Cybersecurity Selling Playbook for the Modern Technology Advisor

A holistic approach to transforming cyber conversations into strategic business value

Publish Date: October 2025

Table of Contents

Introduction
Cyber's Expanding Landscape (w/ Interactive Infographic)

Section 1:
Understanding Key Buyer Personas

Section 2:
Emerging Trends & How to Use Them to Sell

Section 3:
Compliance & Regulation Selling Framework

Section 4:
Positioning MSSPs vs In-House SOCs

Section 5:
Tailoring Cyber to Industry Needs

Section 6:
Conclusion

Section 7:
Your Telarus Cyber Experts

Introduction

The cybersecurity landscape demands proactive, dynamic solutions. As a Telarus technology advisor, you're not just solving cybersecurity problems; you're leading clients toward robust digital safety with tailored solutions. This guide equips you to strategically position Managed Security Service Providers (MSSPs) and deliver business-aligned security outcomes.

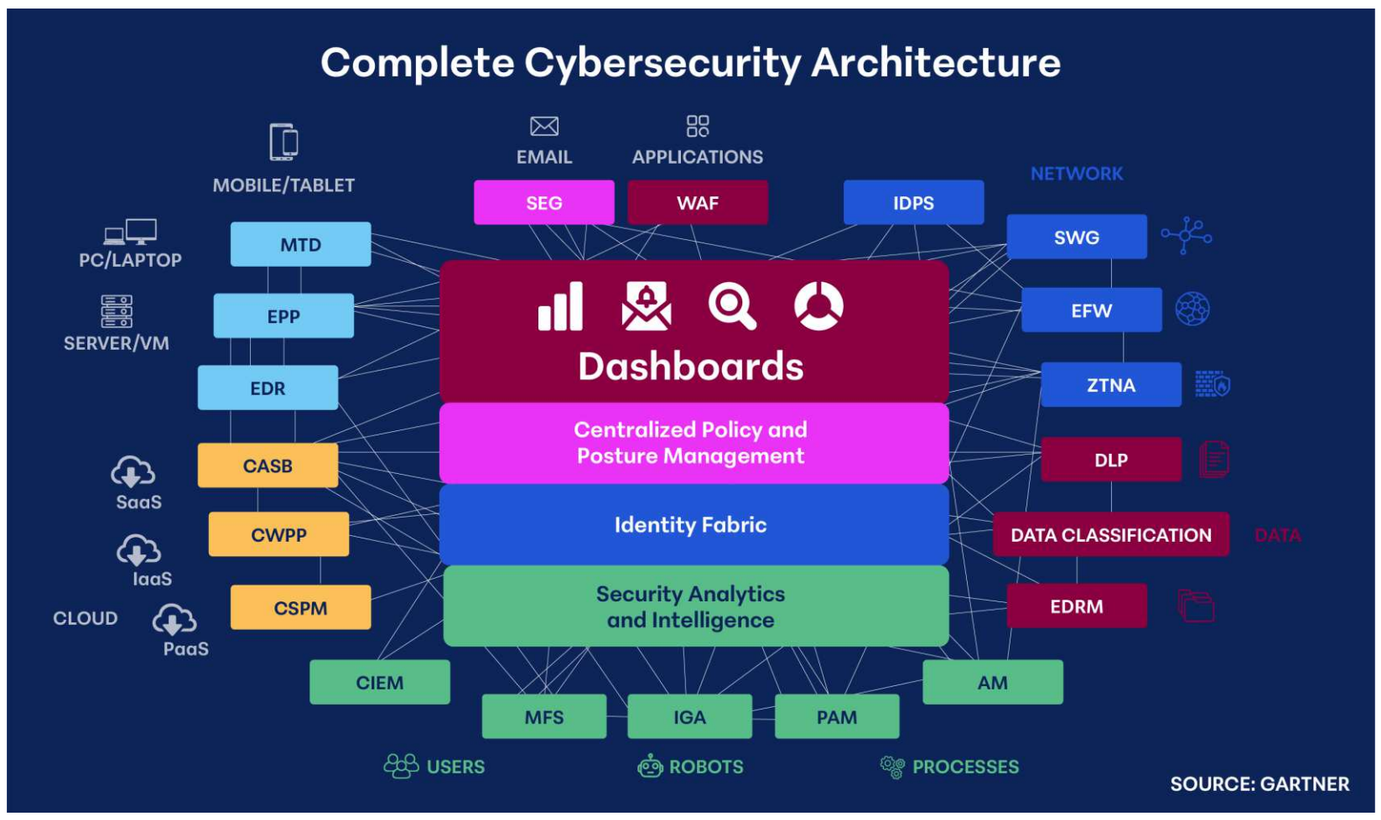
Cybersecurity's Expanding Landscape

The stakes have never been higher. Cyberattacks are constantly evolving, regulations are tightening, and businesses must adapt. Today's organizations aren't just looking for reactive security measures; they expect proactive, dynamic solutions—integrating technologies like artificial intelligence, machine learning, and Zero Trust frameworks just to stay ahead. And as compliance requirements continue to evolve and reshape operational landscapes, the need for MSSPs has never been clearer.

This guide arms you with critical strategies to redefine stakeholder conversations, effectively communicate the value of MSSP solutions, and transform cost concerns around building a Security Operations Center (SOC) into compelling narratives for leveraging MSSPs.

Setting the Stage for Holistic Cyber Selling

To enhance your understanding, we've complemented this playbook with an interactive infographic that visually captures the key concepts and benefits associated with engaging MSSPs. Together, these insights bridge the gap between complex information and actionable intelligence, ensuring you can effectively communicate the value of cybersecurity solutions to your clients.



Access the Full Interactive Infographic

The future of cybersecurity is here, and with this guide in hand, you'll lead the charge.

Section 1: Understanding Key Buyer Personas

Successful cybersecurity engagement requires connecting with key decision-makers like CISOs, CFOs, and heads of IT by addressing their unique priorities—risk reduction, cost control, and tool management. By understanding their challenges, you can position solutions that align with their security goals and business value, ultimately driving more meaningful conversations and sales.

Chief Information Security Officer (CISO)

Priorities

- Alert fatigue
- Disparate toolsets
- Risk reduction
- Budget management
- Incident response
- Regulatory alignment
- Internal SOC vs MSSP justification
- AI and AI governance
- Compliance audits
- Staff retention

Talking Point

"How are you validating your current risk exposure and aligning tools to compliance mandates?"

Sales Focus

- MSSP as SOC extension
- Compliance automation
- Advisory posture

Chief Information Officer (CIO)

Priorities

- IT budget efficiency
- Operational resilience
- Cloud transformation
- Network segmentation
- Headcount
- Retention of resources

Talking Point

"What’s the balance between innovation and securing your digital estate?"

Sales Focus

- ROI-driven security
- Co-sourcing to protect business uptime

Chief Compliance Officer (CCO) / Risk Officer

Priorities

- Avoiding fines
- Reporting readiness
- Cross-functional controls

Talking Point

"How confident are you that your organization could pass an unannounced audit or meet new AI governance rules?"

Sales Focus

- GRC dashboards
- Automated evidence collection
- MSSP alignment to frameworks

Chief Financial Officer (CFO)

Priorities

- Cost management
- Liability reduction
- Insurance premiums

Talking Point

"Would lowering cybersecurity insurance premiums or avoiding fines offset the cost of managed security? How many days can your company go without earning revenue and still stay alive in the event of a ransomware attack?”

Sales Focus

- Cost calculator
- Breach cost avoidance
- Subscription-based MSSP value

Head of IT / Director of Infrastructure

Priorities

- Tool fatigue
- Limited staff
- Need for 24/7 visibility

Talking Point

"What are your biggest gaps today—tool sprawl, false positives, after-hours response?”

Sales Focus

- MSSP as Tier 1-2-3 SOC
- Tool consolidation
- Rapid IR

Legal Counsel / General Counsel

Priorities

- Incident disclosure compliance
- Litigation defense
- Vendor risk

Talking Points

"Do you have a clear record of access controls, logging, and security events for legal defensibility?"

Sales Focus

- Audit trails
- Chain of custody
- MSSP response playbooks

Line of Business Executives (e.g., VP Operations, COO)

Priorities

- Productivity
- Business continuity
- Secure digital enablement

Talking Points

"What would a 24-hour ransomware delay mean for your operations or customer SLAs?”

Sales Focus

- Downtime reduction
- Secure growth
- Enablement over disruption

Summary

To effectively engage in the cybersecurity space, tailor your messaging to the priorities of each decision-maker. For CISOs, emphasize risk reduction and regulatory alignment; for CIOs, highlight secure IT agility; and for CFOs, focus on ROI and cost avoidance. Address legal counsels' compliance needs and heads of IT's operational challenges with tailored solutions. By aligning cybersecurity with business value, you position yourself as a partner in resilience, risk reduction, and sustainable growth.

Section 2: Emerging Trends & How to Use Them to Sell

Cybersecurity is evolving faster than ever and staying ahead of threats requires both innovation and strategy. With game-changing technologies like AI-driven threat detection, Zero Trust architectures, and MSSPs, businesses are gaining new ways to reduce risk and improve efficiency. Yet, the pressure to meet compliance, manage costs, and mitigate breaches adds layers of complexity for your clients. As a cybersecurity technology advisor (TA), you hold the keys to guiding organizations toward smarter, scalable, and cost-effective security frameworks that align with modern challenges, ensuring confidence in their operations while driving strategic engagement.

