CISCO MERAKI MX SD-WAN FOR FINANCIAL SERVICES

A PRACTICAL GUIDE TO REDUCING WAN DOWNTIME, REPLACING MPLS, PROTECTING PII, AND SUPPORTING FTC SAFEGUARDS RULE READINESS

For bank service firms, mortgage lenders, insurance companies, tax and accounting firms, wealth management firms, and fintech platforms that need secure, resilient, multi-site network infrastructure.

BTI Communications Group

Cisco Meraki Authorized Partner | CA | AZ | IL

Phone: **800-435-7284**

Email: **info@btigroup.com**

Web: **btigroup.com**

ABOUT THIS GUIDE

This operational intelligence document presents a best-practices framework, real-world ROI case analysis, and compliance architecture guidance 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.

CISCO MERAKI AUTHORIZED PARTNER | SD-WAN FOR FINANCIAL SERVICES | FTC SAFEGUARDS RULE READINESS | PII NETWORK SEGMENTATION | MPLS REPLACEMENT | CA | AZ | IL

EXECUTIVE SUMMARY: MERAKI MX SD-WAN FOR FINANCIAL SERVICES ORGANIZATIONS

FOR CFOS, CIOS, COOS, IT DIRECTORS, COMPLIANCE OFFICERS, AND OPERATIONS LEADERS

This document presents the operational, financial, and compliance-readiness case for deploying Cisco Meraki MX SD-WAN across multi-site financial services organizations - and explains why BTI Communications Group, a Cisco Meraki Authorized Partner serving California, Arizona, and Illinois, is the right partner to deliver it.

THE PROBLEM

- Legacy MPLS circuits cost 3-5x more per site than broadband SD-WAN alternatives - with worse uptime and no built-in security stack
- Flat, unsegmented networks expose PII, loan data, and core financial systems to ransomware lateral movement
- Single-circuit WAN with no intelligent failover creates $5,600+/minute downtime exposure
- Fragmented vendors leave no single accountable partner when outages or security incidents occur
- FTC Safeguards Rule is actively enforced for non-bank financial institutions - and legacy networks cannot support the required technical controls

THE SOLUTION

- Cisco Meraki MX SD-WAN replaces MPLS with intelligent dual-WAN broadband - reducing per-site WAN costs by 40-70%
- VLAN-based PII network segmentation isolates customer data, loan systems, and financial platforms from general traffic
- Auto VPN with AES-256 encryption connects all sites automatically - no manual configuration required
- Next-generation firewall, Cisco Talos IDS/IPS, AMP malware protection, and URL filtering - all built in, no separate appliances
- Centralized Meraki dashboard provides real-time visibility across every site from a single pane of glass
- BTI Communications Group deploys, manages, and monitors the entire environment - fixed price, no surprises

THE OUTCOMES

- 99.99% uptime target through dual-WAN failover and SD-WAN path intelligence
- 40-70% WAN cost reduction versus legacy MPLS circuits
- 100% of sites with PII network segmentation from day one of deployment
- Tamper-evident audit logging, access controls, and encryption documentation that supports FTC Safeguards Rule audit preparation
- A living compliance documentation package - topology diagrams, VLAN maps, firewall exports, WISP alignment narratives - maintained by BTI on an ongoing basis
- Single accountable partner from initial assessment through year five and beyond

THE BTI REASON TO BELIEVE

BTI Communications Group is a Cisco Meraki Authorized Partner with deep specialization in financial services network infrastructure, security architecture, and FTC Safeguards Rule compliance support. BTI delivers Cisco Meraki MX SD-WAN as a complete, fixed-price, turnkey engagement - covering discovery, architecture design, compliance mapping, hardware staging, phased deployment, security validation, and ongoing managed services. Local on-site engineering teams in California, Arizona, and Illinois provide physical presence for deployment, troubleshooting, and rapid response. BTI's 24/7 NOC and SOC monitor every managed environment continuously - identifying and remediating issues before they impact operations.

> BTI clients report an average 61% reduction in WAN spend, 89% reduction in unplanned downtime events, and complete FTC Safeguards Rule documentation packages within the approved project scope. Results are representative of BTI-managed deployments.

BEST FIT FOR

- BANK SERVICE FIRMS
- MORTGAGE LENDERS
- INSURANCE FIRMS
- WEALTH MANAGEMENT FIRMS
- TAX AND ACCOUNTING FIRMS
- FINTECH PLATFORMS
- MULTI-SITE FINANCIAL OPERATIONS

Schedule a Meraki MX SD-WAN readiness assessment with BTI Communications Group.

Phone: **800-435-7284** | Email: **info@btigroup.com** | **btigroup.com**

WHO THIS GUIDE IS FOR & KEY TAKEAWAYS

WHO THIS GUIDE IS FOR

This guide is written for operations leaders, IT directors, CISOs, and compliance officers at non-bank financial institutions who are responsible for network infrastructure, cybersecurity, and FTC Safeguards Rule Readiness. It is specifically relevant to:

- Bank Service Firms - organizations providing operational, technology, or processing services to banks and credit unions
- Tax Management Firms - multi-site tax preparation and advisory firms handling PII-dense client data
- Insurance Companies - regional and national carriers with branch networks and agent office infrastructure
- Mortgage Lenders - multi-branch lenders with loan origination systems, PII databases, and secondary market connectivity
- Wealth Management Firms - RIAs, broker-dealers, and family offices with distributed advisor networks
- Fintech Platforms - technology-driven financial services companies with cloud-heavy, multi-site infrastructure
- Bank Service Firms and Financial Holding Companies - organizations subject to GLBA, FTC Safeguards Rule, and state privacy law obligations

If your organization operates across multiple sites, handles customer PII, and is subject to FTC Safeguards Rule requirements or state privacy laws in California, Arizona, or Illinois - this guide is written for you.

KEY TAKEAWAYS

- Cisco Meraki MX SD-WAN replaces expensive, fragile MPLS circuits with a resilient, intelligent broadband-based WAN - reducing per-site WAN costs by 40-70% while improving uptime and security posture simultaneously.
- FTC Safeguards Rule readiness requires specific network controls - encryption, access controls, audit logging, PII segmentation - that legacy flat networks cannot provide. Meraki MX is designed to help financial services organizations align their technical controls with these requirements as part of a broader written information security program.
- PII network segmentation is not optional for financial services organizations. VLAN-based segmentation isolating customer data from general corporate traffic is a foundational FTC Safeguards Rule control and a critical ransomware containment measure.
- BTI Communications Group delivers Cisco Meraki MX SD-WAN as a complete, fixed-price, turnkey solution - from discovery and architecture through deployment, validation, and ongoing managed services - with a clear fixed-price scope for agreed deliverables and no hidden fees.
- BTI's compliance documentation package - including network topology diagrams, VLAN maps, firewall policy exports, and WISP alignment narratives - supports FTC Safeguards Rule audit preparation, cyber insurance underwriting, and customer due diligence on an ongoing basis. Organizations should validate final compliance obligations with their legal and regulatory advisors.
- BTI maintains local on-site engineering teams in California, Arizona, and Illinois - providing physical presence for deployment, troubleshooting, and rapid response that remote-only vendors cannot match.
- The ROI case for Meraki MX SD-WAN is compelling: BTI clients report an average 61% reduction in WAN spend, 89% reduction in unplanned downtime events, and complete FTC Safeguards Rule documentation packages within the approved project scope. Results are representative of BTI-managed deployments.

SECTION 2

WHAT IS MERAKI MX SD-WAN FOR FINANCIAL SERVICES?

