



SUCCESS STORY

Cyber Security and Networking Firm



Overview

Client: Cyber Security and Networking Firm

Revenue: \$12B Annual Revenue

Summary : The firm was losing market share in its endpoint and cloud security portfolio. Product Insight conducted an in-depth competitive analysis to aid strategic planning and arm the sales team with talking points and collateral to increase their confidence in competitive sales situations.

Challenge

The client, once hailed as a cutting-edge market leader by analysts, had recently started falling behind the competition. Competitors were achieving record-breaking revenue numbers and were perceived as inspiring and innovative by the market. New market entrants had quickly surpassed the firm, leading to flat revenues. Customer satisfaction was adequate but lacked enthusiasm. Key customers began leaving for competitors. The business struggled to respond effectively to these challenges and regain its market position.

Solution

Product Insight undertook a comprehensive 3-month competitive analysis process. The steps included:

Internal Understanding (2 weeks)



Conducted interviews with key stakeholders across product, engineering, professional services, sales, and marketing.



Gathered insights on challenges, advantages, and direct experiences competing against the top three competitors.



Synthesized notes to identify common themes.

External Research (6 weeks per competitor)

- Investigated publicly available information for each competitor.
- Examined sources such as 10Ks, websites, demo videos, whitepapers, customer testimonials, partner/system integrator content, social networks, and high-level pricing.
- Analyzed how competitors positioned themselves against each other.
- Examined, interpreted, and developed narratives against the test results of independent researchers (MITRE ATT&CK)
- Logged details about each competitor across 150+ attributes in 20 categories, focusing on product capabilities, GTM strategies, partnerships, deployment models, and customer support.

1	Comparison Matrix	Firm A	Competitor A	Competitor B	Comp
71	Workload Detection Techniques				
82	Container Detection Techniques				
90	Network Detection Techniques				
98	Identity Detection Techniques				
108	Threat Hunting				
115	Incident Management / Response				
127	Product Capabilities and Features				
143	Performance				
147	Public Efficacy Tests				
	MITRE Engenuity 2022				
148					
	SE Labs				
149					
	Virus Bulletin				
150					
	AV-Test				
151					
	AV-Comparatives				
152					
153	Integration				
174	Licensing Types				
175	Subscription type				
	Pricing				
176					
	Packaging				
177					
180	Coverage				
186	Maintenance				
193	Ease of Use / Management				
205	Uncategorized Items				
210	Vendor Support/Professional Services				
212	Total Cost of Ownership				

Scoring and Positioning:

- Objectively scored the client's offerings against each competitor across the 20 categories.
- Identified areas of differentiation and weakness against each competitor.
- Created positioning statements highlighting one key takeaway and three supportive counter-positioning illustrations and stories for sales enablement

Product Comparison

Deployment	Co	Us	Details
+ Cloud	●	●	+ Both solutions offer cloud-based products.
+ On premises	●	●	+ They offer on-premise support through a virtual appliance. We offer on-premise solutions to support all support-related
+ Agent/sensor	●	●	+ Both offer agent deployment methods including scripts, MDM, group policy, or other configuration management tools. They
Agent / Sensor	Co	Us	
+ Agent Management	●	●	+ Both solutions offer a single agent per OS.
+ Endpoint Performance Impact	○	○	+ While no independent assessments have been performed, they have many testimonials of the agent having a significant
+ Device/OS Support	●	●	+ Both offer support for Windows 7, Windows Server 2008, Mac OS, and Linux. Both have support for legacy Windows OS
Data Collection / Telemetry / Visibility	Co	Us	
+ Endpoint	●	●	+ Both offer comprehensive endpoint telemetry.
+ Network	○	●	+ They do not assess network telemetry. They pick up IP addresses/ports, URLs, and DNS connection records on endpoint &
+ Workloads	●	●	+ Both solutions offer comprehensive workload protection.
+ Containers	○	●	+ Both solutions gain visibility into containers by using API probes. They offer container protection. We offer protection of
+ Identity	●	○	+ Both solutions offer endpoint authentication records. They offer additional identity solutions that include more identity &
+ Email Security	○	○	+ Both solutions rely on integrations with 3rd party solutions to be used through with endpoint telemetry.
+ Web Security	○	○	+ Both solutions rely on integrations with 3rd party solutions.
Threat Prevention Techniques	Co	Us	
+ NGAV	●	●	+ Both solutions offer NGAV protection.
+ Endpoint FW	○	○	+ Both solutions offer endpoint FW protection.
+ Host IPS	○	●	+ They have scripts but lack ability to detect network attacks or the ability to set custom block rules and as such is not a
+ Device Control	○	○	+ Both offer device control for Windows and macOS. We offer more granular and robust policy creation than they have for
+ App Control	○	●	+ They offer a limited version of application control for cloud workloads only, whereas we offer a comprehensive applicat
+ Memory, Registry, and File Integrity Protection	●	●	+ Both solutions offer file, memory, and registry protection, we also offer binary files.
+ Vulnerability / Exploit	○	○	+ Both solutions offer granular vulnerability assessments for all asset types. They only perform assessments on workload
+ Agent Anti-tampering	●	●	+ Both solutions offer agent anti-tampering capabilities.
Services	Co	Us	
+ Managed Detection and Response (MDR)	●	●	+ Both solutions offer MDR services.
+ Threat Hunting	●	○	+ They offer threat hunting services.
+ Incident Response (IR)	●	○	+ They offer IR services.

