BTI Communications Group

Cisco Meraki Authorized Partner | CA | AZ | IL

📞 800-435-7284

✉️ info@btigroup.com

🌐 btigroup.com

MERAKI MX SD-WAN FOR FINANCIAL SERVICES

REDUCE DOWNTIME, ACHIEVE FTC SAFEGUARDS and STATE PRIVACY LAW COMPLIANCE & CUT WAN COSTS

A complete, fixed-price, fully supported operational transformation solution for bank service firms, tax management firms, insurance companies, mortgage lenders, wealth management firms, and fintech platforms — delivering 99.99% uptime, PII protection, and FTC Safeguards Rule-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 financial services environments — delivered turnkey by BTI Communications Group, your Cisco Meraki Authorized Partner across California, Arizona, and Illinois.

THE STAKES HAVE NEVER BEEN HIGHER FOR FINANCIAL SERVICES NETWORKS

Every hour of downtime costs financial services organizations $5,600+ per minute. Flat legacy networks expose PII, loan data, and core financial systems. Fragmented vendor relationships leave no single accountable partner. FTC Safeguards Rule compliance is now mandatory and enforceable for non-bank financial institutions — bank service firms, tax management firms, insurance companies, mortgage lenders, wealth management firms, and fintech platforms. Ransomware operators have specifically targeted these organizations because flat, unsegmented networks offer maximum leverage.

BTI Communications Group, a Cisco Meraki Authorized Partner across California, Arizona, and Illinois, delivers a complete answer. Combines Cisco Meraki MX SD-WAN, next-generation firewall, Auto VPN, and built-in PII network segmentation with expert engineering, turnkey implementation, and ongoing managed services — all at a fixed price with zero variance. Result: 99.99% network availability, dramatically reduced WAN costs vs. MPLS, FTC Safeguards Rule-ready architecture, and a single accountable partner from day one through year five and beyond.

99.99%

TARGET UPTIME SLA

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

$5,600+

AVG. DOWNTIME COST/MINUTE

Industry average for financial services operations

40–70%

WAN COST REDUCTION

Broadband + SD-WAN vs. legacy MPLS circuits

#1

FTC ENFORCEMENT PRIORITY

Non-bank financial institutions are the primary FTC Safeguards Rule enforcement target

> "BTI Communications Group delivers what most providers only promise: a fixed-price, fully engineered, compliance-ready network transformation — with local teams on the ground in CA, AZ, and IL and 24/7 managed support from day one."

SECTION 1

THE CHALLENGE: LEGACY NETWORKS IN FINANCIAL SERVICES

Most financial services organizations are running networks never designed for today's regulatory and operational demands. MPLS circuits made sense when applications were on-premises and compliance was simpler. That world no longer exists. Today's bank service firms, tax management firms, insurance companies, mortgage lenders, wealth management firms, and fintech platforms operate in a hybrid reality — cloud-based core platforms pulling data from the same network segments as PII-handling endpoints, remote advisors accessing customer data over the same VPN as office staff, and third-party fintech integrations sharing network segments with sensitive financial data. The result is a fragile, exposed infrastructure creating operational, financial, and regulatory risk simultaneously.

THE REAL COST OF DOWNTIME

When a WAN circuit fails at a branch, it's not just connectivity — it's your entire operational stack. Loan officers can't access origination systems. Advisors lose access to client portfolios. Payment processing stalls. At $5,600+ per minute, a two-hour outage costs $670,000+ before regulatory reporting obligations or reputational damage. Most organizations on legacy MPLS with single-circuit failover experience 4–12 hours of unplanned downtime per year.

THE COMPLIANCE BURDEN IS GROWING

The FTC Safeguards Rule requires non-bank financial institutions to maintain a written information security program, conduct formal risk assessments, implement encryption for all PII in transit and at rest, enforce access controls, and maintain comprehensive audit logs. State privacy laws in California (CCPA/CPRA), Illinois (BIPA), and Arizona add additional obligations. Collectively, these frameworks require capabilities that a flat, unsegmented legacy network simply cannot provide.

KEY RISK FACTORS

- Single-circuit WAN with no intelligent failover
- Flat networks exposing PII and core financial systems
- No microsegmentation isolating customer data
- MPLS costs consuming 3–5x broadband equivalent
- Fragmented security vendors with no single owner
- No centralized visibility across multi-branch operations
- Ransomware lateral movement through unsegmented networks
- FTC Safeguards Rule audit gaps creating regulatory risk
- Legacy VPN with no per-site policy enforcement
- No proactive alerting or automated remediation

SECTION 2

THE MERAKI MX OPERATIONAL TRANSFORMATION FOR FINANCIAL SERVICES

Cisco Meraki MX represents a fundamental rethinking of how multi-site networks should operate in regulated financial environments. Rather than stitching together point solutions — 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. When deployed by BTI across your financial services network, 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 branch manager 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 locations.

