SECHARD
Complete Zero Trust

Cybersecurity Vendor Consolidation

(Enhancing Security Posture and Operational Efficiency)

Cybersecurity vendor consolidation streamlines your security infrastructure, reducing complexity and management overhead. By working with fewer vendors, you decrease the number of potential attack surfaces, simplify integration between tools, and gain better visibility into your overall security posture.

www.sechard.com

INTRODUCTION

The Need for Vendor Consolidation: 2024's Focus on Security Simplification

The cybersecurity landscape is in a state of overload. A recent report (by the Ponemon Institute) found that the average organization utilizes a staggering 75 cybersecurity tools. While intended to bolster defenses, this sprawl of solutions brings unintended consequences – maintenance burdens, fragmented visibility, skyrocketing costs, and overwhelming strain on security teams. In response, vendor consolidation has emerged as a top priority.

Vendor consolidation is increasingly gaining steam among security practitioners. As noted in the 2023 Pen Testing Report, 80% of participants consider vendor consolidation to be at least somewhat important. Organizations are tired of 'shelfware' and the wasted resources that complex ecosystems incur. It's clear that a shift towards simplification is vital – streamlining operations, amplifying efficiency, and making the most of valuable cybersecurity budgets.

The push is towards multi-functional platforms that easily integrate, maximizing functionality while minimizing vendor juggling. Security teams seek intuitive dashboards that paint a complete picture of their risk landscape, empowering them to proactively respond to threats. The age of endless point solutions accumulating alerts is waning. 2024 is demanding streamlined control, optimized spending, and an emphasis on strategic, focused technology in the fight against modern cyberthreats.

Here's why companies should seriously consider vendor consolidation:

Complexity is Risk

Trying to manage an overgrown vendor landscape poses its own risks. Consolidation minimizes supply chain issues, and potential vulnerabilities from unmaintained technology. It simply takes the strain off of teams trying to do too much.

Boost Operational Efficiency

Businesses waste significant time and resources dealing with multiple vendors and navigating separate interfaces. Consolidated solutions mean simpler management, fewer handoffs between teams, and a clearer understanding of responsibilities.

Ease Compliance Burden

Regulatory landscapes have also grown in complexity. Having fewer vendors to manage, audit, and track streamlines compliance processes and makes demonstrating adherence to regulations a smoother task.

Build Stronger Vendor Partnerships

Organizations benefit from fostering deeper relationships with a select group of key vendors. This gives businesses better support, greater alignment with long-term goals, and a voice in shaping product development.

Gain Greater Visibility

A fragmented solution set leads to blind spots and security gaps. Consolidating tools lets a company get a single, comprehensive view of their security posture. This improved visibility is key to spotting potential problems and responding to incidents quickly.

Optimize Costs

Multiple vendors bring multiple invoices and hidden costs. Opting for fewer, more strategic vendors simplifies billing, provides opportunities for bulk discounts, and allows budgets to be better allocated towards proactive security needs.

