiq-key-security-trends-vars-and-isvs-should-prioritize-in-2026/

4. CalCom Hardening Solution: Pricing, Free Demo & Features - Software Finder, accessed December 10, 2025, https://softwarefinder.com/cybersecurity/calcom-hardening-solution
5. Automate Server Hardening | Reduce Downtime with CHS - CalCom Software, accessed December 10, 2025, https://calcomsoftware.com/server-hardening-suite/
6. Data for ESG - Veridion, accessed December 10, 2025, https://veridion.com/data-for-esg/
7. Data for TPRM - Veridion, accessed December 10, 2025, https://veridion.com/data-for-tprm/
8. How NIS2 is redefining cybersecurity for industrial and energy systems, accessed December 10, 2025, https://iebmedia.com/technology/cybersecurity/how-nis2-is-redefining-cybersecurity-for-industrial-and-energy-systems/
9. DORA: What does the EU regulation have to do with System Hardening? [Update], accessed December 10, 2025, https://www.fb-pro.com/eu-regulation-dora/
10. GYTPOL - AWS Marketplace, accessed December 10, 2025, https://aws.amazon.com/marketplace/pp/prodview-loyro4dd4vfls
11. What is the DORA Act? Security, Risk Requirements Explained - Concentric AI, accessed December 10, 2025, https://concentric.ai/what-is-the-dora-act-a-guide-to-dora-security-and-risk-requirements/
12. What Is the NIS2 Directive? Compliance Requirements | Proofpoint US, accessed December 10, 2025, https://www.proofpoint.com/us/threat-reference/nis2-directive
13. NIS2 Directive: Cybersecurity requirements and obligations - SailPoint, accessed December 10, 2025, https://www.sailpoint.com/identity-library/nis2-directive
14. NIS2 Directive: All You Need to Know - Entrust, accessed December 10, 2025, https://www.entrust.com/resources/learn/nis-2
15. NIS2 Requirements | 10 Minimum Measures to Address - The NIS2 Directive, accessed December 10, 2025, https://nis2directive.eu/nis2-requirements/
16. What are CIS Benchmarks? - IBM, accessed December 10, 2025, https://www.ibm.com/think/topics/cis-benchmarks
17. Top Senteon System Hardening Alternatives in 2025 - Slashdot, accessed December 10, 2025, https://slashdot.org/software/p/Senteon-System-Hardening/alternatives
18. Coalfire® and C3 Integrated Solutions Announce Strategic Partnership to Accelerate CMMC Compliance, accessed December 10, 2025, https://coalfire.com/insights/news-and-events/press-releases/coalfire-and-c3-integrated-solutions-announce-strategic-partnership-to-accelerate-cmmc-compliance
19. Configuration Management Market Share | Industry Report, 2032 - Fortune Business Insights, accessed December 10, 2025, https://www.fortunebusinessinsights.com/configuration-management-market-109790

20. Configuration Management Market Size, Share and Analysis | Trends – 2032, accessed December 10, 2025, https://www.skyquestt.com/report/configuration-management-market
21. Security Automation Market Report 2025, Share And Analysis, accessed December 10, 2025, https://www.thebusinessresearchcompany.com/report/security-automation-global-market-report
22. Product Analysis, accessed December 10, 2025, https://gytpol.com/hubfs/Downloadable%20Assets/Comparison-Analysis.pdf?hsLang=en
23. Tenable Pricing Overview: A Guide on Security Products - UnderDefense, accessed December 10, 2025, https://underdefense.com/industry-pricings/tenable-pricing-2025-ultimate-guide-for-security-products/
24. CalCom Hardening Suite (CHS) - SoftwareOne Marketplace, accessed December 10, 2025, https://platform.softwareone.com/product/calcom-hardening-suite-chs/PCP-7739-5006
25. Best Coalfire Alternatives & Competitors - SourceForge, accessed December 10, 2025, https://sourceforge.net/software/product/Coalfire/alternatives
26. About us - Cyscale, accessed December 10, 2025, https://cyscale.com/about-us/
27. Predictive Analysis from Massive Knowledge Graphs on Neo4j, accessed December 10, 2025, https://neo4j.com/blog/knowledge-graph/predictive-analysis-from-massive-knowledge-graphs-on-neo4j/
28. Why the world needs Cyscale in a post-Wiz era, accessed December 10, 2025, https://cyscale.com/blog/why-the-world-needs-cyscale-post-wiz-era/
29. 2025 Trends on AI Security: How AppSec Must Evolve with the AI-Shifted SDLC, accessed December 10, 2025, https://checkmarx.com/learn/ai-security/2025-trends-on-ai-security-how-appsec-must-evolve-with-the-ai-shifted-sdlc/
30. The 10 Hottest Cybersecurity Startups Of 2025 - CRN, accessed December 10, 2025, https://www.crn.com/news/security/2025/the-10-hottest-cybersecurity-startups-of-2025
31. 1 year Calcom Hardening Solution subscription per server - minimum of — XTIVIA, accessed December 10, 2025, https://software.xtivia.com/products/1-year-calcom-hardening-solution-subscription-per-server-minimum-of-100-servers
32. Gytpol validator - Digital Marketplace, accessed December 10, 2025, https://www.applytosupply.digitalmarketplace.service.gov.uk/g-cloud/services/273889516897725
33. Page 17 | Top Cybersecurity Software for Startups in 2025 - Slashdot, accessed December 10, 2025, https://slashdot.org/software/cybersecurity/f-startup/?page=17

34. Tenable pricing 2025: Is it worth It? - Beagle Security, accessed December 10, 2025, https://beaglesecurity.com/blog/article/tenable-pricing.html
35. Best Security Automation Tools & SOAR Platforms in 2025 - Aikido, accessed December 10, 2025, https://www.aikido.dev/blog/top-security-automation-tools
36. Stellar Startup Security Technology Vendors To Know In 2025 - CRN, accessed December 10, 2025, https://www.crn.com/news/security/2025/stellar-startup-security-technology-vendors-to-know-in-2025
37. 26 Best Security Testing Tools Reviewed in 2025 - The CTO Club, accessed December 10, 2025, https://thectoclub.com/tools/best-security-testing-tools/
38. Unlock Value In Your Enterprise By Repositioning Your Tech Base As A Product, accessed December 10, 2025, https://www.avi.com/content-hub/unlock-value-in-your-enterprise-by-repositioning-your-tech-base-as-a-product/
39. Drum Cussac - ScaleUp Capital, accessed December 10, 2025, https://scaleupcapital.com/case-study/drum-cussac/
40. Cloud Security Consulting: Why you need a DevOps Mindset - base2Services, accessed December 10, 2025, https://blog.base2services.com/cloud-security-consulting-why-you-need-a-devops-mindset
41. IOS - NXOS Hardening | PDF - Scribd, accessed December 10, 2025, https://www.scribd.com/document/448718084/IOS-NXOS-Hardening
42. Cisco NX-OS Software Hardening Guide, accessed December 10, 2025, https://sec.cloudapps.cisco.com/security/center/resources/securing_nx_os.html
43. Top 10 Best Security Orchestration, Automation, And Response (SOAR) Tools In 2025, accessed December 10, 2025, https://cyberpress.org/best-security-orchestration-automation-and-response-tools/