The 2026 MSP Cybersecurity Buyer's Guide

Everything European MSPs need to evaluate, build, and sell a modern cybersecurity practice – from the threat landscape to the vendor decision

WITHSECURE PARTNER EDITION – 2026

The MSP Cybersecurity Buyer's Guide

WithSecure
2026

Contents

Why MSP Success in 2026 Depends on Business Outcomes, Not IT Operations

One manages tools. The other delivers resilience. That gap – between operating technology and owning outcomes – is the defining business decision every MSP faces right now. Not in three years. Now.

The pressure is already visible. Customers are asking harder questions at renewal. Margins on break-fix and device management are thinning. And across Europe, a wave of regulation – NIS2, DORA, GDPR enforcement – is pushing cyber risk from the IT team to the boardroom. The customers who used to ask "is our antivirus up to date?" are now asking "can you prove our business is resilient?"

That question is the opportunity.

MSPs who can answer it – with data, with expertise, with a managed service wrapped around a platform that actually delivers – are winning the best customers, the longest contracts, and the highest margins in the market right now. MSPs who can't are competing on price for customers they can't afford to keep.

This guide is built for European MSPs who have decided to make the transition. It is not a product catalogue or a technology briefing. It is a practical blueprint for building a security practice that generates 20–30% of your total revenue, raises your average contract value, and puts you in front of your customers' boards as a trusted advisor – not a supplier.

Everything in it is grounded in real market data, real partner results, and a platform built specifically for the economics of MSP delivery at scale in Europe.

$106B Global managed security market in 2026[1] (Omdia)

€7.6B EMEA cybersecurity services market[2] (Gartner, 2024)

40% confirmed breaches targeting small businesses[3] (Verizon DBIR 2024)

21% compliance service growth in 2026[4] (Canalys)

From Managing Tools to Providing Outcomes

The MSP market is entering its next evolution. Managing tools is no longer enough. AI is automating core IT tasks, and customers are shifting from buying services to buying outcomes – security, continuity and resilience.

The MSPs that succeed will be the ones that make that transition. Those that don't risk being commoditized.

Old MSP Model		New MSP Model
Operate tools	→	Deliver outcomes
Sell licenses	→	Sell protection
Monitor alerts	→	Resolve incidents automatically
Add headcount to scale	→	Use automation to scale
IT support	→	Business resilience
Technology partner	→	Strategic advisor

1. Omdia. *MSSP Trends and Predictions.* 2025. https://omdia.tech.informa.com/om143904/managed-security-services-provider-mssp-trends-and-predictions-for-2026
2. Gartner. *Global Information Security Spending Forecast.* 2024. https://www.gartner.com/en/newsroom/press-releases/2024-08-28-gartner-forecasts-global-information-security-spending-to-grow-15-percent-in-2025
3. Verizon. *Data Breach Investigations Report (DBIR).* 2024. https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf
4. Canalys. *MSP Trends.* 2025. https://canalys.com/insights/msp-trends-2025-es

1. The MSP Cybersecurity Opportunity

Why the window to become a cybersecurity leader is now – and what is at stake if you wait

Your customers no longer just want IT support. They want resilience. The businesses in your portfolio face the same threat actors as enterprises – with a fraction of the resources. That gap is your opportunity.

Market Context

Global managed security services will reach $106 billion in 2026, growing at 14% annually[1]. In EMEA, the market stands at €7.6 billion with 13% growth[2]. Compliance services lead at 21% growth, now 20–30% of MSP contract value[3].

Small businesses are three times more likely to be targeted by attackers, with 40% of confirmed breaches hitting SMBs[4]. MSPs serve the exact segment under acute threat, creating urgent customer demand for security expansion.

AI is reshaping managed services toward automation and outcome-based delivery, where value ties to measurable business results rather than billable hours[5]. The industry is moving decisively toward outcomes over inputs.

MSPs that fail to expand into security and compliance services risk irrelevance. Without these capabilities, MSPs may not sustain operations in the near future[6]. The transition window is narrowing.

The MSP Revenue Case

The MSP market is undergoing a fundamental shift. Success no longer depends on scaling headcount – it depends on scaling automation and value delivery. Leading MSPs are repositioning their business models accordingly.

Old Model		New Model
Revenue grows with headcount	→	Revenue grows with automation
High tool complexity	→	Unified platforms
Alert noise	→	AI prioritisation
Security as add-on	→	Security as foundation
Technical value	→	Business value

From Headcount to Automation
Consolidating fragmented security tools into unified platforms eliminates tool sprawl and reduces operational overhead. This allows teams to scale revenue without scaling headcount proportionally. MSPs adopting this approach experience 5× higher revenue growth compared to IT-only competitors.

From Noise to Intelligence
Alert fatigue degrades team productivity and customer experience. Modern XDR and AI-driven solutions deliver high-fidelity alerts that surface only actionable threats, maintaining the critical balance between security and productivity. For smaller security teams managing multiple customers, this shift frees resources for strategic advisory work and faster incident response.

1. Omdia. *MSSP Trends and Predictions.* 2025. https://omdia.tech.informa.com/om143904/managed-security-services-provider-mssp-trends-and-predictions-for-2026
2. Gartner. *Global Information Security Spending Forecast.* 2024. https://www.gartner.com/en/newsroom/press-releases/2024-08-28-gartner-forecasts-global-information-security-spending-to-grow-15-percent-in-2025
3. Canalys. *MSP Trends.* 2026. https://canalys.com/insights/msp-trends-2025-es
4. Verizon. *Data Breach Investigations Report (DBIR).* 2024. https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf
5. Forrester. *Managed Services as Software.* 2024. https://www.forrester.com/blogs/managed-services-as-software-offer-a-vision-for-the-future-of-managed-services
6. Omdia. *MSP Trends and Predictions – Executive Summary.* 2025. https://omdia.tech.informa.com/blogs/2025/jan/msp-trends-and-predictions-2025---executive-summary

From Add-On to Foundation
Security is no longer optional. Businesses managing their own IT infrastructure still require enterprise-grade protection. By positioning security as a foundational service rather than an add-on, MSPs expand their addressable market and strengthen customer relationships. Improved retention follows naturally – when security is critical to operations, switching costs rise. This repositioning alone generates an additional 20% in new recurring revenue through advisory services.

From Technical to Business Value
Larger deal sizes emerge when security is bundled as a strategic business enabler rather than a technical checkbox. MSPs offering AI-native detection capabilities command premium per-seat pricing and win mid-market customers actively evaluating security innovation in vendor selections

The Model Shift: From Tools to Outcomes

The most successful MSPs have stopped thinking about security as a product to resell. They've shifted to a fundamentally different business model – one that transforms unit economics while positioning themselves as trusted advisors rather than service vendors.

Reactive to Proactive
Traditional security operates in firefighting mode. The new model prevents breaches before they happen. By integrating automated threat detection with proactive exposure management, MSPs shift from incident response to risk prevention. Prevention generates margins that incident response never will.

Product Resale to Managed Service
Reselling security products generates thin margins and high acquisition costs. Managed security services – delivered through unified platforms – unlock recurring revenue at significantly higher margins. With automation filtering noise and AI providing remediation guidance, MSPs achieve lower cost per alert and structurally stronger margins.

Research shows 73% of MSPs cite security as their fastest-growing service, and approximately 60% of organizations cite cybersecurity as the primary reason for outsourcing to MSPs[1].

Vendor to Trusted Partner
When you operate a reactive security tool, you're a vendor. When you deliver proactive outcomes, you become a strategic advisor. Single-agent deployment reduces time-to-revenue, while compliance alignment strengthens win rates in regulated sectors. Embedded risk reporting brings you to the board table. Customers who rely on you for strategic guidance don't leave.

Compliance as Differentiation
Regulatory readiness – NIS2, DORA, GDPR – has become table stakes. The EU's NIS2 directive took effect January 2023, with DORA becoming fully enforceable January 17, 2025. Essential entities face fines up to €10 million or 2% of global revenue for non-compliance.

MSPs that integrate compliance into their security stack turn regulation into competitive advantage. Platforms built under EU jurisdiction with data sovereignty allow you to own compliance leadership. See the official NIS2 framework[2] and EU DORA guidance[3].

Co-Security Model: Extend, Don't Build
The highest-margin MSPs partner with vendors for monitoring and threat response while keeping the customer relationship and revenue. This approach provides expert monitoring without building a SOC – which requires $1.5–$2.5 million annually for basic capabilities[4].