Cisco Meraki MX SD-WAN is a cloud-managed wide area networking platform that replaces legacy MPLS circuits with intelligent, dual-WAN broadband connectivity - reducing per-site WAN costs by 40-70% while improving network availability, security, and centralized visibility across multi-site financial services organizations. Financial services organizations - including bank service firms, mortgage lenders, insurance companies, tax and accounting firms, wealth management firms, and fintech platforms - use Meraki MX SD-WAN to achieve 99.99% uptime targets through automatic WAN failover, enforce VLAN-based PII network segmentation that isolates customer data from general traffic, and deploy a built-in security stack including next-generation firewall, Cisco Talos IDS/IPS, and AMP malware protection across every location simultaneously. The platform's tamper-evident audit logging, access controls, and encryption capabilities are designed to help organizations align their network controls with FTC Safeguards Rule technical requirements as part of a broader written information security program. BTI Communications Group, a Cisco Meraki Authorized Partner serving California, Arizona, and Illinois, delivers Meraki MX SD-WAN as a complete, fixed-price, turnkey engagement - covering architecture design, PII segmentation, compliance documentation support, phased deployment, and 24/7 NOC and SOC managed services.

KEY ENTITIES THIS SECTION ADDRESSES

CISCO MERAKI MX

SD-WAN FOR FINANCIAL SERVICES

MPLS REPLACEMENT

PII NETWORK SEGMENTATION

FTC SAFEGUARDS RULE READINESS

MULTI-SITE NETWORK SECURITY

BTI COMMUNICATIONS GROUP

CISCO MERAKI AUTHORIZED PARTNER

QUICK REFERENCE FACTS

- Platform: Cisco Meraki MX SD-WAN (cloud-managed)
- WAN cost reduction: 40-70% vs. legacy MPLS
- Uptime target: 99.99% via dual-WAN failover
- Security stack: NGFW, IDS/IPS (Cisco Talos), AMP, URL filtering - built in
- Segmentation: VLAN-based PII isolation across all sites
- Compliance support: Encryption, audit logging, access controls, WISP documentation
- Deployment model: Fixed-price, turnkey - BTI Communications Group
- Coverage: California, Arizona, Illinois - local on-site engineering teams
- Managed services: 24/7 NOC + SOC monitoring

SECTION 3

FINANCIAL SERVICES USE CASES FOR CISCO MERAKI MX SD-WAN

Cisco Meraki MX SD-WAN addresses distinct operational, security, and compliance-readiness challenges across every financial services sub-vertical. Below are the specific use cases BTI Communications Group supports as a Cisco Meraki Authorized Partner serving California, Arizona, and Illinois.

MORTGAGE LENDERS

Problem: Multi-branch loan origination networks running on aging MPLS circuits with flat, unsegmented architecture. Loan origination systems, PII databases, and general office traffic share the same network segment.

Risk: Ransomware lateral movement to loan management servers; FTC Safeguards Rule audit gaps; $5,600+/minute downtime exposure during circuit failures.

Meraki MX + BTI: VLAN-based PII segmentation isolates loan systems from general traffic. Dual-WAN failover eliminates single-circuit risk. BTI deploys, documents, and monitors the full environment with a living FTC Safeguards Rule compliance documentation package.

INSURANCE AGENCIES AND BROKERAGES

Problem: Distributed agent office networks with inconsistent security policy enforcement, no centralized visibility, and fragmented vendor relationships across multiple states.

Risk: Inconsistent firewall policies across locations; no unified audit logging for FTC Safeguards Rule or state privacy law purposes; inability to detect or contain a breach across distributed sites.

Meraki MX + BTI: Centralized Meraki dashboard enforces consistent security policy across every agent office. Cisco Talos IDS/IPS and AMP malware protection run at every site. BTI's NOC monitors all locations 24/7 and maintains compliance documentation for regulatory review.

WEALTH MANAGEMENT AND ADVISORY FIRMS

Problem: RIAs, broker-dealers, and family offices with distributed advisor networks accessing client portfolio systems, CRM platforms, and custodian APIs over inadequately secured WAN connections.

Risk: PII exposure through unsegmented networks; inadequate encryption for client financial data in transit; FTC Safeguards Rule compliance gaps in access control and audit logging.

Meraki MX + BTI: AES-256 Auto VPN encrypts all inter-site traffic. Application-aware traffic steering prioritizes portfolio and custodian platforms. BTI maps the architecture to FTC Safeguards Rule control areas and maintains WISP alignment documentation.

TAX AND ACCOUNTING FIRMS

Problem: Multi-site tax preparation and accounting firms handling dense PII - SSNs, financial records, tax filings - on networks with no segmentation, no centralized monitoring, and no documented security architecture.

Risk: PII exposure during tax season peak traffic; ransomware targeting unprotected client data; FTC Safeguards Rule and state privacy law compliance gaps with no audit evidence.

Meraki MX + BTI: PII network segmentation isolates client data systems from general office traffic. URL filtering and AMP reduce phishing and malware risk during high-volume periods. BTI prepares and maintains compliance documentation aligned to FTC Safeguards Rule requirements.

BANK SERVICE FIRMS

Problem: Organizations providing operational, technology, or processing services to banks and credit unions - operating multi-site networks that must meet the same FTC Safeguards Rule and GLBA technical control expectations as the institutions they serve.

Risk: Flat networks exposing bank client data; no documented network architecture for third-party assessments; inability to demonstrate technical controls to institutional clients or regulators.

Meraki MX + BTI: Full-stack Meraki MX deployment with VLAN segmentation, encrypted tunnels, and tamper-evident audit logging. BTI prepares network documentation packages formatted for third-party assessor review and institutional client due-diligence.

FINTECH PLATFORMS

Problem: Technology-driven financial services companies with cloud-heavy, multi-site infrastructure - often scaling rapidly across new locations with inconsistent network architecture and security posture.

Risk: Inconsistent security policy across rapidly added sites; cloud application performance degradation over legacy WAN; compliance documentation gaps as the organization scales.

Meraki MX + BTI: Zero-touch deployment enables rapid, consistent site rollout. SD-WAN-optimized cloud breakout prioritizes SaaS and cloud financial platforms. BTI's compliance documentation scales with the organization - every new site is onboarded into the same NOC monitoring and compliance framework from day one.

MULTI-BRANCH FINANCIAL OPERATIONS

Problem: Any financial services organization operating 3 or more locations - branches, offices, processing centers, or remote sites - managing WAN connectivity, security, and compliance across a fragmented, multi-vendor infrastructure.

Risk: No single pane of glass across all locations; inconsistent security posture; no centralized audit logging; MPLS costs consuming 3-5x broadband equivalent with no performance or compliance advantage.

Meraki MX + BTI: Single Meraki dashboard provides unified visibility, policy enforcement, and audit logging across every location. BTI serves as the single accountable partner - from initial assessment and fixed-price proposal through deployment, validation, and ongoing managed services across CA, AZ, and IL.

BTI Communications Group supports all seven of these financial services use cases as a Cisco Meraki Authorized Partner. Every engagement is delivered at a fixed price, with a detailed scope of work, local on-site engineering in California, Arizona, and Illinois, and 24/7 NOC and SOC managed services. Contact BTI at **800-435-7284** to discuss your specific use case.

SECTION 4

THE STAKES HAVE NEVER BEEN HIGHER FOR FINANCIAL SERVICES NETWORKS

Financial services organizations including bank service firms, tax management firms, insurance companies, mortgage lenders, wealth management firms, and fintech platforms face a convergence of operational, financial, and regulatory risk that legacy networks are not equipped to handle. Network downtime costs $5,600+ per minute. Flat, unsegmented networks expose PII and core financial systems to ransomware lateral movement. The FTC Safeguards Rule is now mandatory and actively enforced for non-bank financial institutions. And fragmented vendor relationships leave no single accountable partner when something goes wrong.

