Drive Operational Excellence with IT Competencies

Contents

Executive summary

As organizations accelerate their industrial transformation, a partnership between Information Technology (IT) and Operational Technology (OT) has become essential to drive innovation, efficiency, and resilience across industrial environments.

Traditionally, IT and OT teams have operated in silos, resulting in fragmented systems, limited visibility, and increased security risks. Cisco's industrial networking solutions bridge this gap by providing the technology and tools that empower IT and OT teams to collaborate effectively. By enabling network standardization, centralized management, and integrated security, Cisco helps organizations unlock the full potential of industrial connectivity, streamline operations, and enhance cybersecurity—laying the foundation for smart, connected operations.

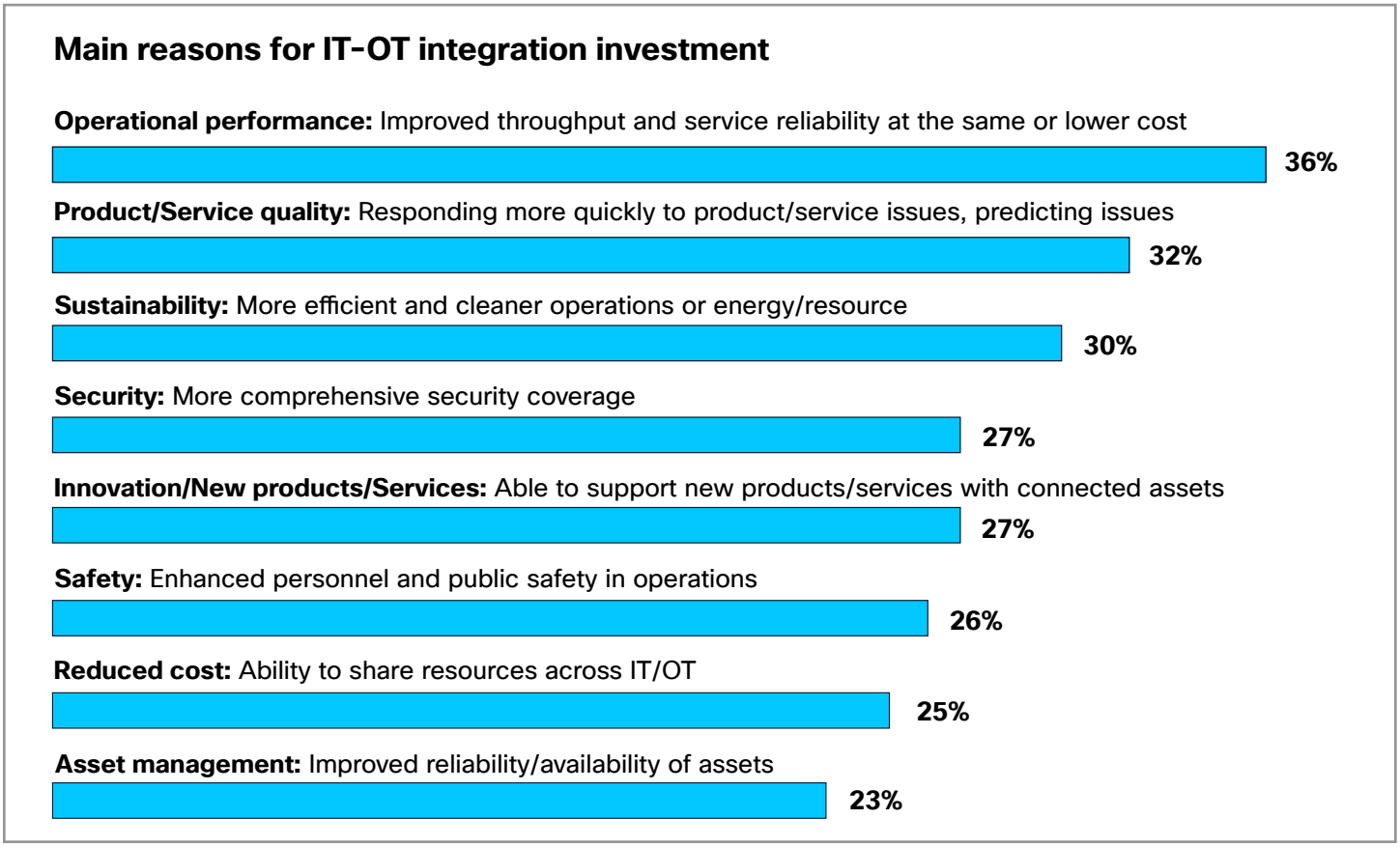


Figure 1. Respondents to an IDC survey recognize the benefits of closer alignment between IT and OT teams

Challenges and opportunities for IT-OT alignment

Historically, IT has managed data, applications, and communications, while OT oversaw physical processes, equipment, and industrial control systems. However, the growing digitization of industrial environments and the resulting expansion of industrial networks have created new challenges and opportunities that demand a new approach.