Trend #1: AI-Driven Threat Detection

Category: Managed Security / AI Security Tools / Compliance

Trend Insight: Generative AI, large language models (LLMs), and agentic AI platforms are rapidly transforming security operations. These tools reduce detection and triage times, eliminate noise, and improve compliance readiness through automated documentation and response mapping. Many companies are looking to adopt AI without a framework, roadmap, or governance to guide them through this journey.

How to Position this Trend as a TA

Buyer Persona	Key Focus Area	Positioning Strategy
CISO / Security Leader	Detection speed, SOC efficiency, AI innovation	Position AI as an extension of the security team—not a replacement—especially helpful in talent-strapped environments
CIO / VP of IT	Tech stack consolidation, measurable ROI	Highlight AI's role in reducing tool sprawl by combining detection, response, and compliance reporting in one platform
Compliance / GRC Manager	Audit readiness, documentation automation	Showcase automated logging, evidence collection, and policy mapping using LLMs and GRC integration
Finance / COO	Cost efficiency, operational resilience	Present AI as a force multiplier: lower incident cost, reduce headcount pressure, and accelerate compliance timelines

Key Talk Tracks

Use these conversation starters to guide client discussions:

1 Security Operations Bottlenecks

"What's your average time to detect and respond to a threat today? How much of that process is still manual?"

2 AI as a Co-Pilot in Security

"How are you leveraging AI to reduce alert fatigue, false positives, or staff burnout in your SOC?"

3 Compliance-Driven Automation

"Do your audit reports still take weeks to compile? Some of our clients are using AI to generate audit-ready summaries in real time."

4 Risk & Cost Impact

"Every hour of downtime or delay in breach response has a real cost. Have you measured that impact?"

Market Impacts

- Security labor shortage: 3.4M global cybersecurity job gap (ISC², 2024)—AI is filling the talent void.
- AI-driven SOC platforms: Platforms like ReliaQuest, Expel, and Blumira are now embedding LLMs into core services.
- Insurance incentives: Carriers increasingly recognize AI-based response platforms in underwriting for premium discounts.
- Compliance acceleration: AI-infused GRC tools reduce prep time for frameworks like HIPAA, CMMC, PCI-DSS, and SOX by up to 70%.

Advisor Checklist to Position AI-Driven Threat Detection Effectively

- ❑ Use MTTD/MTTR benchmarks to establish urgency.
- ❑ Tie AI tools directly to specific frameworks (HIPAA, NIST, PCI, CMMC).
- ❑ Bring supplier demos early—focus on UI simplicity and real-time analytics.
- ❑ Propose QBRs as checkpoints for improving AI outcomes (false positives, detection rate, ROI).

Use Cases from TA Sales Experience

Industry	Use Case	Supplier Role	TA Sales Strategy
Healthcare	Automated detection of insider threats to ePHI using AI-based behavior analytics	Supplier deployed AI-enhanced MDR with role-based anomaly detection	TA introduced compliance-aligned supplier after HIPAA audit failed; positioned AI as a cost-saving automation layer
Finance	Reduced MTTR from 6 hours to under 30 minutes by integrating GenAI into SIEM for smart alert triage	Supplier implemented GenAI-based triage engine	TA asked: "What's the cost of every hour an incident goes undetected?" to pivot into an ROI-based close
Public Sector	Agentic AI platform automated report generation for CJIS compliance	Supplier provided GRC platform with AI-powered audit logs and auto-mapped security events	TA engaged procurement and security leads by focusing on audit readiness and risk visibility
Manufacturing	GenAI-enabled EDR used for predictive threat hunting and malware sandboxing	Supplier used AI for dynamic threat correlation across global environments	TA leaned on "downtime cost" framing to connect security automation to operational uptime

Trend #2: New Regulatory Landscape

Category: Managed Security / Compliance

Trend Insights: Recent regulations such as the SEC Cybersecurity Rules, FTC Safeguards, and the EU AI Act are reshaping the compliance requirements organizations face. These frameworks demand heightened transparency for AI models, stricter breach disclosure timelines, and greater accountability at the executive and board levels. As compliance becomes more complex, companies must proactively align their operations to adhere to these regulations, demonstrating responsible AI usage to avoid penalties and reputational risks.

How to Position this Trend as a TA

Buyer Persona	Key Focus Area	Positioning Strategy
Compliance/GRC Manager	Audit readiness, automation tools	Highlight how AI streamlines regulatory workflows (e.g., logging, reporting), minimizing the burden on manual processes.
CISO	Incident response efficiency	Present compliance automation as a way to reduce breach impact through faster reporting and recovery cycles.
CFO / COO	Cost of non-compliance	Showcase financial impacts of non-compliance and emphasize how automation mitigates risks while reducing costs.

Key Talk Tracks

Use these conversational prompts when exploring regulatory readiness:

1 **Regulatory Readiness**

"What mechanisms do you have in place to meet increasingly stringent breach disclosure timelines under regulations like the SEC Cybersecurity Rules?"

2 **Accountability at the Board Level**

"With the EU AI Act emphasizing model accountability, how are you addressing transparency and explainability in your AI systems?"

3 **AI for Transparency**

"How are you ensuring that board members are properly trained to oversee cybersecurity and compliance efforts in alignment with FTC and SEC requirements?"

4 **Executive-Compliance Team Collaboration**

"Are your executive and compliance teams equipped to work efficiently and effectively under the pressure of these heightened regulatory demands?"

Market Impacts

- **Increasing Regulatory Complexity**: New frameworks pile pressure on stakeholders to stay ahead of compliance demands while managing limited resources.
- **Non-Compliance Penalties**: Fines for regulatory violations can reach millions, making proactive compliance readiness a non-negotiable priority.
- **AI as Compliance Enabler**: AI tools reduce the time required for documentation and evidence collection, freeing up compliance teams to focus on critical governance tasks.

Advisor Checklist to Position Compliance Effectively

- ❑ **Understand Regulatory Needs**: Familiarize yourself with client-specific compliance requirements. Compliance-as-a-Service (CaaS) solutions simplify adherence to frameworks like HIPAA, PCI, and more, offering tools like policy development and vulnerability assessments.
- ❑ **Leverage Automation**: Highlight automated tools with AI capabilities, which streamline audits by identifying risks and enabling real-time supervision.
- ❑ **Host Strategy Workshops**: Conduct workshops to uncover compliance gaps. Ongoing expert guidance ensures readiness and effective compliance strategies.
- ❑ **Deploy Compliance Tools**: Use centralized reporting tools, such as executive dashboards and compliance scorecards, to enhance efficiency and reduce costs.
- ❑ **Plan Regular Reviews**: Schedule ongoing check-ins to adapt strategies as regulations evolve. Year-round monitoring ensures consistent compliance and regulatory readiness.

See Section 3 for a detailed Compliance and Regulation Selling Framework.

Use Cases from TA Sales Experience

Industry	Use Case	Supplier Role	TA Sales Strategy
Finance	AI-enabled compliance audit automation reduces reporting time by 70%	Supplier embeds automated logging via GRC tools	TA encouraged adoption by highlighting ROI tied to reduced audit and reporting costs
Healthcare	Automating security incident reporting timelines for HIPAA compliance	Supplier provided AI-powered incident response compliance	TA introduced solution during discussions about breach disclosure readiness after client uncertainty about HIPAA compliance audits
Public Sector	Real-time AI analysis for GDPR breach reporting disclosures	Supplier deployed automated reporting via integrated AI tools	TA positioned compliance alignment with high penalties for GDPR non-compliance as decision-driver
Retail	AI simplifies tracking of regulatory transparency for FTC safeguards	Supplier used AI dashboards for compliance accountability	TA leveraged stakeholder concerns about board-level liability to advocate for automated solutions

Trend #3: Cyber Insurance Dependencies

Category: Managed Security / Compliance / Cyber Risk Management

Trend Insights: Insurance providers are increasingly mandating proof of security controls such as multi-factor authentication (MFA), endpoint detection and response (EDR), incident response plans, and data encryption. Organizations failing to meet these requirements are subject to elevated premiums or denial of claims. As cyber threats escalate, compliance with insurer-preferred controls is essential for maintaining affordable coverage and qualifying for payouts.

How to Position this trend as a TA

Buyer Persona	Key Focus Area	Positioning Strategy
CISO / Security Leader	Risk reduction, threat mitigation, security control validation	Position cyber insurance compliance as a security validation framework that demonstrates control effectiveness while reducing organizational risk exposure and potential breach impact costs.
CIO / VP IT	Infrastructure modernization, operational continuity, technology alignment	Emphasize how insurance-mandated controls like MFA and EDR modernize IT infrastructure while ensuring business continuity and avoiding coverage gaps that could disrupt operations.
Compliance Manager	Regulatory adherence, audit preparation, documentation standards	Showcase how aligning security controls with insurer requirements streamlines compliance reporting, simplifies audit processes, and creates defensible documentation for regulatory frameworks.
Finance / CFO	Premium optimization, cost predictability, claim protection	Highlight the direct financial impact: Implementing required controls reduces premiums, prevents claim denials, and protects against the 3x cost increases faced during policy renewals without proper security measures.
Risk Manager	Enterprise risk assessment, insurance optimization, business resilience	Focus on how proactive security control implementation reduces overall enterprise risk profile, ensures favorable insurance terms, and maintains business resilience against evolving cyber threats.

Key Talk Tracks

Use these conversation prompts to highlight cyber insurance-related risk management:

1 Review Coverage

"Have you reviewed your cyber insurance coverage recently to ensure compliance with evolving requirements, such as MFA and EDR implementation?"

2 Adapt Payment Structures

"Are you facing higher premiums or difficulty securing claims due to missing cybersecurity controls? What steps are you taking to minimize these risks?"