1. JumpCloud. *MSP Statistics & Trends 2025.* https://jumpcloud.com/blog/msp-statistics-trends
2. European Union. *NIS 2 Directive.* https://www.nis-2-directive.com/
3. GRC Solutions. *DORA, ISO 27001, NIS2 & GDPR Alignment.* https://grcsolutions.io/how-dora-fits-with-iso-27001-nis2-and-the-gdpr/
4. Todyl. *MSP Security: Build vs. Buy SOC.* Feb 2026. https://www.todyl.com/blog/msp-security-build-vs-buy-soc-costs
5. Jumpfactor. *Managed IT Services Market Trends.* Dec 2025. https://www.jumpfactor.net/managed-it-services-market-size-growth-trends-research/

Market Reality
68% of MSPs saw year-over-year revenue growth in 2024, with 40% reporting growth above 10%[5]. The global MSP sector is expected to hit $350 billion by end of 2024 and surpass $1 trillion by 2033, at a CAGR of 12.9%.

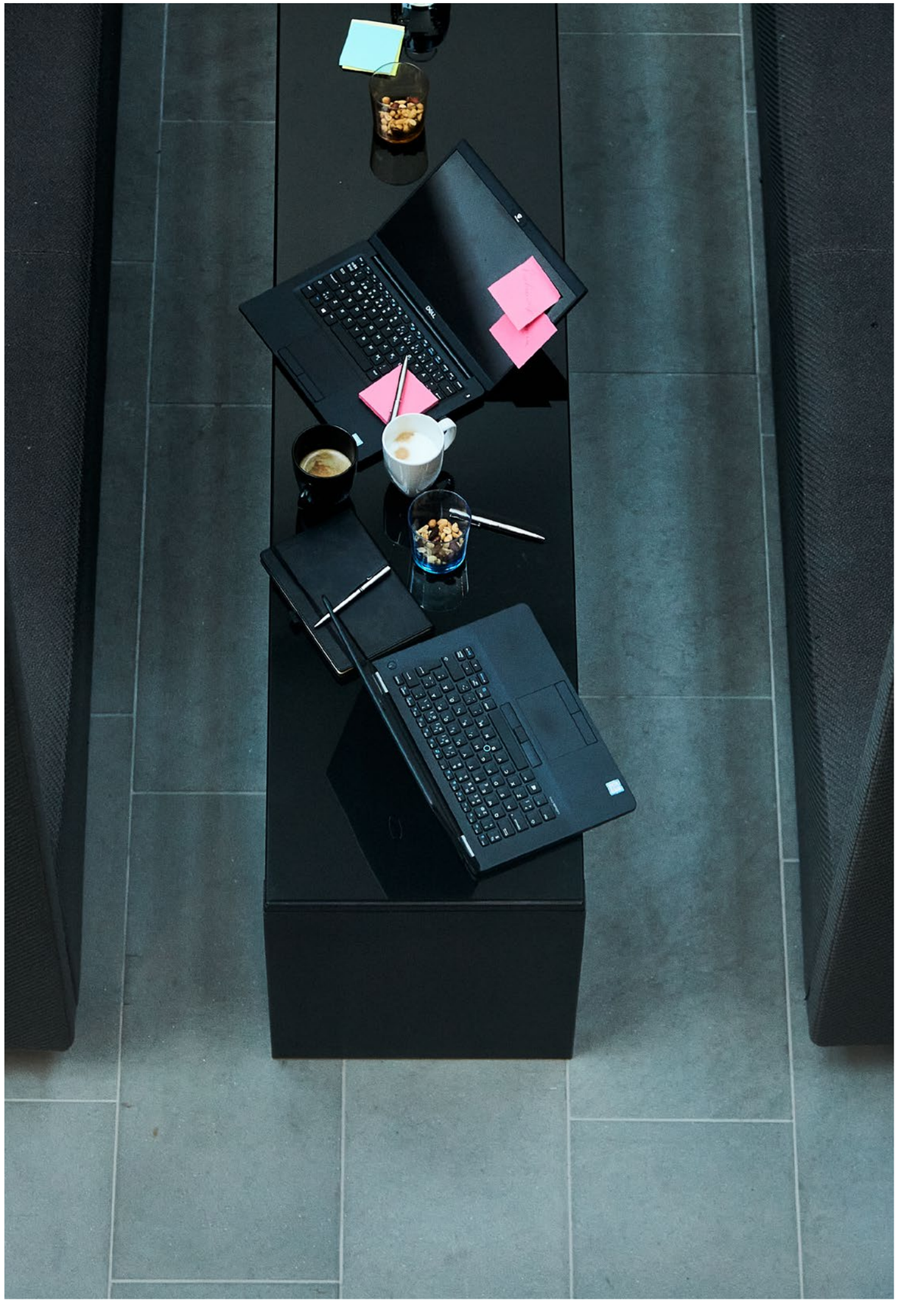
The shift from reactive to proactive, from vendor to partner, from product to outcome – this is where MSP economics are headed.

WithSecure Perspective

WithSecure operates a partner-first model where 6,000+ MSPs are the primary route to market. The entire Elements platform is architected around MSP economics: unified management, automated delivery, and a Co-security model that extends your team – not replaces it. Partners report up to 70% higher margins vs. building in-house security operations, with 95% customer retention among partner portfolios.

Key Questions for Your Business

- What percentage of your current revenue comes from security-specific services vs. general IT management?
- How many of your customers are subject to NIS2, DORA, or ISO 27001 compliance obligations?
- If a customer asked you today to prove their security posture to their board, could you do it in 48 hours?
- What is your current security revenue per seat, and what would a 3× increase mean for your business?



2. The Evolving Threat Landscape

AI-powered attacks, identity exploitation, and why endpoint protection alone is no longer enough

The threat actors targeting your customers in 2026 are faster, more automated, and more effective than they were two years ago. Understanding what changed – and where attacks now start – is the foundation of an effective security conversation with any customer.

AI-Powered Attacks: Speed Is the New Asymmetry

The AI-driven threat ecosystem has fundamentally reshaped attack economics. The median timeline from new CVE disclosure to active exploitation is now measured in hours – a compression that will push exploitation under 24 hours throughout 2026. This is not a future concern; it is the operational environment we inhabit today. CVEs are now competing directly with compromised identities as the most common initial attack vector. The era when defenders had days to patch vulnerabilities has simply ended.

Attackers are leveraging generative AI to craft hyper-personalized phishing campaigns at scale, abandoning generic mass-mailing tactics in favor of surgically targeted social engineering. Simultaneously, AI dramatically compresses attack timelines from initial access through lateral movement, collapsing what once took days of reconnaissance into hours of fully automated exploitation. Credential stuffing and identity abuse now require no human operator. Fully automated systems scan for vulnerable accounts and pivot through networks with minimal friction or detection.

AI-generated malware variants defeat signature-based detection faster than ever, rendering traditional endpoint protection increasingly obsolete. The uncomfortable truth is clear: defenders must adopt AI capabilities too, or watch the defensive gap widen irreversibly. Organizations without machine learning-powered threat detection are already losing the speed war.

Identity: The Fastest-Growing Initial Access Vector

Identity-based attacks are rapidly growing as the most common entry point into customer networks. Compromised Entra ID and Azure AD credentials grant attackers cloud-wide access instantly, bypassing perimeter controls entirely. Business Email Compromise via M365 accounts ranks as the top attack vector because these accounts sit at the intersection of corporate communications and sensitive data access.

The machine identity problem demands urgent attention. Attackers increasingly abuse overprivileged and poorly monitored machine identities – service accounts, API keys, and OAuth tokens – to maintain persistence while bypassing MFA and user-centric security controls. These non-human identities rarely receive the same audit rigor as user accounts, yet they hold the keys to entire systems and represent a persistent blind spot in most security programs. Traditional EDR is fundamentally blind to identity-layer attacks, which is why XDR combined with Identity Threat Detection and Response (ITDR) capabilities have become essential investments for any MSP serving enterprise customers.

Cloud and Collaboration Surface Expansion

Every M365 tenant represents a distinct attack surface. Email, Teams, SharePoint, and OneDrive are not merely communication platforms – they become persistent access vectors when misconfigured or compromised. Cloud misconfigurations in Azure and AWS remain persistent, ever-growing exposures that many organizations struggle to identify and remediate at scale.

