A Comprehensive Comparative Analysis of Leading Operational Technology Security Platforms: The Strategic Case for Preemptive Cyber Defense

The Strategic Case for Preemptive Cyber Defense

Audio File: Beyond the Air Gap: Deception and Autonomous Defense for Critical Infrastructure

Executive Summary: A Strategic Guide to a Fragmented Market

The Operational Technology (OT) security market is in a state of rapid evolution, moving beyond a traditional, monolithic ecosystem to a fragmented landscape defined by three distinct strategic philosophies. A comprehensive analysis of this market reveals that a critical distinction exists between vendors that prioritize visibility, those that offer integrated IT/OT platforms, and a new, emerging category of solutions built on a preemptive and active defense model.

This report presents a detailed comparative analysis of the leading platforms, including Claroty, Dragos, Nozomi Networks, Fortinet, Armis, and PacketViper. The analysis reveals a significant gap in the market: while many vendors excel at passive asset discovery, vulnerability management, or threat intelligence, their models often rely on a reactive, human-led response that introduces a critical latency gap. This delay is particularly dangerous in fragile OT environments where a machine-speed attack can result in physical damage or operational downtime.

The central finding of this report is that PacketViper occupies a unique and defensible position by offering a purpose-built, OT-native solution with a paradoxical, preemptive defense model.[1] The solution's in-line, agentless, and autonomous containment capabilities directly address the latency problem that other solutions introduce through out-of-band or orchestrated responses.[1] Unlike platforms that provide telemetry for an analyst to act upon, PacketViper is designed to automatically and instantaneously neutralize a threat at its source.[1]

For critical infrastructure organizations, the choice of a security platform is a strategic decision that must align with their operational realities and risk tolerance. The analysis in this report provides a definitive case for adopting a new security paradigm that provides non-disruptive, real-time protection against lateral movement and offers a demonstrable and auditable compensating control for legacy systems. This approach is no longer a luxury but a critical business driver that transcends purely technical considerations and enables a resilient, sustainable security posture for the future of critical infrastructure.

The Modern OT Threat Landscape: The Imperative for a New Defense

The security of industrial environments has rested for decades on a fragile foundation of isolation and perimeter defense. This legacy model, most notably codified by the Purdue Model, has been systematically eroded by modern operational realities, including the push for IT/OT convergence and the proliferation of remote, unattended sites.[1] An increasing body of evidence from government agencies and threat intelligence frameworks confirms that these foundational assumptions are now dangerous illusions, not reliable security controls.[3]

The vulnerabilities of this legacy architecture are not isolated technical flaws but form a causal chain that modern adversaries are actively exploiting. The Purdue Model, designed in the 1990s on the premise of a static, isolated "air-gapped" environment, is now largely obsolete.[3] A 2024 SANS survey confirms this reality, indicating that only 8.2% of organizations maintain 100% isolated systems, proving that the model’s central assumption is no longer valid.[3] This breakdown of isolation creates a critical "east-west" blind spot, which is the unhindered communication between systems *within* the Electronic Security Perimeter that traditional perimeter defenses fail to monitor.[1]

This is no longer a theoretical flaw but an actively exploited vulnerability. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has consistently identified poor network segmentation as a significant risk during its cyber threat hunts.[1] The MITRE ATT&CK for ICS framework details specific techniques that adversaries use to achieve lateral movement within these poorly segmented networks, such as exploiting remote services and using valid but compromised accounts.[1] The 2021 Colonial Pipeline ransomware attack serves as a definitive real-world example of this vulnerability, where a single compromised credential for an inactive VPN account was used to gain a foothold, which then allowed attackers to move laterally and cause a catastrophic shutdown.[1] This demonstrates that once an attacker bypasses the perimeter, a network built on the flawed assumption of internal trust offers little to no resistance.