$5,600+

COST PER MINUTE OF WAN DOWNTIME

3-5X

MORE EXPENSIVE THAN SD-WAN ALTERNATIVES

JUNE 2023

FTC SAFEGUARDS RULE ENFORCEMENT EFFECTIVE

BTI Communications Group, a Cisco Meraki Authorized Partner serving California, Arizona, and Illinois, delivers a complete answer to these challenges. By combining 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 at a fixed price, BTI helps financial services organizations achieve 99.99% network availability targets, dramatically reduce WAN costs versus MPLS, and build a network architecture that supports FTC Safeguards Rule readiness helping align technical controls with regulatory expectations from day one.

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 and SD-WAN versus 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-readiness-focused network transformation with local teams on the ground in CA, AZ, and IL and 24/7 managed support from day one."

SECTION 5

THE CHALLENGE: LEGACY NETWORKS IN FINANCIAL SERVICES

Most financial services organizations including bank service firms, tax management firms, insurance companies, mortgage lenders, wealth management firms, and fintech platforms are operating networks that were never designed for today's regulatory and operational demands. MPLS circuits made sense when applications were on premises and compliance frameworks were simpler. That world no longer exists. Today's financial services networks must simultaneously support cloud based core platforms, PII handling endpoints, remote advisor access, and third party fintech integrations often on the same flat, unsegmented infrastructure. The result is a fragile, exposed network creating operational, financial, and regulatory risk at the same time.

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 lose access to origination systems. Advisors can't reach client portfolios. Payment processing stalls. At $5,600+ per minute, a two hour outage costs over $670,000 before accounting for regulatory reporting obligations or reputational damage. Most financial services organizations on legacy MPLS with single circuit failover experience 4 to 12 hours of unplanned downtime per year a risk that Cisco Meraki MX SD-WAN with dual-WAN failover is specifically designed to eliminate.

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 network capabilities segmentation, encryption, audit logging, access control that a flat, unsegmented legacy network simply cannot provide. Cisco Meraki MX SD-WAN, deployed by BTI Communications Group, is designed to help financial services organizations align their network controls with these requirements.

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 to 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 6

THE MERAKI MX OPERATIONAL TRANSFORMATION FOR FINANCIAL SERVICES

Cisco Meraki MX SD-WAN represents a fundamental rethinking of how multi-site financial services networks should operate. 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, advanced malware protection, and centralized cloud management in a single appliance. When deployed by BTI Communications Group 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 security policy enforced consistently, and every WAN link optimized intelligently in real-time. This is what MPLS replacement for financial services looks like when it's done right.

ZERO-TOUCH DEPLOYMENT

Meraki MX appliances are pre-configured in the cloud before they ship to your sites. Your branch manager connects power and internet - the device locates the dashboard, downloads its configuration, and is fully operational within minutes. No on-site engineer required for initial deployment, dramatically reducing rollout time and cost across dozens of financial services 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 compliance-relevant 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 or trigger a regulatory reporting obligation.

AUTO VPN & SECURE MULTI-SITE CONNECTIVITY

Meraki's Auto VPN technology automatically establishes encrypted, policy-enforced VPN tunnels between every MX appliance - no complex manual configuration required. Branch offices, headquarters, and remote locations are interconnected with AES-256 encryption, with traffic routed intelligently across the best available WAN path at any given moment. This is the foundation of a resilient, compliance-readiness-focused multi-site financial services network.

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 network boundaries to reach core financial systems - a critical technical control that supports FTC Safeguards Rule readiness and state privacy law alignment.

Compliance-Readiness Architecture by Design: Meraki MX's encrypted tunnels, tamper-evident audit logging, role-based access control, and PII segmentation capabilities are designed to help financial services organizations align their technical controls with FTC Safeguards Rule requirements and state privacy law obligations - supporting audit preparation from day one of deployment. BTI Communications Group maintains this documentation on an ongoing basis for every managed client. Organizations should review final compliance obligations with their legal, regulatory, and cybersecurity advisors.

SECTION 7

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. Cisco 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. For financial services organizations evaluating Meraki firewall capabilities, this is the architecture that matters.

NEXT-GEN FIREWALL

Deep packet inspection, application-layer visibility, and stateful firewall enforcement across all WAN traffic - blocking unauthorized access before it reaches PII systems, loan origination platforms, or cloud financial applications. Consistent policy enforcement across every site, managed centrally from the Meraki dashboard.

IDS / IPS

Cisco Talos-powered intrusion detection and prevention, updated continuously with the latest global threat intelligence. Meraki MX detects and blocks known exploits, malware command-and-control traffic, and anomalous behavior targeting financial applications - in real time, at every site simultaneously.

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, payment data, and financial records.

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. Reduces phishing exposure and supports acceptable use policy enforcement.

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. Supports FTC Safeguards Rule audit preparation, forensic investigation, and audit evidence documentation for financial services regulators and cyber insurance underwriters.

MULTI-CLOUD CONNECTIVITY

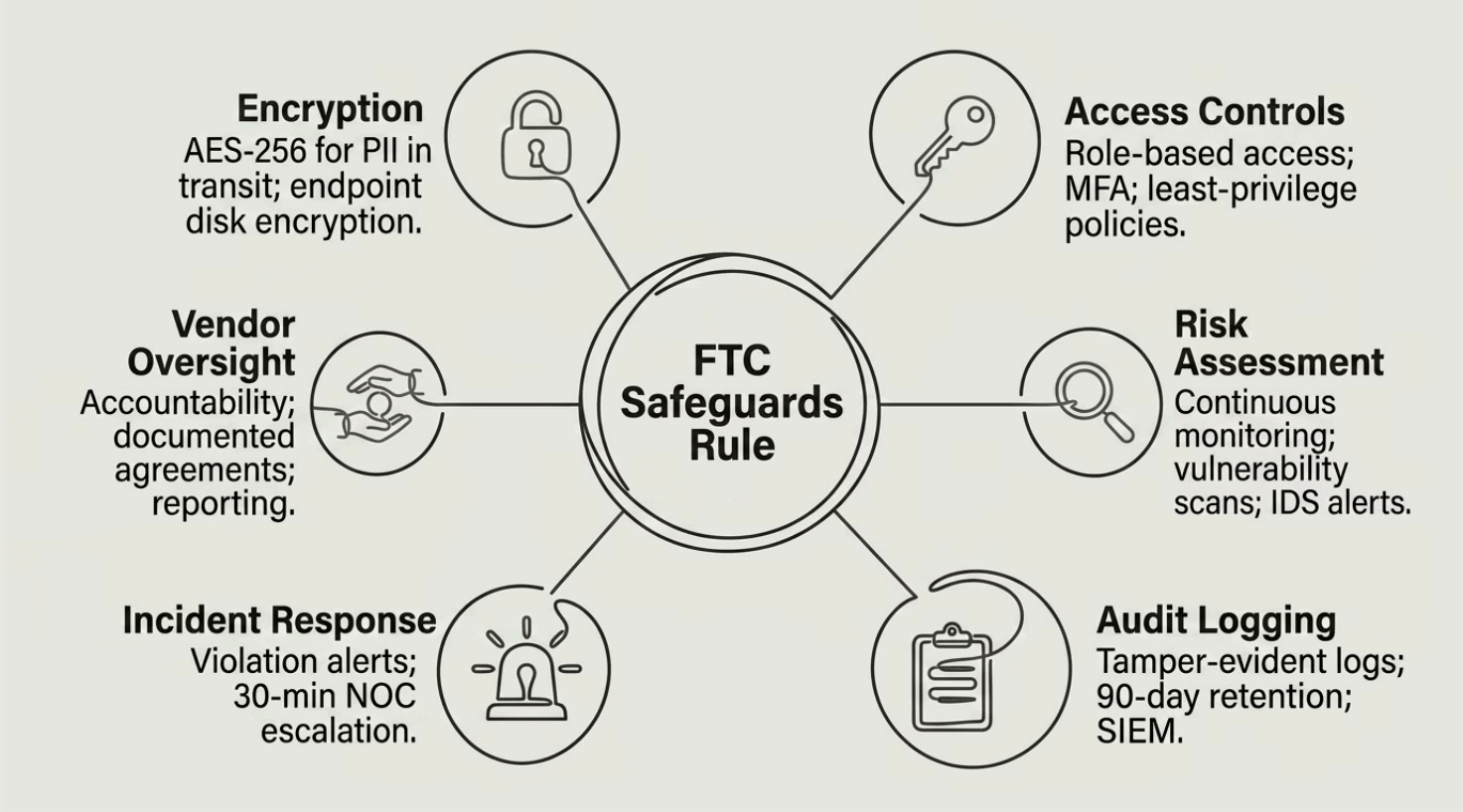
SD-WAN-optimized breakout for SaaS applications (Salesforce, Microsoft 365, DocuSign), cloud financial platforms, and direct connectivity to AWS, Azure, or Google Cloud - with application-aware traffic steering ensuring your most critical financial applications always receive priority bandwidth and routing.