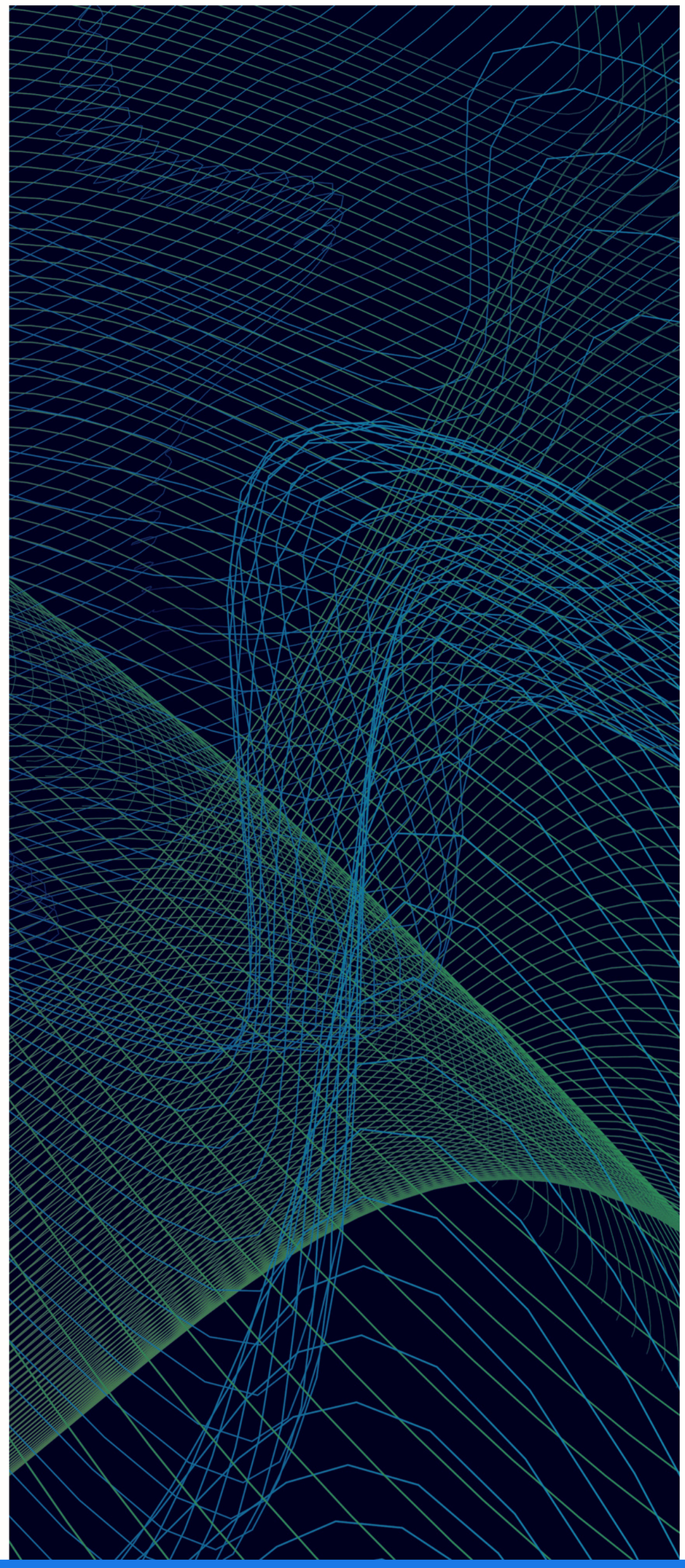
SECHARD
Complete Zero Trust

Reducing Complexity Lowers Risk

Complex landscapes breed unseen vulnerabilities. Each vendor has its own potential supply chain risk and an extra attack surface that's difficult to fully secure.

Consolidation lessens the number of integrations requiring oversight and eliminates potential issues around software compatibility and unexpected patch conflicts. A simplified stack provides a clearer picture of where threats are most likely to originate, reducing the likelihood of attacks slipping past outdated systems or neglected third-party integrations.

