cisco Meraki

BTI Communications Group

Cisco Meraki Authorized Partner | CA | AZ | IL

📞 800-435-7284

✉️ info@btigroup.com

🌐 btigroup.com

MERAKI MX SD-WAN FOR LOGISTICS & MANUFACTURING

REDUCE DOWNTIME, ACHIEVE SUPPLY CHAIN COMPLIANCE & CUT WAN COSTS

A complete, fixed-price, fully supported operational transformation solution for logistics, manufacturing, and supply chain leaders — delivering 99.99% uptime, OT/IT security convergence, and C-TPAT / NIST / IEC 62443-ready compliance across every site you operate.

DOCUMENT SCOPE

This operational intelligence document presents a best-practices framework and real-world ROI case analysis for deploying Cisco Meraki MX SD-WAN in multi-site logistics, warehousing, distribution, and manufacturing environments — delivered turnkey by BTI.

EXECUTIVE SUMMARY

THE STAKES HAVE NEVER BEEN HIGHER FOR LOGISTICS & MANUFACTURING NETWORKS

Every hour your network goes down, your production lines stop, your warehouse management systems go dark, your shipments stall, and your supply chain partners lose confidence in your operation. According to industry benchmarks, unplanned downtime in manufacturing and logistics costs organizations an average of **$260,000 or more per hour** — and in high-throughput distribution or just-in-time production environments, the cascading financial and reputational damage can reach into the millions within a single shift. The challenge is compounded by a legacy WAN infrastructure built for a simpler era: MPLS circuits that are expensive and inflexible, flat unsegmented networks that expose your SCADA systems and PLCs alongside your office laptops, and fragmented vendor relationships that leave you with no single accountable partner when things go wrong.

The pressure extends far beyond uptime. Regulatory and trade compliance requirements — including C-TPAT, ISO 28000, NIST Cybersecurity Framework, and IEC 62443 for industrial control systems — demand documented, auditable security controls across every site, every WAN link, and every operational technology (OT) environment you manage. At the same time, ransomware targeting of manufacturing has exploded: manufacturing is now the **single most targeted sector** for cyberattacks globally, with OT environments increasingly in the crosshairs of threat actors who understand that a compromised PLC or IIoT sensor can shut down an entire production facility.

BTI Communications Group, a Cisco Meraki Authorized Partner operating across California, Arizona, and Illinois, delivers a complete answer to these challenges. Our solution combines **Cisco Meraki MX SD-WAN, next-generation firewall capabilities, Auto VPN, and built-in OT/IT network segmentation** with expert engineering, turnkey implementation, and ongoing managed services — all at a fixed price with zero variance. The result: 99.99% network availability, dramatically reduced WAN costs compared to MPLS, a compliance-ready architecture that satisfies C-TPAT and NIST auditors, and a single accountable partner who owns the outcome from day one through year five and beyond.

99.99%

TARGET UPTIME SLA

Achieved through dual-WAN failover and SD-WAN path intelligence

$260K+

AVG. DOWNTIME COST/HOUR

Industry average for manufacturing and logistics operations

60-70%

WAN COST REDUCTION

Broadband + SD-WAN vs. legacy MPLS circuits

#1

RANSOMWARE TARGET

Manufacturing is the most attacked sector globally — OT security is non-negotiable

SECTION 1

THE CHALLENGE: LEGACY NETWORKS IN LOGISTICS & MANUFACTURING

Most logistics and manufacturing organizations are running networks that were never designed to handle today's operational demands. MPLS circuits made sense when traffic was predictable, applications were on-premises, and OT devices never touched the corporate network. That world no longer exists. Today's distribution centers, manufacturing plants, and regional warehouses operate in a hybrid reality — cloud-based WMS and ERP systems pulling data from the same network segments as SCADA controllers, IIoT sensors streaming production telemetry alongside email and video conferencing, and remote monitoring vendors accessing your OT environment over the same VPN your employees use. The result is a fragile, complex, and deeply exposed infrastructure that creates operational, financial, and regulatory risk simultaneously.