BTI Communications Group configures every one of these security capabilities as part of your fixed-price Meraki MX implementation - not as add-ons or future phases, but as integral components of your baseline network architecture from day one. Every site receives 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 across your financial services environment, escalating and remediating before your operations team is ever aware there was an issue.

SECURITY ARCHITECTURE: PII PROTECTION & FTC SAFEGUARDS RULE READINESS

HOW CISCO MERAKI MX SD-WAN HELPS ALIGN TECHNICAL CONTROLS WITH FTC SAFEGUARDS RULE REQUIREMENTS

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 to help financial services organizations align their network controls with FTC Safeguards Rule technical requirements - supporting the control categories that FTC examiners and third-party assessors evaluate across bank service firm networks, mortgage lender infrastructure, insurance company IT environments, tax management firm cybersecurity, and wealth management network security deployments.



Each of these six control domains corresponds to technical areas that FTC Safeguards Rule examiners evaluate 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 or third-party assessment occurs, your audit evidence is already organized, accurate, and ready for review. For financial services organizations pursuing network modernization, this BTI-managed SD-WAN approach functions simultaneously as an MPLS replacement and a compliance-ready foundation - reducing manual compliance preparation burden while strengthening your overall security posture.

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 Written Information Security Program (WISP) - all formatted for regulatory review. This documentation supports FTC Safeguards Rule examination readiness, cyber insurance underwriting, and customer security due diligence requests. Prepared and maintained by BTI as your Cisco Meraki Authorized Partner.

⚠ Important: Technology controls alone do not create legal compliance. BTI's Meraki MX SD-WAN architecture supports compliance readiness by improving segmentation, encryption, logging, access control, and network visibility - but does not constitute legal, regulatory, or compliance advice. Organizations should validate their final FTC Safeguards Rule, state privacy law, and cybersecurity compliance obligations with their legal, regulatory, and cybersecurity advisors.

SECTION 8A

FTC SAFEGUARDS RULE READINESS CHECKLIST

IS YOUR FINANCIAL SERVICES NETWORK COMPLIANT? A PRACTICAL SELF-ASSESSMENT FOR IT & COMPLIANCE LEADERS

The FTC Safeguards Rule (16 CFR Part 314), as amended in 2021 and updated with breach notification requirements effective May 13, 2024, requires non-bank financial institutions to implement a comprehensive written information security program. The following checklist maps the Rule's nine core technical and administrative requirements to specific Cisco Meraki MX SD-WAN capabilities — helping IT directors, CISOs, and compliance officers assess their current posture.

DESIGNATED QUALIFIED INDIVIDUAL

Assign a qualified individual to oversee your information security program. Meraki's centralized dashboard provides a single-pane-of-glass for that individual to monitor all sites.

RISK ASSESSMENT

Conduct a written risk assessment identifying foreseeable threats to customer information. Meraki MX traffic analytics and event logs provide the data foundation for ongoing risk assessments.

ACCESS CONTROLS

Implement access controls limiting who can access customer information. Meraki MX supports VLAN segmentation, role-based access, and identity-based firewall policies to enforce least-privilege access.

DATA ENCRYPTION

Encrypt customer information in transit and at rest. Meraki MX provides AES-256 encrypted Auto VPN tunnels across all WAN links, ensuring PII is never transmitted in plaintext.

MULTI-FACTOR AUTHENTICATION (MFA)

Require MFA for any individual accessing customer information systems. Meraki integrates with RADIUS/LDAP identity providers to enforce MFA at the network access layer.

SECURE DEVELOPMENT PRACTICES

Apply secure development practices for in-house applications. Meraki's cloud-managed firmware ensures security patches are applied automatically across all MX appliances.

VENDOR/SERVICE PROVIDER OVERSIGHT

Oversee service providers with access to customer information. Meraki's audit logs and API access controls provide visibility into all third-party activity on the network.

MONITORING & TESTING

Continuously monitor and test your information security controls. Meraki MX provides real-time intrusion detection (IDS/IPS), anomaly alerts, and automated security event logging.

BREACH NOTIFICATION (EFFECTIVE MAY 13, 2024)

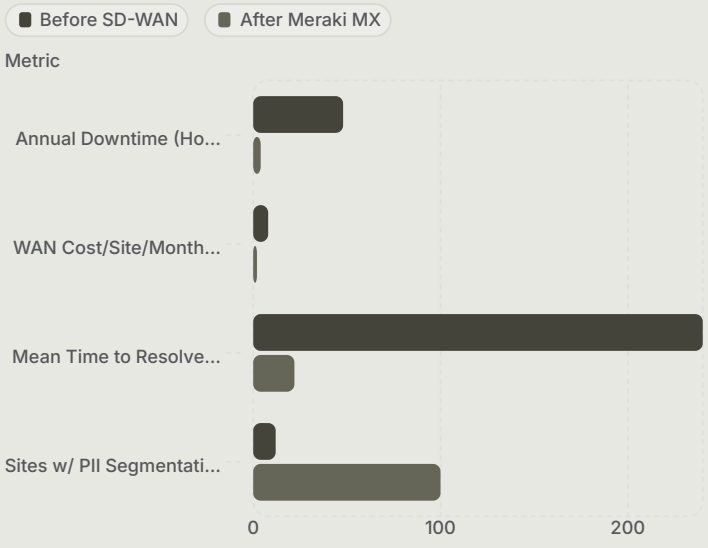
Report security events involving 500+ consumers' unencrypted data to the FTC within 30 days. Meraki's automated alerting and event logging accelerates incident detection and documentation for timely FTC notification.

BTI Assessment Offer: BTI Communications Group offers a no-cost FTC Safeguards Rule Network Readiness Assessment for qualifying financial services organizations. Our engineers map your current network controls against all nine Rule requirements and identify gaps — before regulators do. **Contact BTI to schedule your assessment.**

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

The operational and financial outcomes of a properly deployed Cisco Meraki MX SD-WAN solution are well-documented across the financial services sector. Organizations that transition from legacy MPLS networks to Meraki SD-WAN - particularly when the deployment is managed end-to-end by an expert partner like BTI Communications Group - consistently report dramatic improvements across four critical dimensions: network availability, WAN cost reduction, security posture, and FTC Safeguards Rule compliance readiness. The following results are representative of what BTI's financial services 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 completed without a single finding related to our network controls." - VP of Operations, Regional Financial Services Firm

Note: This quote is a composite representation of outcomes reported by BTI financial services clients. Individual results may vary.