3 Incident Response Plans

"In light of insurer mandates for detailed incident response plans, how are you preparing your teams and systems to meet these expectations?"

4 Encryption Readiness

"Are encryption policies in place that satisfy insurer regulations for secure data management and breach prevention?"

5 Trigger the Budget Shift

"Your policy may not be renewed — or will cost 3x more — unless these gaps are addressed."

6 Highlight Claim Denials

"Without controls like MFA or EDR, did you know your insurer can legally deny a breach claim?"

7 Tie to Audit Support

"Many MSSPs provide policy-aligned reporting that simplifies cyber insurance audits."

8 Leverage Peer Pressure

"Have you considered security bundles? Your competitors are already leveraging them to reduce premiums and protect cash flow."

Sample Customer Triggers

- "We just got our renewal quote, and it jumped 50%."
- "Our broker says we need to show evidence of a response plan."
- "We had a breach, but the claim was denied due to missing controls."
- "Legal is pushing us to improve our risk posture for the next underwriting."

Market Impacts

- **Evolving Insurer Requirements**: Cyber insurance providers are tightening requirements, mandating controls like multi-factor authentication (MFA), endpoint detection and response (EDR), incident response plans, and encryption to manage escalating claims exposure.
- **Impact on Premiums and Claims**: Organizations lacking these mandated security measures face increased premiums or risk being denied coverage and claims, making compliance with insurer-preferred controls a financial necessity.
- **Rising Cyber Threats**: As cyberattacks grow in sophistication and frequency, businesses must align their security posture with insurer demands to mitigate risk and ensure affordable, uninterrupted coverage.

Advisor Checklist to Position Cyber Insurance Dependencies Effectively

- ❑ **Underwrite Control Requirements:** Guide clients in understanding the minimum security controls insurers mandate and how solutions like MFA, EDR, and encryption enhance claim eligibility while lowering premium costs.
- ❑ **Promote Proactive Compliance:** Position compliance as a leverage point, demonstrating how aligning with insurer-mandated controls prevents operational disruptions during coverage reviews or breach-related audits.
- ❑ **Highlight Risk Mitigation:** Explain how adopting insurer-preferred tools reduces exposure to threats and ensures faster breach recovery while maintaining insurer confidence in the client's risk posture.
- ❑ **Deploy Post-Breach Strategies:** Emphasize the importance of post-incident preparedness, including tailored incident response (IR) plans that meet insurance specifications, to avoid claim disputes after cyber events.
- ❑ **Leverage Use Cases:** Share industry-specific examples, such as using EDR regulations to satisfy post-attack audit criteria or MFA to lower finance sector premiums, to illustrate proven outcomes of compliance efforts.
- ❑ **Enable Coverage Reviews:** Encourage regular reviews of cyber insurance policies, ensuring that clients stay ahead of evolving insurer demands while addressing gaps in their coverage or security posture.

Use Cases from TA Sales Experience

Industry	Use Case	Supplier Role	TA Sales Strategy
Finance	Implementing MFA for reduced premiums under cyber insurance policies	Supplier provided centralized authentication tools	TA recommended compliance alignment to reduce premiums after reviewing insurer policies with accounts payable teams
Healthcare	Deploying EDR solutions to meet insurer cybersecurity claims thresholds	Supplier utilized AI-powered MDR and EDR solutions	TA positioned supplier offerings as key tools during post-breach insurer audits to protect claims eligibility
Retail	Encryption systems visibly meeting insurer data security requirements	Supplier offered cloud-based encryption technology	TA highlighted the lowered risk exposure as a key benefit during conversations about rising premiums after a competitor attack
Manufacturing	Incident response plans customized to insurer requirements	Supplier deployed industry-specific IR frameworks	TA drove compliance discussions following industrial client feedback about claim denials tied to insufficient response readiness

Selling Cybersecurity through Cyber Insurance Requirements

Cyber insurance carriers increasingly mandate specific cybersecurity controls for coverage eligibility or to reduce premiums. These mandates are now a built-in sales accelerator, especially for companies undergoing policy renewal, premium hikes, or denial of claims.

Control Category	Common Insurance Requirement	Selling Angle
Multi-Factor Authentication (MFA)	Mandatory for all remote access & privileged accounts	“Without MFA, most carriers won’t offer coverage.”
Endpoint Detection & Response (EDR)	Required for real-time threat detection	“Qualifies you for premium discounts and breach containment.”
Incident Response Plan	Required with documented testing	“An IR plan cuts breach-related costs by up to 58%.” (Ponemon Institute, IBM)
Email Security / Phishing Protection	Required due to high frequency of social engineering claims	“Helps reduce most common cause of claim triggers.”
Backup & Recovery	Secure, immutable, off-network backups	“Critical to insurability in case of ransomware.”
Privileged Access Management (PAM)	Required to minimize breach impact	“A must-have to limit liability and access abuse.”
Vulnerability Management	Ongoing scanning and patching cadence	“Proactive risk mitigation that insurers look for.”
Security Awareness Training	Often required quarterly for staff	“Ties directly into claim defensibility and coverage retention.”

Partner Integration Opportunities

Many MSSPs and security vendors now **offer built-in cyber insurance services** such as:

- Risk scoring and gap analysis tools
- Incident response retainers that integrate with insurance workflows
- Insurability readiness reports

This creates an opportunity to bundle **security solutions + insurance guidance** — providing measurable ROI and C-suite buy-in.

Trend #4: SOC Modernization Pressure

Category: Managed Security / Cybersecurity Operations / MSSP Utilization

Trend Insights: Maintaining a 24/7, in-house Security Operations Center (SOC) is financially and logistically challenging for many organizations. Managed Security Service Providers (MSSPs) are emerging as a practical alternative, offering efficient incident monitoring, response capabilities, and operational coverage outside of business hours. MSSP adoption enables companies to enhance cybersecurity without incurring significant staffing and infrastructure costs.

How to Position it as a TA

Buyer Persona	Key Focus Area	Positioning Strategy
CISO / Security Leader	24/7 threat detection, incident response, security talent gaps	Position MSSPs as force multipliers that deliver continuous threat monitoring and expert-level incident response without the burden of recruiting and retaining scarce security talent. Emphasize access to cutting-edge threat intelligence and proven playbooks that enhance detection capabilities beyond what in-house teams can achieve alone.
CIO / VP IT	Operational efficiency, technology stack optimization, business enablement	Highlight how MSSPs eliminate the operational overhead of managing complex security tools while providing enterprise-grade monitoring. Frame MSSP partnerships as a way to free internal IT resources to focus on innovation and strategic initiatives rather than alert triage and 24/7 security operations.
CFO / Finance Executive	Cost predictability, capital expense avoidance, ROI justification	Demonstrate the total cost of ownership advantage: MSSPs convert unpredictable SOC capital expenses (infrastructure, tools, staffing) into a predictable operational expense model. Quantify the avoided costs of hiring 15-20 FTEs needed for 24/7 coverage, plus ongoing training, retention, and technology refresh cycles.
VP Operations / COO	Business continuity, minimal disruption, scalability for growth	Position MSSPs as business continuity enablers that ensure security operations never create bottlenecks or disruptions. Emphasize scalability—MSSPs grow with the business without requiring headcount planning, recruitment delays, or infrastructure buildouts that could slow operational expansion.
Compliance / Risk Manager	Regulatory requirements, audit readiness, third-party risk management	Showcase how MSSPs provide continuous compliance monitoring and audit-ready reporting across frameworks (SOC 2, ISO 27001, NIST, industry-specific regulations). Highlight how MSSP documentation and incident response capabilities satisfy auditor requirements while reducing the compliance burden on internal teams.
Board Members / Executive Leadership	Strategic risk mitigation, competitive advantage, stakeholder confidence	Frame MSSP adoption as a strategic risk management decision that demonstrates mature security governance to investors, customers, and partners. Position it as enabling the organization to compete with larger enterprises by accessing Fortune 500-level security capabilities at a fraction of the cost.

Key Talk Tracks

Use these conversational prompts to effectively address SOC modernization pressure:

1 24/7 Incident Coverage

"What's your plan for covering security incidents outside of business hours? Do you have the team and tools to respond around the clock?"

2 In-House Resource Constraints

"Given the high costs and staffing challenges of maintaining an in-house SOC, have you considered outsourcing to an MSSP for more scalable and reliable service?"

3 Budget Optimization

"How are you balancing the need for advanced monitoring with the financial realities of in-house SOC expenses?"

4 Security Maturity Goals

"Are you aware of MSSPs that can enhance your security posture while delivering industry-specific threat management?"

Market Impacts

- **Rising Costs of In-House SOCs:** Building and maintaining a 24/7, in-house Security Operations Center (SOC) demands significant financial investment in infrastructure, tooling, and staffing, which is often unfeasible for many organizations.
- **Efficiency of MSSP Models:** Managed Security Service Providers (MSSPs) are becoming the go-to solution for businesses looking to reduce costs while ensuring comprehensive threat detection, incident response, and operational coverage.
- **Focus on Core Operations:** Organizations can allocate resources to core business objectives while leveraging MSSPs to handle day-to-day cybersecurity operations with a high level of expertise and scalability.

