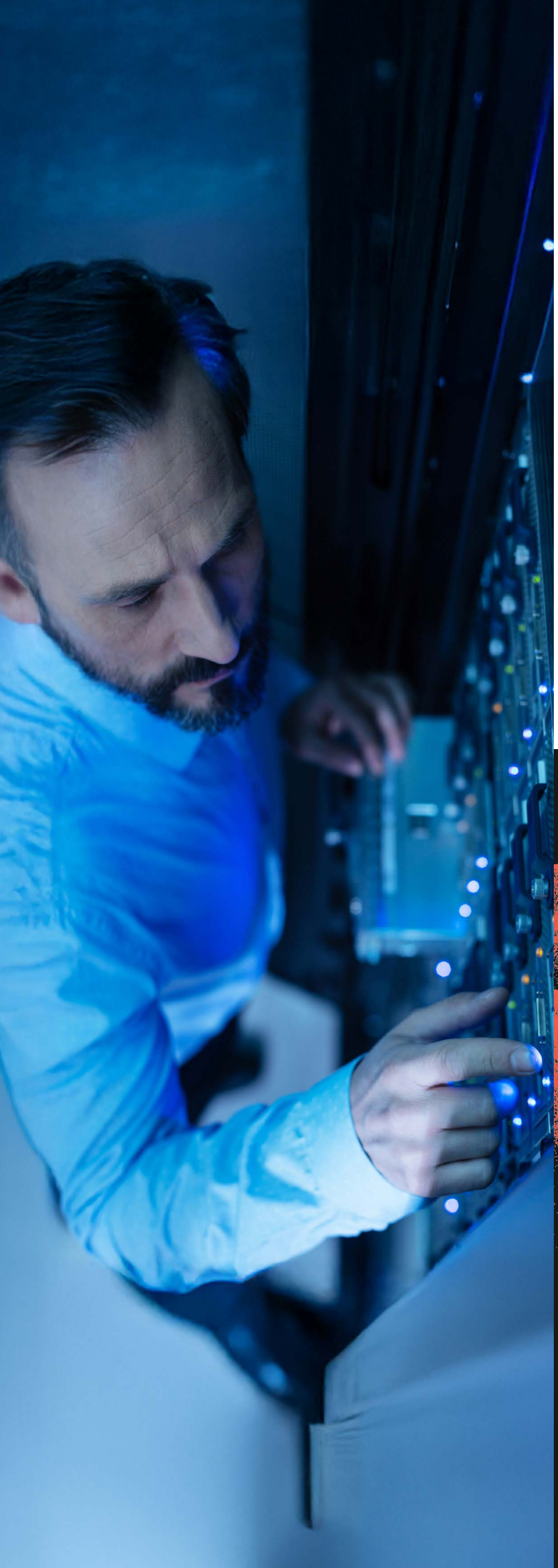


LTM | cisco

WHITEPAPER

Beyond the Perimeter: Achieving Seamless, Secure Access with Cisco and LTM

How Cisco and LTM Simplify Security for the Hybrid Enterprise

Secure Service Edge (SSE) for the Hybrid Enterprise

This white paper examines how Cisco® and LTM help organizations modernize security for a cloud-first, hybrid-work world. It explores the challenges of fragmented, perimeter-based defenses and explains how SSE architectures unify networking and security to simplify operations, strengthen visibility, and align protection with Zero Trust principles.

Your Network has Evolved So Your Security Needs to Catch Up

Hybrid work, cloud adoption, and digital transformation have redefined how business operates. Yet many organizations still rely on legacy, perimeter-based security models built for a time when users, applications, and data lived inside the same walls. Today, your users work from everywhere, your applications span multiple clouds, and your data flows across countless endpoints. The perimeter is fluid now but many of the tools and strategies protecting it remain unchanged.

This white paper is written for Security and IT leaders facing a familiar challenge: how to protect a distributed, hybrid workforce without increasing complexity or cost.