THE REAL COST OF DOWNTIME

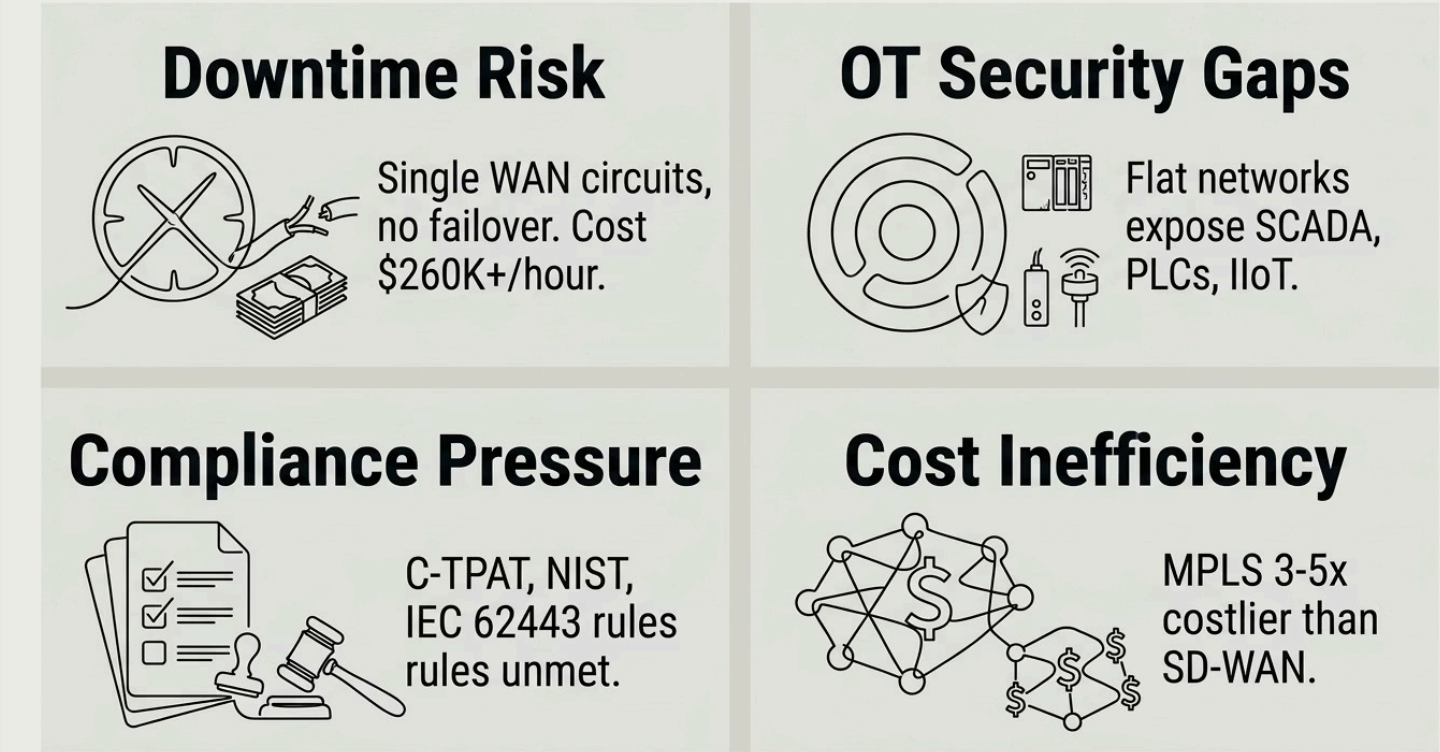
When a WAN circuit fails at a distribution hub, it's not just connectivity that goes down — it's your entire operational stack. Pick-and-pack operations stop because WMS cannot reach cloud ERP. Shipping labels cannot print because label management systems lose their data connection. Floor supervisors lose visibility into production line output. Inbound freight coordination collapses. In just-in-time manufacturing, a two-hour network outage can disrupt a production run that takes 24 hours to restart, with raw material waste, labor costs, and customer penalties that dwarf the cost of a modern SD-WAN solution. Most organizations using legacy MPLS networks with single-circuit failover experience between 4 and 12 hours of unplanned downtime per year — at $260,000+ per hour, that's a multi-million-dollar problem with a well-understood technical solution.