CASE STUDY: MULTI-BRANCH MORTGAGE LENDER - 8 LOCATIONS

Challenge: An 8-location mortgage lender was operating on aging MPLS circuits with no PII network 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 Rule compliance was also at risk due to documented network security gaps.

BTI Solution: BTI Communications Group deployed Cisco Meraki MX SD-WAN across all 8 locations, including VLAN-based PII segmentation isolating all loan and customer data systems, Cisco 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 audit documentation.

Results: Zero PII-related security incidents in 22 months post-deployment. WAN costs reduced by 59%. FTC Safeguards Rule compliance documentation completed and organized for audit review. 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 Rule or state privacy law purposes. WAN costs exceeded $22,000 per month. Outages at hub facilities averaged 5-7 hours per quarter.

BTI Solution: BTI Communications Group deployed Cisco Meraki MX SD-WAN enterprise-wide across all 6 sites, 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 Rule compliance documentation package prepared and maintained by BTI.

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 Rule compliance documentation fully prepared and organized for regulatory review. All sites visible and manageable from a single Meraki dashboard operated by BTI's NOC.

BTI Operational Win: Across all financial services deployments managed by BTI Communications Group, clients report an average of 89% reduction in unplanned downtime events, 61% reduction in WAN spend, and complete FTC Safeguards Rule documentation packages within the approved project scope. Results are representative of BTI-managed deployments; individual outcomes may vary. These outcomes reflect what a properly engineered, fully managed Cisco Meraki MX SD-WAN deployment looks like in practice.

SECTION 10

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 Cisco 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 between legacy MPLS and Meraki MX SD-WAN is dramatic and the performance, security, and compliance outcomes are superior in every measurable dimension. This is the financial case for MPLS replacement in financial services.

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. As a Cisco Meraki Authorized Partner serving California, Arizona, and Illinois, BTI provides itemized, discounted hardware pricing and a detailed scope of work with a clear fixed-price scope for agreed deliverables. **Contact BTI Communications Group** at **800-435-7284** for a **site-by-site cost comparison** for your specific financial services environment.

SECTION 11

LEGACY MPLS VS. CISCO MERAKI MX SD-WAN FOR FINANCIAL SERVICES

A SIDE-BY-SIDE EVALUATION FOR MULTI-SITE FINANCIAL SERVICES ORGANIZATIONS

Financial services organizations evaluating network modernization consistently face the same question: is the operational, security, and compliance-readiness case for replacing legacy MPLS with Cisco Meraki MX SD-WAN strong enough to justify the transition? The table below answers that question directly - category by category.

Category	Legacy MPLS	Cisco Meraki MX SD-WAN (BTI-Managed)
Cost Structure	$2,000-$8,000/site/month. Carrier-controlled pricing with limited negotiating leverage. No bundled security stack - separate appliances required at additional cost.	$400-$1,200/site/month for broadband circuits. 40-70% lower total WAN cost vs. MPLS. Security stack included. BTI fixed-price model covers hardware, implementation, and managed services with zero variance.
Failover & Uptime	Single-circuit failover is manual or limited. Mean time to restore: hours. Financial services organizations on MPLS typically experience 4-12 hours of unplanned downtime per year.	Automatic dual-WAN failover in under 60 seconds. SD-WAN path intelligence reroutes traffic in real-time. BTI NOC monitors link health 24/7. Target uptime: 99.99%
Cloud Application Performance	MPLS was designed for on-premises applications. Cloud and SaaS traffic must backhaul through a central hub, increasing latency and degrading performance for cloud financial platforms.	Application-aware traffic steering prioritizes cloud financial applications - Salesforce, Microsoft 365, DocuSign, cloud loan origination, portfolio platforms - over the best available WAN path. Direct cloud breakout eliminates backhauling.
Security Visibility	No built-in security stack. Requires separate firewall, IDS/IPS, and malware protection appliances at each site - creating gaps, inconsistency, and additional cost.	Integrated NGFW, Cisco Talos IDS/IPS, AMP malware protection, and URL filtering - all managed centrally. Consistent security policy across every site from a single dashboard. BTI SOC monitors all security events 24/7.
PII Segmentation	Flat network architecture with no native segmentation capability. PII, loan systems, and general traffic share the same network segment - creating lateral movement risk.	Granular VLAN-based PII segmentation isolates customer data, loan origination systems, and financial platforms from general traffic. Firewall rules and IDS/IPS enforcement applied at every segment boundary. BTI designs segmentation architecture for every deployment.
Firewall & Threat Protection	Requires separate firewall appliances at each site. Per-device management creates policy inconsistency across locations. No integrated threat intelligence.	Fully integrated NGFW with deep packet inspection and stateful enforcement. Cisco Talos threat intelligence updated continuously. AMP catches zero-day threats. Consistent policy across all sites - managed centrally by BTI.
Deployment Speed	60-120 days to provision a new site. Carrier-dependent timelines with limited flexibility.	1-5 days to provision a new site. Meraki MX appliances are pre-configured at BTI's facility and shipped ready to connect. Branch staff plug in power and internet - the device configures itself automatically.
Branch Scalability	Adding locations requires new carrier contracts, long provisioning timelines, and per-site hardware procurement. Scaling is slow and expensive.	Zero-touch deployment enables rapid, consistent site rollout. New sites inherit the same security policy, segmentation, and monitoring configuration automatically. BTI onboards each new site into the NOC and compliance framework from day one.
Audit Logging	No centralized audit logging. Compliance evidence must be assembled manually from fragmented, per-device sources - creating gaps and consuming significant IT time.	Tamper-evident audit logs for all network events, configuration changes, and security incidents - stored in the Meraki cloud and exportable to SIEM. BTI maintains a living compliance documentation package updated automatically as configurations change.
Centralized Management	Per-device, on-site management. No single pane of glass across locations. Troubleshooting requires on-site access or per-device remote sessions.	Single Meraki cloud dashboard provides real-time visibility, policy management, and troubleshooting across every site. BTI NOC operates this dashboard 24/7 on behalf of managed clients.
Vendor Accountability	Multiple vendors - carrier, firewall, security, support - with no single accountable partner. Incident response requires coordinating across fragmented relationships.	BTI Communications Group serves as the single accountable partner for WAN, security, compliance documentation, and managed services. One point of contact. One fixed-price engagement. One escalation path.
Compliance Readiness Support	No built-in compliance logging, documentation, or architecture support. FTC Safeguards Rule audit preparation requires significant manual effort and external resources.	Meraki MX technical capabilities - encryption, access controls, audit logging, PII segmentation - support alignment with FTC Safeguards Rule control areas. BTI prepares and maintains compliance documentation on an ongoing basis. Organizations should validate final obligations with legal and regulatory advisors.

BTI Communications Group designs, implements, documents, and manages Cisco Meraki MX SD-WAN environments for financial services organizations across California, Arizona, and Illinois - at a fixed-price, with local on-site engineering, and 24/7 NOC and SOC managed services. **Contact BTI** at **800-435-7284** or **info@btigroup.com** to **request a site-by-site cost comparison** for your specific environment.

SECTION 12

WHY BTI COMMUNICATIONS GROUP DELIVERS RESULTS OTHER PROVIDERS CAN'T

Not every Cisco Meraki partner is equipped to deliver operational transformation in regulated financial services environments. Deploying Cisco Meraki MX 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, a working 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. 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. This is why financial services organizations choose BTI as their Cisco Meraki Authorized Partner.