If you are a business or technical decision maker—CISO, CIO, IT Director, or Security Architect—you are likely re-evaluating how to modernize your defenses for today's realities:

- Users and devices connect from anywhere
- Applications live in the cloud, not the data center
- Threats evolve faster than teams can respond

The Question is No Longer Whether to Modernize, But How:

- Which approach reduces risk without sacrificing agility?
- Which investments deliver measurable value without adding operational burden?
- Which partners can help you make the shift safely and at your own pace?



Cisco and LTM believe the answer begins with rethinking the foundation.

Rather than protecting what used to be your network, you must secure the way people work now. That means converging network and security functions into a single, cloud-delivered architecture built on Zero Trust principles in which access is contextual, policies are unified, and protection follows the user everywhere.

In the pages that follow, you'll learn:

- What market forces are reshaping enterprise security and creating pressure for change
- Why traditional models can no longer keep pace with cloud and hybrid work
- How Cisco and LTM SSE solutions that combine Cisco technology with LTM's integration and operational expertise to simplify management, strengthen visibility, and support Zero Trust at scale

This paper provides a practical view of the decisions ahead, the trade-offs to consider, and how a unified Cisco and LTM approach can help you build a resilient, future-ready security foundation.

The Environment Driving Change and the Challenges It Creates

The Way You Work—and the Way Attackers Operate—Have Changed Permanently

Your users now connect from everywhere, including home offices, airports, branch locations, and customer sites. They access a mix of public cloud, Software as a Service (SaaS), and private applications across multiple devices and networks. The traditional network perimeter—once defined by firewalls and fixed boundaries—no longer exists. This new reality requires a different approach to delivering, managing, and experiencing security. For Security leaders, this shift has created a growing gap between how people work and how security is delivered.

Work Without Boundaries

Hybrid work is now the standard. Employees and contractors move between office, home, and public networks multiple times per day. Each transition introduces another potential point of exposure. Traditional, hardware-based architectures built for static environments cannot keep up with this always-on, anywhere-access model.

Security policies that were designed for a single location no longer align with the way you operate. This misalignment increases risk, adds administrative effort, and slows down transformation initiatives.

Cloud First, Visibility Last

Most organizations have adopted multi-cloud and SaaS strategies to improve agility and scalability. However, these architectures have outpaced traditional security tools. Solutions designed for on-premises networks were never meant to protect data moving directly between users and cloud applications. Traffic now bypasses centralized inspection points, creating blind spots where threats can hide and data can be lost.

Legacy VPNs and firewalls cannot protect traffic that no longer passes through the corporate network. They lack the flexibility, context awareness, and scalability required for today's distributed environments.

Complexity Crisis

In an effort to close these gaps, many organizations have layered on more tools and vendors.

The result is complexity without clarity. On average, organizations manage 60 to 70 separate security tools across 10 to 15 different vendors, each with its own policies and management console.[1]

Too Many Dashboards Lead to Too Little Visibility

Only 36 percent of organizations say they are very confident that their controls work as intended.[2] Instead of improving security, tool sprawl creates inconsistencies, drives up operational cost, and slows your team's ability to respond.

Expanding and Exploited Attack Surface

Attackers have evolved alongside this complexity. They target remote connections, unmanaged devices, and misconfigured cloud services. Meanwhile, the average cost of a U.S. data breach is now US$4.45 million, and 73 percent of organizations expect disruption from a cyber incident within two years.[3], [4] Similarly, the average cost of a data breach in India reached an all-time high of US$2.2 million in 2024.[5]

Architectures Based On Implicit Trust Cannot Defend Against Today's Persistent Threats

Once an attacker gains access, lateral movement and privilege escalation are relatively simple and expensive.