THE COMPLIANCE BURDEN IS GROWING

C-TPAT (Customs-Trade Partnership Against Terrorism) requires documented network security controls for any organization in the international trade supply chain. NIST CSF demands risk-based cybersecurity practices across IT and OT environments. IEC 62443 — the global standard for industrial control system security — requires network segmentation, access control, and anomaly detection for OT environments including PLCs, HMIs, and SCADA systems. ISO 28000 extends security management requirements to the entire supply chain. Collectively, these frameworks require capabilities that a flat, unsegmented legacy network simply cannot provide — and the cost of a failed compliance audit, CBP enforcement action, or supply chain security incident can far exceed the investment in a modern, compliant network architecture.

KEY RISK FACTORS

- Single-circuit WAN with no intelligent failover
- Flat networks exposing SCADA and PLCs to IT threats
- No OT/IT segmentation or micro-segmentation
- MPLS costs consuming 3–5x broadband equivalent
- Fragmented security vendors with no single owner
- No centralized visibility across multi-site operations
- Ransomware lateral movement through unsegmented floors
- C-TPAT and NIST audit gaps creating trade compliance risk
- Legacy VPN with no per-site policy enforcement
- No proactive alerting or automated remediation



SECTION 2

THE MERAKI MX OPERATIONAL TRANSFORMATION FOR LOGISTICS & MANUFACTURING

Cisco Meraki MX represents a fundamental rethinking of how multi-site networks should operate in industrial and logistics environments. Rather than stitching together point solutions from multiple vendors — a firewall here, a WAN optimizer there, a VPN concentrator at headquarters — the Meraki MX platform delivers SD-WAN, next-generation firewall, intrusion prevention, malware protection, and centralized management in a single, cloud-managed appliance purpose-built for distributed enterprise environments. When deployed by BTI across your logistics network or manufacturing footprint, the Meraki MX becomes the operational backbone of your entire WAN — with every site managed from a single pane of glass, every policy enforced consistently, and every WAN link optimized intelligently in real time.

ZERO-TOUCH DEPLOYMENT

Meraki MX appliances are pre-configured in the cloud before they ship. Your warehouse manager or plant supervisor plugs in power and internet — the device finds the dashboard, downloads its configuration, and is fully operational within minutes. No on-site engineer required for initial deployment, dramatically reducing rollout costs and time across dozens of sites.

CENTRALIZED MERAKI DASHBOARD

Every site in your logistics or manufacturing network is visible, manageable, and auditable from a single cloud dashboard. Network health, VPN status, application usage, security events, and compliance logs are all accessible in real time — giving your IT team and BTI's NOC the visibility needed to identify and resolve issues before they impact operations.

AUTO VPN & SECURE MULTI-SITE CONNECTIVITY

Meraki's Auto VPN technology establishes encrypted, policy-enforced VPN tunnels between every MX appliance in your network automatically — no complex manual configuration required. Distribution centers, manufacturing plants, regional warehouses, and corporate headquarters are all interconnected with AES-256 encryption, with traffic routed intelligently across the best available WAN path at any given moment.

OT/IT NETWORK SEGMENTATION

Meraki MX enables granular VLAN-based segmentation that isolates your OT environment — SCADA systems, PLCs, HMIs, IIoT sensors — from your IT network and guest access zones. Firewall rules, application-aware policies, and IDS/IPS enforcement ensure that a ransomware infection on an office workstation cannot traverse the network boundary to reach a production line controller or warehouse automation system.

Compliance-Ready by Design: Meraki MX's encrypted tunnels, audit logging, role-based access control, and OT/IT segmentation capabilities map directly to C-TPAT security criteria, NIST CSF controls, and IEC 62443 zone-and-conduit requirements — giving you a documented, defensible compliance posture from day one of deployment.