Expanding networks: As OT environments become increasingly networked, connecting machines, devices, and sensors across locations, the need to adopt proven IT networking practices is critical. IT expertise in network design, monitoring, security, and management, ensures the OT infrastructure can scale securely and adapt faster to change.

Increasing complexity: The growing complexity of industrial operations increases the risk of misconfigurations, downtime, and inefficiencies. IT's mature methodologies for asset management, configuration control, and standardized processes help OT teams maintain visibility, consistency, and control over expanding operational environments.

Growing cyberthreats: Many legacy OT systems were not designed with modern security in mind, making them highly vulnerable to cyberthreats like malware, ransomware, and unauthorized access. The need to connect OT systems with IT also significantly expands the attack surface. Aligning IT and OT enables a unified security framework—leveraging IT's advanced security practices like identity and access management, network segmentation, continuous monitoring, and incident response—to better protect industrial assets and ensure regulatory compliance.

The need to innovate: Aligning IT with OT unlocks the potential to apply Artificial Intelligence (AI), machine learning, and advanced analytics to operational data. A common networking infrastructure between IT and OT domains enables the real-time flow of production data. By leveraging this reliable data stream, organizations can gain valuable insights, make informed decisions, and realize their AI strategies.

Fostering a partnership between IT and OT is essential for organizations seeking to modernize operations, manage complexity, expand securely, and drive innovation. By bridging the gap between these traditionally siloed domains, organizations can realize greater operational resilience, improved efficiency, and sustained competitive advantage.

Adopting IT practices in OT networks

To keep pace with new demands and compete more effectively, organizations are increasingly extending IT capabilities to secure and manage industrial environments. The most successful industrial organizations are applying advanced IT capabilities into their operational spaces. They're seeking to bring the advantages of decades of IT innovation into OT environments, to achieve better results in standardization, security, and network automation.

"Forward-thinking organizations are addressing these challenges by applying proven Information Technology (IT) principles and methods including network automation, software-defined networking, advanced cybersecurity frameworks, and standardization to OT networks. IT network proficiency and expertise can be shared and used to foster collaboration with OT teams to unlock new efficiencies, improve resilience and future-proof workplaces."

The Business Case for IT/OT Collaboration in Modernizing Industrial Networks
~ Harbor Research, April 2025

Forging a partnership with OT allows IT to move beyond traditional enterprise functions, becoming a more strategic partner to the entire business and extending its established cybersecurity tools, best practices, and expertise to the OT environment, whereas the OT organization can better achieve its core priorities of safety, reliability, and efficiency.

Cisco recognizes that successful modernization of industrial environments requires seamless collaboration between IT and OT. To foster this partnership, Cisco provides a comprehensive technology framework and portfolio designed to bridge gaps, enhance security, and enable innovation across both domains.