Advisor Checklist to Position SOC Modernization Effectively

- ❑ **Highlight 24/7 Availability:** Address client concerns around after-hours coverage, emphasizing MSSPs' ability to monitor, detect, and respond to threats at all times without the need for internal resource strain.
- ❑ **Discuss Cost Benefits:** Outline how MSSPs eliminate the capital expenses of maintaining physical SOC infrastructure and the staffing costs associated with a 24/7 security team. Use industry-specific case studies as evidence.
- ❑ **Focus on Scalability:** Present MSSPs as a scalable solution, capable of growing alongside the client's operations while adapting to changing threat landscapes without additional internal investment.
- ❑ **Position MSSPs as Strategic Partners:** Frame MSSPs as an extension of the client's team, with expertise in managing security tools, interpreting data, and mitigating risks effectively.
- ❑ **Leverage Industry Alignment:** Tailor MSSP recommendations based on the client's industry. For example, highlight the customization of healthcare data security protocols or the focus on critical infrastructure for manufacturing.
- ❑ **Schedule Regular Updates:** Emphasize the importance of periodic reviews with MSSPs to ensure alignment with current business goals, regulatory requirements, and emerging threat vectors. Use these reviews to highlight results and demonstrate the ongoing value of MSSP services.

Use Cases from TA Sales Experience

Industry	Use Case	Supplier Role	TA Sales Strategy
Healthcare	Implemented MSSP to provide round-the-clock monitoring	Supplier utilized cloud-based SOC solutions	TA emphasized the importance of 24/7 coverage, positioning healthcare data sensitivity as justification for an MSSP-driven SOC
Finance	Replaced in-house SOC with MSSP services for comprehensive support	Supplier introduced enterprise-grade SOC solutions	TA highlighted MSSPs as cost-effective for reducing financial institution liability tied to after-hours data breaches
Retail	Adopted MSSP to handle Tier 1 security events across global stores	Supplier delivered managed detection services	TA positioned MSSPs as efficient tools for distributed systems, focusing on retail's need for regional threat detection capability
Manufacturing	MSSP augmented limited SOC staffing to handle advanced threat hunting	Supplier provided combined EDR and SOC solutions	TA demonstrated MSSP capabilities aligned with manufacturing's cybersecurity maturity goals, reducing operational downtime risks

See Section 4 to learn more about how to position MSSPs vs in-house SOCs in your sales conversations.

Trend #5: Zero Trust Evolution

Category: Managed Security / Zero Trust Network Access (ZTNA) / Secure Remote Access

Trend Insights: Virtual Private Networks (VPNs) are becoming outdated as organizations shift to Zero Trust Network Access (ZTNA). ZTNA enables more granular, identity-aware access, ensuring secure communication across users, devices, and applications. This evolution is becoming a foundational strategy for securing hybrid workforces and cloud-native environments. With a "never trust, always verify" model, ZTNA reduces the attack surface and mitigates lateral movement risks beyond what legacy VPNs can offer.

How to Position this Trend as a TA

Buyer Persona	Key Focus Area	Positioning Strategy
CISO / Security Leader	Mitigating insider threats, reducing attack surface	Focus on ZTNA's ability to prevent lateral movement and enforce per-session, identity-based access across all applications.
CIO / VP of IT	Hybrid work, secure app access, futureproofing	Focus on ZTNA's ability to prevent lateral movement and enforce per-session, identity-based access across all applications.
Compliance / GRC Manager	Achieving regulatory security standards	Showcase how ZTNA simplifies compliance reporting and aligns access policies with regulated frameworks.
Finance / COO	Operational security and cost effectiveness	Highlight ZTNA as a scalable solution that improves operational resilience while reducing costs related to breaches.

Key Talk Tracks

Use these conversation starters to establish discovery and drive engagement:

1 Remote Work and Cloud Expansion

"Are you shifting to Zero Trust? What's your current approach to securing user-to-app communication, especially with remote work and cloud access?"

2 VPN Challenges and Limitations

"With VPNs creating network chokepoints and enabling lateral movement, how are you managing user and device access in your environment?"

3 Identity-Based Access Control

"How important is contextual access control for your organization? Zero Trust ensures access is granted only based on verified identity and device posture."

4 Regulatory Compliance

"With compliance requirements becoming stricter, have you explored how ZTNA supports frameworks like HIPAA, PCI-DSS, and SOC 2?"

Market Impacts

- **VPN Limitations in Modern Environments:** Traditional VPNs lack the scalability, granularity, and identity-awareness needed to support dynamic remote workforces and cloud adoption, posing risks to secure, app-to-user communication.
- **Rising Demand for Zero Trust:** ZTNA adoption is accelerating as organizations recognize its ability to reduce the attack surface by verifying user identities and device postures before granting access.
- **Compliance Benefits of ZTNA:** Implementing ZTNA not only mitigates network threats but also aligns with emerging regulatory guidelines that emphasize identity-based access control and least-privilege principles.

Advisor Checklist to Position Zero Trust Solutions Effectively

- ❑ **Assess Current Security Gaps:** Begin by understanding gaps in the client's existing secure access solutions, such as outdated VPNs or unmanaged remote access pathways. Highlight how ZTNA addresses these challenges by enforcing identity and context-aware access policies.
- ❑ **Focus on Compliance Alignment:** Position ZTNA as a solution that simplifies adherence to compliance mandates (e.g., SOC 2, HIPAA, PCI). Emphasize its role in supporting frameworks that require logging, monitoring, and least-privilege access.
- ❑ **Showcase Operational Efficiency:** Explain that ZTNA reduces the complexity and operational costs associated with VPN sprawl by providing centralized, scalable, and context-driven access management.
- ❑ **Introduce Identity-Based Access Control:** Discuss how ZTNA strengthens the security posture by continuously validating user identities, device health, and geolocation, offering more granular enforcement compared to VPNs.
- ❑ **Utilize Tailored Workshops:** Offer Zero Trust strategy sessions or workshops to engage key stakeholders in identifying immediate opportunities to enhance app-to-user communication. Regularly reference proven success stories and outcomes.
- ❑ **Propose Periodic Reviews:** Schedule quarterly security and compliance reviews to ensure the ZTNA environment aligns with ongoing regulatory updates, user behavior shifts, and cloud expansion. This approach mirrors ZTNA's adaptive and scalable nature.

Use Cases from TA Sales Experience

Industry	Use Case	Supplier Role	TA Sales Strategy
Healthcare	Transitioned from VPN to ZTNA to protect patient data in hybrid workforces	Supplier implemented identity-aware ZTNA framework	TA aligned the shift with HIPAA compliance by emphasizing the security benefits of per-user, context-aware access control
Finance	Implemented ZTNA to secure remote work and SaaS-based banking apps	Supplier deployed ZTNA integrated with existing IAM	TA discussed ZTNA as a cost-effective alternative to scaling VPNs, while highlighting its capability to meet stringent compliance
Retail	Migrated legacy VPN users to ZTNA for secure POS app connectivity	Supplier introduced ZTNA combined with cloud security tools	TA focused on reducing business risk from lateral movement and ensuring uptime across distributed endpoints
Public Sector	Deployed ZTNA to replace a flat network design for secure user access	Supplier provided Zero Trust as a managed solution	TA emphasized ZTNA's alignment with government security mandates to address remote workforce risks and cloud application exposure

Trend #6: Cloud and Edge Security Integration

Category: Managed Security / Cloud Security / Edge Networking

Trend Insights: As applications and data increasingly traverse hybrid environments—on-premises, cloud, and edge—organizations face growing complexity in securing these interconnected systems. Unified security policies and real-time visibility across all environments are becoming critical for reducing vulnerabilities and enabling efficient operations.

How to Position this Trend as a TA

Buyer Persona	Key Focus Area	Positioning Strategy
CISO / Security Leader	End-to-end policy integrity across environments	Offer unified SASE-style solutions to enhance enforcement, visibility, and real-time incident response capabilities.
CIO / VP of IT	Hybrid integration simplicity, cost efficiency	Highlight platform consolidation benefits for networking and security tools, alongside improved scalability.
Edge Infrastructure Manager	Risk mitigation, operational reliability	Present edge computing security enhancements as part of a cohesive IT modernization strategy.
Compliance Manager	Audit-ready alignment, data protection	Showcase integrated tools (CASB, ZTNA) as evidence collectors and access regulators for frameworks like HIPAA or GDPR.

Key Talk Tracks

Use these conversation prompts to address challenges related to cloud-edge security integration:

1 **Unified Policy Enforcement Across Environments**

"Can you enforce the same security and access policies across on-prem, cloud, and edge environments? Where are the gaps?”

2 **Reducing Risk in Hybrid Environments**

"Have you faced challenges securing hybrid environments where core systems connect with edge locations?”

3 **Visibility and Incident Response**

"How do you monitor and respond to threats when data and applications are distributed across cloud and edge networks?”

4 **Zero Trust Adoption**

"Have you assessed how Zero Trust frameworks could safeguard access and protect key assets across both your cloud and edge environments?"

Market Impacts

- **Edge and Hybrid Growth:** By 2026, 75% of enterprise-generated data is projected to be processed outside traditional datacenters (Gartner).
- **Zero Trust Adoption:** Organizations adopting Zero Trust frameworks are 50% more likely to minimize access gaps in hybrid cloud and edge environments.
- **Regulatory Pressures:** GDPR and sector-specific mandates such as HIPAA, PCI and CMMC are driving demand for enhanced security across all data processing points.