[1] Gartner, "Simplify Cybersecurity with a Platform Consolidation Framework," Dionisio Zumerle & John Watts, 26 March 2024 (Research ID G00781423)
[2] Spiceworks, "Security Vendor Consolidation: Why Now and What's the Benefit?"
[3] Statista: Average cost incurred by a data breach in the U.S., 2024
[4] Cisco Cybersecurity Readiness Index, 2024
[5] IBM Report: Escalating Data Breach Disruption Pushes Average Cost of a Data Breach in India to All-Time High of INR 195 Million in 2024

When Access Becomes a Barrier

Traditional VPNs were built for connectivity, not for context. They grant broad network access instead of enforcing per-application permissions, expanding the potential impact of compromised credentials. Centralized VPN gateways also introduce latency and degrade user experience.

When access slows productivity, users find workarounds. Research shows that 67 percent of employees have ignored cybersecurity policies at least once because compliance felt cumbersome.[6] Each shortcut introduces risk and underscores a fundamental reality: usability is now a security requirement.

Fragmentation Fuels Risk

Multiple logins, repetitive multifactor authentication (MFA) prompts, and inconsistent user experiences create what many describe as "security fatigue." When employees turn to unsanctioned applications to stay productive, they create a hidden shadow IT ecosystem. These fragmented experiences lead to fragmented defenses that undermine visibility, data governance, and Zero Trust alignment.

Inconsistent Policy and Governance.

As workloads move between SaaS, Infrastructure as a Service (IaaS), and on-premises systems, policies applied at the perimeter no longer reach the data they are meant to protect. Security teams face policy drift, different configurations across regions and platforms that lead to unmanaged risk and audit failures. Without a centralized governance framework, maintaining compliance with standards such as GDPR, HIPAA, or ISO 27001 becomes increasingly difficult.

Escalating Threats, Shrinking Resources

The hybrid attack surface continues to expand while qualified security professionals remain in short supply. 54 percent of organizations experienced a cybersecurity incident in the past year, and 73 percent of them expect another within two years.[7]

> On-premise-based solutions don't really cut it—you don't necessarily want a firewall installed in every location.
>
> — Sumesh Unnikrishnan Nair
> Associate Vice President, LTM

Maintaining 24×7 coverage and manual tuning across dozens of systems is unsustainable. As LTM's Sumesh notes, "We actually have nine Cyber Defense Resiliency Centers, but enterprises often cannot match that level of 24×7 coverage internally."

[6] Harvard Business Review, "Why Employees Violate Cybersecurity Policies," 2022
[7] Cisco Cybersecurity Readiness Index, 2024

The Cost and Agility Trap

Each legacy system introduces its own licensing, maintenance, and staffing costs. Hardware refresh cycles for firewalls and VPNs drain resources that could otherwise support innovation. As the environment grows more distributed, managing multiple vendors and redundant tools has become financially unsustainable.

Increasingly Clear Economics

Maintaining disconnected systems now costs more than modernizing. Every dollar spent maintaining legacy infrastructure is a dollar not spent improving resilience, user experience, or business agility.

Perfect Storm for Change

Today's security challenges are converging:

- Users everywhere and security still tied to data centers
- Dozens of overlapping tools and no single source of truth
- Rising breach costs and limited skilled staff
- Frustrated users and inconsistent experiences

Without modernization, security remains the obstacle to transformation rather than its foundation

The pressures of hybrid work, multicloud adoption, and escalating threats have pushed traditional models to their breaking point, creating an urgent need to rethink enterprise security from the ground up.

Traditional Approaches and why They Fall Short

For Decades, Security Revolved Around Fixed Perimeters and Trusted Networks.

Organizations built strategies around firewalls, VPNs, and network access controls that protected users and data within well-defined boundaries. These models worked when work was predictable. But as users, devices, and applications moved outside the data center, these once-reliable approaches have become sources of complexity and cost.

Perimeter-Centric Security Models

Early enterprise security depended on centralized inspection at the corporate edge, including firewalls, proxies, and VPN gateways in data centers. This model offered proven stability and mature practices for office-bound employees and predictable network flows. However, the perimeter has dissolved. In addition, backhauling traffic from branch offices and remote workers adds latency and cost, while siloed network and security operations cause policy drift.