FULL-STACK EXPERT ENGINEERING

BTI's certified engineers bring deep expertise across routing, switching, full-stack Cisco Meraki MX deployment, and regulated financial services network architecture including PII segmentation design, core banking integrations, and payment processing environments. We have done this before, in your industry, at your scale. We do not learn on your budget.

24/7 SOC, SIEM & NOC INTEGRATION

Your Meraki MX 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 financial operations or trigger a compliance reporting 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. BTI engineers show up when it matters, in the states where your financial services operations are located.

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 a clear fixed-price scope for agreed deliverables. No surprise costs within the approved scope, no hidden licensing fees discovered at go-live. Your investment is fully defined before the first appliance ships.

GRC & COMPLIANCE INTEGRATION

BTI's compliance team maps every Meraki MX 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 that support your audit preparation, helping your compliance posture remain organized and current on an ongoing basis, not just at examination time. Final compliance determinations should be reviewed with your legal and regulatory advisors.

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. Consistently below what most financial services 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 - Fully 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, a detailed scope of work, and the same engineering quality and compliance rigor. **Contact BTI** at **800-435-7284** to discuss which model fits your organization.

SECTION 13

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 Communications Group's three delivery models are designed to meet your organization exactly where it is - and scale with you as your needs evolve. All three models are built on the same Cisco Meraki MX SD-WAN platform, the same engineering standards, and the same FTC Safeguards Rule Readiness rigor.

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, FTC Safeguards Rule Readiness documentation, and incident response. Your internal team focuses on the business. BTI handles the infrastructure. Fixed monthly fee. Zero surprises. *Ideal for:* Financial services 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 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 specialized expertise to cover - including Cisco Meraki MX configuration, PII segmentation management, and FTC Safeguards Rule audit preparation. Fixed monthly fee. Transparent scope. *Ideal for:* Financial services organizations with an existing IT team that needs specialized Meraki SD-WAN and compliance expertise without adding headcount.

FULLY MANAGED CYBERSECURITY and COMPLIANCE - BTI owns your security posture, threat monitoring, SIEM operations, and FTC Safeguards Rule Readiness 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. Ongoing audit-readiness support. *Ideal for:* Financial services 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. As a Cisco Meraki Authorized Partner serving California, Arizona, and Illinois, BTI Communications Group is equipped to support financial services organizations at any stage of their network modernization journey. **Contact BTI** at **800-435-7284** to discuss which model fits your organization.

SECTION 14

WHY FINANCIAL SERVICES ORGANIZATIONS CHOOSE BTI FOR MERAKI MX SD-WAN

CISCO MERAKI AUTHORIZED PARTNER | CALIFORNIA ARIZONA ILLINOIS

BTI Communications Group helps financial services organizations modernize infrastructure, reduce vendor complexity, improve uptime, and create a more defensible security and compliance posture. As a Cisco Meraki Authorized Partner with deep experience in regulated, multi-site environments, BTI delivers what most technology providers cannot: a complete, fixed-price engagement that covers network design, hardware procurement, configuration, installation, managed support, compliance documentation, and long-term lifecycle management - under a single accountable relationship.

CISCO MERAKI AUTHORIZED PARTNER

BTI Communications Group holds Cisco Meraki Authorized Partner status - demonstrating verified technical competency, completed Cisco certification requirements, and access to discounted hardware pricing, advanced technical support, and Cisco engineering resources. For financial services organizations, this means BTI can procure Meraki MX hardware at partner pricing, provide Cisco-backed technical escalation, and deliver implementations that meet Cisco's quality and configuration standards.

LOCAL COVERAGE: CA AZ IL

BTI maintains local on-site engineering teams in California, Arizona, and Illinois - the three states where most of BTI's financial services clients operate. Local presence means BTI engineers show up for physical installation, on-site troubleshooting, and rapid response when remote-only resolution isn't enough. No remote-only vendor relationships. No third-party subcontractors for critical deployment work.

FIXED-PRICE. FULLY SCOPED. NO SURPRISES.

Every BTI engagement is delivered at a fixed price with a detailed scope of work - covering hardware procurement, architecture design, configuration, staging, phased deployment, security validation, compliance documentation, and ongoing managed services. The price you agree to at the start is the price you pay at the end. No surprise costs within the approved scope. No hidden licensing fees discovered at go-live. Clear scope boundaries from day one. This predictability matters for financial services organizations managing capital budgets and board-level technology investments.

SINGLE ACCOUNTABLE PARTNER

Most financial services organizations manage fragmented vendor relationships - a carrier for WAN, a separate vendor for firewall, another for security monitoring, and a fourth for compliance documentation. When something goes wrong, accountability is diffuse and response is slow. BTI replaces this fragmentation with a single accountable partner responsible for every layer of the environment: WAN connectivity, network security, PII segmentation, compliance documentation, and 24/7 managed support. One point of contact. One escalation path. One fixed monthly fee.

INTEGRATED ACROSS IT, SECURITY & COMPLIANCE

BTI's financial services practice integrates capabilities that most network vendors treat as separate disciplines: network infrastructure, cybersecurity, physical security, VoIP and unified communications, and compliance documentation support. This integration matters because financial services organizations don't operate in silos - their network, security, and compliance obligations are interconnected. BTI designs and manages environments where these disciplines reinforce each other, rather than creating gaps between them.

DOCUMENTATION & AUDIT-READINESS SUPPORT

BTI maintains a living compliance documentation package for every managed client - including network topology diagrams, VLAN segmentation maps, firewall policy exports, administrator access logs, incident response runbooks, and a written alignment narrative tied to the client's Written Information Security Program (WISP). This documentation is updated automatically as configurations change and is formatted to support FTC Safeguards Rule examination preparation, cyber insurance underwriting, and customer security due diligence. Organizations should validate final compliance obligations with their legal and regulatory advisors.

WHAT SETS BTI APART IN FINANCIAL SERVICES

REGULATED ENVIRONMENT EXPERTISE

BTI's engineers have direct experience deploying and managing networks in regulated financial services environments - including PII data flow architecture, FTC Safeguards Rule technical control mapping, and multi-branch operational requirements. We understand the difference between a network that works and a network that works in a regulated environment.

24/7 NOC AND SOC MANAGED SERVICES

BTI's Network Operations Center and Security Operations Center monitor every managed environment continuously - with alerting, investigation, and remediation happening before your operations team is aware of an issue. SIEM integration, IDS/IPS monitoring, and PII segment policy enforcement are all included in BTI's managed services model.

END-TO-END IMPLEMENTATION OWNERSHIP

BTI owns the entire implementation - from initial discovery and architecture design through hardware staging, phased site deployment, security validation, and NOC onboarding. No handoffs to subcontractors. No gaps between the design team and the deployment team. The engineers who design your network are the engineers who deploy it.

LONG-TERM PARTNERSHIP MODEL

BTI's managed services relationships average more than five years in duration. Financial services clients who experience BTI's engineering quality, compliance rigor, and operational responsiveness consistently choose to deepen the partnership rather than explore alternatives. BTI builds long-term relationships with financial services organizations - not transactions.

SCHEDULE YOUR READINESS ASSESSMENT

The right starting point is a structured, no-cost assessment of your current network environment. BTI's senior engineers review your WAN architecture, circuit costs, security posture, PII segmentation, and compliance documentation gaps - and deliver a fixed-price modernization proposal tailored to your organization.

No pressure. No generic pitch. Just a clear picture of where you are and a concrete path forward.