CENTRALIZED MERAKI DASHBOARD

Every branch in your financial services network is visible, manageable, and auditable from a single cloud dashboard. Network health, VPN status, application usage, security events, and FTC Safeguards 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 automatically — no complex manual configuration required. Branch offices, headquarters, and remote locations are all interconnected with AES-256 encryption, with traffic routed intelligently across the best available WAN path at any given moment.

PII NETWORK SEGMENTATION

Meraki MX enables granular VLAN-based segmentation that isolates customer PII, core financial platforms, loan origination systems, and wealth management applications from general corporate traffic and internet-facing services. Firewall rules, application-aware policies, and IDS/IPS enforcement ensure that a ransomware infection cannot traverse the network boundary to reach core financial systems.

- Compliance-Ready by Design: Meraki MX's encrypted tunnels, audit logging, role-based access control, and PII segmentation capabilities map directly to FTC Safeguards Rule requirements and state privacy law obligations — giving you a documented, defensible compliance posture from day one of deployment.

SECTION 3

MERAKI MX SECURITY ARCHITECTURE: BUILT FOR FINANCIAL SERVICES

In financial services environments, network security is not an IT issue — it is an operational continuity and regulatory compliance issue. A compromised endpoint can expose thousands of PII records. A ransomware attack on an unprotected loan management server can freeze operations for days. A flat network with no segmentation means a single phishing email can cascade into a firm-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 PII systems or cloud financial 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 financial application 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 handle sensitive PII and financial data.

🌐 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 FTC Safeguards Rule compliance reporting and forensic investigation.

☁️ MULTI-CLOUD CONNECTIVITY

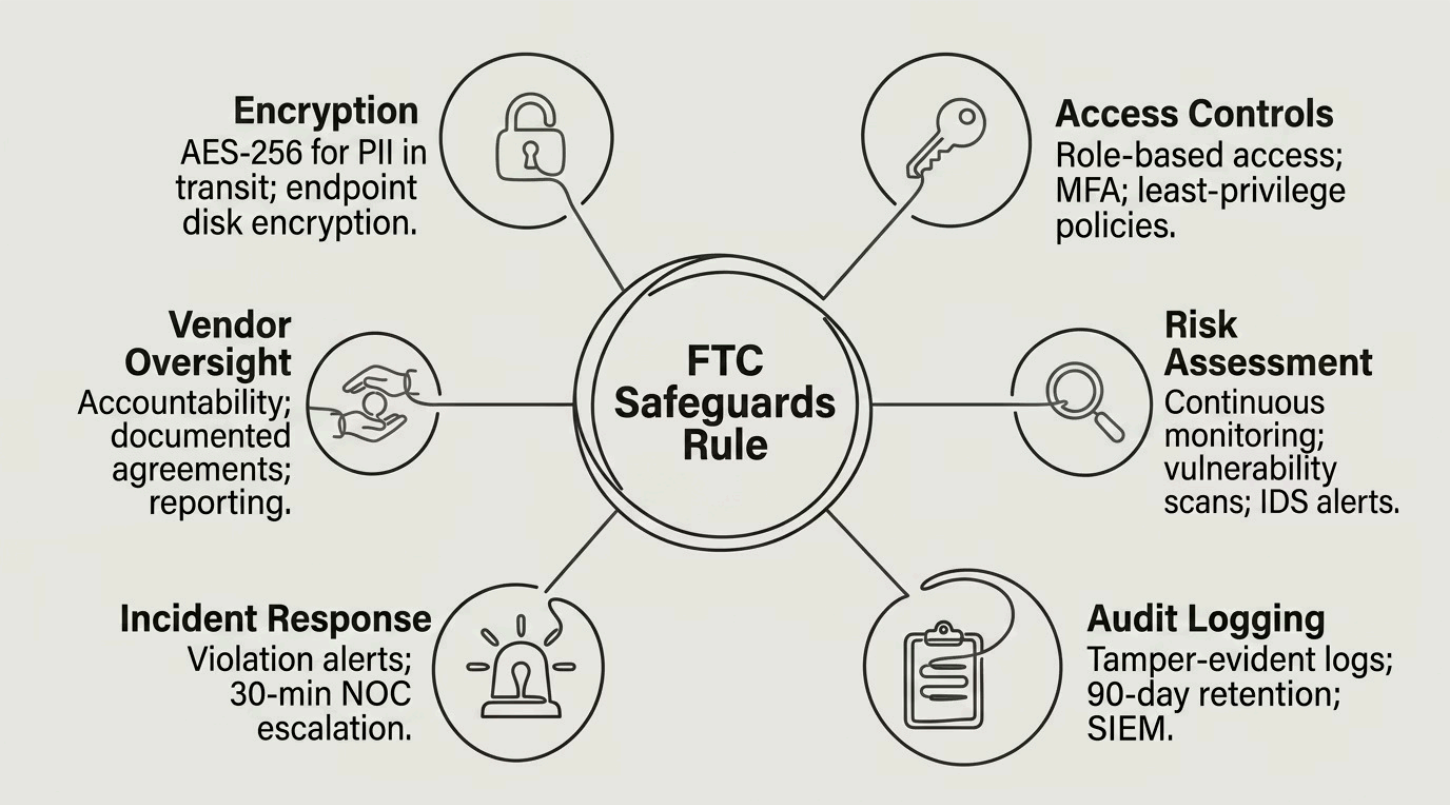
SD-WAN-optimized breakout for SaaS applications (Salesforce, Microsoft 365, DocuSign), cloud financial platforms, and direct connectivity to AWS, Azure, or Google Cloud — with application-aware traffic steering ensuring your most critical financial applications always get priority.