Advisor Checklist to Position Cloud and Edge Security Integration Effectively

- ❑ **Assess Security Gaps:** Identify vulnerabilities in hybrid environments (e.g., siloed policies, weak encryption) and demonstrate how solutions like SD-WAN and CASB enhance security and compliance.
- ❑ **Align with Compliance**: Showcase the role of integrated solutions in adhering to standards like HIPAA, PCI, and GDPR, using industry-specific examples to highlight success.
- ❑ **Promote Efficiency**: Highlight operational benefits such as unified policy enforcement, reduced costs, and scalability through tools like Zero Trust frameworks.
- ❑ **Enforce Unified Policies**: Explain how consistent policy enforcement across all environments strengthens security and minimizes gaps with Zero Trust frameworks.
- ❑ **Host Use Case Workshops**: Offer industry-specific workshops to demonstrate immediate benefits, sharing success stories like IoT security in retail or secure financial data pathways.
- ❑ **Conduct Regular Reviews**: Schedule quarterly evaluations to keep security frameworks aligned with regulatory updates, user behavior changes, and system expansions.
- ❑ **Share Trending Insights**: Emphasize key trends like Zero Trust adoption, hybrid growth, and increasing regulatory pressures to underline the urgency of robust security integration.

Use Cases from TA Sales Experience

Industry	Use Case	Supplier Role	TA Sales Strategy
Healthcare	Unified security framework for enforcing HIPAA compliance across on-prem and cloud systems	Supplier implemented combined Cloud-Native Security (CNS) and Edge Access Control solutions	TA emphasized seamless reporting and compliance alignment for hybrid environments to satisfy auditors
Finance	Secure data transfer and real-time monitoring between cloud infrastructures and regional edge data centers	Supplier deployed encryption-enhanced SD-WAN with integrated CASB tools	TA positioned supplier's solution as a low latency option for secure transactional data pathways
Retail	Integrated Zero Trust policies across cloud-based operations and edge IoT endpoints	Supplier provided unified IAM (Identity Access Management) and Edge Security services	TA discussed IoT security risks at edge locations to highlight the need for unified policy enforcement
Manufacturing	Protecting IP and regulating access across distributed edge sites and cloud-based tools	Supplier delivered Zero Trust Network Access (ZTNA) paired with CASB integration	TA highlighted supplier's ability to prevent data leakage and streamline access audits for industrial clients

Trend #7: Hybrid and Remote Workforces

Category: Managed Security / Identity and Access Management / Endpoint Security

Trend Insights: As organizations embrace hybrid and remote work models, securing access, data, and devices for diverse and distributed teams has become a critical challenge. Businesses must navigate remote device management, identity verification, and application control across numerous environments to mitigate risks effectively.

How to Position this Trend as a TA

Buyer Persona	Key Focus Area	Positioning Strategy
CISO / Security Leader	Endpoint integrity, Zero Trust enforcement	Highlight endpoint protection and Zero Trust NAC to reduce BYOD risks and support scalable remote policies.
CIO / VP of IT	Hybrid IT modernization, cloud integration	Emphasize unified solutions that consolidate remote security tools and simplify integration into existing SaaS/cloud infrastructures.
Workforce Enabler (HR/IT)	User experience, minimal access friction	Showcase seamless SSO and MFA-based systems that balance employee productivity with uncompromising data security.
Compliance / GRC Manager	Regulatory adherence, audit readiness	Position secure remote access controls and encryption as necessary steps for meeting frameworks like HIPAA, PCI-DSS, or GDPR.

Key Talk Tracks

Use these targeted conversation prompts to identify client challenges and highlight solutions:

1 Remote Device Security

"Have you faced risks with personal device usage (BYOD) or outdated security tools for remote workforces? If so, how did those challenges impact your operations?"

2 Simplifying Identity Verification

"What are your current hurdles in verifying user identity before granting access to critical apps or data remotely?"

3 Policy Enforcement Across Hybrid Teams

"As your workforce becomes more distributed, how are you ensuring consistent policy enforcement across locations and devices?"

4 Balancing Productivity and Security

"Are you finding it difficult to secure remote workflows without hindering productivity or user experience?"

Market Impacts

- **Growth of Remote Work:** As of 2025, between 58% and 64% of organizations have adopted hybrid or fully remote work models, according to several major workplace surveys and research reports – exposing gaps in traditional security approaches.
- **BYOD Surge:** Unpatched personal devices accounted for 22% of endpoint vulnerabilities exploited in 2025, according to recent cybersecurity industry research.
- **Compliance Prioritization:** Businesses in regulated industries face increasing scrutiny over how they secure distributed workforces.

Advisor Checklist to Position Hybrid and Remote Workforce Solutions Effectively

- ❑ **Assess Communication Needs**: Identify specific collaboration requirements (e.g., video, messaging, voice) and address challenges like dropped calls or poor tool functionality with UCaaS.
- ❑ **Unify Collaboration Tools**: Highlight UCaaS as a one-platform solution to integrate voice, video, and messaging, boosting productivity and connectivity.
- ❑ **Showcase Scalability**: Emphasize how UCaaS scales with workforce changes and integrates AI-powered analytics for enhanced remote collaboration.
- ❑ **Address Security and Compliance**: Detail UCaaS's encrypted communications, strong authentication, and compliance support for call recording and data security.
- ❑ **Highlight Integration**: Explain seamless integration with tools like CRMs, Microsoft Teams, and Zoom, improving productivity with familiar platforms.
- ❑ **Provide Tailored Demos**: Offer custom demonstrations to address specific hybrid workforce challenges, showcasing adaptability across devices and locations.
- ❑ **Plan for Optimization**: Propose regular reviews to ensure the UCaaS solution evolves with workforce needs, new tools, and advanced features.

Use Cases from TA Sales Experience

Industry	Use Case	Supplier Role	TA Sales Strategy
Healthcare	Deployed device-agnostic endpoint protection policies for remote clinicians	Supplier integrated endpoint management with Zero Trust controls	TA emphasized meeting stringent HIPAA compliance while securing BYOD resiliency for a remote staff
Finance	Rolled out identity-aware VPN replacement solutions for global workforces	Supplier implemented cloud-native NAC with SSO and MFA	TA positioned it as a way to minimize credential fraud and support hybrid regulatory standards
Technology	Unified access to SaaS tools for developers on personal devices	Supplier standardized Zero Trust SASE for employees and contractors	TA connected developer efficiency and API protection to enhanced security ROI
Retail	Safeguarded inventory systems and payment gateways accessed remotely during work-from-home	Supplier automated endpoint checks and granular policy controls	TA focused on retail's unique need for compliance-ready access for seasonal employees or contractors

Section 3: Compliance & Regulation Selling Framework

Regulatory mandates shape cybersecurity priorities across industries, but selling compliance effectively requires a structured, phased approach. Start by uncovering regulations and gaps, then map solutions to compliance obligations. Use risk and regulatory pressure to create urgency, and design solution stacks that enable audit readiness. Co-sell with compliance and risk stakeholders to expand influence, and finally, reinforce continuous compliance to drive renewals and upsell opportunities. Together, these phases create a repeatable path that turns regulations from obstacles into revenue growth.

1. Understand the Regulatory Landscape (Discovery Phase)

Objective:

Identify what compliance mandates apply and assess gaps.

Key Activities:

- Ask what industry regulations apply (e.g., HIPAA, PCI-DSS, CCPA, GDPR, FINRA, SOX, NIST, CJIS, FedRAMP).
- Map to business impact (fines, legal action, revenue disruption, reputational damage)
- Identify compliance-driven pain points:
  - Incomplete audits or failing scores
  - Manual processes for compliance reporting
  - Gaps in endpoint, network, or identity protection
  - Lack of SOC visibility or logging for forensic reporting

Sample Questions:

“What frameworks or regulatory audits are top of mind this year?”

“How are you currently tracking and reporting compliance status?”

“What gaps are you most concerned about with your cybersecurity posture?”

Industry Compliance Framework Matrix

Industry	Primary Compliance Frameworks	Compliance Focus Areas
Healthcare	HIPAA, HITRUST, NIST 800-66	ePHI protection, data access, breach reporting, audit logging
Finance	SOX, GLBA, PCI-DSS, FFIEC, SEC Cyber Rules, NYDFS	Financial data integrity, customer data privacy, auditability
Retail	PCI-DSS, CCPA, GDPR, FTC Safeguards Rule	Payment data security, consumer privacy, fraud prevention
Public Sector	NIST 800-53, FedRAMP, CJIS, FISMA, CMMC	System security, access control, incident response, audit trail
Education	FERPA, CIPA, COPPA	Student data privacy, internet safety, parental consent
Technology / SaaS	GDPR, CCPA, SOC 2, ISO 27001, NIST CSF	Data residency, privacy controls, secure dev practices
Energy / Utilities	NERC CIP, DOE Cybersecurity Framework, NIST 800-82	Critical infrastructure security, real-time monitoring, physical & cybersecurity access controls
Manufacturing	ITAR, DFARS, NIST 800-171, ISO 27001	Export controls, IP protection, secure supply chain, DoD compliance

2. Align Cybersecurity to Compliance Requirements (Mapping Phase)

Objective:

Translate security controls into compliance outcomes.

Key Activity:

Align security solutions to compliance obligations:

Security Function	Compliance Tie-In
SIEM/SOC	Logging, audit trail, anomaly detection
MDR/XDR	Threat detection/response aligned to breach notification
Endpoint Protection	Device controls, PHI/PII protection
IAM/Zero Trust	Access control, least privilege, separation of duties
DLP	Preventing data exfiltration (HIPAA/PCI)
GRC Tools	Governance, reporting, risk scoring

Sales Tip: Use the regulation's own language (e.g., "breach notification within 72 hours") to position technical controls.

3. Use Risk & Regulatory Pressure to Elevate Urgency (Influence Phase)

Objective:

Engage executives by quantifying risk, exposure, and business consequences.