SaaS sprawl creates shadow IT that MSPs frequently cannot see or control. Employees adopt best-of-breed tools independently, data migrates to unknown cloud locations, and security policies become theoretical rather than enforced. Hybrid work has fundamentally dissolved the traditional network-centric security perimeter, forcing a reorientation of visibility requirements toward identity, cloud, and collaboration layers rather than the network edge. IoT and OT devices in customer environments remain largely unmanaged and unprotected, creating vulnerable footholds that attackers exploit to establish persistent presence in supposedly secure networks.

Regulation as a Forcing Function

Compliance frameworks are driving security investment with increasing urgency. NIS2 (October 2024) is mandatory for EU essential and important entities, specifically including MSPs in its scope. DORA (January 2025) requires digital resilience frameworks for the financial sector with mandatory ICT risk management structures. GDPR enforcement is intensifying simultaneously with tightening breach notification timelines. ISO 27001 is increasingly demanded by enterprise supply chains as a baseline for vendor engagement. MSPs that cannot demonstrate compliance readiness will simply lose regulated customers entirely.

Speed: The New Attacker Advantage

The mean time from initial access to data exfiltration is now measured in hours, not days. Ransomware operators employ "double extortion" tactics – encrypt data while simultaneously threatening publication, forcing organizations to treat this threat with absolute seriousness. Alert-heavy security tools slow down defenders precisely when speed matters most, drowning analysts in noise while real threats advance undetected. Twenty-four-hour monitoring is no longer a premium service offering – it is the minimum viable response capability for any organization handling sensitive data.

What This Means for MSP Delivery

Endpoint protection alone is demonstrably insufficient for defending 2026's threat landscape. Security coverage must extend comprehensively to identity and cloud layers to address actual attack vectors. Alert fatigue kills analyst productivity and obscures genuine threats in the noise. Customers increasingly expect proactive risk reduction and threat neutralization before breaches occur.

Attack path visibility has become the operational standard for enterprise-grade customers. Detection alone is necessary but insufficient; customers need to understand which combinations of vulnerabilities and permission misconfigurations enable attackers to reach critical assets.

MSPs must prevent attacks before they start and execute this at scale automatically. This means delivering continuous, automated security posture optimization without requiring human intervention for each decision. More critically, MSPs themselves are now high-value attack targets. A single MSP breach exposes dozens of customer environments simultaneously. This is not aspirational – your own security posture is a due diligence requirement for prospects and a liability exposure in supply-chain incidents.

WithSecure Response to the Threat Landscape

For MSPs, the threat landscape described above creates two parallel obligations: protecting customers effectively and delivering that protection efficiently at scale. WithSecure addresses both. Elements XDR covers endpoints, identities (Entra ID), cloud (Azure + AWS), and M365 collaboration from a single platform – purpose-built for the attack vectors dominating 2025–26.

Elements XM and XDR together enable proactive security by continuously turning threat intelligence into action. Elements XM provides real-time visibility into exposures such as vulnerable software, misconfigurations, and emerging attack paths, while Elements XDR supplies live sensor data and response capabilities from endpoints. By fusing XM insights with XDR detections and response actions, security posture can be adjusted immediately – before exploitation occurs. This closed loop shifts defense left, enabling preemptive mitigation of risks even when patches or known exploits do not yet exist. Luminen GenAI assistant is included across all tiers, reducing analyst workload by surfacing and contextualizing threats automatically.

WithSecure is one of only two vendors globally to participate in all 7 MITRE ATT&CK Enterprise Evaluation rounds – with the lowest detection-to-alert ratio among European vendors in 2025 evaluations[1].

Key Questions for Your Business

- How many of your customers have Microsoft Entra ID – and do you have visibility into identity threats in those tenants today?
- If a customer's M365 account was compromised at 2am, how long before you would know?
- Can you currently show customers their attack surface – the paths a real attacker would use to reach their critical assets?
- Which of your customers are subject to NIS2 or DORA, and are you prepared to support their compliance obligations?

1. MITRE. *ATT&CK Evaluations: Enterprise (Round 7).* https://evals.mitre.org/enterprise/er7

3. Know Your Customer

Segmentation, Ideal Customer Profiles (ICP), buyer personas, and matching the right security offer to the right customer

Not every customer needs the same security offer. The most profitable MSP security practices start with clear customer segmentation – knowing which customers are ready for what, and how to have the right conversation with the right decision-maker.

Segment A: SMB (10–100 employees)

Pain: No IT or security staff – completely dependent on MSP
Budget: Cost-sensitive; needs simple, affordable protection
Trigger: Breach at a peer company; cyber insurance requirements
Decision-maker: Owner / MD – business risk framing needed
Right offer: Endpoints only or Protect bundle; monthly reporting; simple SLA
Upsell path: Compliance requirements, cyber insurance premium reduction

Segment B: Mid-Market (100–1,000 employees)

Pain: Part-time IT staff, no security expertise, growing compliance burden
Budget: Can invest in proper managed security; values outcome over price
Trigger: NIS2 obligation; board-level risk discussion; M&A due diligence
Decision-maker: IT Manager + CFO/CEO – risk AND cost framing
Right offer: Protect or Proactive bundle; MDR + quarterly reviews
Upsell path: vCISO retainer; Continuous Exposure Management service; ISO 27001 support

Segment C: High-Risk / Regulated (any size)

Pain: Regulatory compliance is non-negotiable; audit burden is heavy
Budget: Security is a board-level investment – price is secondary to risk reduction
Trigger: Regulation deadline; failed audit; insurance exclusion; sector mandate
Decision-maker: CISO / CFO / Board – compliance and liability framing
Right offer: Proactive bundle + vCISO + Compliance-as-a-Service
Upsell path: Full managed compliance program; annual audit support contracts

The Platform Buyer: A Cross-Segment Trend

Platform consolidation is the #1 procurement trend across all SMB and mid-market segments. Buyers are actively reducing the number of security vendors they manage, making vendor ecosystem integration a buying criterion as important as feature coverage.
For MSPs, this means positioning yourself as the platform integrator – not just a product reseller – using PSA/RMM integration depth as a selection criterion, and presenting single-pane, single-agent architecture as a consolidation offer – not just a security purchase.

Buyer Persona: The Business Owner

Language: Risk, liability, insurance, business continuity
Fear: "A breach will bankrupt us or destroy our reputation"
Message: "We protect your business, not just your computers"
Evidence they want: Peer case studies; insurance outcomes; breach statistics

Buyer Persona: The IT Manager

Language: Alerts, coverage gaps, tool consolidation, workload
Fear: ”A breach happened on my watch and I missed it”
Message: ”We reduce your alert noise and extend your team’s capability”
Evidence they want: MITRE scores; detection demos; ease-of-use proof; AI detection demos – show how Luminen GenAI assistant surfaces and contextualises threats automatically, reducing the alerts they need to act on and the risk of something slipping through

Buyer Persona: The CFO

Language: Cost, ROI, risk quantification, insurance, compliance costs
Fear: ”We’ll spend more on a breach than we’d spend on prevention”
Message: ”Security done right costs less than security done after a breach”
Evidence they want: Cost comparison; insurance premium data; ROI models