Developing Collateral



Consolidated
research into sales
battle cards



Developed positioning
deck for internal sales
enablement and product
strategy teams



Created objection
handling and roadblock
guidance for expected
head-to-head sales
discussions




Highlighted
opportunities for
product investments
to deepen competitive
advantages and shore
up material weaknesses

Why we are the better choice for protecting your organization.





With us, you are empowered to succeed	With Competitor, you are on your own	We are a balanced, complete security solution	Competitor is scientific chaos theory	We deliver high value	Competitor delivers high cost
Security professionals need tools that have both strong out-of-the-box capabilities and the ability to customize and extend. Security tools that limit your visibility and control slow your detection and response actions when it matters most.	Competitor limits security professionals to what they feel is important:	Security is achieved by blending knowledgeable people, best-practice processes, and technology that empowers. If the blend of people, processes, and technology isn't balanced, then security and the people who try to deliver it suffer.	Competitor's 'AI/ML-Only' security approach delivers mixed results. They detect everything, including FPs. Leaving security teams to either: <ul style="list-style-type: none">• Struggle to filter the noise to find the real threats• Report false positives, overwhelming analysts that aren't empowered	The value of security tools must exceed the price you feel they are worth. Unfortunately, security tools have had a history of overhyping capabilities only to under-deliver.	Competitor lacks core capabilities that are critical to a security team:
We are designed for security professionals by delivering: <ul style="list-style-type: none">• End-to-end visibility• Detection across all endpoints• Detection of phishing threats• Detection of insider threats• App control across all major systems• User activity and device control across all devices with full visibility• Customizable policies	Competitor limits security professionals to what they feel is important: <ul style="list-style-type: none">• Only the customer detection rules• Detection of phishing threats• Detection of insider threats• No network visibility• Limited visibility into the endpoint system and network traffic• No visibility into the cloud• No visibility into the cloud	We deliver the most comprehensive XDR solution by providing: <ul style="list-style-type: none">• End-to-end visibility• Detection across all endpoints• Detection of phishing threats• Detection of insider threats• App control across all major systems• User activity and device control across all devices with full visibility• Customizable policies	Competitor's 'AI/ML-Only' security approach delivers mixed results. They detect everything, including FPs. Leaving security teams to either: <ul style="list-style-type: none">• Struggle to filter the noise to find the real threats• Report false positives, overwhelming analysts that aren't empowered	We provide sophisticated security teams: <ul style="list-style-type: none">• The ability to detect and respond to threats• The ability to detect and respond to threats• The ability to detect and respond to threats	Competitor lacks core capabilities that are critical to a security team: <ul style="list-style-type: none">• The ability to detect and respond to threats• The ability to detect and respond to threats• The ability to detect and respond to threats

Top 10 Reasons to Choose Us over Competitor

OUR DIFFERENTIATORS

 1 Delivering innovative XDR, built on Threat Intel and ML cloud <small>Threat Intel: Internal Threat Intel and is easily extendable upon it, resulting in high FPs, and your team is left to figure it all out</small>	 2 Robust Network, Identity, & Cloud Telemetry/Detection <small>Threats: No Network Telemetry for Endpoint correlation or hunting</small>	 3 Superb ROI without breaking the bank <small>Threats: 100% more expensive with lower overall ROI (2023 from Forrester Q3 Report)</small>	 4 View Query any device across 2K attributes with 100+ OOTB Queries <small>Threats: Revenue theft and you are on your own, handcuffed to basic sets of data</small>	 5 Full EDR replacement included as part of EDR <small>Threats: Markets as full EDR replacement, it doesn't analyze for network attacks or support robust custom block rules</small>
---	---	--	--	--

OUR PLATFORM & XDR DIFFERENTIATORS

 6 App Control for Mac/Win/Linux (air-gap & active/inactive OSEs) <small>Threats: Minimal to no Application Control to close the attack surface on critical servers or third-party devices</small>	 7 Vuln Assessment for Build, Deploy, and Run of Cloud Workloads/K8s <small>Threats: Limited to customer assessment, no SaaS, no SaaS</small>	 8 Transparent/informed detections, granular policies, powerful control <small>Threats: NoML-based threat detection & response functionality with limited customizability</small>	 9 Robust tools for hunting, investigations, & remediation efforts <small>Threats: Remediation capabilities that won't work for modern threats and regularly require endpoint performance</small>	 10 High-performance sensors, reliable there when you need them <small>Threats: History of downtime, slow performance, and advanced incident response by forcing high resource use</small>
--	---	---	---	--