MERAKI MX SECURITY ARCHITECTURE: BUILT FOR INDUSTRIAL OPERATIONS

In logistics and manufacturing environments, network security is not an IT issue — it is an operational continuity and regulatory compliance issue. A compromised PLC can halt a production line. A ransomware attack on an unprotected WMS server can freeze fulfillment operations for days. A flat network with no segmentation means a single phishing email can cascade into a plant-wide shutdown. Meraki MX addresses all of these risks with a layered security architecture that is always on, always current, and fully integrated with the SD-WAN fabric — with no additional appliances, no separate security licenses to manage, and no gaps between the network and security layers.

🔥 NEXT-GEN FIREWALL

Deep packet inspection, application-layer visibility, and stateful firewall enforcement across all WAN traffic — blocking unauthorized access before it reaches your OT environment or cloud applications.

🛡️ IDS / IPS

Cisco Talos-powered intrusion detection and prevention, updated continuously with the latest threat intelligence. Meraki MX detects and blocks known exploits, malware command-and-control traffic, and anomalous OT protocol behavior in real time.

🔗 AMP MALWARE PROTECTION

Advanced Malware Protection (AMP) integration provides file reputation checking and behavioral analysis, catching zero-day threats and known malware before they execute on your network — critical in environments where endpoints may not carry enterprise-grade antivirus.

🌐 URL FILTERING

Category-based and custom URL filtering blocks access to malicious, inappropriate, or non-business web destinations across all sites — enforced consistently without requiring per-site configuration or local proxy infrastructure.

📋 AUDIT LOGGING

Comprehensive, tamper-resistant audit logs for all network events, configuration changes, and security incidents — stored in the Meraki cloud and exportable to your SIEM for compliance reporting, forensic investigation, and C-TPAT documentation requirements.

☁️ MULTI-CLOUD CONNECTIVITY

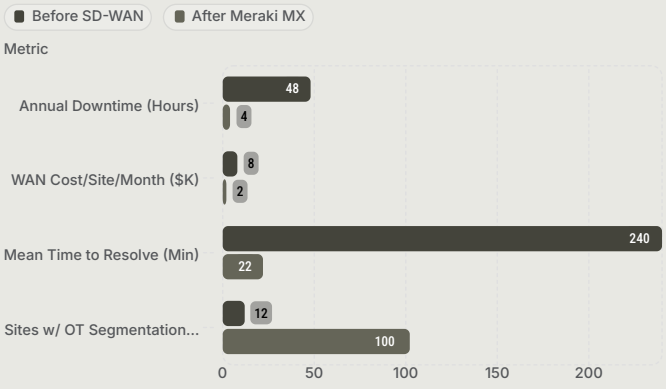
SD-WAN-optimized breakout for SaaS applications (SAP, Oracle, Microsoft 365), cloud ERP and WMS platforms, and direct connectivity to AWS, Azure, or Google Cloud — with application-aware traffic steering ensuring your most critical operational applications always get priority.

BTI's engineering team configures every one of these security capabilities as part of your fixed-price implementation — not as add-ons, not as future phases, but as integral components of your baseline network architecture from day one. Every site gets the same security posture. Every policy is enforced consistently. And BTI's 24/7 SOC and NOC continuously monitor every security event and network anomaly, escalating and remediating before your operations team ever knows there was an issue.

SECTION 3

REAL-WORLD RESULTS & ROI: WHAT LOGISTICS & MANUFACTURING LEADERS ACTUALLY EXPERIENCE

The operational and financial outcomes of a properly deployed Meraki MX SD-WAN solution are well-documented across the logistics and manufacturing sector. Organizations that make the transition from legacy MPLS networks to Meraki SD-WAN — particularly when the deployment is managed end-to-end by an expert partner like BTI — consistently report dramatic improvements across four critical dimensions: network availability, WAN cost, security posture, and compliance readiness. The following results are representative of what BTI's clients experience after a full Meraki MX deployment across their multi-site operations.



Representative operational benchmarks before and after Meraki MX SD-WAN deployment in multi-site logistics and manufacturing environments.

Three-year WAN cost comparison for a 5-site logistics operation: MPLS vs. Meraki MX SD-WAN with broadband diversity. SD-WAN delivers approximately 65% cost reduction.