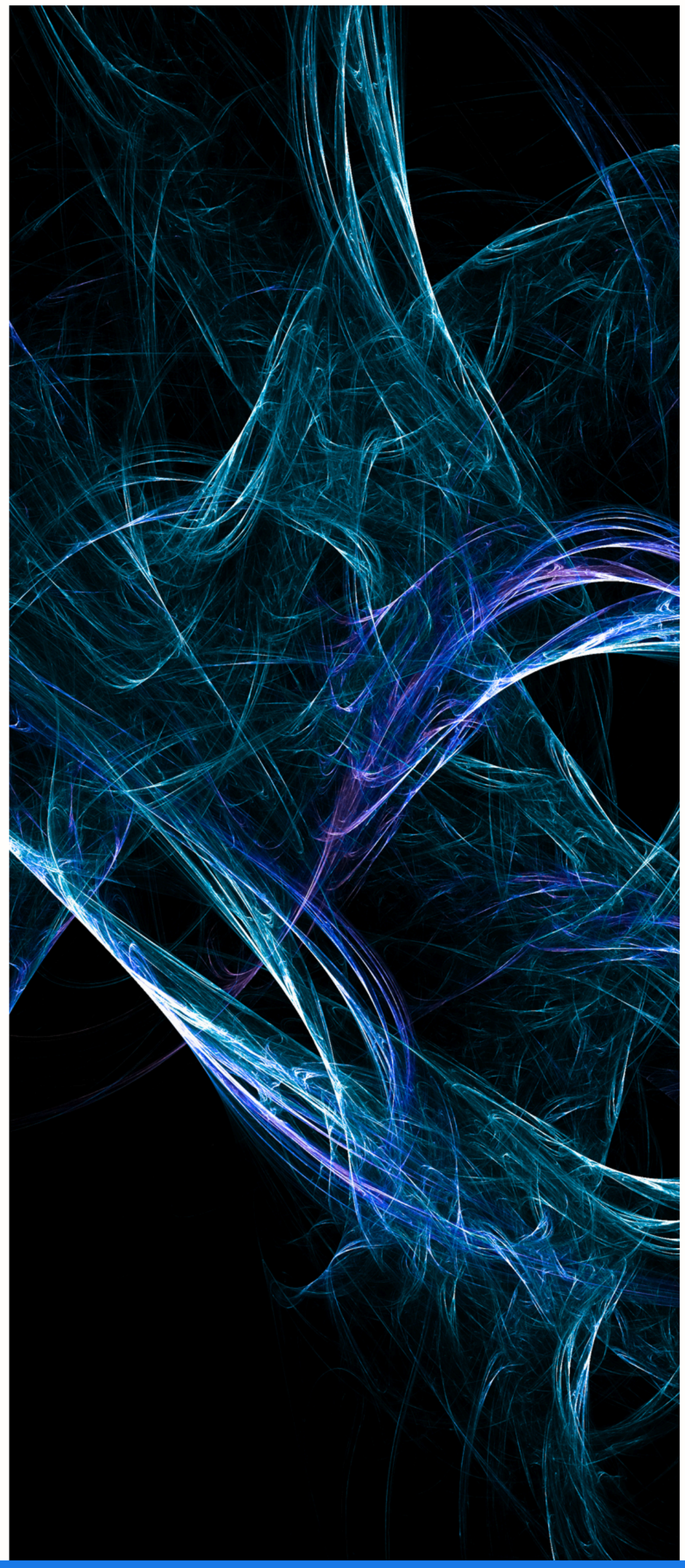
Additionally, an overly complex stack puts a strain on IT and security teams. Juggling disparate tools creates greater opportunities for misconfiguration errors, missed updates, or misapplied policy settings. Simplifying the security environment creates room for focus, attention to detail, and a reduced likelihood of human error that might invite threat actors.



SECHARD
Complete Zero Trust

Enhanced Visibility and Control

When tools are scattered and unintegrated, security teams lack a bird's eye view of their vulnerabilities. This is akin to a fragmented map – you can see pieces, but not the full picture of risk exposure. Consolidating vendors provides a comprehensive dashboard and insights across your environment. You'll understand where critical data lives, where access controls are inconsistent, and how different systems interact (and where those interactions pose threats). With this heightened visibility, you can quickly pinpoint anomalies and proactively remediate weaknesses, rather than reacting to threats that have already caused damage.



This streamlined, centralized view reduces the attack surface. Uncovering redundant tools allows you to sunset unnecessary solutions, and gaps in protection become immediately apparent. This focus on critical needs lets you allocate resources appropriately and prevents wasting budget and effort on tools that have little impact on your security posture.

Streamlined Operations and Efficiency

Vendor sprawl is a drain on productivity. Each vendor means different interfaces, policy structures, and reporting mechanisms. IT and security teams lose valuable time switching between applications and deciphering different alert structures. This operational chaos diverts focus from strategic planning and vulnerability analysis. Vendor consolidation brings consistency and clarity. Teams can dedicate more time to proactive security actions instead of juggling different vendors and trying to integrate their tools.

This streamlined approach empowers teams to become specialists in a smaller number of core security platforms. It also reduces 'alert fatigue' from a never-ending stream of unprioritized notifications. With more consistent management practices, and an increased understanding of what 'normal' looks like in your system, threat detection and response times improve dramatically.

Stronger Vendor Relationships

Working with a carefully managed circle of vendors creates a foundation for real partnership. Instead of juggling a dizzying number of representatives and support desks, you can develop long-term relationships with core security suppliers. This translates into faster, more efficient issue resolution and troubleshooting as vendors grow familiar with your unique needs and infrastructure.