VPN-Based Remote Access

VPNs extended secure connectivity to remote users through encrypted tunnels.

Their advantages—simplicity, ubiquity, and low cost—made VPNs a default choice for many years. Yet VPNs provide network-wide rather than application-specific access, violating Zero Trust principles. They create single choke points that can limit scalability and degrade user experiences. Meanwhile, if credentials are compromised, attackers can move freely across the network, and expanding concentrator capacity becomes a perpetual expense.

Point Solutions and Multivendor Toolsets

To adapt to hybrid work, many organizations layered specialized tools such as secure web gateway (SWG), cloud access security broker (CASB), data loss prevention (DLP), and MFA from different vendors. This "best-of-breed" approach delivered depth in isolated domains but introduced serious side effects: tool sprawl, integration complexity, and rising burnout among defenders.



In one study, over one third (36 percent) of IT professionals cite excessive complexity.[8] In another study, 43 percent say they struggle with compatibility issues.[9] In addition, nearly 83 percent of IT security professionals say burnout contributes to data breaches.[10] Siloed systems hinder threat correlation and drive high operational cost. As a result, fragmentation overwhelms teams instead of improving protection.

Do-It-Yourself Modernization

Some organizations attempt modernization internally, integrating CASB, SWG, zero trust network access (ZTNA), and DLP tools on their own. While this practice helps to preserve control and leverage existing investments, it introduces steep learning curves and high risk of misconfiguration. Furthermore, scaling global performance and maintaining 24×7 operations demand expertise and automation that internal teams often lack.

> **Enterprises can avoid trial-and-error by leveraging LTM's proven blueprints and global engineering teams.**
>
> — Sumesh Unnikrishnan Nair
> Associate Vice President, LTM

Traditional architectures provided the foundation for enterprise security, but not for today's distributed, cloud-first world. Their inherent fragmentation, operational overhead, and inconsistent user experience have created a need for something simpler, more adaptive, and more unified.



[8] Kaspersky, "Over Half of Security Experts Overwhelmed Managing Cybersecurity Tools," 2023
[9] Xalient, "Too Many Tools, Too Little Control," 2023
[10] Devo, "IT Security Professionals Say Burnout Causes Data Breaches," 2023

The Cisco and LTM approach

Modernizing Security Through a Managed SSE

Cisco and LTM are redefining enterprise security for the cloud-first era. Together, they deliver an SSE solution that unifies security and network access into a single, cloud-managed platform built on Zero Trust principles and optimized for hybrid work. This joint approach replaces hardware-heavy, siloed architectures with a cloud-delivered, policy-driven model that adapts dynamically to users, devices, and data wherever people work and wherever data resides.

Figure 1 below shows the Cisco secure access platform and the LTM differentiated services provided in the Managed SSE offering.