Key Tactics:

- Share fines, breaches, and lawsuits in the same industry (peer pressure).
- Use risk calculators or compliance readiness scorecards (MSSPs often provide these).
- Emphasize cyber insurance dependencies (e.g., needing EDR to qualify or reduce premiums).

Talk Tracks:

“Without audit-ready logging and response, the liability post-breach skyrockets.”

“Regulators don’t care if you’re small. Compliance is table stakes now.”

“Your cyber insurer may not pay out if you’re not enforcing MFA or segmentation.”

4. Build a Compliance-Driven Solution Stack (Design Phase)

Objective:

Present a layered solution that enables audit-readiness and controls mapping.

Approach:

- Bundle MSSP + GRC platform + endpoint or cloud security solutions
- Emphasize automation of compliance reporting
- Show how audit evidence is gathered passively via security tools

Example Solution Packages:

- **Healthcare Compliance Stack:** MDR, DLP, Zero Trust + HIPAA compliance portal
- **Financial Compliance Stack:** SIEM/SOC + IAM + PCI/FINRA reporting modules
- **Public Sector Stack:** NIST 800-53 controls, FedRAMP-ready security tools

5. Co-Sell with Compliance & Risk Stakeholders (Engagement Phase)

Objective:

Expand deal size and velocity by bringing in legal, compliance, and risk management teams.

Best Practices:

- Host joint compliance and cybersecurity workshops
- Include compliance officers in demo/POC processes
- Show how the solution reduces manual compliance tasks and audit prep time

Stakeholder Personas to Engage:

- General Counsel or Legal
- Chief Compliance Officer / Risk Manager
- Internal Audit Lead

6. Drive Ongoing Value with Continuous Compliance (Land & Expand Phase)

Objective:

Position MSSPs and security vendors for renewals and upsell via evolving regulatory demands.

Opportunities:

- Managed compliance monitoring
- Quarterly compliance health checks or mock audits
- Add-on services (incident response retainer, audit documentation support)

Land and Expand Triggers:

- New regulations (e.g., SEC, FTC, EU AI Act)
- M&A activity or expansion into new geographies
- New board directives or risk posture updates

Section 4: Positioning MSSPs vs In-House SOCs

As threats grow more sophisticated and regulations increase, maintaining a full in-house Security Operations Center (SOC) is not only cost-prohibitive for most companies—it's often inefficient. MSSPs offer scalable, cost-effective, and expertly managed alternatives.

Cost Model Comparison

In-House SOC	MSSP Services
Requires heavy investment: • Infrastructure and tools: More than $1.5M upfront • Staffing: 6 analysts, 2 engineers, 1 CISO = $2M–$3M annually • Licensing, monitoring, and training: $500K+ per year	**Predictable subscription pricing**: • 24/7 monitoring, EDR/MDR, compliance support bundled for $250K–$400K annually

Sales Positioning Guidance for TAs:

Start the Conversation with These Questions:

- "Do you currently have 24/7 visibility and coverage for security incidents?"
- "How confident are you in your team’s ability to meet compliance requirements or handle breaches?"
- "Have you evaluated the total cost and complexity of your current security operations?"

Common Client Objections and Rebuttals:

Objection: "We handle everything in-house."
Response: "Let’s compare the cost and coverage side-by-side. Most mid-sized companies are spending far more and still have blind spots."

Objection: "Outsourcing security feels risky."
Response: "Top MSSPs maintain SLAs, compliance certifications, and 24/7 coverage—often better than internal teams can provide."

Objection: "We don’t have budget."
Response: "Consider the hidden cost of downtime, breach fines, and compliance penalties. MSSPs offer savings and risk reduction."

Selling Products vs. Solutions

Selling Products

- Point solutions like firewalls, endpoint protection, and email security
- **Pros:** Fast sales cycle, easy to scope
- **Cons:** Reactive approach, not aligned to overall strategy
- **Conversation Starter:** "Do you currently manage these tools internally? What challenges do you face with integration or coverage gaps?"

Selling Solutions

(CoSource/Outsource):

- MSSP bundles that include detection, response, compliance reporting
- **Pros:** Strategic relationship, recurring revenue, broader coverage
- **Cons:** Longer cycle, more education required
- **Conversation Starter:** "What would it mean to have a security partner that manages threats and audits so your team can focus on innovation?"

Positioning Strategy by Client Type:

- **SMBs:** Emphasize affordability, 24/7 support, scalable packages
- **Enterprise:** Highlight integrations with SIEM, compliance, and hybrid SOC design
- **Regulated Industries:** Showcase compliance mapping, audit logs, and reporting

MSSP Value Proposition for Clients

- 24/7 monitoring and threat detection
- Access to certified experts and rapid response teams
- Scalable coverage across users, locations, clouds
- Cost savings over building internal SOCs
- Embedded compliance reporting and risk analytics

MSSP Sales Process Best Practices

- Educate clients on evolving threats and compliance expectations
- Perform a gap and cost analysis using available calculators
- Present MSSPs as strategic partners who align to business and audit goals
- Share case studies and regulatory success stories

Next Steps

Positioning MSSPs effectively requires understanding client pain points, emphasizing cost efficiencies, and showcasing the long-term value of managed services over isolated point products.

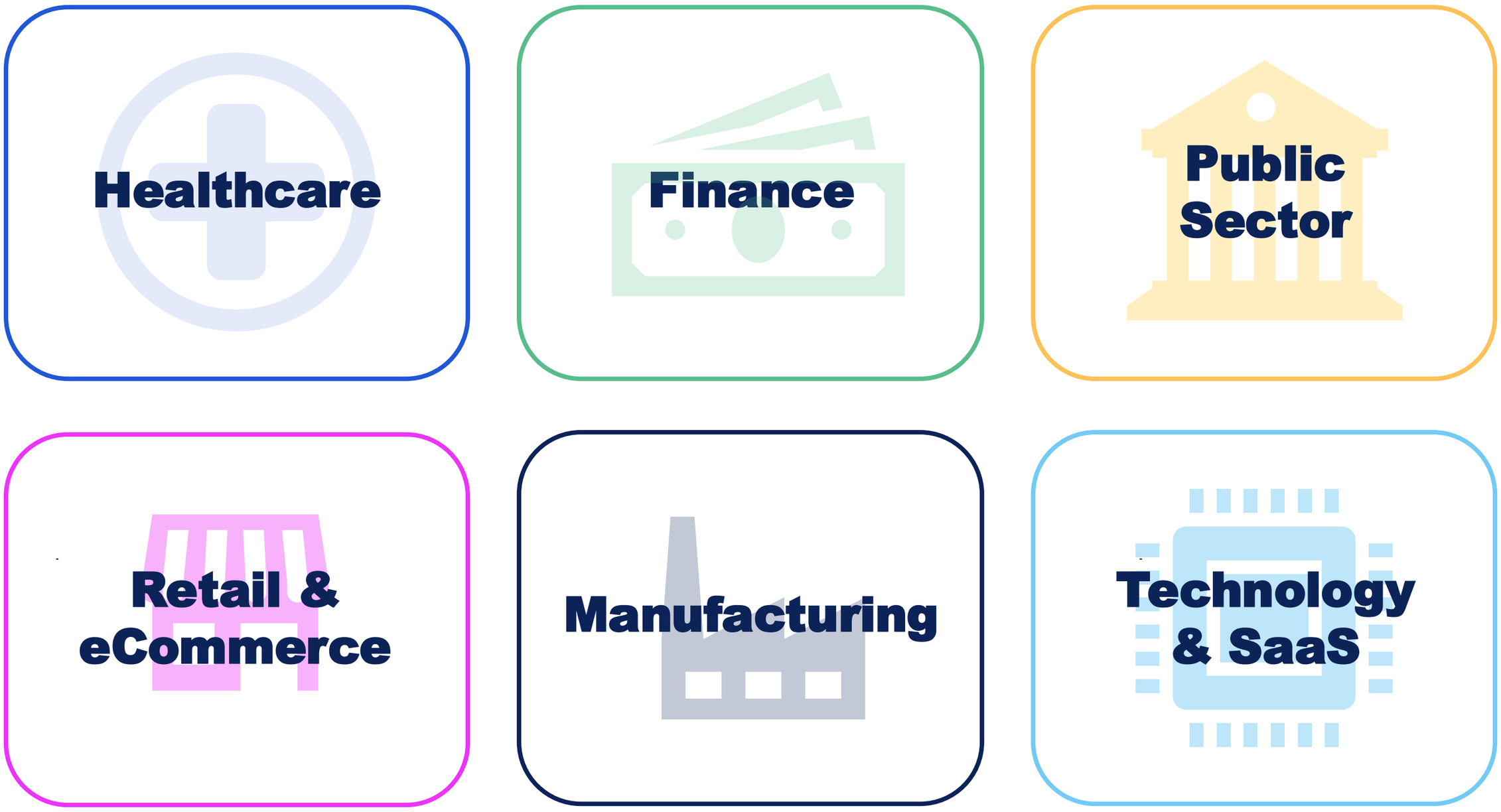
- Leverage Telarus tools and calculators
- Schedule client demos with vetted MSSP vendors
- Stay current with compliance trends and threat evolution