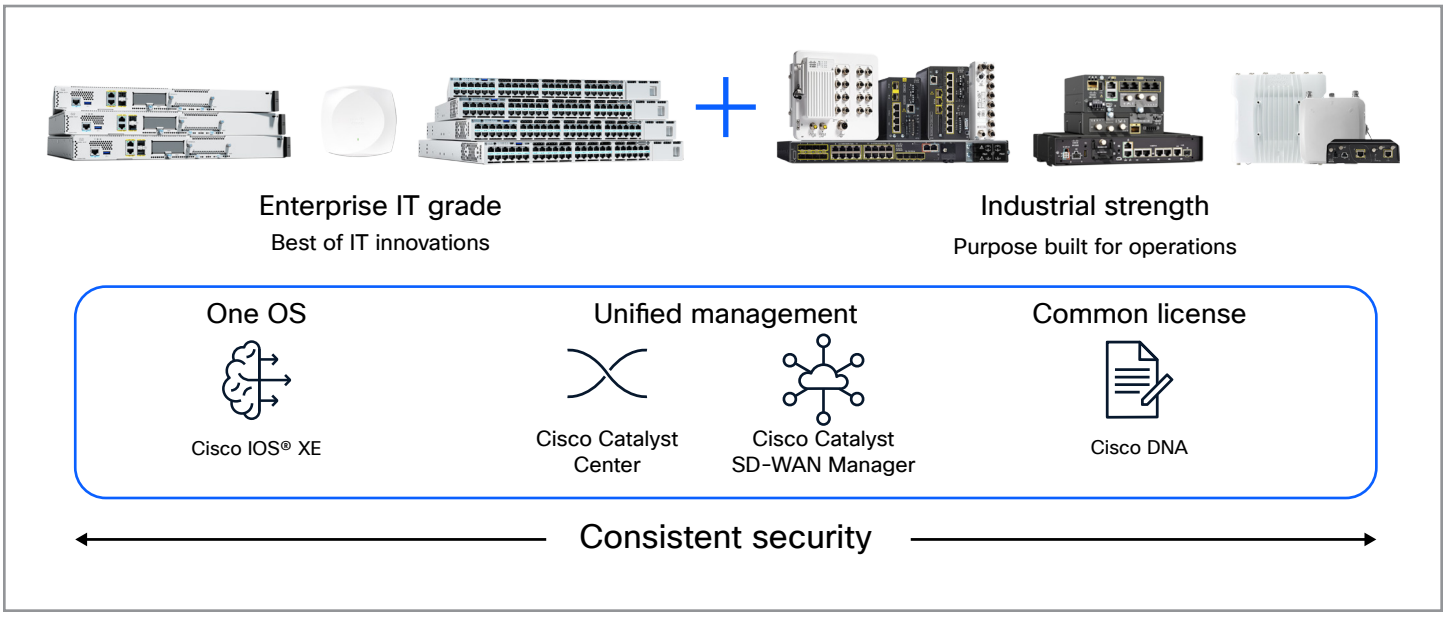


Figure 2. Cisco bridges IT and OT with an industrial portfolio that shares the same OS, management, security, and licensing with the enterprise

Standardized networking equipment

Standardized networking equipment primarily helps both IT and OT by simplifying and streamlining network architectures, which leads to lower costs, easier management, and improved security. IT teams are experts in deploying, automating, and managing large and complex networks. Using similar, but hardened, industrial equipment allows IT to apply their current skillsets to the OT network immediately, thereby reusing their skills and avoiding the expense and time of extensive training for OT teams.

Cisco's enterprise and industrial networking equipment share common foundations in operating systems, security, scalability, and management, helping ensure consistent policies and user experiences across both environments. While enterprise equipment is optimized for office and data center environments, Cisco's industrial networking equipment is specially ruggedized to withstand harsh physical conditions, such as extreme temperatures, humidity, vibrations, electromagnetic interference, and more.

Cisco switches: Both Cisco's enterprise and industrial switches use the same core technologies. They have powerful specialized chips (ASICs) that ensure consistent performance across different switch types. Both run the Cisco IOS® XE operating system and offer the same networking features, such as Layer 2 and Layer 3 services, software-defined networking, Cisco TrustSec technology based segmentation, and an open environment to host applications. Both Cisco enterprise and industrial switches are managed by the same platform—Cisco Catalyst™ Center.

The only primary difference between Cisco enterprise and industrial switches is that the industrial switches are ruggedized—featuring fanless designs and hardened enclosures—to function effectively in harsh conditions, but their technical alignment allows organizations to extend their security, automation, and operational expertise—technologies that IT knows and trusts—directly into industrial environments.

Cisco routers: Cisco enterprise and industrial routers share a unified platform by running the Cisco IOS XE operating system, supporting advanced networking features like SD-WAN, which is managed centrally via Cisco Catalyst SD-WAN Manager, and integrating built-in Next-Generation Firewall (NGFW) security.

Cisco wireless: Cisco integrates Wi-Fi and Cisco® Ultra-Reliable Wireless Backhaul (URWB) technologies into a single infrastructure managed through a common platform, the Cisco Catalyst Center. This unified approach enables simultaneous operation of Wi-Fi and URWB on the same access points. The same infrastructure connects both traditional and industrial devices. This convergence bridges the gap between IT and OT by providing end-to-end visibility and a single pane of glass for managing wireless networks, reducing complexity, and optimizing investments without duplicating infrastructure.