Competitor Product XDR Offering Overview

Description
"Product XDR Platform" pushes the boundaries of autonomous technology. It provides protection, detection, response, and threat hunting across user endpoints, containers, cloud workloads, and IoT devices.
Positioning
<ul style="list-style-type: none">• "Next-gen (undetected) cybersecurity platform to deliver (undetected) for the enterprise"• "Threat of AI" to protect the endpoint, secure the cloud, and fortify identities.• "Undetected cybersecurity"
Primary Points of Emphasis/Differentiation
<ul style="list-style-type: none">• AI - built to be the enabler for the fastest, most effective threat detection, response• 3rd party validation<ul style="list-style-type: none">• Gartner Magic Quadrant, highest score for critical capabilities• Best MITRE Degradeability performance• Single platform - optimize user experience, consolidate vendors, improve efficiency
Pricing and Deployment
3 core packages, with additional purchases available
<ul style="list-style-type: none">• Product 1 - MLML, Scalable/Secure• Product 2 - EDR, Scalable/Secure• Product 3 - EDR, Scalable/Secure
Additional purchases:
<ul style="list-style-type: none">• Product 4 - Scalable/Secure, Product 5, Remote Ops, Cloud Forensic Data Lake Streaming, Binary Vault, Mobile endpoint support• Identity, Product 6 AI, Product 7 AI, Product 8, Product 9, Product 10, Product 11, Product 12• Services: Remote (24/7, 24/7, 24/7), Managed (Managed threat hunting)

Silver Bullets for Defeating Competitor Product XDR

INTERNAL ONLY

We provide comprehensive visibility into the foundational XDR telemetry to detect, investigate, and hunt threats.

The foundation for XDR is the combination of endpoint and network. We support both. They lack network visibility and detection.

- Of the 230 MITRE ATT&CK Techniques, there are 107 endpoint Techniques (46%) and 122 network Techniques (53%). Do you want a solution that only provides 46% coverage for MITRE ATT&CK or one that provides 100%?

We are a strong investment that doesn't break the bank and delivers best-in-class, comprehensive XDR technology

On - Low, on-infected users with best of breed XDR	Superior, comprehensive XDR technology	Higher overall Forrester Q3 EDR 2023
On - Premium pricing	Lacks foundational XDR telemetry/detections, Network	Lower overall Forrester Q3 EDR 2023

We empower your investigators, not handcuff them

When an incident occurs, being able to investigate endpoints comprehensively is critical. While they tout a library of queries you can run against endpoints, if the queries can only identify rudimentary telemetry on the endpoints, they are worthless. With our (undetected), customers get 100+ OOTB queries that examine over 2K attributes on an endpoint... empowering your team to understand what the adversary has done. Our interface provides clear threat actor attribution, MITRE ATT&CK mapping, clear threat detection details, and extensive threat-related context such as correlated vulnerabilities and third-party context.

We are built on our full-fidelity threat intelligence and ML-powered cloud

We agree machine learning and AI are powerful tools for detecting threats, but without rich threat intelligence the result is high false positives and lack of threat attribution. This leaves analysts and responders in the dark, wasting time chasing down threats that aren't real. Their "AI/ML Only" strategy of detecting every possible threat works great until you must sift through noise to find true positives. Since found, they lack threat researchers who can provide threat IO articles with threat attribution and an understanding of the tendencies and intent of the adversary. We combine (undetected) (24x7 data science/PhDs & 24x7 threat researchers) and AI/ML-based engines to deliver not only high-fidelity detections but also rich telemetry, attribution, and threat details. Our full-fidelity threat intelligence and ML-powered cloud mapped over 1,200 reconnaissance attacks in the last 90 days.

How will you best secure your most critical systems such as fixed-purpose systems, air-gapped systems, and critical servers?

EDR and XDR are valuable technologies to identify and respond to attackers, but some systems and servers are so important that resources should be taken to reduce their attack surface. We created the (undetected) market and still today provide the leading technology. By (undetected) fixed-purpose systems, air-gapped systems, and critical servers you prevent attackers from executing any applications or making changes to these systems, eliminating risk. Other than tight application control for cloud workloads, this doesn't offer this capability.



Impact

The ultimate goal was to arm the sales team with information to confidently compete against the top three competitors. The presentation to the entire sales organization was a resounding success. The sales team felt well-informed and knowledgeable about the strengths of their product and potential pitfalls when discussing specific competitors. This newfound confidence led to more assertive and effective sales engagements.

Product Insight also provided the Product Management team with strategic focus areas and pivots to their roadmaps that would instill customer confidence and show the market that they were innovators.

Testimonial



The project with Product Insight was a phenomenal success. Their deep expertise and competitive intelligence approach gave us incredible insight into where we win and why. Our GTM teams are now well informed, confident, and armed with the right positioning and our product team knows where to invest to achieve the largest ROI.

- Head of Security Product Marketing



info@productinsight.net



www.productinsight.net