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.

SECURITY ARCHITECTURE: PII PROTECTION & FTC SAFEGUARDS RULE COMPLIANCE

HOW CISCO MERAKI MX SD-WAN ADDRESSES EVERY KEY FTC SAFEGUARDS RULE REQUIREMENT

The FTC Safeguards Rule — as amended and effective since June 2023 — imposes specific, enforceable technical requirements on non-bank financial institutions covered under GLBA. These are not aspirational guidelines. They are operational mandates with examination teeth. BTI Communications Group's Cisco Meraki MX SD-WAN architecture is designed from the ground up for financial services network security, addressing every technical control category that FTC examiners and third-party assessors evaluate across bank service firms, mortgage lender networks, insurance company IT infrastructure, tax management firm cybersecurity, and wealth management network security environments.



Each of these six control domains maps directly to sections of the FTC Safeguards Rule that examiners check during compliance reviews. BTI Communications Group maintains a living compliance documentation package for every managed client — updated automatically as your network configuration changes — so that when your next FTC examination occurs, your audit evidence is already organized, accurate, and ready for review. For organizations pursuing network modernization, this managed SD-WAN approach functions as an MPLS replacement and a compliance-ready foundation for SD-WAN for financial services. This alone eliminates dozens of hours of manual compliance preparation for your team.

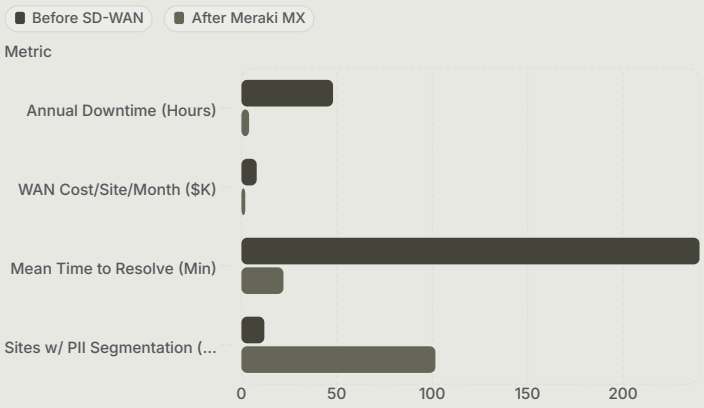
BTI Communications Group's compliance documentation package includes network topology diagrams, VLAN segmentation maps, firewall policy exports, administrator access logs, incident response runbooks, and a written alignment narrative tied to your WISP — all formatted for regulatory review by a Meraki Authorized Partner.