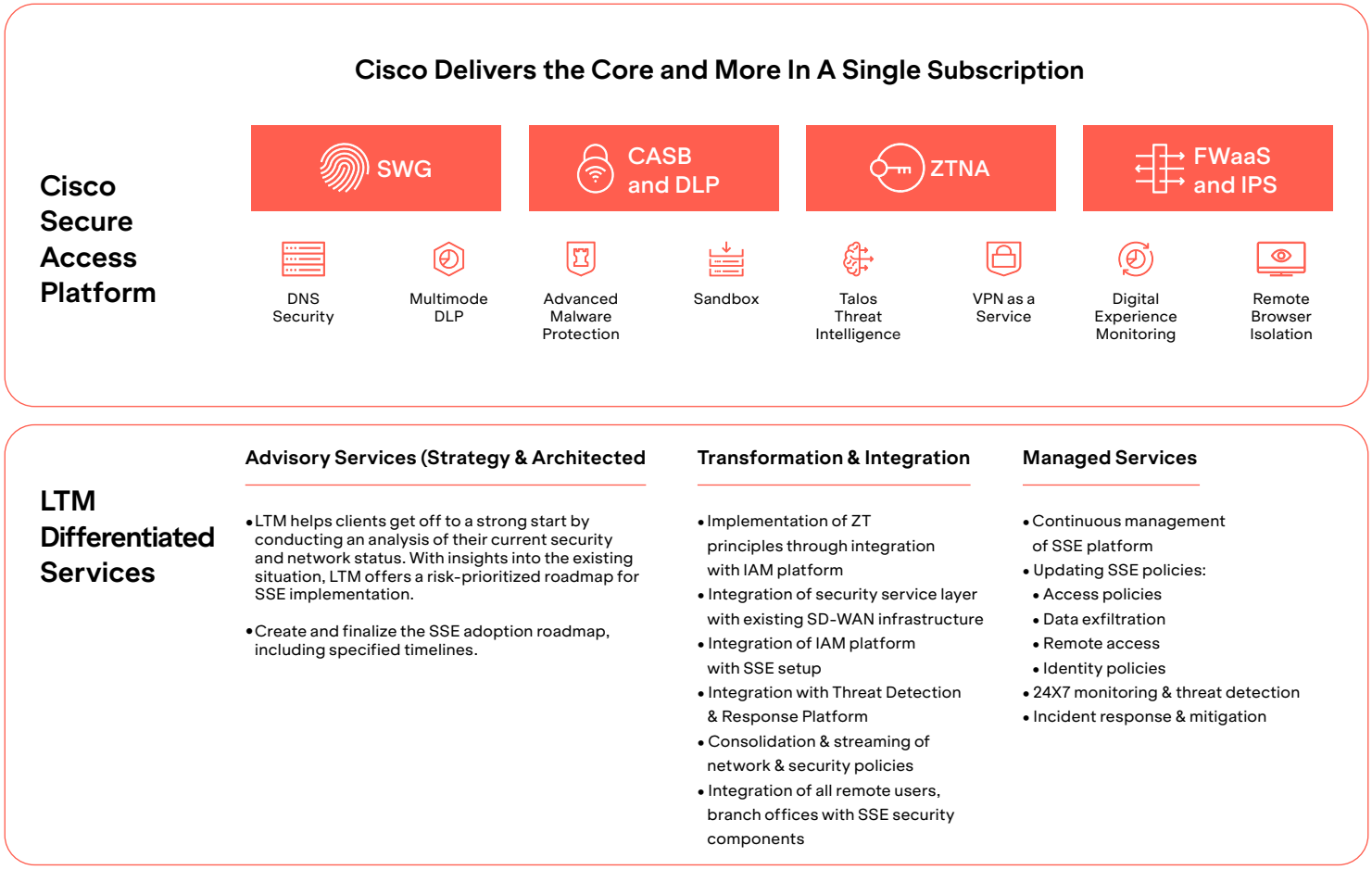


Figure 1 LTM Managed SSE Offering Powered by Cisco

A Unified Cloud-Delivered Architecture

At the core of this approach is Cisco Secure Access, a comprehensive, cloud-native platform that converges multiple technologies—SWG, CASB, ZTNA, firewall as a service (FWaaS), DLP, DNS-layer security, and remote browser isolation (RBI)—into a single, consistent framework. This unification helps to eliminate tool sprawl and simplify management by reducing the number of consoles, vendors, and integration points your teams must maintain.

You gain one policy engine, one management console, and end-to-end visibility across users, devices, and applications. The result is more consistent protection across all traffic without the latency or complexity of legacy appliances.

Zero Trust by Design

Unlike VPNs that grant broad network access, Cisco Secure Access validates every user, device, and session in real time, enforcing least-privilege, per-application access. This approach drastically reduces the blast radius of compromised credentials and eliminates the need to backhaul traffic through centralized gateways.

Every connection is continuously verified

Access decisions adapt dynamically to user identity, device posture, location, and behavior, extending Zero Trust principles seamlessly from the data center to the cloud edge.