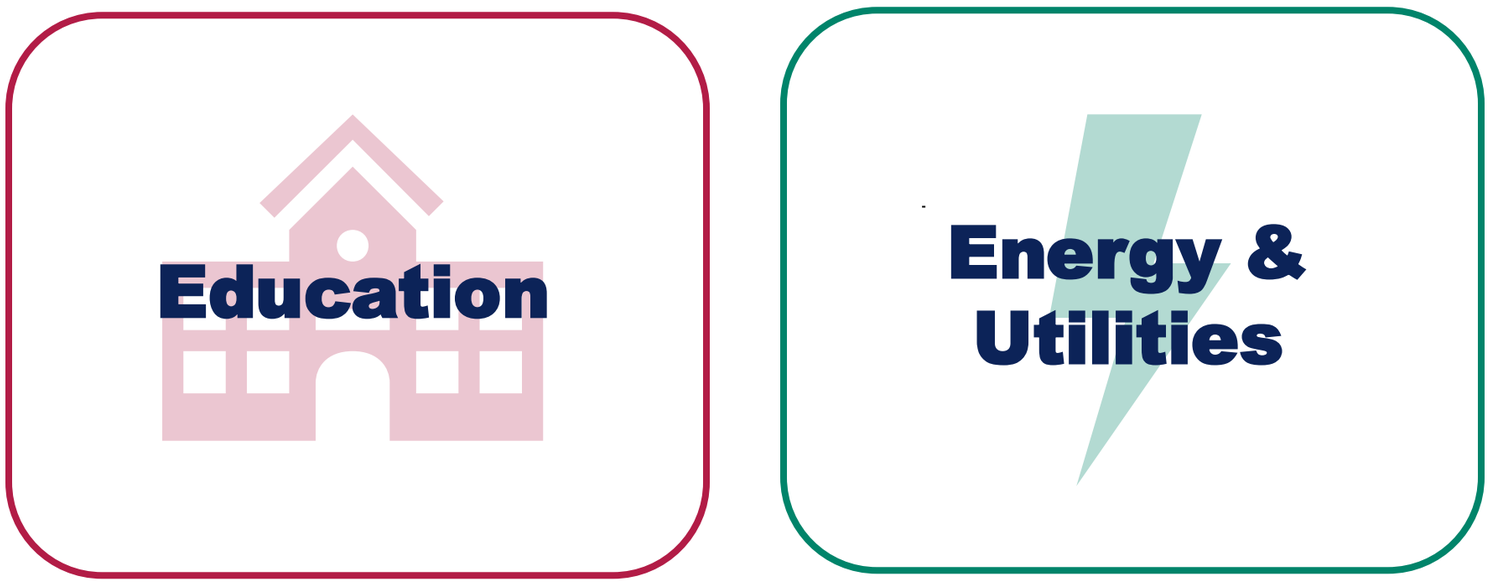
Empower your clients with the security, resilience, and peace of mind offered by trusted MSSP partners.

Section 5: Tailoring Cyber to Industry Needs

Cybersecurity demands industry-specific approaches to address unique challenges, compliance requirements, and threat landscapes. Whether guiding healthcare providers on HIPAA, financial firms on SOX and PCI-DSS, or manufacturers on CMMC, tailored solutions establish you as a trusted advisor. By aligning tools with vertical-specific priorities, you help clients view security as a strategic enabler rather than just a requirement.

Click on the icons below to for talk tracks, conversation-starters, and use cases by vertical.





Learn more: View Telarus case studies by vertical.

Healthcare

Focus: HIPAA, HITRUST regulations, patient data protection, telehealth security, and ransomware threats

Talk Track: "As healthcare continues to embrace telehealth and digital innovation, how are you ensuring compliance with HIPAA while protecting sensitive patient information from emerging security threats?"

Emphasize: MDR, DLP, IAM, compliance dashboards

Door-Opening Questions:

- “How are you tracking and ensuring ongoing compliance with HIPAA and HITRUST regulations?”
- “What steps are you taking to secure electronic Protected Health Information (ePHI) across devices and networks?”
- “How do you evaluate and verify vendor compliance with your cybersecurity standards?”
- “What measures are in place to prepare for ransomware attacks that could target patient medical records?”
- “Are your staff properly trained on cybersecurity protocols, particularly for remote work scenarios?”

Use Case: HIPAA-Driven MSSP Deployment

Client Profile: Regional health system with 12 clinics and two outpatient surgery centers

Challenge: Increasing HIPAA scrutiny and lack of internal resources to manage 24/7 threat monitoring

TA Role:

- Set meetings with supplier security teams
- Brought in supplier-led team to perform a HIPAA-focused cybersecurity gap assessment
- Managed proposal logistics and scheduled stakeholder briefings to maintain momentum

Outcome:

- Supplier implemented MDR, log management, and risk-based vulnerability scanning
- Cyber insurance premium reduction post-deployment due to improved risk posture
- Client signed a 3-year MSSP agreement with QBRs facilitated by TA

Finance

Focus: SOX, PCI-DSS, GLBA, SEC cyber rules, breach fines, and insider threats

Talk Track: "In today's fast-paced financial landscape, how are you ensuring SOX compliance, safeguarding customer data, and addressing SEC rules on cyber incident disclosures—all while minimizing the burden on your team?"

Emphasize: SIEM, EDR, ZTNA, cyber insurance alignment

Door-Opening Questions:

- "How are you preparing for SEC's cyber incident reporting deadlines?
- "What controls do you have in place to protect financial data and ensure PCI-DSS alignment?"
- "Are there challenges in correlating logs across systems to meet SOX audit requirements?"
- "Has your cyber insurance provider recommended technology upgrades for policy alignment?"
- "How are you detecting and responding to real-time insider threats?"

Use Case: Financial Services: GLBA and Zero Trust Strategy

Client Profile: Community bank with $1.4B in assets, 26 branches

Challenge: GLBA audit findings and legacy firewall infrastructure

TA Role:

- Scheduled discovery and scoping sessions with Telarus cybersecurity experts
- Introduced supplier engineers to conduct GLBA gap analysis and regulatory mapping
- Acted as sales project manager, aligning executives, procurement, and legal

Outcome:

- Supplier implemented managed firewall and SIEM with 24/7 monitoring
- The board approved the deal faster due to supplier-prepared compliance roadmap
- TA continued to guide ongoing roadmap phases with supplier partnership

Public Sector

Focus: FedRAMP, NIST 800-53, CJIS regulations, risk management, and inter-agency collaboration

Talk Track: "As federal regulations continue to evolve, how are you aligning your cybersecurity strategy with NIST 800-53 while ensuring seamless compliance across inter-agency operations?"

Emphasize: GRC tools, FedRAMP-ready MSSPs, compliance co-management

Door-Opening Questions:

- “Are your security frameworks consistently mapped to NIST 800-53 controls?”
- “What tools or processes are in place to mitigate cybersecurity risks across departments or agencies?”
- “How are you preparing for CJIS compliance audits and addressing challenges?”
- “Are penetration tests conducted regularly to evaluate your security readiness?”
- “How do you enhance inter-agency collaboration for real-time threat communication?”

Use Case: Public Sector: CJIS and FedRAMP-Aligned Cloud Security

Client Profile: County government with 1,200 endpoints and hybrid workloads

Challenge: CJIS compliance needs and fragmented endpoint protection systems

TA Role:

- Coordinated an introduction call with Telarus Supplier Management Team experienced in public sector compliance
- Supplier conducted full CJIS and FedRAMP controls assessment
- TA presented proposal bundles, set up live demos, and managed proposal revisions
- Created an executive summary packet to assist funding approval from the county council

Outcome:

- Client deployed a co-managed SOC with endpoint detection, access control, and audit logging
- Supplier support enabled usage of ARPA funding
- TA ensured timely contract execution and established recurring QBRs

Retail & eCommerce

Focus: PCI-DSS compliance, CCPA, GDPR, supply chain security, and customer trust

Talk Track: "In today's digital retail ecosystem, how are you proactively ensuring PCI-DSS compliance while strengthening customer trust and securing your supply chain operations?"

Emphasize: SWG, DLP, SEG, vulnerability management

Door-Opening Questions:

- "How are you ensuring all payment platforms consistently comply with PCI-DSS requirements?"
- "What incident response strategies are in place to mitigate the impact of data breaches?"
- "How are you monitoring and managing the security posture of third-party vendors handling customer data?"
- "Are you effectively leveraging Data Loss Prevention (DLP) tools to safeguard sensitive information?"
- "What steps are you taking to educate customers on their data privacy rights under regulations like CCPA and GDPR? "

Use Case: Retail: PCI-DSS Compliance with Managed Endpoint + DLP

Client Profile: National specialty retailer with 180 stores and robust e-commerce footprint

Challenge: Failed PCI-DSS assessment due to weak endpoint protection and no DLP solution

TA Role:

- Introduced supplier-side PCI experts and scheduled a compliance readiness workshop
- Supplier team conducted technical controls mapping and created a remediation plan
- TA supported pricing and packaging with Telarus proposal tools and compliance mapping visuals
- Handled coordination between CISO, IT, and procurement throughout the buyer's journey

Outcome:

- Supplier deployed DLP and EDR across all endpoints with policy controls
- PCI-DSS certification achieved within compliance window
- Client retained TA for future phases involving email filtering and cloud security

Manufacturing

Focus: CMMC, NIST 800-171, supply chain resilience, IoT security, and operational technology protection

Talk Track: "As CMMC certification becomes critical for government contracts, how are you strengthening your operational technology infrastructure and securing your supply chain?"

Emphasize: Asset Management, EDR for OT, Zero Trust

Door-Opening Questions:

- “What steps have you taken toward achieving CMMC certification, and which stages are already in progress?”
- “Do you have monitoring solutions in place to protect your operational technology environments?”
- “How are you managing the security and integrity of data flow throughout your supply chain?”
- “What measures are you implementing to identify and mitigate risks posed by IoT devices in your manufacturing process?”
- Are regular assessments being conducted to evaluate and improve your cybersecurity protocols?