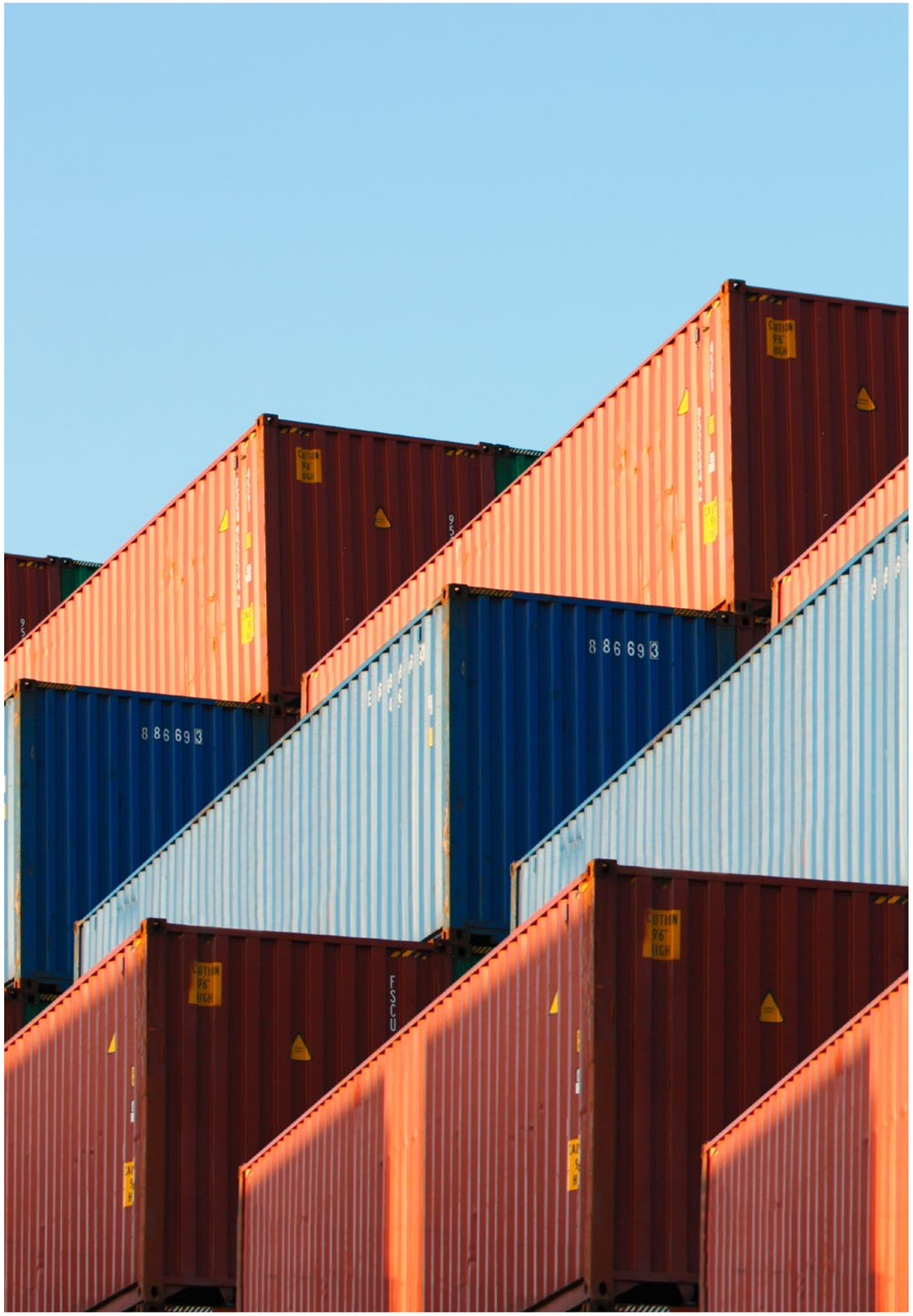
Key Questions for Your Business

- Do you know which of your current customers are subject to NIS2 or DORA? Have you had that conversation with them?
- For each customer segment, do you have a tailored security offer with a clear price and outcome statement?
- Who is actually making the security buying decision at your top 10 customers – IT, the CEO, or the CFO?
- Which vertical markets have the highest regulatory pressure in your geography – and are you positioned as the expert in those?

WithSecure – Compliance as a Sales Trigger

NIS2 applies to any EU entity in an essential or important sector – and their supply chains. DORA applies to all ICT providers serving financial entities. For European MSPs, regulatory pressure is the single most powerful sales trigger in 2026. WithSecure Elements is built with European compliance from day one – native NIS2, GDPR, DORA, and ISO 27001 support, with integrated reporting that turns compliance into a repeatable service revenue stream.

Compliance services are growing at 21% for MSPs in 2026[1]. 64% of SMB customers want guidance on compliance best practices, not just tools[2]. MSPs that own the compliance conversation at board level report structurally higher retention rates – because switching providers means restarting a compliance program.



1. Canalys. *MSP Trends*. 2026. https://canalys.com/insights/msp-trends-2025-es
2. Kaseya. *Global MSP Benchmark Report*. 2025. https://www.kaseya.com/resource/2025-msp-benchmark-report/

The Case for an End-to-End Security Platform

Modern threats no longer follow a single path. They start with compromised identities, move through Microsoft 365, establish persistence in cloud infrastructure, and exploit security gaps that point solutions have never mapped. Your current tool stack wasn't built to stop attacks working in concert. In 2026, MSPs must choose: manage complexity or build scale.

Why Platform Beats Point Solutions

Unified Coverage Across Every Attack Vector
An end-to-end platform covers endpoints, identities, Microsoft 365, cloud environments, and attack surface discovery – continuously. When these components are purpose-built to work together, detection becomes exponentially more powerful. A suspicious sign-in from a compromised device accessing a shared mailbox and modifying cloud infrastructure? A platform sees a coordinated attack. Point solutions see three separate alerts.

Cross-Layer Detection & Response (XDR)
Platform-based XDR correlates signals across endpoint, identity, and cloud in real time. This detects attack chains that isolated tools miss – lateral movements, privilege escalation, data exfiltration. It eliminates noise and focuses your team on genuine threats.

Continuous Exposure Management at Scale
An integrated platform includes automated discovery and prioritization of vulnerabilities, misconfigurations, and identity risks across your entire customer base. Your customers shift from reactive to proactive.

The Operational Advantage

The platform you choose defines your security posture, operational efficiency, and ability to grow. A purpose-built MSP platform includes:

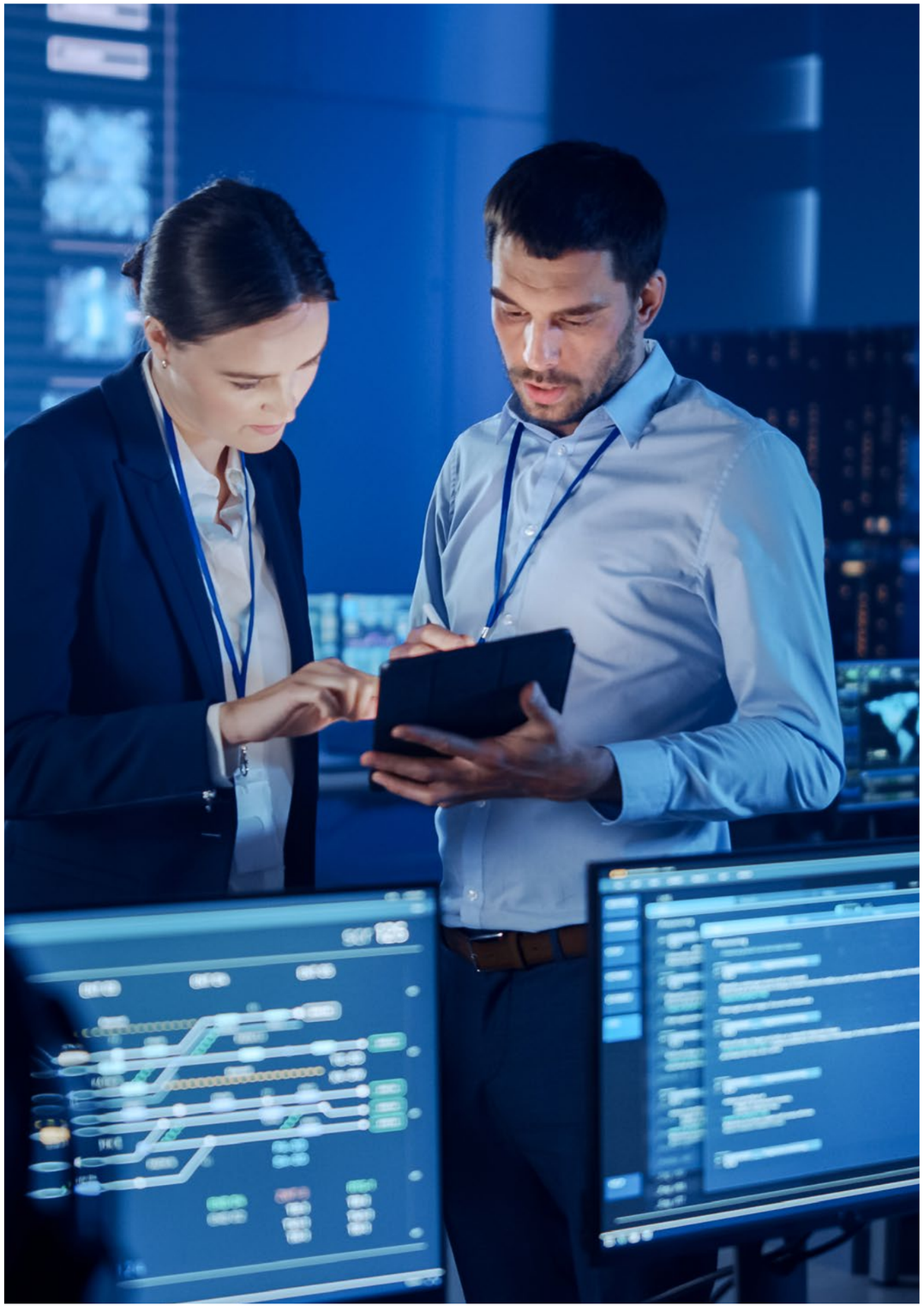
- Multi-tenant management – segregated customer environments, shared operational efficiency
- RMM/PSA integration – ticketing and automation flow directly into existing tools
- AI-assisted triage – reduce analyst burden without sacrificing accuracy

Choosing an end-to-end platform determines your business impact across three dimensions:

Margin: Point solutions mean vendor sprawl and margin pressure. A single platform simplifies billing and increases customer stickiness.