The perimeter itself has become increasingly porous due to new and overlooked attack vectors. "Wireless bleeding," a phenomenon where Wi-Fi and Bluetooth signals extend far beyond physical perimeters, creates unseen pathways for unauthorized access.[1] The U.S. Food and Drug Administration (FDA) has even issued warnings about "SweynTooth" vulnerabilities in Bluetooth, which could allow an unauthorized user to crash or access mission-critical medical devices, providing a clear parallel to industrial control systems.[1] This risk is compounded by the increasing reliance on geographically dispersed, unattended remote sites. These locations, which typically have minimal physical and cyber protections, serve as a critical vulnerability for industrial organizations.[1] The 2021 Oldsmar, Florida, water treatment plant attack, where an attacker leveraged a remote access vulnerability to alter chemical levels to a toxic amount, provides irrefutable evidence that a physical weakness at an unattended remote site can be exploited to manipulate a physical process with devastating consequences.[1]

The challenge for modern OT security is to address this fundamental architectural breakdown. A solution cannot simply build a better firewall; it must provide a definitive answer to the problem of lateral movement *within* the network and secure the unmanaged, unattended edge. This strategic necessity is the core mandate of regulations such as NERC CIP-015-1, which directly addresses the "east-west" blind spot by forcing utilities to adopt a modern, internal-focused security posture.[5]

The New Security Paradigm: From Reactive to Preemptive

In response to the documented failures of static, perimeter-centric security, a new philosophical approach is emerging: Preemptive Cyber Defense. This paradigm fundamentally moves beyond the traditional, reactive "detect and respond" model by proactively neutralizing threats before they can materialize into a successful attack.[2] Gartner, a leading research and advisory firm, defines this approach as one that aims to "prevent and deter cyber attacks before they can launch or succeed".[7] This strategic shift from a "defense in depth" to a "defense in motion" model is a fundamental departure from past security paradigms.[2]

PacketViper's core strategic innovation is its paradoxical approach to managing the attack surface. While traditional security wisdom dictates that an organization should actively shrink its attack surface, PacketViper's counter-intuitive strategy is to intentionally increase the *perceived* attack surface to defend and conceal the *actual* one.[1] This is accomplished by deploying a vast and unpredictable layer of deceptive elements, such as deceptive responders, decoys, and sirens, across both IT and OT environments.[1] This expansion makes the network appear far larger and more complex than it actually is, creating a "target-rich" but "amorphous" and "unreliable" environment for adversaries.[2]

The solution's Automated Moving Target Defense (AMTD) achieves this preemptive posture through a multi-layered approach.[2] Its deceptive technology suite is purpose-built to strategically target the earliest stages of the cyber kill chain, specifically reconnaissance and initial access.[1] The system's deceptive responders, integrated into Remote Security Units (RSUs), mimic legitimate network services and applications, including critical OT assets like PLCs and SCADA systems using industrial protocols like Modbus.[1] Any interaction with one of these deceptive assets is, by definition, an unauthorized and malicious act, which immediately triggers a high-fidelity alert and provides "false positive free" threat intelligence.[1] This approach turns an attacker's own reconnaissance efforts against them by rendering their intelligence-gathering futile and forcing them to reveal themselves before they can inflict damage.

A key differentiator of PacketViper's approach is its in-line, agentless, and non-disruptive deployment model.[1] Unlike traditional IT tools that require agents that cannot be deployed on proprietary or legacy OT equipment, PacketViper's technology passively monitors network traffic, ensuring that its presence does not interfere with the delicate operations of control systems.[1] This in-line model, coupled with native support for industrial protocols, allows the system to autonomously block and contain threats at "wire speed," without the latency of a human-in-the-loop or the complexity of a Security Orchestration, Automation, and Response (SOAR) playbook.[1]

The OT Security Market Landscape: An Overview of Leading Vendors

The OT security market is a fragmented landscape that can be strategically segmented into three primary camps based on their core security philosophies. Understanding these distinctions is critical for making an informed procurement decision.

Visibility & Asset-Centric Platforms

These vendors are the "pure-plays" of the OT security market, providing a foundational layer of deep, protocol-aware visibility into industrial networks. Their primary value proposition is to help organizations understand what assets they have, what vulnerabilities they face, and what risks exist.

- **Claroty:** Positioned as a leader in Cyber-Physical Systems (CPS) protection by Gartner, Claroty's platform prioritizes deep asset visibility, vulnerability management, and secure remote access
- **Dragos:** A recognized thought leader in the market, Dragos's core value proposition is rooted in deep industrial expertise and threat intelligence.[11] The Dragos Platform is known for providing
- **Nozomi Networks:** Nozomi Networks is a leader in asset intelligence and AI-driven analytics, as recognized by Gartner. Its platform provides network and endpoint visibility, and it has made

Integrated IT/OT Platforms

These vendors approach OT security by extending a broad, existing IT security platform to industrial environments. Their primary value proposition is a single, unified "pane-of-glass" management experience and the seamless integration of their product portfolios.