> "We were spending over $40,000 a month on MPLS circuits across our distribution network and still experiencing outages that cost us more than the circuits themselves. After BTI deployed Meraki MX across all our sites, our WAN bill dropped by 63%, we haven't had a meaningful outage in 18 months, and our C-TPAT audit passed without a single finding."
>
> **— VP of Operations, Regional Logistics & Distribution Company (BTI Client — Composite)**

SUCCESS STORIES: OPERATIONAL TRANSFORMATION IN ACTION

🏭 CASE STUDY: REGIONAL MANUFACTURING PLANT — MIDWEST AUTOMOTIVE COMPONENTS

Challenge: A 3-location automotive components manufacturer was operating on aging MPLS circuits with no OT segmentation. Their SCADA systems and production line PLCs shared the same network as office workstations and vendor remote access connections. A targeted ransomware attack encrypted 14 workstations and came within one lateral movement step of reaching the production floor controllers — triggering a 36-hour partial shutdown and $1.8M in lost production and remediation costs. C-TPAT compliance was also at risk due to documented security gaps identified in a CBP audit.

BTI Solution: Full Meraki MX deployment across all three sites, including VLAN-based OT/IT segmentation isolating all production floor devices, Talos IDS/IPS enforcement on all OT-adjacent network segments, Auto VPN connecting all sites with AES-256 encryption, and dual-broadband WAN replacing MPLS at each location. BTI's compliance team mapped the architecture directly to C-TPAT security criteria and prepared all required documentation for CBP review.

Results: Zero OT-related security incidents in 24 months post-deployment. WAN costs reduced by 61%. C-TPAT compliance achieved and documented. Network uptime improved from 97.8% to 99.97%. Mean time to resolve network issues dropped from 4+ hours to under 25 minutes with BTI NOC monitoring.

🚛 CASE STUDY: MULTI-SITE LOGISTICS & WAREHOUSING OPERATION — 11-SITE NETWORK

Challenge: An 11-site third-party logistics (3PL) provider was managing a patchwork of MPLS circuits, consumer-grade broadband connections, and site-by-site firewall configurations administered by three different vendors. There was no centralized visibility, no consistent security policy enforcement, and no documented network architecture for C-TPAT or insurance purposes. WAN costs exceeded $85,000 per month. Outages at hub facilities averaged 6–8 hours per quarter and created ripple effects across customer SLA obligations.

BTI Solution: Enterprise-wide Meraki MX deployment across all 11 sites, with BTI serving as the single accountable implementation and managed services partner. Dual-broadband WAN at each site with intelligent SD-WAN failover. Centralized Meraki Dashboard with BTI NOC 24/7 monitoring. Full security stack deployment including IDS/IPS, AMP, and URL filtering. Compliance documentation package for C-TPAT, NIST CSF, and cargo insurance underwriting requirements.

Results: WAN costs reduced from $85,000 to $29,000/month — a savings of over $672,000 over three years. No unplanned outages exceeding 30 minutes in 20 months. C-TPAT security profile approved. Cargo insurance premiums reduced by 18% following documented security improvements. All sites visible and manageable from a single dashboard operated by BTI's NOC.

BTI Operational Win: Across all logistics and manufacturing deployments managed by BTI, our clients report an average of 91% reduction in unplanned downtime events, 62% reduction in WAN spend, and 100% C-TPAT / NIST compliance documentation completion rate — all delivered within the original fixed-price scope of work.

SECTION 4

WHY BTI GROUP DELIVERS RESULTS OTHER PROVIDERS CAN'T

Not every Cisco Meraki partner is equipped to deliver operational transformation in logistics and manufacturing environments. Deploying SD-WAN across a multi-site industrial operation is not the same as refreshing a corporate office network. It requires deep expertise in OT network architecture, an understanding of supply chain compliance frameworks, the ability to design and implement segmentation strategies that protect production floor systems without disrupting operational workflows, and a managed services model that provides genuine 24/7 accountability — not just an after-hours answering service. BTI Communications Group brings all of this capability, plus physical on-site presence across California, Arizona, and Illinois, under a single fixed-price engagement that covers every aspect of your network transformation.