Analyst workload: Point solutions mean tool switching, manual correlation, and burnout. A platform reduces MTTR and eliminates toil.

Growth capacity: Point solutions don't scale with you. A platform grows with your customer base, improving operational leverage as you expand.



What an Effective Security Platform Looks Like in Practice

EASY TO DEPLOY

Elements™ | Agent

A single, lightweight, multi-purpose agent with easy to deploy, rebootless install, fully automated updates and optional staging for early adopters

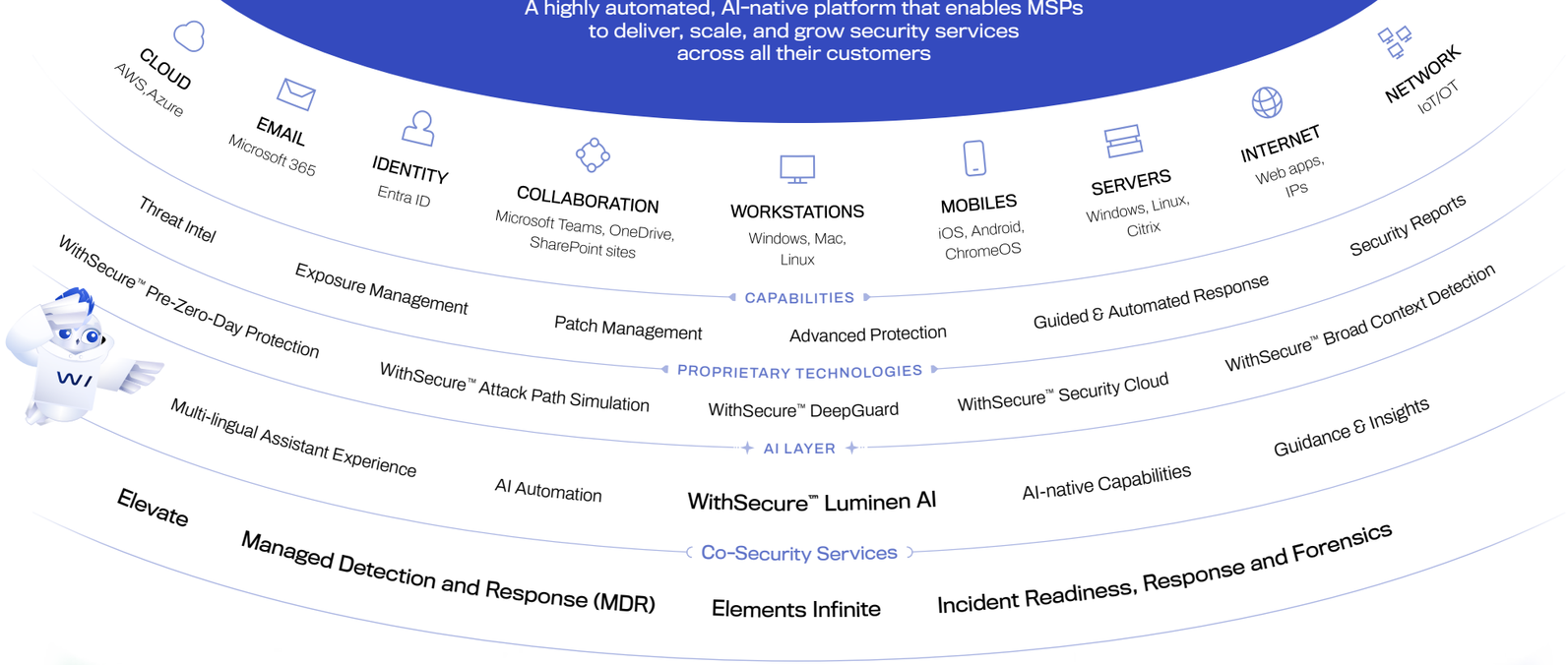
RMM / MDM

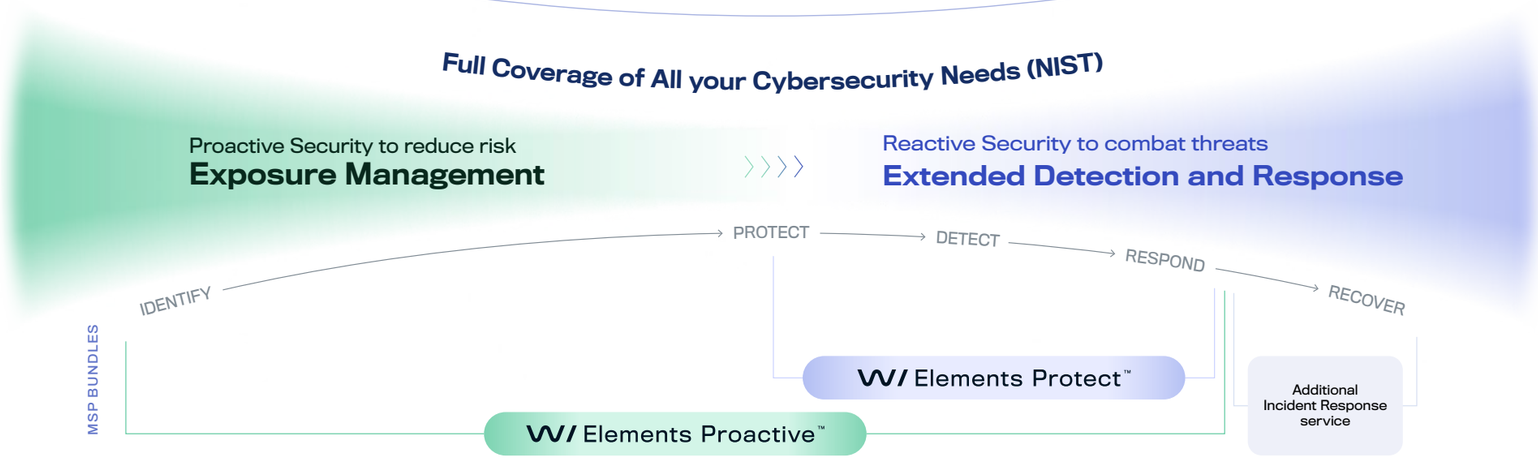
- ConnectWise RMM
- NinjaOne
- datto (A Kaseya COMPANY)
- Microsoft Intune
- Google Workspace
- jamf PRO

and others

WithSecure™ Elements Cloud

A highly automated, AI-native platform that enables MSPs to deliver, scale, and grow security services across all their customers





EASY TO AUTOMATE

Elements™ | Connect

Flexible integration options, APIs, and prebuilt integrations to automate operations and security event flows across your customer environments

PSA / ITSM / SIEM

- Autotask
- ConnectWise PSA
- HALOPSA
- Microsoft Sentinel
- ONEiO and 1000+ integrations
- Elements™ | Connector

and others

4. Building Your MSP Security Stack

A framework for evaluating security technology

The technology you choose has a direct impact on three MSP business fundamentals: cost per alert (how much analyst time each detection consumes), margin per seat (what you keep after tool and labor costs), and time-to-value (how quickly a new customer generates revenue). Most MSP security challenges are not caused by missing capabilities – they are caused by fragmented stacks that increase analyst workload and erode margin. This chapter helps you evaluate what goes in your security stack – and why a unified platform almost always wins at MSP scale.