Simplified User Experience

Traditional access models often trade security for convenience, or vice versa. Cisco Secure Access removes that tradeoff. Its *connect from anything to anywhere* design gives users a single login and unified experience across private, SaaS, and internet applications. Early adopters report up to 50 percent fewer steps to reach private applications, increasing productivity and reducing the temptation to bypass security with shadow IT:

- For your users, security becomes invisible.
- For your IT teams, it becomes more manageable.

Built-In Intelligence and Automation

The platform's AI Policy Assistant transforms natural-language rules into enforceable policies, helping security teams work faster with fewer errors. Cisco Talos Threat Intelligence, one of the world's largest commercial threat intelligence networks, analyzes more than 550 billion events per day to identify and block emerging attacks before they reach your environment.

Together, these capabilities create a proactive, self-optimizing defense that evolves with your risk landscape, something static rule sets and manual processes simply cannot match.

Managed Excellence and Differentiation from LTM

Modernizing security requires both technology and operational expertise

Cisco provides the cloud-delivered foundation. LTM brings the experience, scale, and management depth to operationalize that foundation across global enterprises. Together, they help organizations modernize faster, balancing agility with control and aligning technology outcomes with business priorities.

LTM draws on more than 140 certified engineers with deep deployment and operational experience in Cisco Secure Access. This expertise helps ensure a seamless rollout, combining Cisco secure access architecture with LTM's proven methodology for consistent implementation and faster time to value.

Through its standardized frameworks and experience deploying Cisco Secure Access at scale, LTM has demonstrated the ability to help accelerate deployments by as much as 30 percent compared with self-managed approaches.

> For its own enterprise, LTM deployed Cisco Secure Access to 80,000 users in less than three months, demonstrating the scalability, repeatability, and operational excellence of its approach.
>
> — Chandan Pani
> Cybersecurity Service Line Head, LTM

Global Scale Ensures Reliability and Speed

Operating in 41 countries through its regional Cyber Defense Resiliency Centers (CDRCs), LTM delivers continuous coverage, incident response, and optimization under a follow-the-sun model. With more than 400 Cisco-certified engineers, it provides around-the-clock protection and consistent performance.

In addition, before full-scale deployment, LTM provides customers with the ability to validate Cisco Secure Access performance and policies through managed tenant pilots. These shared environments provide a low-risk way to assess integration and refine configurations before full rollout.

For its own enterprise, LTM deployed Cisco Secure Access for more than 80,000 users in less than three months, demonstrating both the scalability and repeatability of its approach.

Industry Expertise Enables Compliance-Driven Configuration

LTM tailors SSE implementations to each industry's priorities:

- In **manufacturing**, uptime and operational continuity are paramount.
- In **financial services**, confidentiality, integrity, and auditability drive design.
- In **healthcare and insurance**, privacy and regulatory compliance shape every policy.

This domain-specific insight helps ensure that console setups, policies, and reporting frameworks align with governance requirements such as GDPR, ISO 27001, and HIPAA, while maintaining efficiency and usability.

Integrating Multivendor Environments Broadens Visibility

Whether your environment relies primarily on Cisco or includes platforms from other vendors, LTM helps to ensure interoperability that maintains unified visibility and governance without vendor lock-in or workflow disruption.

Operational Accountability and Assurance

Clients benefit from a single, accountable point of contact throughout deployment and ongoing operations. LTM acts as the primary interface, simplifying coordination and helping to ensure that issues are quickly addressed from start to finish. Every engagement is also governed by defined service level agreements (SLAs) that set clear expectations for performance, response times, and resolution metrics, helping maintain continuous reliability and confidence across global deployments.

Flexible Engagement Models Extend Value

Organizations can engage LTM as a system integrator for deployment or as a fully managed SSE provider with ongoing operations, reporting, and compliance management. This flexibility helps reduce pressure on internal teams, bridge cybersecurity skills gaps, and sustain continuous improvement against service-level goals.