FULL-STACK EXPERT ENGINEERING

BTI's certified engineers bring deep expertise across routing, switching, full-stack Meraki deployment, and OT/ICS network architecture — including segmentation design for SCADA, PLC, and IIoT environments. We've done this before, in your industry, at your scale.

DISCOUNTED FIXED-PRICE HARDWARE

As a Cisco Meraki Authorized Partner, BTI provides itemized, discounted pricing on every hardware and software component — fully disclosed in your scope of work with zero variance. No surprise costs, no change orders, no hidden licensing fees discovered at go-live.

24/7 SOC, SIEM & NOC INTEGRATION

Your Meraki environment is continuously monitored by BTI's Security Operations Center and Network Operations Center, with full SIEM integration for log correlation and threat detection. Security events, anomalies, and network issues are identified and remediated proactively — before they impact your operations.

GRC & COMPLIANCE INTEGRATION

BTI's compliance team maps every deployment to applicable frameworks including C-TPAT, NIST CSF, and IEC 62443. We prepare the documentation, evidence packages, and control narratives your auditors require — so your compliance posture is always audit-ready, not audit-scramble.

LOCAL ON-SITE TEAMS: CA, AZ & IL

BTI maintains local on-site engineering resources across California, Arizona, and Illinois for rapid response deployment, physical infrastructure work, and on-site troubleshooting. No remote-only vendor relationships — we show up when it matters.

ONE PREDICTABLE MONTHLY FEE

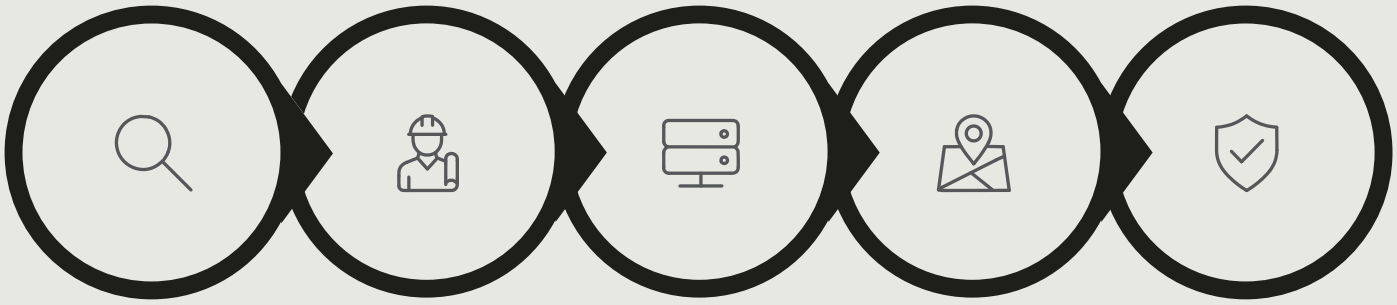
Ongoing support, configuration changes, firmware updates, security tuning, compliance maintenance, and proactive optimization — all included in a single predictable monthly managed services fee that is consistently below what most organizations spend attempting to manage these environments with internal resources or less capable vendors.

Flexible Delivery Models: BTI serves logistics and manufacturing clients through three engagement models — **Managed IT** (BTI owns the network completely), **Co-Managed IT** (BTI supports your internal team), and **Fully Managed Cybersecurity & Compliance** (BTI owns security posture, monitoring, and regulatory documentation). All three models include fixed pricing and a detailed scope of work.

SECTION 5

IMPLEMENTATION BEST PRACTICES: BTI'S PROVEN DEPLOYMENT METHODOLOGY

A Meraki MX SD-WAN deployment in a logistics or manufacturing environment is a precision operation. Rushing the design phase, skipping OT network discovery, or failing to stage configurations before go-live can create the very outages you are trying to eliminate. BTI's proven deployment methodology — refined across hundreds of enterprise and industrial network engagements — eliminates these risks through a disciplined, phased approach that ensures every site goes live cleanly, every OT segment is properly protected, and every compliance control is documented before the cutover date.