Prevention Layer – Must Have

- EPP: Next-generation anti-malware, ransomware protection, device control
- Email security: Phishing, Business Email Compromise (BEC), and malicious attachment filtering
- Collaboration protection: Teams, SharePoint sites, OneDrive
- Mobile: iOS, Android, ChromeOS threat protection
- Disk encryption management: BitLocker / FileVault enforcement
- Web content control / Browsing protection: Improve security with controlled access to websites, prevent access based on categories, and enforce your corporate policy

Detection & Response Layer – Must Have

- EDR: Behavioral detection across endpoints and servers
- XDR: Correlated detection across endpoint + identity + cloud + email
- ITDR: Identity threat detection and response (Entra ID)
- MDR: 24/7 expert monitoring – via Co-security or your own SOC
- Alert triage and automated response playbooks
- Low-noise alerting: quality over quantity is critical for small teams

Proactive Security Layer – High Value

- Exposure Management: vulnerability + attack path + misconfiguration visibility
- Cloud security posture management: Azure and AWS misconfiguration detection
- Identity security posture management: Entra ID configuration hardening
- External attack surface monitoring: what's exposed on the internet
- IoT/OT device discovery: unmanaged asset visibility
- AI attack path simulation: understand how an attacker would move
- Prioritized findings: tailored to business context, using threat intelligence and attack paths
- Remediation and mitigation of exposures: Automatic and AI-guided

Compliance & Reporting Layer – Revenue Driver

- Risk register generation and management
- NIS2 / DORA / ISO 27001 / GDPR compliance mapping
- Executive-ready reporting (board-level, non-technical)
- Audit evidence packaging and audit support
- Quarterly Business Review (QBR) materials from platform data
- Policy templates and governance documentation

MSP Operational Requirements

- Multi-tenancy: true customer isolation with Role-Based Access Control (RBAC)
- Single pane of glass: one console for all customers and all modules
- Single lightweight agent: no agent proliferation across customers
- PSA/RMM integration: prebuilt connectors or open API
- Automated deployment: onboard new customers in hours, not weeks
- MSP-friendly billing: usage-based, monthly, no annual lock-in per customer

Platform vs. Best-of-Breed

Two approaches dominate: best-of-breed (strongest point tools, five consoles, five vendors, five contracts, alert silos, manual triage) and unified platforms (slightly less depth per category, but integrated correlations, single workflow, shared data model).

For mid-market MSPs under 150 staff, the math favors platforms. You get 40% less operational overhead from alert triage, faster onboarding of new customers, better margin per seat through unified licensing, and superior customer reporting because data correlates across modules. Your analysts spend less time wrangling multiple consoles and more time on actual security work.

Best-of-breed makes sense only for large MSPs (250+ staff) with dedicated security practice teams that can manage multiple consoles and custom integrations.

Security Operations Center: Make or Buy?

Building your own SOC demands expensive talent ($60–90K+ per analyst) and requires shift coverage, training, and burnout management. Outsourcing to an MSSP delivers 24/7 monitoring at lower cost – one analyst serves multiple MSP customers, spreading overhead. The financial case is clear: managed SOC is 70% more profitable than in-house for typical MSP scale. The real advantage? Outsourcing frees your team to focus on higher-margin advisory services (virtual CISO, compliance consulting, risk management), adding 20% to revenue. Most mid-market MSPs find that buying beats building, especially when it unlocks the service mix that actually drives profitability.

WithSecure – Platform-First Security for MSP Scale

Most MSP security challenges are not caused by missing capabilities, but by fragmented stacks that increase analyst workload and erode margin. WithSecure Elements is designed for MSP scale, unifying endpoint, identity, M365, cloud, exposure management, MDR, and compliance reporting in a single, multi-tenant platform with native correlation and low alert noise. A single agent and console enable faster onboarding, consistent service delivery, and better analyst efficiency across all customers. Combined with integrated GenAI assistance and European-based Co-security MDR, WithSecure Elements turns security operations into a scalable, repeatable, and profitable MSP business model.

Key Questions for Your Business

- How many consoles does your current security stack require? What is the real cost of analyst time across them?
- Do you have coverage for identity and M365 collaboration threats – not just endpoint?
- Can you onboard a new customer in under 24 hours with your current tooling?
- Is your GenAI capability included in your current platform cost, or an add-on that erodes margin?

Capability Checklist for Your Security Practice

Capability	Priority	What to Evaluate	WithSecure Elements	Competitor 1	Competitor 2	Competitor 3
Endpoint Protection (EPP)	MUST HAVE	AV-TEST / AV-Comparatives scores; ransomware detection; false positive rate	☑ AV-TEST Best Protection ×7; 100% ransomware protection (AV-TEST 2024)[1]	☐	☐	☐
EDR / Behavioral Detection	MUST HAVE	MITRE ATT&CK participation and detection-to-alert ratio	☑ 7/7 MITRE rounds; lowest noise of EU vendors in 2025[2]	☐	☐	☐
Identity Security (ITDR)	MUST HAVE	Entra ID coverage; real-time detection; leaked credential monitoring	☑ Native ITDR + Exposure Management for Entra ID	☐	☐	☐
Collaboration Protection	MUST HAVE	Full M365 coverage: email, Teams, SharePoint sites, OneDrive	☑ M365 suite full protection layer	☐	☐	☐
MDR / Co-security	MUST HAVE	Co-delivery SLAs; European SOC	☑ Co-security MDR with flexible co-delivery models – MSP-enabling, EU-based experts, defined SLAs	☐	☐	☐
Exposure Management	HIGH VALUE	Attack path simulation; cloud coverage; identity security posture	☑ Gartner Visionary 2025[3]; AI attack path; Azure + AWS + Entra ID	☐	☐	☐
Compliance Reporting	HIGH VALUE	NIS2/DORA/ISO built-in; audit evidence; executive reporting	☑ Integrated support for European compliance from day one	☐	☐	☐
GenAI Analyst Assistant	DIFFERENTIATOR	Is it included or an expensive add-on? Actual analyst time saved?	☑ Luminen GenAI assistant – always included, no extra cost, multiple language options	☐	☐	☐
PSA/RMM Integration	MUST HAVE	Prebuilt connectors to your stack; API quality; ticket automation	☑ Prebuilt catalog + open API + Elements Connector for SIEM, SOAR	☐	☐	☐
Multi-tenancy & RBAC	MUST HAVE	True customer isolation; role hierarchy	☑ State-of-the-art multi-tenancy + RBAC, purpose-built for MSP ease of use	☐	☐	☐

1. AV-TEST. *AV-TEST Award 2024: WithSecure.* https://www.av-test.org/en/news/av-test-award-2024-for-withsecure/
2. MITRE. *ATT&CK Evaluations: Enterprise (Round 7).* https://evals.mitre.org/enterprise/er7
3. WithSecure. *Gartner Magic Quadrant – Endpoint Protection Platforms.* https://www.withsecure.com/en/expertise/campaigns/gartner-mq-eap

5. Successful GTM: Bundles, Stickiness & Pricing

Why selling bundles outperforms single-technology sales – and how to build recurring services that create lasting customer loyalty

The MSPs growing fastest in the security market are not selling individual tools. They are selling outcomes – wrapped in managed services that create deep operational dependency and recurring, predictable revenue. This chapter shows you how to build that model. Think of this architecture not as a product menu, but as a three-act customer relationship.

Year 1 →	Year 2 →	Year 3
Protect	**Proactive**	**vCISO Retainer**
Protection + trust You become indispensable to operations	**Insight + authority** You own the risk conversation	**Strategy + indispensability** You sit at the board table

Every customer in your portfolio today is somewhere on this arc. The question is whether you are moving them along it – or whether a competitor will.

The bundle architecture below is a commercial framework developed by WithSecure that has proven to work with MSPs to grow their revenue per customer over time. Each tier is designed to be deliverable without building a SOC, priced to generate healthy margin from day one, and structured to create the kind of operational dependency that makes retention almost automatic.