- **Fortinet:** Fortinet's strategy is built around its "Security Fabric," which provides an integrated and automated platform that extends its IT security capabilities to OT environments.[17] The platfo
- **Armis:** Armis provides an agentless and completely passive platform that delivers deep asset visibility and risk management by monitoring wired and wireless traffic.[20] The platform is cloud-b

Preemptive & Active Defense Platforms

This category represents a new, emerging paradigm of active and deceptive defense. These platforms move beyond passive monitoring and actively engage, mislead, and contain adversaries in real-time.

- **PacketViper:** The central focus of this report, PacketViper's core value is the combination of in-line, autonomous containment with OT-native deception.[1] Its distributed "hive-like" architectur
- **Other Deception Vendors:** The market also includes deception vendors such as Acalvio and Labyrinth. Acalvio's ShadowPlex platform claims to be agentless and support OT protocols, but its

Comparative Analysis: A Deep Dive into Vendor Philosophies and Capabilities

This section provides a detailed, multi-faceted comparative analysis of the leading OT security platforms, directly addressing the user's need for a comprehensive breakdown of the market. The analysis goes beyond a simple feature list to evaluate the core philosophies, deployment models, and strategic differentiators that define each vendor's position.

PacketViper's Distinctive Position

PacketViper's core value proposition is its unique blend of a preemptive defense philosophy and a practical, non-disruptive implementation model.[1] The solution's in-line deployment, coupled with its autonomous, wire-speed containment capabilities, is a direct answer to a critical need in OT environments where a latency gap between detection and response can lead to catastrophic consequences.[1] This differs from many competitors that rely on out-of-band monitoring or orchestrated responses that require human intervention or complex integrations.[1] PacketViper's deceptive technology suite is a patented, OT-native invention that can simulate critical assets like PLCs and SCADA systems, providing a verifiable data feed of unauthorized activity without false positives.[1] This capability makes it an ideal compensating control for unpatchable legacy systems that cannot support modern agents or protocols, a significant challenge for compliance with regulations like NERC CIP-015-1.[2]

Claroty: Visibility as a Foundation

Claroty's platform is built on a "visibility-first" philosophy, providing deep asset intelligence and vulnerability management.[8] The platform offers multiple asset discovery methods, including a patent-pending Edge collector, and a comprehensive view of network and process data.[8] Its strength lies in providing a rich stream of telemetry that feeds into a larger Security Operations Center (SOC) ecosystem, which helps security teams identify, assess, and prioritize risks.[8] While Claroty offers threat detection, its primary value is in providing the context and data

necessary to support a human-led response.[8] The platform's deployment flexibility, including both on-premise (CTD) and cloud-based (xDome) options, is a key selling point, but its response model is inherently more reactive and reliant on integrations with external systems.[9]

Dragos: Threat Intelligence as a Differentiator

Dragos is positioned as a thought leader with deep industrial expertise, and its platform is centered around a threat intelligence-first philosophy.[11] The Dragos Platform's value lies in its ability to provide contextualized, threat-specific analytics and detailed response playbooks that are continuously updated by its team of ICS security practitioners.[11] Dragos's approach is to empower human-led threat hunting and incident response, which requires a highly skilled and trained team to leverage its full capabilities.[11] The platform's primary function is to provide the data and insights to enable this human action, which is a key philosophical difference from an autonomous solution.[11] Dragos is an excellent tool for organizations that want to build a mature, threat intelligence-driven security program but it is not designed to provide a real-time, autonomous enforcement capability.[11]

Nozomi Networks: Monitoring with Orchestrated Access Control

Nozomi Networks is a leader in asset intelligence and AI-driven analytics, as recognized by Gartner.[13] Its platform provides network and endpoint visibility and has made investments in detecting wireless assets, a key differentiator.[13] While Nozomi Networks' core products like Guardian and Guardian Air are focused on monitoring and notification, they do not provide preemptive stopping capabilities.[11] The solution's containment and enforcement model relies on administrators acting on alerts to terminate a session.[3]