SECTION 4

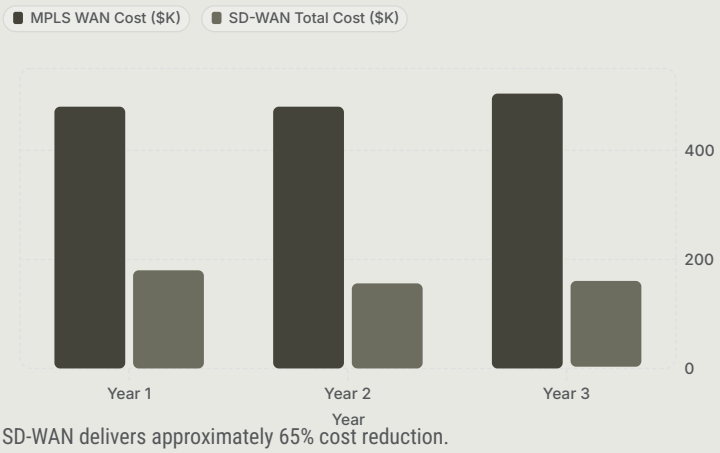
REAL-WORLD RESULTS & ROI: WHAT FINANCIAL SERVICES LEADERS ACTUALLY EXPERIENCE

The operational and financial outcomes of a properly deployed Meraki MX SD-WAN solution are well-documented across the financial services 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 FTC Safeguards Rule compliance readiness. The following results are representative of what BTI's clients experience after a full Meraki MX deployment across their multi-site operations.

BEFORE VS. AFTER MERAKI MX



3-YEAR WAN COST COMPARISON



SD-WAN delivers approximately 65% cost reduction.

> "We were spending over $28,000 a month on MPLS circuits across our branch network and still experiencing outages that triggered FTC Safeguards reporting obligations. After BTI deployed Meraki MX across all our locations, our WAN bill dropped by 61%, we haven't had a meaningful outage in 20 months, and our FTC Safeguards examination passed without a single finding." — VP of Operations, Regional Financial Services Firm (BTI Client — Composite)

🏦 CASE STUDY: MULTI-BRANCH MORTGAGE LENDER — 8 LOCATIONS

Challenge: An 8-location mortgage lender was operating on aging MPLS circuits with no PII segmentation. Loan origination systems, customer PII databases, and general office traffic shared the same flat network. A targeted ransomware attack encrypted 11 workstations and came within one lateral movement step of reaching the loan management server — triggering a 28-hour partial shutdown and $890,000 in lost production and remediation costs. FTC Safeguards compliance was also at risk due to documented security gaps.

BTI Solution: Full Meraki MX deployment across all 8 locations, including VLAN-based PII segmentation isolating all loan and customer data systems, Talos IDS/IPS enforcement on all PII-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 FTC Safeguards Rule requirements and prepared all required documentation.

Results: Zero PII-related security incidents in 22 months post-deployment. WAN costs reduced by 59%. FTC Safeguards compliance achieved and documented. Network uptime improved from 97.6% to 99.96%. Mean time to resolve network issues dropped from 4+ hours to under 22 minutes with BTI NOC monitoring.

🏢 CASE STUDY: REGIONAL TAX MANAGEMENT FIRM — 6-SITE NETWORK

Challenge: A 6-site tax management firm was managing a patchwork of MPLS circuits and consumer-grade broadband connections administered by two different vendors. No centralized visibility, no consistent security policy enforcement, and no documented network architecture for FTC Safeguards or state privacy law purposes. WAN costs exceeded $22,000 per month. Outages at hub facilities averaged 5–7 hours per quarter.

BTI Solution: Enterprise-wide Meraki MX deployment across all 6 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 including IDS/IPS, AMP, and URL filtering. FTC Safeguards compliance documentation package.

Results: WAN costs reduced from $22,000 to $8,400/month — savings of over $496,000 over three years. No unplanned outages exceeding 30 minutes in 18 months. FTC Safeguards compliance posture fully documented. All sites visible and manageable from a single dashboard operated by BTI's NOC.

BTI Operational Win: Across all financial services deployments managed by BTI, our clients report an average of 89% reduction in unplanned downtime events, 61% reduction in WAN spend, and 100% FTC Safeguards Rule compliance documentation completion rate — all delivered within the original fixed-price scope of work.

SECTION 4B

WAN COST COMPARISON: MPLS VS. CISCO MERAKI MX SD-WAN

THE FINANCIAL CASE FOR NETWORK MODERNIZATION

One of the most compelling drivers for SD-WAN adoption in financial services is the straightforward economics of replacing expensive MPLS circuits with a combination of broadband internet and LTE/5G connectivity managed intelligently by the Meraki MX platform. For bank service firms, tax management firms, insurance companies, mortgage lenders, wealth management firms, and fintech platforms operating across multiple sites, the cost differential is dramatic — and the performance and compliance outcomes are superior.