Customers can also choose how to consume Cisco Secure Access, either by maintaining their own Cisco licenses or opting for a fully managed model in which LTM administers the licensing and lifecycle management. This flexibility supports diverse operational and procurement strategies.

> You outsource the entire deployment to us—from design to operation. We bring in our accelerators and ensure a seamless rollout.
>
> — Chandan Pani
> Cybersecurity Service Line Head, LTM

As a Cisco Security Solutions collaborator, LTM brings expertise spanning the entire Cisco security portfolio—from Talos Threat Intelligence to Splunk Observability—helping organizations unify visibility and governance across hybrid environments.

Together, Cisco and LTM deliver a Managed SSE that unites cloud innovation with global operational expertise, helping your organization strengthen resilience, meet compliance goals, and operate securely at enterprise scale.

Partnership, Not Just A Platform

The Cisco and LTM partnership goes beyond traditional vendor engagement. It's a co-innovation alliance with alignment across engineering and service delivery. For you, this means consistent execution—from strategy to deployment to ongoing optimization—with clear accountability and measurable outcomes.

Why This Approach is Different and Better

Table 1 highlights how the Cisco and LTM approach compares with traditional models across key dimensions.

Dimension	Traditional Models	Cisco and LTM SSE
Architecture	Hardware-based, perimeter-bound	Designed to be cloud-native, global, and Zero Trust
Visibility and control	Fragmented across multiple tools	Unified through a single policy and management plane
Operations	Manual, reactive, staff-intensive	Automated, AI-driven, and continuously managed
User experience	Degraded by latency and friction introduced by VPNs	Seamlessly, consistently accessed from any device
Cost efficiency	Impacted by redundant tools and licenses	Consolidated, subscription-based, and simplified
Scalability	Limited by data center hardware	Elastic and globally distributed through the cloud

Table 1 Comparison with Traditional Models Across Key Dimensions

Balanced Considerations

As with any architectural transformation, there are many considerations. Migrating to a cloud-delivered SSE requires careful planning, staged deployment, and change management. For instance, some organizations may choose a hybrid coexistence period with legacy controls.

Cisco and LTM help to simplify this through structured migration playbooks, risk-prioritized onboarding, and co-managed options that allow you to retain oversight while reducing complexity. By unifying security functions and managed operations under one trusted framework, Cisco and LTM help your organization to evolve securely and at your own pace.

Bottom Line

Cisco Secure Access, delivered and managed by LTM, provides a unified and practical path to Zero Trust by:

- Simplifying protection
- Improving visibility across users, devices, and applications
- Replacing fragmentation with consistency, manual effort with automation, and complexity with control

This approach helps your organization operate securely wherever work happens.

Evolving Security for a Borderless Enterprise

As hybrid work, cloud migration, and digital transformation continue to redefine enterprise operations, legacy models can no longer keep pace. Cisco Secure Access with LTM Managed SSE unifies security and networking in the cloud, helping your organization simplify operations, strengthen visibility, and align protection with how modern work happens. Together, Cisco and LTM enable a practical path toward Zero Trust, a path that replaces fragmentation with consistency and adapts as your business grows.

Take the Next Step Toward Zero Trust

Explore how Cisco and LTM can help your organization modernize security through a managed SSE. Visit Cisco Secure Access and/or LTM – Cisco Partnership to learn how a unified, cloud-delivered approach can simplify operations, improve visibility, and help secure your hybrid enterprise.



LTM is a global technology services and consulting company and the Business Creativity partner to the world's largest and most disruptive companies. We bring human insights and intelligent systems together to help enterprises across industries rewire their business models, accelerate innovation, and drive AI-centric growth. With our integrated operations, transformation, and business AI services, we design and deliver solutions that create new productivity paradigms and new roads to value. Together with 87,000 employees across 40 countries and our global network of hyperscaler partners, LTM — A Larsen & Toubro company — owns business outcomes for over 700 clients, helping them to not simply outperform the market, but to Outcreate it.

LTM | cisco

© LTM