Use Case: Manufacturing: CMMC-Readiness Strategy with DFARS Requirements

Client Profile: Defense contractor with 400 employees and multi-site operations

Challenge: Urgent need to meet CMMC 2.0 and DFARS cybersecurity requirements for renewal

TA Role:

- Scheduled an advisory call with Telarus engineering and a CMMC-specialized supplier
- Supplier conducted readiness review and provided a NIST 800-171 gap assessment
- TA supported executive briefings and ensured smooth alignment between supplier, IT, and legal
- Used *HIPAA-to-Security Crosswalk Tool* adapted for manufacturing to present aligned security controls

Outcome:

- Supplier implemented endpoint control, IAM, logging, and secure enclaves
- Compliance readiness completed ahead of deadline
- TA created a 12-month renewal roadmap with upsell potential for managed cloud services

Technology & SaaS

Focus: SOC 2, ISO 27001, privacy regulations, cloud security, and customer trust

Talk Track: "In the fast-paced SaaS industry, how are you securing your cloud services while meeting rigorous auditing standards like SOC 2 and ISO 27001?"

Emphasize: CSPM, CIEM, cloud-native MDR, secure SDLC

Door-Opening Questions:

- “Are your current procedures audit-ready for SOC 2 or ISO 27001, and what initiatives have been implemented to achieve compliance?”
- “How are you managing security consistently across multiple cloud platforms or hybrid environments?”
- “What threat detection and response mechanisms do you rely on to protect your infrastructure?”
- “How do you ensure that secure development practices are integrated into your teams' workflows?”
- “What strategies have you adopted to maintain transparency and communicate effective security practices to customers?”

Use Case: Technology & SaaS – SOC 2 and ISO 27001 Compliance Strategy with Enhanced Cloud Security Measures

Client Profile: SaaS provider specializing in enterprise productivity software with 300 employees and a global customer base

Challenge: Faced the need to achieve SOC 2 and ISO 27001 compliance to meet customer demand while managing a multi-cloud environment and a growing target for cybersecurity threats

TA Role:

- Scheduled consultations with Telarus engineers and a cloud-security-focused provider
- Provider conducted a thorough SOC 2 and ISO 27001 gap analysis, identifying compliance and security posture gaps
- TA facilitated alignment between the SaaS provider's IT, compliance, and development teams
- Assisted in integrating the provider’s Cloud Security Posture Management (CSPM) and Cloud Infrastructure Entitlement Management (CIEM) tools
- Guided the implementation of a secure software development lifecycle (SDLC) process in collaboration with the SaaS provider’s development team

Outcome:

- Achieved SOC 2 and ISO 27001 compliance ahead of the scheduled audit deadline
- Implemented a multi-cloud-native Managed Detection and Response (MDR) solution, enhancing threat detection and remediation capabilities
- Improved developer workflows through embedded secure SDLC practices, reducing the risk of vulnerabilities in code
- The SaaS provider’s customers gained increased confidence in the company’s security posture, solidifying long-term partnerships
- TA developed a 24-month roadmap, recommending continuous compliance management and paving the way for future upsell opportunities in managed security services

Education

Focus: FERPA, student data privacy, remote learning security, and improving cyber hygiene

Talk Track: "As technology plays an increasingly vital role in education, how are you safeguarding student data and ensuring FERPA compliance while adapting to the challenges of remote learning and device security?"

Emphasize: Endpoint security, secure remote access, incident response plans.

Door-Opening Questions:

- “How is your institution ensuring the protection of student data and maintaining ongoing compliance with FERPA requirements?”
- “What specific security measures have you implemented to protect remote learning platforms against cyber threats?”
- “How are you promoting and addressing cyber hygiene practices among both faculty and students?”
- “What protocols are in place to secure personal devices (BYOD) used by students and staff in your academic environment?”
- “Do you regularly perform vulnerability assessments to strengthen the security posture of your academic systems?”

Use Case: Education – FERPA Compliance and Strengthening Cybersecurity in Remote Learning

Client Profile: Large public university with over 20,000 students and faculty operating across multiple campuses and delivering remote learning programs.

Challenge: The university needed to ensure compliance with FERPA while adapting to the rapid adoption of remote learning platforms. They faced challenges including securing endpoint devices, providing secure access to academic systems, and improving overall cyber hygiene among students and faculty.

TA Role:

- Scheduled an assessment with a security-focused provider to evaluate existing vulnerabilities in remote learning platforms and endpoint devices
- The provider conducted a FERPA compliance gap analysis and proposed solutions for secure data handling and network protection
- TA coordinated the deployment of endpoint detection and response (EDR) solutions to secure student and faculty devices.
- Assisted in introducing a VPN-based secure remote access system for students and faculty to access academic platforms safely
- Partnered with the institutions’ IT team to develop a robust incident response plan tailored for education-specific cyber threats

Outcome:

- Achieved full FERPA compliance by adopting best practices for data handling and educational platform security
- Implemented campus-wide endpoint security measures, significantly reducing risks associated with remote device usage
- Strengthened remote access controls with advanced authentication, improving the safety of sensitive student records and academic systems
- Conducted workshops for students and faculty to enhance cyber hygiene practices, leading to a 30% reduction in phishing-related incidents over six months
- TA delivered a forward-looking roadmap for continuous vulnerability management and future integration of additional security services

Energy & Utilities

Focus: NERC CIP, DOE cybersecurity initiatives, critical infrastructure protection, and incident response

Talk Track: "With the energy sector facing increasing cyber threats, how are you aligning your cybersecurity strategies with NERC CIP standards to ensure critical infrastructure protection and operational resilience?"

Emphasize: EDR for SCADA, Zero Trust, log aggregation

Door-Opening Questions:

- “Are your control systems and processes fully compliant with NERC CIP regulations?”
- “What incident response strategies and frameworks are in place to address threats to critical infrastructure?”
- “How do you ensure that your workforce receives ongoing training in cybersecurity protocols aligned with industry standards?”
- “What methods do you use to evaluate and reduce supply chain risks that could impact infrastructure security?”
- “How are your security measures evolving to counter new and emerging cybersecurity threats specific to the energy sector?”

Use Case: Energy & Utilities – NERC CIP Compliance and Critical Infrastructure Protection

Client Profile: Regional electric utility provider with 2,500 employees, operating multiple generation and distribution facilities within a high-regulation environment

Challenge: The utility provider needed to meet NERC CIP compliance requirements while addressing evolving cybersecurity threats targeting critical infrastructure. They faced challenges in securing SCADA systems, implementing incident response strategies, and ensuring supply chain security in alignment with industry standards.

TA Role:

- Partnered with a cybersecurity vendor to conduct a comprehensive NERC CIP readiness assessment, including a security gap analysis of SCADA systems
- Assisted in deploying Endpoint Detection and Response (EDR) solutions tailored for SCADA environments to monitor and secure operational technology (OT)
- Worked with the client’s IT and operations teams to adopt a Zero Trust security framework, improving network segmentation and access control for critical infrastructure
- Supported the implementation of a centralized log aggregation platform with advanced analytics to detect anomalies and streamline compliance reporting
- Developed a workforce training program focused on NERC CIP compliance and cybersecurity best practices for OT and IT personnel

Outcome:

- The organization achieved NERC CIP compliance, meeting regulatory requirements ahead of the audit deadline
- Enhanced SCADA system security through the integration of EDR solutions, enabling real-time threat detection and mitigation
- Strengthened the utility provider’s overall cybersecurity posture with Zero Trust principles, reducing attack surfaces across IT and OT networks
- Improved incident response readiness by centralizing threat monitoring and log management, allowing faster identification and containment of cyber incidents
- Increased employee awareness and adherence to cybersecurity protocols, resulting in significant risk reduction and operational efficiencies
- TA created a three-year roadmap for maintaining compliance with NERC CIP, integrating advanced cybersecurity tools, and ensuring long-term resilience against emerging threats

Section 6: Conclusion

The Technology Advisor’s Strategic Role in Cybersecurity Growth

As cybersecurity shifts from technical product conversations to strategic business outcomes, the role of the technology advisor has never been more critical.

The good news is you don’t need to be a compliance officer or an engineer. You just need to know how to:

- Introduce the right resources at the right time
- Translate cybersecurity into risk reduction and ROI
- Use compliance pressure and insurance requirements to create urgency and unlock budget

With Telarus tools, supplier relationships, and engineering support behind you, you’re positioned to lead clients through their entire cybersecurity journey—without ever needing to configure a firewall or write a security policy.

Lead with confidence. Sell with compliance. Grow with Telarus.

TELARUS

GO BEYOND

Your Telarus Cybersecurity Experts – Ready to Help

These leaders drive the Telarus cybersecurity, engineering, and advisory frameworks that power your sales success:

Josh Lupresto

SVP of Sales Engineering

Josh leads the global engineering organization at Telarus, overseeing pre-sales architecture, partner enablement, and technical thought leadership across cloud, security, UCaaS, and AI.

Jason Stein

VP of Cybersecurity

Jason manages enablement programs that help TAs accelerate their time to value, win key opportunities, and grow expertise across the Telarus portfolio.

Jason Kaufman

Cybersecurity Architect

Jason directs the advanced solutions strategy for cybersecurity and cloud, translating emerging trends into actionable go-to-market strategies.

Sumera Riaz

Cybersecurity Architect

Sumera leads Telarus' cybersecurity strategy, aligning the supplier ecosystem with evolving threat landscapes and regulatory requirements.

Trevor Burnside

Cybersecurity Architect

Trevor leads the Security and Compliance engineering practice at Telarus, developing frameworks that help TAs bridge the gap between risk, compliance, and technology.