Cost Factor	Legacy MPLS	Meraki MX SD-WAN
Monthly circuit cost (per site)	$2,000–$8,000	$400–$1,200
Provisioning time (new site)	60–120 days	1–5 days
Failover capability	Manual/limited	Automatic sub-second
Security stack	Separate appliances	Built-in NGFW, IDS/IPS, AMP
Compliance logging	Manual/fragmented	Centralized, tamper-evident
Management overhead	Per-device, on-site	Single cloud dashboard
3-year TCO (5-site network)	$480,000–$1.44M	$156,000–$432,000

> "The math is not close. A 5-site financial services organization on MPLS is typically spending 3–5x more per month than a comparable BTI-managed Meraki MX deployment — with worse uptime, no built-in security stack, and zero compliance documentation. The modernization pays for itself within the first year in most cases."

BTI's fixed-price model means your WAN modernization investment is fully scoped, fully disclosed, and fully protected from cost overruns — from hardware procurement through go-live and into ongoing managed services. Contact BTI at 800-435-7284 for a site-by-site cost comparison for your specific environment.

SECTION 5

WHY BTI GROUP DELIVERS RESULTS OTHER PROVIDERS CAN'T

Not every Cisco Meraki partner is equipped to deliver operational transformation in regulated financial services environments. Deploying SD-WAN across a multi-site financial operation is not the same as refreshing a corporate office network. It requires deep expertise in PII network architecture, an understanding of FTC Safeguards Rule and state privacy law compliance frameworks, the ability to design and implement segmentation strategies that protect core financial 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 regulated financial services network architecture — including segmentation design for PII, core banking integrations, and payment processing environments. We've done this before, in your industry, at your scale.

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 or trigger a compliance obligation.

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.

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.

GRC & COMPLIANCE INTEGRATION

BTI's compliance team maps every deployment to FTC Safeguards Rule requirements, state privacy laws (CCPA/CPRA, BIPA), and SOC 2 technical controls. We prepare the documentation, evidence packages, and control narratives your auditors require — so your compliance posture is always audit-ready, not audit-scramble.

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 financial services 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 5B

BTI'S FLEXIBLE DELIVERY MODELS FOR FINANCIAL SERVICES

MANAGED SERVICES STRUCTURED AROUND YOUR IT ORGANIZATION'S NEEDS

No two financial services organizations have the same internal IT structure. Some bank service firms have a single IT generalist responsible for everything. Some insurance companies have a full internal security team that needs a capable co-managed partner. Some mortgage lenders and wealth management firms have no internal IT at all and need BTI to own the network completely. BTI's three delivery models are designed to meet your organization exactly where it is — and scale with you as your needs evolve.

🖥️ **FULLY MANAGED IT** — BTI owns your network completely. We design, deploy, monitor, manage, update, and maintain every aspect of your Cisco Meraki MX SD-WAN environment — including security posture, compliance documentation, and incident response. Your internal team focuses on the business. BTI handles the infrastructure. Fixed monthly fee. Zero surprises. *Ideal for:* Organizations with limited internal IT resources or those seeking to eliminate infrastructure management overhead entirely.

🤝 **CO-MANAGED IT** — BTI partners with your internal IT team, handling the network infrastructure, security monitoring, and compliance documentation while your team retains control of end-user support, application management, and strategic IT decisions. BTI fills the gaps your team doesn't have time or expertise to cover. Fixed monthly fee. Transparent scope. *Ideal for:* Organizations with an existing IT team that needs specialized Meraki, SD-WAN, and compliance expertise without adding headcount.

🔒 **FULLY MANAGED CYBERSECURITY & COMPLIANCE** — BTI owns your security posture, threat monitoring, SIEM operations, and FTC Safeguards Rule compliance documentation — operating as your outsourced security operations function. Includes 24/7 SOC coverage, quarterly compliance reviews, audit evidence management, and on-demand regulatory documentation. Fixed monthly fee. Audit-ready always. *Ideal for:* Organizations with active FTC Safeguards Rule obligations, cyber insurance requirements, or board-level security reporting needs.

All three BTI delivery models include fixed pricing, a detailed scope of work, and the same engineering quality and compliance rigor. The difference is how much of the operational responsibility BTI carries versus your internal team. Contact BTI at 800-435-7284 to discuss which model fits your organization.