Nozomi Networks has a documented partnership with Dispel to provide Moving Target Defense (MTD) functionality through a cloud-to-cloud integration that leverages Dispel’s SD-WAN infrastructure for secure remote access.[16] This combined solution is limited to internet-connected OT environments and provides secure access control rather than in-network deception.[16] The core of the solution is to discover assets with Nozomi Networks and take action with Dispel, which requires an administrator to

quickly terminate the session after a user demonstrates abnormal behavior.[3] This is in direct contrast to PacketViper's in-line, autonomous defense which provides internal fortification, containment, and deception, even in air-gapped environments.[1]

Fortinet: The Integrated IT/OT Security Fabric

Fortinet's approach is to extend its IT "Security Fabric" to OT environments, leveraging its broad product portfolio to provide a unified platform for both.[17] The platform's value proposition is the "single-pane-of-glass" management and the seamless integration of its various security solutions, including firewalls, switches, and deception (FortiDeceptor for OT).[17] Fortinet's virtual patching and compensating controls allow organizations to secure aging infrastructure without operational disruption.[24] The platform is designed to automate workflows and pass security incidents to an Information Technology Service Management (ITSM) solution, which reduces response times.[18] While FortiDeceptor for OT is an integrated deception product, it is part of a broader ecosystem and does not offer the same in-line, self-contained, and autonomous response as PacketViper.[19]

Armis: Passive Discovery and Risk Management

Armis provides an agentless and completely passive platform for deep asset visibility and risk management in OT and IoT environments.[20] Its primary value proposition is its ability to discover every device on the network without disruption, including wired and wireless assets, and to provide a real-time baseline of device behavior.[21] Armis excels at providing deep asset inventory and risk management by monitoring connectivity and tracking asset behavior.[20] Its enforcement capabilities, such as micro segmentation, are often achieved through a partnership with other vendors like ColorTokens, which differs from PacketViper's native, in-line blocking.[22]

The OT Security Vendor Comparison Matrix

The following table provides a comprehensive, at-a-glance comparison of the leading OT security vendors, synthesizing the analysis from the preceding section. This matrix is designed to highlight the fundamental differences in vendor philosophies and capabilities, providing a clear and actionable overview for a strategic decision-maker.

Capability	PacketViper	Claroty	Dragos	Nozomi Networks	Fortinet	Armis
Core Security Philosophy	Preemptive Defense [2]	Visibility-First, Asset-Centric [8]	Threat Intelligence-First [11]	AI-Driven Analytics, Asset Intelligence [13]	Integrated IT/OT Platform [17]	Passive Discovery, Risk Management [21]
Deployment Model	In-line [1]	Out-of-band/Passive [27]	Out-of-band/Passive [11]	Out-of-band/Passive [13]	In-line [17]	Out-of-band/Passive [21]
OT/ICS Protocol Support	Yes (Native) [1]	Yes [8]	Yes (600+ protocols) [11]	Yes [13]	Yes (70+ protocols) [17]	Yes [20]
Deception Capabilities	Yes (Native, In-line) [1]	No [8]	No [11]	Yes (Partnered via SD-WAN for remote	Yes (Integrated	No [20]

				access) [16]	FortiDeceptor) [19]	
Containment/Enforcement	Autonomous, Wire-Speed [1]	Orchestrated via SIEM/SOAR [8]	Human-Led/Playbooks [11]	Orchestrated via SIEM/SOAR/Admin intervention [23]	Orchestrated via SOAR [18]	Orchestrated via Partner/API [22]
Internal Defense against Lateral Movement	Yes (In-line, Deception) [1]	No (Out-of-band monitoring) [9]	No (Out-of-band monitoring) [11]	No (Monitoring only) [3]	Yes (via FortiDeceptor) [19]	No (Out-of-band monitoring) [21]
Third-Party Validation	Third-party Pen Test Success; featured in 15+ Gartner Emerging Tech Bulletins [28]	Gartner Leader [10]	Gartner Leader, Thought Leader [10]	Gartner Leader, Customer Choice [10]	Gartner/IDC Leader, 93% fewer incidents [24]	Gartner Leader [10]
Compensating Controls	Yes [5]	Yes (via micro segmentation) [8]	N/A	Yes [23]	Yes (Virtual Patching) [24]	Yes (via micro segmentation) [22]
Cost/ROI	Traffic Reduction (30-70%), Lower SIEM costs [28]	Downtime Avoidance ($125K/hr) [31]	N/A (Pricing is high) [32]	N/A	Cost Reduction (93% fewer incidents) [24]	N/A