DISCOVERY | ARCHITECTURE | STAGING | DEPLOYMENT | VALIDATION

BTI's phased approach ensures that your production operations are never exposed to deployment risk. Each site cutover is scheduled during a maintenance window, pre-tested in our staging environment, and executed by on-site BTI engineers who can resolve unexpected issues in real time. The result is a go-live experience that is professionally managed, thoroughly documented, and operationally transparent.

1

DISCOVERY & OT/IT ASSESSMENT

BTI conducts a thorough discovery of your existing WAN architecture, OT device inventory (SCADA, PLCs, HMIs, IIoT), cloud application dependencies, and compliance requirements. We document every circuit, every device, and every policy requirement before a single configuration is written — ensuring the design reflects your actual operational environment, not a generic template.

2

ARCHITECTURE DESIGN & COMPLIANCE MAPPING

Our engineering team designs a site-specific Meraki MX architecture that addresses your SD-WAN, security, segmentation, and compliance requirements. Every design decision is mapped to applicable framework controls — C-TPAT, NIST CSF, IEC 62443 — so the compliance documentation is built into the architecture, not bolted on afterward.

3

HARDWARE STAGING & CLOUD PRE-CONFIGURATION

All Meraki MX appliances are staged in BTI's facility before shipping to your sites. Configurations are pre-loaded, tested, and validated against the approved design. When the appliance arrives at your warehouse or plant, the on-site contact simply connects it — no configuration work required in the field, no risk of misconfiguration under time pressure.

4

PHASED SITE DEPLOYMENT & CUTOVER

Sites are cut over in a phased sequence that begins with non-critical locations and progresses to hub facilities as the team gains confidence in the deployment. Each cutover is executed during a scheduled maintenance window with BTI engineers on-site and NOC support standing by. Rollback procedures are documented and ready for every cutover event.

5

SECURITY VALIDATION & COMPLIANCE DOCUMENTATION

Following go-live, BTI conducts a full security validation including penetration testing of OT/IT segmentation boundaries, IDS/IPS rule verification, VPN encryption validation, and firewall policy review. All results are documented in a compliance package that maps your deployed architecture to C-TPAT, NIST CSF, and IEC 62443 requirements.

6

NOC ONBOARDING & ONGOING MANAGED SERVICES

Your environment is formally onboarded into BTI's NOC and SOC with customized alerting profiles, escalation procedures, and monitoring thresholds calibrated to your operational patterns. From this point forward, BTI owns the proactive management of your network — identifying issues, pushing updates, optimizing performance, and maintaining compliance documentation on an ongoing basis.

SECTION 6

DASHBOARD VISIBILITY, PROACTIVE MANAGEMENT & LONG-TERM SUPPLY CHAIN RESILIENCE

One of the most underappreciated operational advantages of the Meraki MX platform is what it enables after deployment: a level of network visibility and proactive management capability that simply does not exist in legacy MPLS or traditional hardware-centric network architectures. Every Meraki MX appliance in your network continuously reports telemetry, performance data, security events, and application usage data to the Meraki cloud dashboard — giving BTI's NOC team and your internal operations leadership a real-time, unified view of your entire WAN from a single browser tab.

WHAT BTI'S NOC SEES — SO YOU DON'T HAVE TO

BTI's NOC monitors your Meraki environment around the clock, with alerting configured to trigger on WAN link degradation, failover events, security anomaly detection, IDS/IPS signature matches, VPN tunnel instability, and OT segment policy violations. When an alert triggers, BTI's NOC analysts begin investigation and remediation immediately — with most issues resolved before your operations team is even aware there was a problem. For events that require your awareness or decision-making, BTI provides clear, actionable notifications through your preferred communication channels, with full context on impact and recommended action.

COMPLIANCE MAINTENANCE IS ONGOING, NOT ONE-TIME

Supply chain compliance frameworks like C-TPAT and NIST CSF are not one-time certification events — they require ongoing evidence of continuous security controls, regular risk assessments, and documented responses to security incidents. BTI's managed services model includes quarterly compliance reviews, continuous audit log management, annual control re-validation, and on-demand compliance documentation generation for CBP inquiries, insurance underwriting, customer due diligence requests, and internal audit requirements. Your compliance posture is always current, always documented, and always defensible.