Integrated security framework

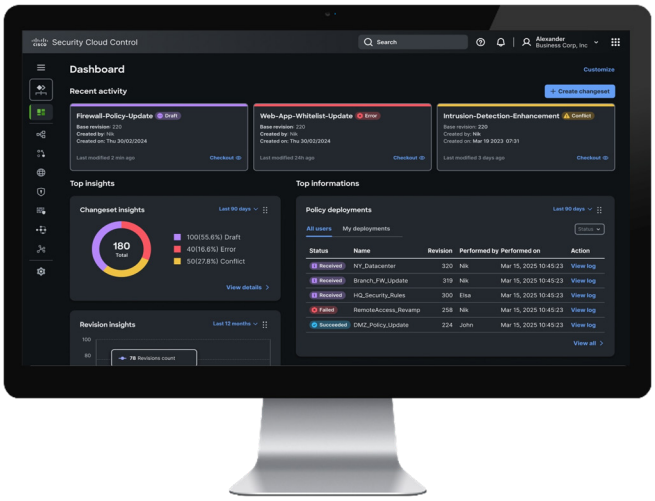
Industrial cybersecurity demands expertise from both IT and OT teams because the attack surface has converged. However, OT personnel typically lack specialized cybersecurity skills, which necessitates collaboration between teams to effectively secure industrial environments. The organization needs to combine OT's deep operational understanding with IT's broad security knowledge to implement cybersecurity best practices using best-of breed tools. IT is responsible for establishing the enterprise's overall security policies and risk management frameworks, as well as delivering scalable, enterprise-grade technologies for continuous monitoring, vulnerability scanning, and credential management. OT brings essential domain expertise that IT typically lacks, including knowledge of proprietary protocols like Modbus and PROFINET, specialized hardware such as Programmable Logic Controllers (PLCs), Supervisory Control and Data Acquisition (SCADA) systems, and Human-Machine Interfaces (HMIs).

"Adopting scalable unified solutions is critical for organizations looking to strengthen resilience and ensure industrial security. By fostering IT-OT collaboration and making strategic investments in security, businesses can safeguard their industrial operations today and prepare for the future."

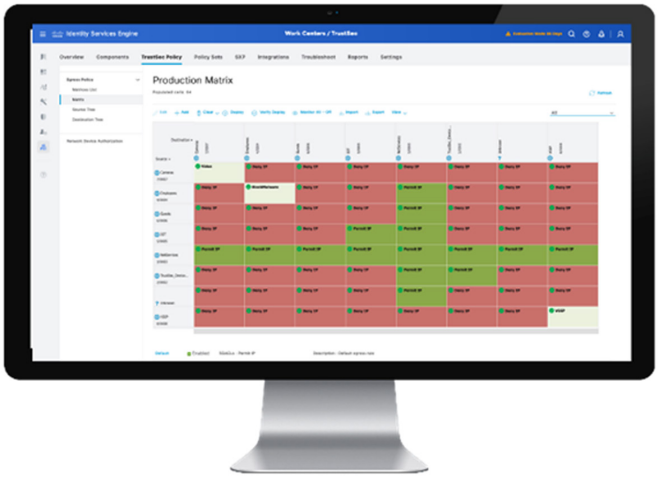
~ The Future of Industrial Network Security, an IDC InfoBrief, March 2025

Cisco's integrated security architecture allows IT and OT networks to operate under the same zero-trust principles, in which no user or device is implicitly trusted, and access is continuously verified. The segmentation and access control mechanisms, such as those provided by Cisco Identity Services Engine (ISE), are extended to both environments to enforce least-privilege access, even identifying and segmenting specialized industrial devices. Furthermore, core security functions like policy enforcement and perimeter defense are handled by unified tools, specifically Cisco Secure Firewall. This unified approach helps ensure that all security events and breaches—from operations to the campus—are collected, analyzed, and responded to through a single pane of glass using integrated platforms like Splunk® or Cisco XDR, enabling faster threat detection and a coordinated incident response across the entire enterprise network.