Strategic Synthesis: PacketViper's Unique Position

The comparative analysis reveals a striking and highly differentiated position for PacketViper within the OT security market. While many of the leading vendors are recognized for their excellence in visibility, threat intelligence, or integrated platforms, their models are fundamentally rooted in a reactive, "detect and respond" philosophy. These solutions are built to provide a rich stream of telemetry and alerts, but the crucial step of containment and enforcement is often reliant on a human in the loop or complex, multi-vendor orchestration via a SIEM/SOAR platform.[1] This creates a critical "latency gap"—a window of opportunity where an attacker, having been detected, can still move laterally and inflict damage before a response can be executed.[2]

PacketViper's value proposition is a compelling counterpoint to this reactive model. It is the only vendor in the analysis that combines in-line deployment, autonomous containment, and OT-native deception in a single, purpose-built platform.[1] The solution’s distributed "hive-like" architecture and "Enterprise Sync" capability allow a threat detected at one location to be instantly contained across the entire enterprise at "wire speed," which is typically within seconds.[1] This instantaneous response fundamentally alters the cyber kill chain, neutralizing an attacker's reconnaissance efforts and preventing lateral movement before it can begin.[1]

The economic and operational benefits of this preemptive approach are significant. The solution's ability to reduce network "noise" by 30% to 70% drastically reduces "alert fatigue" for SOC analysts and lowers operational costs for volumetrically priced SIEM/SOC services.[1] This makes the technology a force multiplier for understaffed security teams, allowing them to do more with less.[28] Furthermore, the platform provides a proven, auditable "compensating control" for unpatchable legacy systems and high-risk, vendor-managed networks, solving a major compliance and operational problem that many organizations face.[5]

PacketViper's efficacy is not merely theoretical; it is validated by a compelling real-world use case in a Fortune 500 Oil & Gas company. A third-party penetration test was a failure for the attackers, who were "unable to complete the test until the automated threat detection and prevention tool was turned off".[1] This third-party-validated endorsement is a powerful, non-academic proof of the technology's ability to neutralize even the most sophisticated attack attempts.

Strategic Recommendations for Implementation & Conclusion

The analysis confirms that the OT security market is defined by a philosophical schism between passive and active defense. For security leaders, the primary challenge is to select a solution that aligns not only with their technical requirements but also with their strategic security objectives and operational realities.

The strategic recommendation is to move beyond an incremental upgrade of existing tools and adopt a new security paradigm that provides real-time, autonomous protection at the network edge. Based on the comprehensive comparative analysis, PacketViper is recommended for organizations that:

- **Face High-Stakes Threats in Geographically Distributed Networks:** The solution's distributed, "hive-like" architecture is purpose-built to secure remote, unattended sites and contain threats
- **Require a Force Multiplier for Understaffed Security Teams:** The platform's ability to drastically reduce network noise and false positives makes it an invaluable asset for organizations faci
- **Need Auditable Compensating Controls for Legacy Systems:** For organizations with unpatchable, legacy equipment, PacketViper provides a proven and auditable compensating control that
- **Cannot Afford a "Latency Gap" Between Detection and Containment:** In environments where even a few seconds of delay can lead to physical damage, PacketViper's in-line, autonomous

The analysis concludes that PacketViper's technology represents a fundamental reorientation of defensive strategy. It is not merely a tool but a foundational platform for a new era of proactive security, forcing the attacker to play on a field where the rules are constantly changing. By moving beyond a reactive compliance mindset, organizations can build a truly resilient, intelligent, and preemptive defense for the future.