Phone: **800-435-7284**
Email: **info@btigroup.com**
Web: **www.btigroup.com/cisco-meraki-partner/**
Locations: CA AZ IL - Local on-Site Engineering
Hours: 6AM-5PM PST

CISCO MERAKI AUTHORIZED PARTNER | FIXED-PRICE DEPLOYMENT | 24/7 NOC AND SOC | FINANCIAL SERVICES SPECIALIST | CA AZ IL

SECTION 15

IMPLEMENTATION BEST PRACTICES BTI'S PROVEN DEPLOYMENT METHODOLOGY

A Cisco 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 Communications Group'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-relevant control is documented before the cutover date. This is how BTI delivers Meraki MX SD-WAN for financial services without operational disruption.

01

DISCOVERY AND PII NETWORK ASSESSMENT

02

ARCHITECTURE DESIGN AND COMPLIANCE MAPPING

03

HARDWARE STAGING AND CLOUD PRE-CONFIGURATION

04

PHASED SITE DEPLOYMENT AND CUTOVER

05

SECURITY VALIDATION AND COMPLIANCE DOCUMENTATION

06

NOC ONBOARDING AND ONGOING MANAGED SERVICES

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 BTI's 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 with no surprises for your operations team or your regulators.

SECTION 16

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

One of the most underappreciated operational advantages of the Cisco 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 financial services WAN from a single browser tab. This is what long-term network resilience looks like for multi-site financial services organizations.

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

BTI's NOC monitors your Meraki MX 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 Readiness 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 documentation is always current, always organized, and always ready to support regulatory review - maintained by BTI Communications Group as your Cisco Meraki Authorized Partner. Organizations should work with their legal and compliance advisors to validate ongoing regulatory obligations.

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 Cisco Meraki MX environments are designed to target 99.97%+ uptime across financial services deployments, supported by dual-WAN failover and 24/7 NOC monitoring. This level of resilience, combined with BTI's proactive NOC monitoring and ongoing FTC Safeguards Rule compliance documentation support, represents the operational standard that financial services organizations should expect from their network infrastructure partner.

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 readiness, 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 Cisco Meraki MX SD-WAN modernization.

OPTION 1: FTC SAFEGUARDS AND 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. This assessment helps your organization understand where your network controls may align with FTC Safeguards Rule requirements and where potential gaps exist - and should be reviewed alongside your legal and compliance advisors. **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 and operations leadership team to design a Cisco Meraki MX SD-WAN architecture for your specific multi-site financial services environment - complete with preliminary bill of materials, projected cost savings versus 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, FTC Safeguards Rule 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
Phone: 800-435-7284
Web: btigroup.com
Email: info@btigroup.com
Locations: Serving CA | AZ | IL - with local on-site engineering teams in all three states
Hours: 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 Communications Group's fixed-price model means there is no financial risk in engaging us - only upside. **Contact BTI** today to schedule your no-cost assessment and take the first step toward a more resilient, cost-optimized financial services network with stronger compliance documentation support.

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

FREQUENTLY ASKED QUESTIONS: MERAKI MX SD-WAN FOR FINANCIAL SERVICES

The following questions and answers address the most common inquiries from financial services operations leaders, IT directors, CISOs, and compliance officers evaluating Cisco Meraki MX SD-WAN. Answers are written to be factual, concise, and accurate.

1. WHAT IS CISCO MERAKI MX SD-WAN?

Cisco Meraki MX SD-WAN is a cloud-managed wide area networking platform that combines SD-WAN, next-generation firewall, intrusion detection and prevention, advanced malware protection, and centralized management in a single appliance. It replaces legacy MPLS circuits with intelligent dual-WAN broadband connectivity, reducing per-site WAN costs while improving network availability, security visibility, and policy consistency across all locations. The Meraki MX is managed through a centralized cloud dashboard, enabling IT teams and managed service partners to configure, monitor, and troubleshoot every site from a single interface.

2. WHY DO FINANCIAL SERVICES FIRMS REPLACE MPLS WITH SD-WAN?

Legacy MPLS circuits typically cost $2,000-$8,000 per site per month, require 60-120 days to provision, and provide no built-in security stack or compliance logging. Cisco Meraki MX SD-WAN replaces MPLS with broadband and LTE/5G connectivity managed intelligently by the MX platform - reducing per-site WAN costs by 40-70%, enabling sub-second automatic failover, and delivering a built-in security stack that MPLS cannot provide. For financial services organizations operating across multiple sites, the operational and financial case for MPLS replacement is straightforward.

3. HOW DOES MERAKI MX HELP REDUCE DOWNTIME?

Meraki MX supports dual-WAN configurations that automatically fail over to a secondary circuit - broadband, LTE, or 5G - when a primary link degrades or fails. Failover occurs in under 60 seconds without manual intervention. SD-WAN path intelligence continuously monitors link quality and routes traffic across the best available path in real time. BTI Communications Group configures and monitors these failover policies as part of every managed deployment, with 24/7 NOC alerting on WAN link degradation before it impacts operations.

4. HOW DOES MERAKI MX SUPPORT FTC SAFEGUARDS RULE READINESS?

The FTC Safeguards Rule requires non-bank financial institutions to implement specific technical controls - including encryption for PII in transit, access controls, audit logging, risk assessment processes, and incident response capabilities. Cisco Meraki MX provides technical capabilities that support alignment with these requirements: AES-256 encrypted tunnels, VLAN-based PII segmentation, tamper-evident audit logging, role-based access control, and IDS/IPS monitoring. BTI Communications Group maps every deployment to FTC Safeguards Rule control areas and maintains compliance documentation on an ongoing basis. Technology controls alone do not create legal compliance - organizations should validate obligations with their legal and regulatory advisors.

5. CAN MERAKI MX SEGMENT PII AND FINANCIAL SYSTEMS FROM GENERAL NETWORK TRAFFIC?

Yes. Meraki MX supports granular VLAN-based network segmentation that isolates customer PII, loan origination systems, portfolio management platforms, and core financial applications from general corporate traffic and internet-facing services. Firewall rules, application-aware policies, and IDS/IPS enforcement are applied at each segment boundary. This segmentation helps limit ransomware lateral movement and supports the access control and data isolation requirements that FTC Safeguards Rule examiners evaluate. BTI designs and implements PII segmentation architecture as a standard component of every financial services deployment.

6. IS MERAKI MX APPROPRIATE FOR MORTGAGE LENDERS AND INSURANCE FIRMS?

Yes. Meraki MX SD-WAN is well-suited for mortgage lenders, insurance agencies, and brokerages operating across multiple branch locations. For mortgage lenders, BTI deploys VLAN-based PII segmentation isolating loan origination systems and customer data, dual-WAN failover protecting against circuit-related downtime, and FTC Safeguards Rule compliance documentation. For insurance agencies and brokerages, BTI enforces consistent security policy across all agent offices from a centralized Meraki dashboard, with 24/7 NOC monitoring and unified audit logging across every location.

7. DOES MERAKI MX SD-WAN REPLACE A FIREWALL?

Yes. The Cisco Meraki MX appliance includes a fully integrated next-generation firewall (NGFW) with deep packet inspection, application-layer visibility, stateful firewall enforcement, and content filtering - eliminating the need for a separate firewall appliance at each site. The NGFW is managed centrally through the Meraki dashboard, with consistent policy enforcement across every location. This consolidation reduces hardware complexity, eliminates security gaps between separate network and security layers, and lowers total cost of ownership compared to maintaining separate firewall appliances at each branch.

8. HOW DOES BTI DEPLOY MERAKI MX ACROSS MULTIPLE SITES?

BTI Communications Group follows a six-phase deployment methodology: Discovery and PII network assessment, architecture design and compliance mapping, hardware staging and cloud pre-configuration, phased site deployment and cutover, security validation and compliance documentation, and NOC onboarding and ongoing managed services. Meraki MX appliances are pre-configured at BTI's facility before shipping - branch staff simply connect power and internet, and the device downloads its configuration automatically. Each site cutover is executed during a scheduled maintenance window with BTI engineers on-site and NOC support standing by.