Stronger relationships can also help shape the future security landscape. When a vendor becomes a true partner, you gain direct influence over a tool's development roadmap. Your pain points, threat assessments, and future security plans become valuable feedback that they can incorporate into product updates, increasing the value alignment between your business needs and your tools.

Improved Compliance

With multiple vendors, demonstrating compliance requires coordinating security audits and evidence gathering across many platforms. This is time-consuming and prone to errors.

Consolidation eases the compliance burden by providing a single view of risk posture aligned with compliance frameworks. Centralized logging and reporting streamline the audit process, allowing you to quickly generate required documentation and reports.

Consolidation also reduces the surface area for breaches that could disrupt compliance or trigger costly reporting processes. You have fewer vendors to track in terms of their own security practices, giving you more confidence when facing third-party compliance scrutiny.

Cost Optimization

Managing numerous vendor relationships carries high overhead. Each software vendor brings unique licensing, maintenance, and renewal cycles. Tracking these details becomes a complex task in itself.

This is compounded by the cost of training personnel to use distinct solutions. With vendor consolidation, organizations can negotiate volume discounts and streamlined contracts. This frees up capital that might be better spent on advanced security tools, user awareness programs, or increasing headcount in critical areas.

Beyond pure cost savings, consolidation helps find hidden waste. Auditing your ecosystem will uncover licenses for forgotten tools, services for underutilized systems, and overlapping redundancies. When you reduce complexity, you stop paying for things you no longer need or which provide duplicate capabilities.

SECHARD
Complete Zero Trust

www.sechard.com

X

To simplify and streamline the security hardening process, consider implementing SecHard Zero Trust Orchestrator. With this comprehensive solution, you can have a consolidated set of tools that work together seamlessly to protect your entire network.

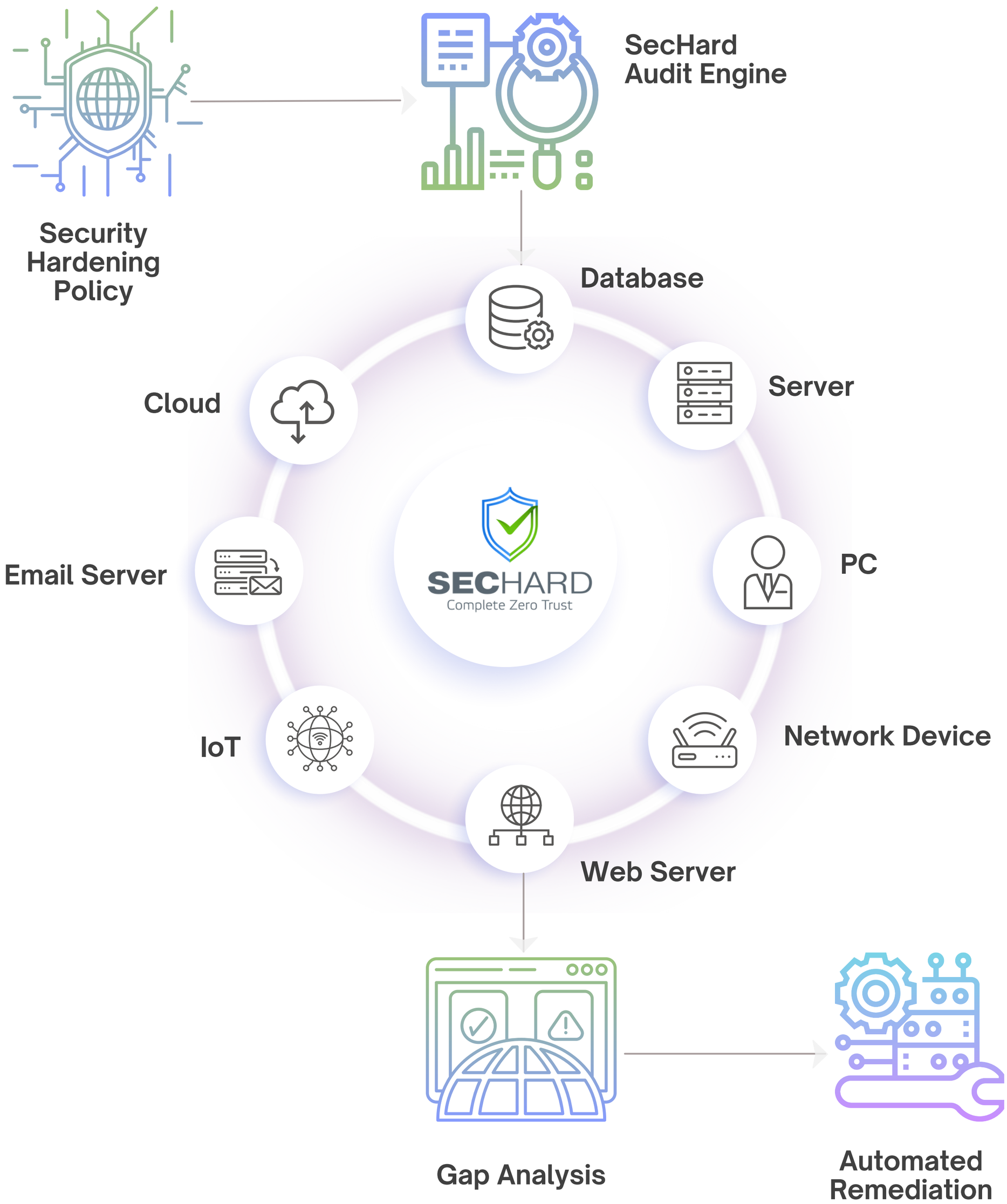
SecHard Zero Trust Orchestrator is highly scalable and adaptable, ensuring it will grow with your enterprise and keep up with changing security needs.