Works cited

1. A Comprehensive Analysis of the PacketViper OT360 Solution and Preemptive Cyber Defense for Critical Infrastructure
2. The Dawn of Preemptive Cyber Defense: PacketViper's Automated Moving Target Defense for the Future of Cybersecurity
3. Fortifying the Illusion: A Strategic Analysis of Modern Industrial Control System Vulnerabilities and the Case for Preemptive Defense
4. The Illusion of Protection_ Why Wireless Bleeding, Remote Site Gaps, and Flawed Purdue Model Assumptions Endanger Industrial Control Systems (1).pdf
5. Expert Report - Aligning Electric Utilities with NERC CIP-015-1 Through Preemptive Cyber Defense
6. CISA and USCG Identify Areas for Cyber Hygiene Improvement After Conducting Proactive Threat Hunt at US Critical Infrastructure Organization, accessed August 17, 2025
7. Preemptive Cybersecurity Solutions: A Must in Modern Tech Products - Gartner, accessed August 17, 2025, https://www.gartner.com/en/articles/preemptive-cybersecurity-solu
8. THE CLAROTY PLATFORM, accessed August 17, 2025, https://f.hubspotusercontent40.net/hubfs/4487147/002%20Products/Cyber%20Security/Claroty%20Assets/ClarotyP
9. Platform | Claroty, accessed August 17, 2025, https://claroty.com/platform
10. Gartner's first Magic Quadrant for OT security suggests... - The Stack, accessed August 17, 2025, https://www.thestack.technology/gartners-first-magic-quadrant-for-ot-securit
11. The Dragos Platform - Cybersecurity Excellence Awards, accessed August 17, 2025, https://cybersecurity-excellence-awards.com/candidates/the-dragos-platform-2024-2/
12. Dragos Named a Leader in CPS Protection Platforms, Focused on Protecting OT from Cyber Disruption, accessed August 17, 2025, https://www.dragos.com/blog/dragos-nam
13. Cloud-Powered OT & IoT Security | Vantage - Nozomi Networks, accessed August 17, 2025, https://www.nozominetworks.com/products/vantage
14. Gartner 2025 Magic Quadrant - Leader Cyber-Physical System ..., accessed August 17, 2025, https://www.nozominetworks.com/gartner-cps-magic-quadrant
15. Claroty, Nozomi, Armis Top Cyber-Physical Security Rankings, accessed August 17, 2025, https://www.bankinfosecurity.com/claroty-nozomi-armis-top-cyber-physical-securi
16. Nozomi Networks & Dispel for OT Security, accessed August 17, 2025, https://www.nozominetworks.com/resources/nozomi-networks-dispel-joint-solution
17. Fortinet Secure Operational Technology Solutions | AVFirewalls.com, accessed August 17, 2025, https://www.avfirewalls.com/ot-security.asp
18. OT Security Simplified and Unified with Fortinet, accessed August 17, 2025, https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/sb-plant-operations-ot-secu
19. FortiDeceptor | Data Sheet | Fortinet, accessed August 17, 2025, https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiDeceptor.pdf
20. Armis Centrix™ for OT/IoT Security (SaaS), accessed August 17, 2025, https://www.armis.com/platform/armis-centrix-for-ot-iot-security/
21. Operational Technology Security | Armis, accessed August 17, 2025, https://www.armis.com/solution-briefs/operational-technology-security/
22. Secure Your OT/IoT Environments with Precision with ColorTokens ..., accessed August 17, 2025, https://media.armis.com/sb-secure-ot-iot-environments-colortokens-en.pdf
23. Nozomi Networks | Dispel Integration, accessed August 17, 2025, https://dispel.com/resources/integrations/nozomi-networks
24. Fortinet's OT Security Leadership and Platform Strategy: A Catalyst for Sustained Growth in a High-Demand Market - AInvest, accessed August 17, 2025, https://www.ainves
25. FortiDeceptor - Deceive, Expose & Eliminate Attacks - Acora, accessed August 17, 2025, https://acora.com/about-us/our-partners/fortinet/fortideceptor/
26. Professional Services in Cybersecurity | Dragos, accessed August 17, 2025, https://www.dragos.com/services/
27. THE CLAROTY PLATFORM, accessed August 17, 2025, https://web-assets.claroty.com/resource-downloads/82fe90b77c2ead30d473bc6d56276280-The-Claroty-Platform-D
28. PacketViper Cost Savings and Cost Avoidance Use Cases 1224.pdf
29. Claroty vs Dragos 2025 | Gartner Peer Insights, accessed August 17, 2025, https://www.gartner.com/reviews/market/cps-protection-platforms/compare/claroty-vs-dragos-secur
30. A Practical Guide to Designing and Applying Compensating Controls - Fortinet, accessed August 17, 2025, https://www.fortinet.com/resources/cyberglossary/compensating-c
31. ROI Calculator | Claroty, accessed August 17, 2025, https://claroty.com/roi-calculator
32. Dragos Pricing – Pay Monthly or Annually with Capchase Financing, accessed August 17, 2025, https://www.capchase.com/invoice-financing/dragos