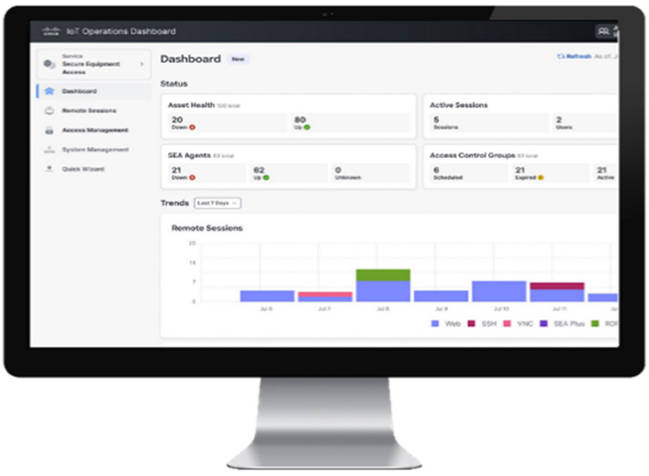
Cisco Cyber Vision: Cisco Cyber Vision plays a pivotal role in fostering IT-OT partnership by providing comprehensive and continuous visibility into OT assets, their security posture, and their communication patterns. It automatically inventories all connected industrial devices and maps their interactions, enabling OT and IT teams to collaboratively define logical zones and conduits for network segmentation that protect industrial operations without disrupting production, supporting compliance with standards like IEC 62443. Additionally, Cyber Vision's Secure Equipment Access enables zero-trust remote access to OT assets, empowering operations teams with secure, least-privilege access while reducing the attack surface. By bridging OT visibility with IT security tools, Cyber Vision helps to extend security policies into OT environments effectively, enabling the entire organization to maintain a strong security posture and reduce cyber risks across both IT and OT domains.



Cisco Secure Firewall: Cisco Secure Firewall delivers a unified security solution that spans both IT and OT environments. It provides advanced threat protection, comprehensive visibility, and granular control across IT and OT networks, enabling effective segmentation and safeguarding of critical OT assets. Secure Firewall integrates with Cisco's broader security ecosystem and facilitates shared threat intelligence and coordinated incident response, effectively bridging the gap between IT and OT.



Cisco ISE: ISE plays a critical role in securing both IT and OT infrastructures by providing comprehensive user and device authentication and enabling consistent access policy enforcement through network segmentation. It integrates with Cisco Cyber Vision to gain detailed visibility and profiling of industrial OT assets. It uses groups created in Cyber Vision to map network access policies to each OT asset and automate micro-segmentation of the industrial network, enforced by Cisco networking equipment.

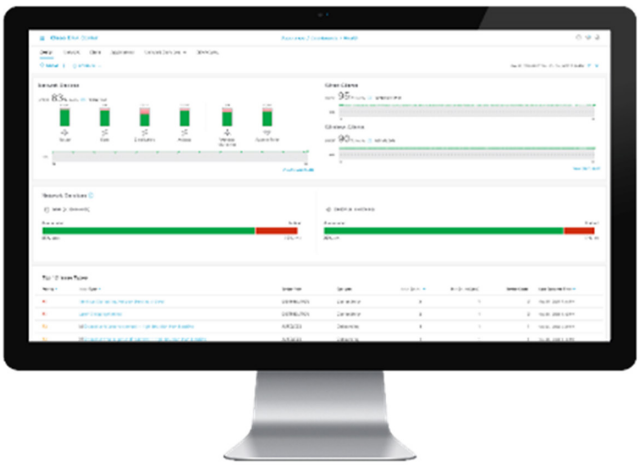


Cisco Secure Equipment Access (SEA): Part of Cyber Vision, Cisco Secure Equipment Access, combines all the benefits of a Zero Trust Network Access (ZTNA) solution with a network architecture that makes it simple to deploy at scale in industrial environments, and a self-service portal to help OT run operations as they need. It empowers OT teams with operational agility while providing IT teams with centralized policy management, session monitoring, and audit trails, thus bridging IT and OT requirements for secure, scalable remote access in industrial environments.

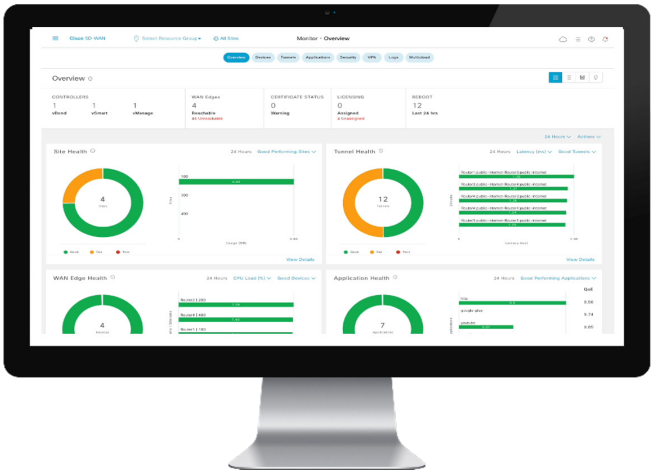
Common management

Using common tools for management allows the IT team to apply its core expertise to the operational environment, making management simpler and more comprehensive. It also helps the OT team increase uptime by providing better diagnostic tools and enabling proactive maintenance. Common management tools promote a shared understanding of issues, improving cross-functional collaboration.