Bundle 1: Elements Protect (MDR + XDR)

- EPP + EDR + Collaboration + Identity + MDR
- Example sell price target: Starting from €30 / seat / month
- You deliver: First-contact support; WithSecure experts validate and escalate; AI-driven triage via Luminen GenAI assistant reduces noise and surfaces what matters before your team reviews it
- Stickiness: MDR relationship, IR involvement, monthly security reviews
- Upsell trigger: First exposure finding via Elements XM trial or compliance audit request

Bundle 2: Elements Proactive (Exposure + Compliance)

- Protect + Exposure Management (devices, identities)
- Example sell price target: Starting from €40 / seat / month
- You deliver: Quarterly assessments, risk register, executive reviews, compliance reports
- Stickiness: Audit dependency, QBRs, board relationship, risk register ownership
- Upsell trigger: Board-level security briefing; vCISO need; ISO 27001 audit

MSP Service: 24/7 MDR

- Co-deliver via WithSecure's European certified expert SOC
- Monthly threat report + ongoing advisory
- Platform management and automated response fine-tuning
- Compliance-aligned operations (NIS2, GDPR)
- Base bundle: Elements Protect

MSP Service: Exposure Management

- Quarterly executive risk briefing from real platform data
- Remediation-as-a-service: remediate and mitigate exposures on customer's behalf
- Attack path simulation reports for board communication
- ISO/NIS2 audit evidence packaging
- Base bundle: Elements Proactive

MSP Service: Virtual CISO Retainer

- Strategic advisory on top of Proactive bundle
- Example sell price target: +€2,000–10,000 / month retainer (per customer)
- You deliver: Security strategy aligned to business goals, policy ownership, regulatory guidance, executive board liaison, IR plan ownership
- Stickiness: Board-level relationship; strategic plan ownership; irreplaceable advisor role; annual contract structure
- Upsell trigger: Board request for CISO-level expertise without full-time hire cost

Pricing note: the recommended selling prices represent the full managed service price (technology + your services). Bundles should be priced to reflect your operational value-add on top of the WithSecure platform cost. A WithSecure Partner Manager can provide current RRP and margin guidance.

Real Partner Result – Ictivity, the Netherlands

Ictivity (170 employees, Dutch mid-market) leveraged WithSecure Co-security and the Proactive bundle to deliver 24/7 MDR without building their own SOC. Security revenue grew 100% in 12 months.

> **"Our joint go-to-market strategy, combined with co-selling and co-marketing initiatives, has enabled us to scale rapidly."**
>
> *– Dominique Frison, Security Consultant, Ictivity*

Key Questions for Your Business

- What is your average security revenue per seat today? What would each tier look like across your top 20 customers?
- Do you have a structured Quarterly Business Review process tied to your security delivery?
- Which of your customers are currently EPP-only, and what would it take to move them to the Protect bundle this quarter?
- Is there a customer in your portfolio right now who needs a vCISO – but can't afford a full-time hire?
- How much analyst time does your current security stack consume per week in alert triage, console switching, and manual reporting? Would a 40–70% reduction in ticket resolution time change your unit economics?
- Which of your customers are ready for a board-level security conversation this quarter – and do you have the exposure data to have it?

6. Vendor Landscape

How to evaluate security platforms as an MSP

Every platform choice you make cascades into business outcomes: revenue timing, margins, analyst headcount, customer retention, and compliance risk. This framework maps platform capabilities to the business metrics that actually matter.

Fast Time to Revenue

The speed you deploy security directly impacts customer onboarding velocity and revenue recognition. Platforms built for MSPs enable deployment through your RMM with minimal manual configuration – hours instead of weeks.

> **Ask:** Can the platform integrate natively with your RMM, PSA, and SIEM? Do prebuilt connectors pull device inventory and deployment status in real-time, or does integration require custom scripting? Does the platform auto-inherit policies across customers, or do you manually replicate config for each account?

These operational gaps don't sound like big deals until your sales team is waiting three weeks to activate a new customer. Platform completeness across endpoints, identity, cloud, and email matters here too – every missing domain adds another deployment cycle and delays revenue.

Profitability of Business

Your licensing structure directly determines gross margin. Platforms with MSP-aligned pricing let you bill monthly per customer with no annual lock-in. Others force annual commitments or per-endpoint costs that penalize growth.

> **Ask:** Evaluate whether the vendor is channel-first or direct-first. Channel-first vendors price to enable your success. Direct-first vendors protect their own sales motion and view MSPs as a secondary channel. After year one, does the discount hold, or does it erode? Can you forecast costs without guessing seat counts six months in advance?

Bundled services (MDR, exposure management, compliance reporting) should expand your service attach rate and allow you to command advisory pricing. Platform vendors who enable this shift – rather than compete with your services – build sustainable margin.

Operational Burden

Your analyst capacity is your limiting resource. Every fragmented console, every manual alert triage workflow, every duplicate asset list erodes productivity. A platform built for MSP operations means one unified console where team leads manage their segment, analysts see only their assigned accounts, and executives pull board-ready reports – without context switching between five tools. Single-pane management isn't about aesthetics; it's about analyst hours.

Intelligent alert correlation and AI-powered triage cut noise by filtering related events into incidents rather than sending 50 individual alerts per day. Low-noise detection that actually works keeps your team focused. High-volume alerting with manual review doesn't scale and drives turnover.

> **Ask:** Does this platform make your analysts more productive, or does it add overhead?

Scalability

Can you grow your customer base without proportionally hiring more analysts? A platform with intelligent correlation and automated response playbooks breaks the linear relationship between seats and analyst headcount. A fragmented best-of-breed stack forces that linearity. For a 2,000-seat MSP, unified platform architecture with AI-driven

triage could save 50+ analyst hours per month – headcount you don't hire, or capacity you redirect to advisory services.

> **Ask:** Evaluate deployment automation, multi-tenancy architecture, and whether the platform supports role-based access at scale. Can you onboard 100 new customers per month without adding operational complexity?

Prove Security Value

Your customers need to see security impact, not just compliance checkboxes. Platforms that surface vulnerabilities, attack paths, and misconfigurations before incidents happen shift your narrative from "we caught the bad guy" to "we prevented the breach."

> **Ask:** Do you provide exposure management – vulnerability assessment, cloud posture, attack path analysis, identity misconfiguration detection?

Platforms that include this natively let you build proactive advisory services that turn security from a cost center into a revenue driver. Platforms that require bolt-on tools fragment your risk picture and your customer reporting. Executive-ready reports that show business impact (prevented breach scenarios, risk reduction over time, compliance readiness) win renewals and upsell opportunities.

Expand Revenue per Customer

Managed Detection and Response (MDR) and co-security models let you offer 24/7 monitoring without building a 24/7 team. But vendor positioning matters. Some vendors enable your analysts as co-responders – they handle routine triage, your team handles escalations and complex response. Other vendors try to become your entire SOC, gating findings behind their console and sidelining your team. Partnership models create revenue expansion. Replacement models create cost centers.

> **Ask:** Evaluate whether the vendor's MDR team escalates with full context, whether your team can define playbooks and SLAs, and whether you have API access to automate responses. The best vendors extend your capability; the worst create dependency.

Security Practice Development

Your ability to deliver proactive security services depends on the platform's breadth and depth.

> **Ask:** Can you offer vulnerability management, cloud security posture assessment, identity hardening, and attack path simulation? Or are these add-ons that fragment your operations?

Platform vendors who include exposure management natively, provide open APIs, and enable custom playbooks let you build advisory services that command premium pricing. Vendors who gate functionality behind expensive add-ons or require their own consultants limit your margin.

European Compliance & Data Sovereignty

For EU operations, this is often a deal-breaker, not a negotiation point. GDPR enforcement is real. NIS2 compliance requirements are tightening.

> **Ask:** Is there native EU data processing, or does data transit to US infrastructure? Does the vendor process, index, and log data in EU facilities? What are their DPA terms – do you negotiate once or separately for each customer? Are audit logs available for compliance demonstrations without vendor intermediation?

Some vendors offer EU options at a premium. Others don't offer them at all. Factor this into your evaluation early.

Vendor Partnership & Stability

Your security platform is foundational to your business. Evaluate whether the vendor is committed to your success long-term.

> **Ask:** Are they investing in channel enablement (training, certification, co-marketing, access to technical experts)? Do their partner economics reward growth, or do you hit annual commitment cliffs? Is their company stable and investing in product roadmap, or are they in survival mode?

The best relationships feel like partnerships. You're working toward shared goals, not negotiating inside constraints. A vendor committed to your success becomes a competitive advantage.

Comparison of MSP Offerings

Score vendors across each of these business outcomes. Weight them by your priorities – EU compliance might be mandatory; scalability might be your primary differentiator; margin expansion might drive your evaluation. Evaluate systematically and you'll avoid surprises. Rush the evaluation and you'll spend the next three years trying to make the wrong platform work.