Contact us • Get Started • Contact us • Get Started

sales@sechard.com

SecHard's Hardening & Remediation Process

SECHARD
Complete Zero Trust



SecHard Zero Trust Orchestrator

SECHARD
Complete Zero Trust

Are you struggling to keep up with the latest cybersecurity standards and guidelines? Do you want to ensure your enterprise network complies with NIST SP 800-207? Look no further than Sechard.

With SecHard Zero Trust Orchestrator, you can easily implement the guidelines and best practices of NIST SP 800-207, the Executive Office of Presidential memorandum (M-22-09), and Gartner Adaptive Security Architecture, ensuring your enterprise network is secure and compliant.

SecHard Zero Trust Orchestrator modules, such as Security Hardening, Privileged Access Manager, Asset Manager, Vulnerability Manager, Risk Manager, Device Manager, Performance Monitor, Key Manager, TACACS+ Server, and Syslog Server, work together seamlessly to provide a comprehensive set of tools that facilitate compliance with industry standards.

Contact us today to learn more about how Sechard can help you achieve your cybersecurity goals!

sales@sechard.com

MEET *the* TEAM

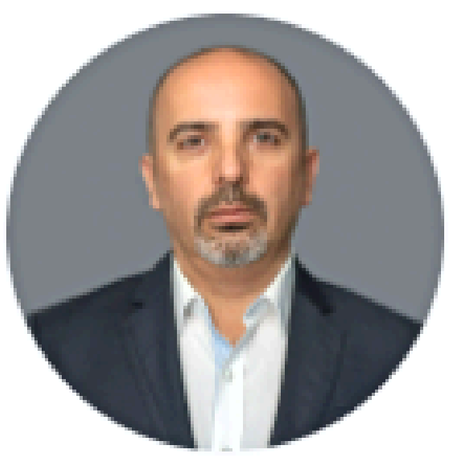
SECHARD
Complete Zero Trust

Serkan Akcan
Chief Executive Officer

Kadir Çakıcı
Chief Technology Officer

Cihat Altuntaş
Chief Software Development Officer

Caner Dağlı
Chief Business Officer



Sinan Yılmaz
Chief Financial Officer

Ömer Çuhadaroğlu
VP of Product

Melis Özen
VP of Sales

Didem Köpük Altınel
VP of Marketing

The Masterminds Behind SecHard

SECHARD
Complete Zero Trust

Share with your friends!

Enjoying our content?

Follow SecHard Page!