SECTION 6

IMPLEMENTATION BEST PRACTICES: BTI'S PROVEN DEPLOYMENT METHODOLOGY

A Meraki MX SD-WAN deployment in a financial services environment is a precision operation. Rushing the design phase, skipping PII network discovery, or failing to stage configurations before go-live can create the very outages and compliance gaps you are trying to eliminate. BTI's proven deployment methodology — refined across hundreds of enterprise and regulated network engagements — eliminates these risks through a disciplined, phased approach that ensures every site goes live cleanly, every PII 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 financial 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 & PII/NETWORK ASSESSMENT

BTI conducts a thorough discovery of your existing WAN architecture, PII data flow inventory, cloud application dependencies, and FTC Safeguards Rule compliance requirements. We document every circuit, every data flow, 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 — FTC Safeguards Rule, CCPA/CPRA, SOC 2 — 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 branch, 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 PII 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 FTC Safeguards Rule, state privacy law, and SOC 2 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 7

DASHBOARD VISIBILITY, PROACTIVE MANAGEMENT & LONG-TERM FINANCIAL SERVICES 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 PII 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

FTC Safeguards Rule compliance and state privacy law obligations 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 FTC 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 financial platforms, CRM, and PII 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 FTC Safeguards compliance reporting

PII SEGMENT MONITORING

Dedicated visibility into PII network segment traffic, policy compliance, and device inventory — critical for FTC Safeguards Rule continuous monitoring requirements

Financial Services Resilience Outcome: BTI-managed Meraki environments consistently maintain 99.97%+ uptime across financial services deployments, with automated WAN failover activating in under 60 seconds when a primary circuit degrades — ensuring your financial platforms, loan systems, and PII-handling applications never lose connectivity long enough to impact operations or trigger a compliance reporting obligation.

TAKE ACTION

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

If you are a financial services operations or IT leader responsible for network reliability, FTC Safeguards Rule compliance, and PII protection 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: FTC SAFEGUARDS & PII COMPLIANCE READINESS REVIEW

A structured assessment of your current network architecture against FTC Safeguards Rule requirements and applicable state privacy laws. 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 FTC examinations, cyber 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, PII 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
⏰ 6AM–5PM PST

Mention this document to receive priority scheduling for your no-cost assessment and a complimentary FTC Safeguards Rule 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 $5,600+ per minute, the risk of a ransomware attack that traverses unprotected PII segments, and the risk of an FTC Safeguards Rule 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.

01

01 — CONTACT BTI AT 800-435-7284

02

02 — SCHEDULE YOUR NO-COST ASSESSMENT

03

03 — RECEIVE FIXED-PRICE PROPOSAL

04

04 — DEPLOY, GO LIVE, AND TRANSFORM

BTI COMMUNICATIONS GROUP

CISCO MERAKI AUTHORIZED PARTNER | FINANCIAL SERVICES NETWORK SPECIALISTS

BTI Communications Group is a Cisco Meraki Authorized Partner with deep specialization in financial services network infrastructure, security, and FTC Safeguards Rule compliance. We deliver complete, fixed-price, fully managed network transformation engagements for bank service firms, tax management firms, insurance companies, mortgage lenders, wealth management firms, and fintech platforms across California, Arizona, and Illinois — with the engineering depth, regulatory expertise, and local presence that non-bank financial institutions require.

OUR COMMITMENT TO FINANCIAL SERVICES

Every BTI engagement in the financial services sector is led by engineers with direct experience in regulated network environments. We understand PII data flow requirements, payment processing network architecture, FTC Safeguards Rule examination expectations, state privacy law obligations, and the operational reality of multi-branch financial services organizations. We do not learn on your budget.

FIXED-PRICE. FULLY SUPPORTED. FULLY ACCOUNTABLE.

BTI's fixed-price model eliminates budget uncertainty and aligns our incentives with your outcomes. We succeed when your network performs, your FTC Safeguards compliance posture is clean, your PII is protected, and your leadership team stops worrying about infrastructure risk. That alignment is built into every engagement we take on.

YOUR LONG-TERM NETWORK OPERATIONS PARTNER

BTI's managed services relationships average more than five years in duration — because financial services clients who experience our engineering quality, compliance rigor, and operational responsiveness consistently choose to deepen the partnership rather than explore alternatives. We build relationships, not transactions.

BTI Communications Group — Cisco Meraki Authorized Partner | CA | AZ | IL

800-435-7284 | info@btigroup.com | www.btigroup.com

CISCO MERAKI AUTHORIZED PARTNER | FTC SAFEGUARDS RULE COMPLIANCE | PII PROTECTION | 24/7 MANAGED SERVICES | FIXED-PRICE DELIVERY | GSA APPROVED CONTRACTOR