Business Outcome & Required Capability	**WithSecure Elements** Mid-market MSP focus	Competitor 1	Competitor 2	Competitor 3
Fast time to revenue *Structured onboarding + MSP packages + sales enablement*	STRONG Single-agent, 24hr onboarding, full MSP package + enablement			
Profitability of business *MSP-aligned pricing + bundled services + margin architecture*	STRONG Partners report up to 70% higher margins; Co-security eliminates SOC build cost			
Operational burden *24/7 MDR + AI triage + clear escalation – without building a SOC*	STRONG ~50 actionable alerts/1,000 seats/month; Luminen GenAI triage included; 1 FTE can manage 5,000+ seats via Co-security			
Scalability *Grow seat count without adding analyst headcount*	STRONG Multi-tenant, single agent, AI-driven triage; scales to 5,000+ seats per FTE			
Prove security value *Executive reporting that demonstrates business impact to customer boards*	MODERATE MSP-oriented executive reporting; Exposure Management data for board QBRs; value proof improving			
Expand revenue per customer *Modular service ladder: Protect → Proactive → vCISO*	STRONG Three-tier bundle progression built in; Exposure Management + vCISO path generates €2K–10K/month retainers			
Security practice development *Co-growth support: service packaging, advisory, business enablement*	STRONG 100% channel; MSP-specific service development, co-marketing, co-selling			
European compliance & data sovereignty *NIS2, DORA, GDPR built-in; EU data residency; EU-delivered service*	STRONG Finnish, founded 1988, EU law from day one; NIS2/DORA/GDPR native; SOC in Europe			
Vendor partnership & stability *Long-term partner; no direct competition; M&A stability*	STRONG Independent; many top partners 10+ years; no direct sales motion			

Sources: Omdia 2025–26; Gartner 2024–25; MITRE ATT&CK Enterprise Evaluations 2025; Kaseya Global MSP Benchmark 2025; WithSecure partner data.

7. The WithSecure Advantage

Building a security practice is a strategic investment. The commercial model you choose determines whether that investment compounds or erodes. WithSecure is designed from the ground up to make MSP security services structurally profitable – not as a feature, but as the foundation.

Higher Margins per Customer – by Design

WithSecure partners report up to 70% higher margins compared to running a self-built security operation. The bundle architecture creates a clear upsell path that drives revenue per seat growth over time. MSPs using this model have doubled security revenue within 12 months, without investing in their own 24/7 SOC. The progression from EPP into Exposure Management and compliance advisory is built into the commercial framework, not bolted on as an afterthought.

Lower Cost to Deliver – Fewer People, More Seats

The Elements platform generates approximately 50 actionable alerts per 1,000 seats per month – not thousands of raw signals that consume analyst hours and erode margin. Luminen GenAI assistant contextualises detections and delivers clear remediation guidance automatically, reducing the manual triage burden. MSPs fully outsourcing monitoring through WithSecure Co-security have managed 5,000+ seats with a single internal IT professional, instead of building a nine-person SOC. That ratio is the difference between a scalable services business and one that requires continuous headcount investment to grow.

Faster Onboarding, Longer Retention

A single lightweight agent across endpoints, identities and cloud means first-customer onboarding can be completed within 24 hours. Time-to-revenue is measured in days, not quarters. Built-in NIS2 and DORA alignment accelerates sales cycles in regulated sectors and reduces the burden of compliance conversations. As the relationship deepens – from protection into risk reporting and advisory – customers become embedded in a program they cannot easily replace. WithSecure partners report a 95% customer retention rate. That is not a satisfaction metric. It is a revenue protection number.

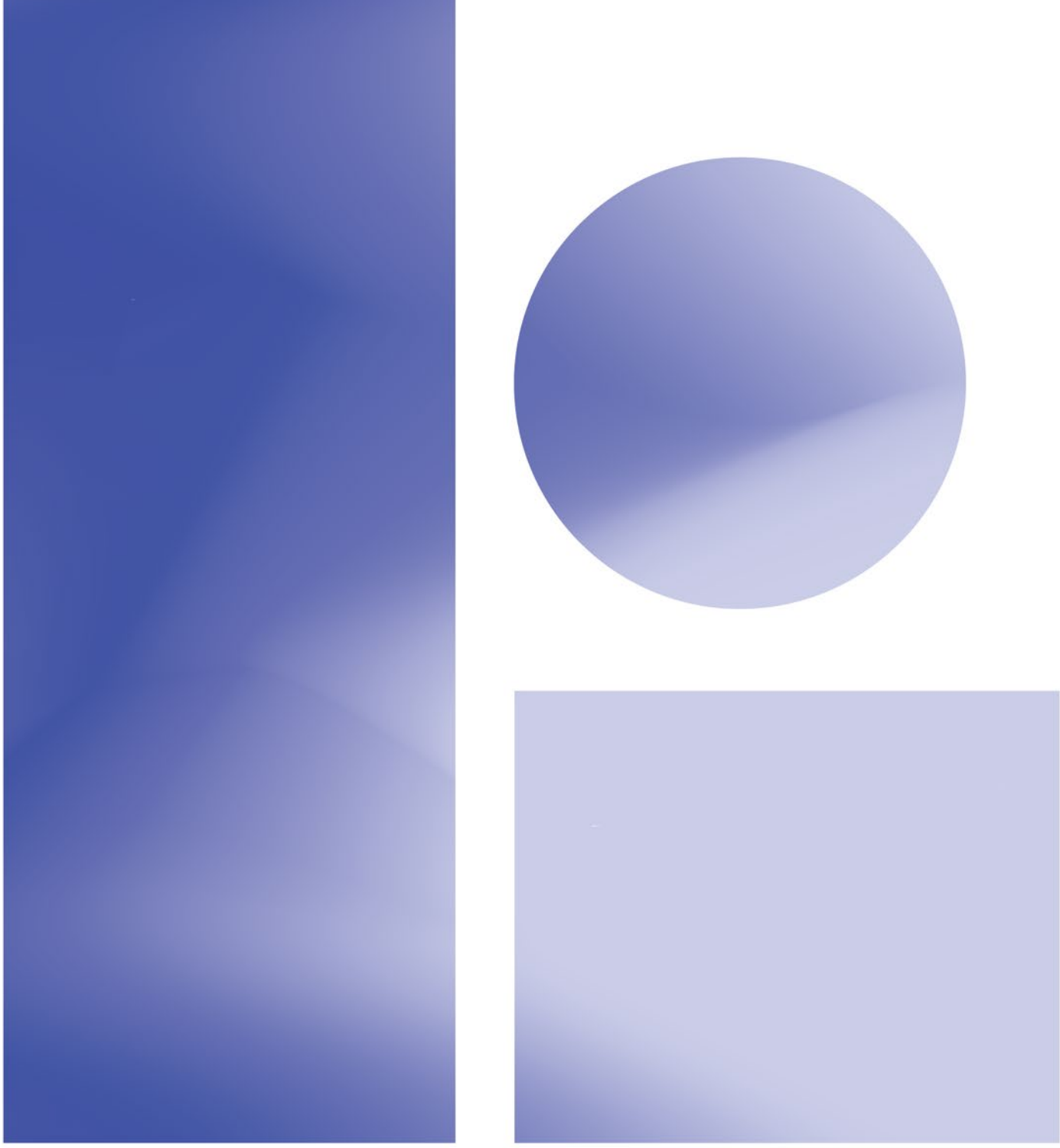
EU Compliance as a Revenue Advantage, Not an Overhead

WithSecure is Finnish, founded in 1988, operating fully under EU jurisdiction. Data sovereignty and regulatory readiness are not configuration options – they are structural properties of the platform.
For EU MSPs serving customers subject to NIS2, DORA or GDPR, this eliminates a compliance risk that US-headquartered vendors cannot resolve through EU region hosting alone. That distinction wins deals. And as regulations tighten, it becomes a more powerful differentiator every year.

A Growth Path that Moves With You

The commercial architecture of WithSecure Elements is built for progression. Protection evolves into proactive Exposure Management, then into advisory and vCISO services – all within a single platform and a single commercial framework. MSPs do not need to re-platform or renegotiate as they move upmarket. This means the investment you make in skills, tooling and customer relationships compounds over time, rather than depreciating as you outgrow your vendor. The path from €8 per seat to €25+ per seat is visible, supported, and already walked by hundreds of WithSecure partners.

Most security vendors build for enterprise and adapt for MSPs. WithSecure builds for MSPs first. The commercial model, the platform architecture, the Co-security delivery model – each is designed to make your practice more profitable, more scalable, and more resilient with every customer you add. With a partner NPS of 65 and many top MSP relationships stretching beyond a decade, the evidence is not theoretical. When you grow, we grow. That is not a sales line – it is the commercial model.



WITH secure

CYBERSECURITY. THE EUROPEAN WAY. | WITHSECURE.COM