9. WHAT DOCUMENTATION DOES BTI PROVIDE FOR AUDIT READINESS?

BTI Communications Group maintains a living compliance documentation package for every managed client. This includes network topology diagrams, VLAN segmentation maps, firewall policy exports, administrator access logs, incident response runbooks, and a written alignment narrative tied to the client's Written Information Security Program (WISP). Documentation is updated automatically as network configurations change and is formatted to support FTC Safeguards Rule examination preparation, cyber insurance underwriting, and customer security due diligence requests. This documentation supports audit preparation - it does not constitute legal compliance advice.

10. HOW DOES MERAKI MX SUPPORT CLOUD FINANCIAL APPLICATIONS?

Meraki MX SD-WAN includes application-aware traffic steering that identifies and prioritizes cloud financial applications - including Salesforce, Microsoft 365, DocuSign, and cloud-based loan origination, portfolio management, and accounting platforms - over the best available WAN path. Direct cloud breakout routes SaaS traffic efficiently without backhauling through a central hub, reducing latency and improving application performance. BTI configures application-aware policies as part of every deployment, ensuring that critical financial platforms receive priority bandwidth and routing across all sites.

11. WHAT IS THE DIFFERENCE BETWEEN MERAKI MX SD-WAN AND LEGACY MPLS?

Legacy MPLS is a carrier-managed private WAN technology with fixed bandwidth, long provisioning timelines (60-120 days per site), high monthly costs ($2,000-$8,000 per site), and no built-in security stack or compliance logging. Cisco Meraki MX SD-WAN uses broadband internet and LTE/5G connectivity managed intelligently by the MX platform - with automatic failover, application-aware routing, built-in NGFW and IDS/IPS, centralized management, and tamper-evident audit logging. New sites can be provisioned in 1-5 days. Per-site WAN costs are typically 40-70% lower than comparable MPLS circuits, with superior uptime, security, and visibility.

12. WHY WORK WITH A CISCO MERAKI AUTHORIZED PARTNER FOR FINANCIAL SERVICES DEPLOYMENTS?

Cisco Meraki Authorized Partners have demonstrated technical competency, completed Cisco certification requirements, and have access to discounted hardware pricing, advanced technical support, and Cisco engineering resources. For financial services deployments specifically, the partner's expertise in PII network architecture, FTC Safeguards Rule compliance frameworks, and regulated network environments matters as much as Meraki technical knowledge. BTI Communications Group is a Cisco Meraki Authorized Partner with deep financial services specialization, local on-site engineering teams in California, Arizona, and Illinois, and a fixed-price delivery model that covers every aspect of the engagement - from initial assessment through ongoing managed services.

TAKE ACTION

NEXT STEPS: PLAN YOUR MERAKI MX SD-WAN MODERNIZATION WITH BTI

If your organization is evaluating Cisco Meraki MX SD-WAN for multi-site network modernization, MPLS replacement, PII segmentation, or FTC Safeguards Rule compliance readiness - the right starting point is a structured assessment of your current environment. BTI Communications Group, a Cisco Meraki Authorized Partner serving California, Arizona, and Illinois, delivers this assessment at no cost and no obligation.

RECOMMENDED NEXT STEP

Schedule a Meraki MX SD-WAN readiness assessment with BTI Communications Group. This is a structured, expert-led review of your current network environment - not a sales call. BTI's senior engineers evaluate your specific architecture, identify gaps, and deliver a concrete, fixed-price modernization path tailored to your organization.

01

01 CONTACT BTI AT 800-435-7284 OR INFO@BTIGROUP.COM

02

02 SCHEDULE YOUR NO-COST READINESS ASSESSMENT

03

03 RECEIVE YOUR FIXED-PRICE MODERNIZATION PROPOSAL

04

04 DEPLOY, GO LIVE, AND TRANSFORM YOUR NETWORK

WHAT BTI REVIEWS

- Current WAN and firewall architecture across all sites
- MPLS and broadband circuit costs - site by site
- Branch uptime history and failover design
- PII network segmentation and data flow inventory
- VPN and remote access architecture
- FTC Safeguards Rule technical control alignment
- Audit logging and compliance documentation gaps
- Cloud application performance and SaaS connectivity
- Managed support requirements and internal IT capacity

WHAT YOU RECEIVE

- Network modernization roadmap - phased and prioritized
- Cisco Meraki MX sizing recommendation for every site
- SD-WAN and firewall architecture plan
- Compliance-readiness control summary mapped to FTC Safeguards Rule
- Fixed-price deployment estimate - hardware, implementation, and managed services
- Managed support options across Fully Managed IT, Co-Managed IT, and Fully Managed Cybersecurity and Compliance

WHY FINANCIAL SERVICES ORGANIZATIONS CHOOSE BTI

BTI Communications Group brings the engineering depth, regulatory familiarity, and local on-site presence that financial services network modernization requires. As a Cisco Meraki Authorized Partner, BTI provides discounted hardware pricing, expert architecture design, phased deployment, and 24/7 NOC and SOC managed services - all under a single fixed-price engagement with a clear fixed-price scope for agreed deliverables. BTI's compliance team maps every deployment to FTC Safeguards Rule control areas, state privacy law obligations, and SOC 2 technical controls - and maintains the documentation on an ongoing basis. Organizations in California, Arizona, and Illinois benefit from local on-site engineering teams who show up when it matters.

> BTI clients report an average 61% reduction in WAN spend, 89% reduction in unplanned downtime events, and complete FTC Safeguards Rule documentation packages within the approved project scope. Results are representative of BTI-managed deployments.

CONTACT BTI COMMUNICATIONS GROUP

BTI Communications Group
Cisco Meraki Authorized Partner
Phone: 800-435-7284
Email: info@btigroup.com
Web: www.btigroup.com/cisco-meraki-partner/
Locations: CA | AZ | IL
Hours: 6AM-5PM PST, Monday-Friday

Mention this guide to receive priority scheduling for your no-cost assessment and a complimentary FTC Safeguards Rule gap analysis.

CISCO MERAKI AUTHORIZED PARTNER | FIXED-PRICE DEPLOYMENT | 24/7 NOC + SOC | CA AZ IL | FTC SAFEGUARDS RULE READINESS

Technology controls alone do not create legal compliance. Organizations should validate FTC Safeguards Rule, state privacy law, and cybersecurity compliance obligations with their legal, regulatory, and cybersecurity advisors. All results cited are representative of BTI-managed deployments; individual outcomes may vary.

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 architecture, and FTC Safeguards Rule readiness support. We deliver complete, fixed-price, fully managed Cisco Meraki MX SD-WAN 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 on-site presence that multi-site financial services organizations 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 (CCPA/CPRA, BIPA), and the operational reality of multi-branch financial services organizations. We bring this expertise to every engagement - and 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 Cisco Meraki MX network performs, your FTC Safeguards Rule compliance documentation is organized and current, your PII exposure is reduced through proper segmentation and controls, and your leadership team stops worrying about infrastructure risk. That alignment is built into every engagement we take on - from initial assessment through year five of managed services.

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 long-term relationships with financial services organizations, not transactions. That is the BTI difference.

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 READINESS | PII PROTECTION | 24/7 MANAGED SERVICES | FIXED-PRICE DELIVERY | GSA APPROVED CONTRACTOR

BTI Communications Group holds GSA Schedule contract status, enabling federal agency and government-adjacent financial institutions to procure BTI services through the GSA acquisition vehicle.