Cisco extends the functionality of familiar enterprise management tools to industrial networks. This unification allows IT teams to deploy consistent network and security policies—including segmentation and monitoring—across the entire domain, from the corporate campus to operations. The ability to use the same tools, protocols, and skillsets, streamlines operations and drastically reduces the complexity and cost of maintaining two separate management infrastructures. This efficiency enables organizations to scale more rapidly, adapt to changing business needs, and leverage existing IT expertise to accelerate troubleshooting and minimize downtime in industrial environments.



Cisco Catalyst Center: Cisco Catalyst Center enables IT and OT to partner effectively by providing a well-understood and trusted management platform that IT professionals are already familiar with, while also addressing the specific management needs of OT environments. Catalyst Center extends its full range of capabilities—including network automation, performance assurance, and policy enforcement and compliance—to OT networks just as effectively as it does to IT networks. Additionally, it offers specialized Layer 2 configuration features and role-based access controls that are particularly valuable for OT environments.



Cisco Catalyst SD-WAN Manager: Cisco Catalyst SD-WAN Manager provides a single, centralized management plane for the configuring and managing all industrial and remote operational sites. This platform allows IT teams to extend SD-WAN's simplified configuration, automated deployment, and comprehensive monitoring capabilities to the OT environment. SD-WAN Manager also makes it simple to apply consistent security policies across all field networks, strengthening the overall cybersecurity posture for both IT and OT domains.

Unified licensing

To simplify purchasing, activation, and management across their entire organization, Cisco offers customers a unified licensing model between our enterprise and industrial products. This single licensing approach, such as Cisco Smart Licensing and Cisco Enterprise Agreement, reduces complexity by allowing customers to transfer licenses across different devices and portfolios, provides access to ongoing innovations, enables economies of scale, and offers additional discounts.

Use cases and benefits

More and more industrial organizations recognize the strategic role improved IT/OT collaboration can play in simplifying operations and increasing efficiency, profitability, and innovation across their organizations. Early indications show a clear trend that the companies adopting this approach are widening the gap between themselves and their competitors.

Industrial organizations increasingly understand that their networks are becoming a key enabler of their digital strategies. The hyper-growth of AI-enabled models and applications being deployed across enterprise and operational domains highlights the need for organizations to view their networks as a core enabler of competitive differentiation and success.

Figure 3. IT-OT alignment brings quantifiable benefits

A recent research report by the analyst firm Harbor Research documented that across a wide range of industrial domains, it is not uncommon to see IT-OT alignment result in a 15% to 35% improvement in operational productivity, a 10% to 30% reduction in cybersecurity risks, and a 15% to 30% reduction in time to market for new products and innovations.

Underscoring the need to involve IT in OT security, an IDC InfoBrief concluded that as their security maturity increases, organizations rely more on IT integration to manage OT security. Less mature organizations leave OT teams operating more in isolation, limiting their ability to address modern threats.

Why Cisco?

Vendors who lack the comprehensive breadth and depth of both IT and OT networking equipment typically adopt a partnership approach to promote IT-OT collaboration. Since they cannot offer a single, unified hardware and operating system platform, their strategies focus on bridging the gap externally through alliances with companies that cover the missing parts of the solution. This reliance on products from multiple vendors ultimately results in increased operational complexity. IT and OT teams still must manage, update, and secure multivendor systems, increasing the cost of ownership and maintaining the very network complexity they were trying to avoid.

Cisco is in a unique position because it is the only vendor that provides a complete, unified network architecture spanning both traditional enterprise IT and rugged OT environments. This unified approach minimizes complexity, reduces risk, and accelerates modernization initiatives like AI integration and industrial IoT deployment by helping ensure that the network foundation is secure and consistent everywhere.

Next steps

The imperative for IT and OT teams to collaborate is no longer a question of if, but how. Cisco provides the unified architecture, visibility, and security controls necessary to foster a true partnership between your operational and informational domains. By leveraging Cisco's robust portfolio, your organization can achieve greater operational efficiency, accelerate digital transformation initiatives, and build a highly resilient and secure industrial environment prepared for the threats and opportunities of tomorrow.

We invite you to move beyond the brief and into a personalized discussion. To explore Cisco's proven solutions, we encourage you to schedule a free, no-obligation, one-on-one consultation. Click here to reach out to one of our specialized experts who can provide a deep-dive analysis of your current infrastructure and map a secure, high-performance path to a truly converged environment.