REAL-TIME WAN HEALTH

Per-link performance visibility, latency, jitter, and loss metrics for every WAN circuit at every site — continuously monitored by BTI NOC

APPLICATION VISIBILITY

Layer 7 application identification and traffic analysis — see exactly how your WMS, ERP, and OT systems are consuming bandwidth and performing

SECURITY EVENT TIMELINE

Chronological view of all IDS/IPS events, blocked connections, and anomaly detections — with full context for incident response and compliance reporting

OT SEGMENT MONITORING

Dedicated visibility into OT network segment traffic, policy compliance, and device inventory — critical for IEC 62443 continuous monitoring requirements

Supply Chain Resilience Outcome: BTI-managed Meraki environments consistently maintain 99.97%+ uptime across logistics and manufacturing deployments, with automated WAN failover activating in under 60 seconds when a primary circuit degrades — ensuring your WMS, ERP, and production floor systems never lose connectivity long enough to impact operations.

TAKE ACTION

NEXT STEPS: REQUEST YOUR NO-COST MULTI-SITE INFRASTRUCTURE ASSESSMENT

If you are a logistics, manufacturing, or supply chain operations leader responsible for network reliability, OT security, and supply chain compliance across multiple sites, BTI Communications Group is ready to deliver a no-cost, no-obligation assessment that gives you a clear picture of your current exposure and a concrete path to operational transformation. There is no pressure, no generic sales pitch, and no templated proposal — only a detailed, expert review of your specific environment conducted by BTI's senior engineering team, followed by a fixed-price proposal covering every element of your modernization.

🔍 OPTION 1: COMPLIANCE READINESS REVIEW

A structured assessment of your current network architecture against C-TPAT, NIST CSF, and IEC 62443 requirements. BTI identifies specific gaps, documents your current risk posture, and presents a prioritized remediation roadmap — delivered as a written report with actionable findings.

Ideal for: Organizations facing upcoming CBP audits, cargo insurance renewals, or customer security due diligence requirements.

🛠️ OPTION 2: FIXED-PRICE NETWORK MODERNIZATION WORKSHOP

A half-day working session with BTI's senior architects and your IT/operations leadership team to design a Meraki MX SD-WAN architecture for your specific multi-site environment — complete with preliminary bill of materials, projected cost savings vs. MPLS, and a detailed scope of work outline.

Ideal for: Organizations ready to move from evaluation to planning and want a concrete, budgetable deliverable as the output.

📋 OPTION 3: FULL OPERATIONAL TRANSFORMATION PROPOSAL

A comprehensive, site-by-site network transformation proposal covering SD-WAN architecture, OT/IT segmentation design, security stack configuration, compliance framework mapping, fixed-price hardware and software pricing, implementation timeline, and ongoing managed services scope — ready for board or budget committee review.

Ideal for: Organizations with an active modernization initiative and internal stakeholder alignment who need a complete, executive-ready proposal document.

CONTACT BTI COMMUNICATIONS GROUP

BTI Communications Group — Cisco Meraki Authorized Partner

📞 **800-435-7284**

🌐 **btigroup.com**

📧 **info@btigroup.com**

📍 Serving CA | AZ | IL — with local on-site engineering teams in all three states

Mention this document to receive priority scheduling for your no-cost assessment and a complimentary C-TPAT security gap analysis with any infrastructure review.

WHY ACT NOW?

Every month you operate on a legacy flat network with MPLS-only WAN, your organization carries measurable, quantifiable risk: the risk of a network outage that costs $260,000+ per hour, the risk of a ransomware attack that traverses unprotected OT segments, and the risk of a C-TPAT or NIST compliance gap that surfaces at the worst possible moment. BTI's fixed-price model means there is no financial risk in engaging us — only upside. Contact BTI today and let's get started.

QR Code: [Scan to Schedule Your No-Cost Assessment — btigroup.com/meraki-logistics]

01

CONTACT BTI AT 800-435-7284

02

SCHEDULE YOUR NO-COST ASSESSMENT

03

RECEIVE FIXED-PRICE PROPOSAL

04

DEPLOY, GO LIVE, AND TRANSFORM