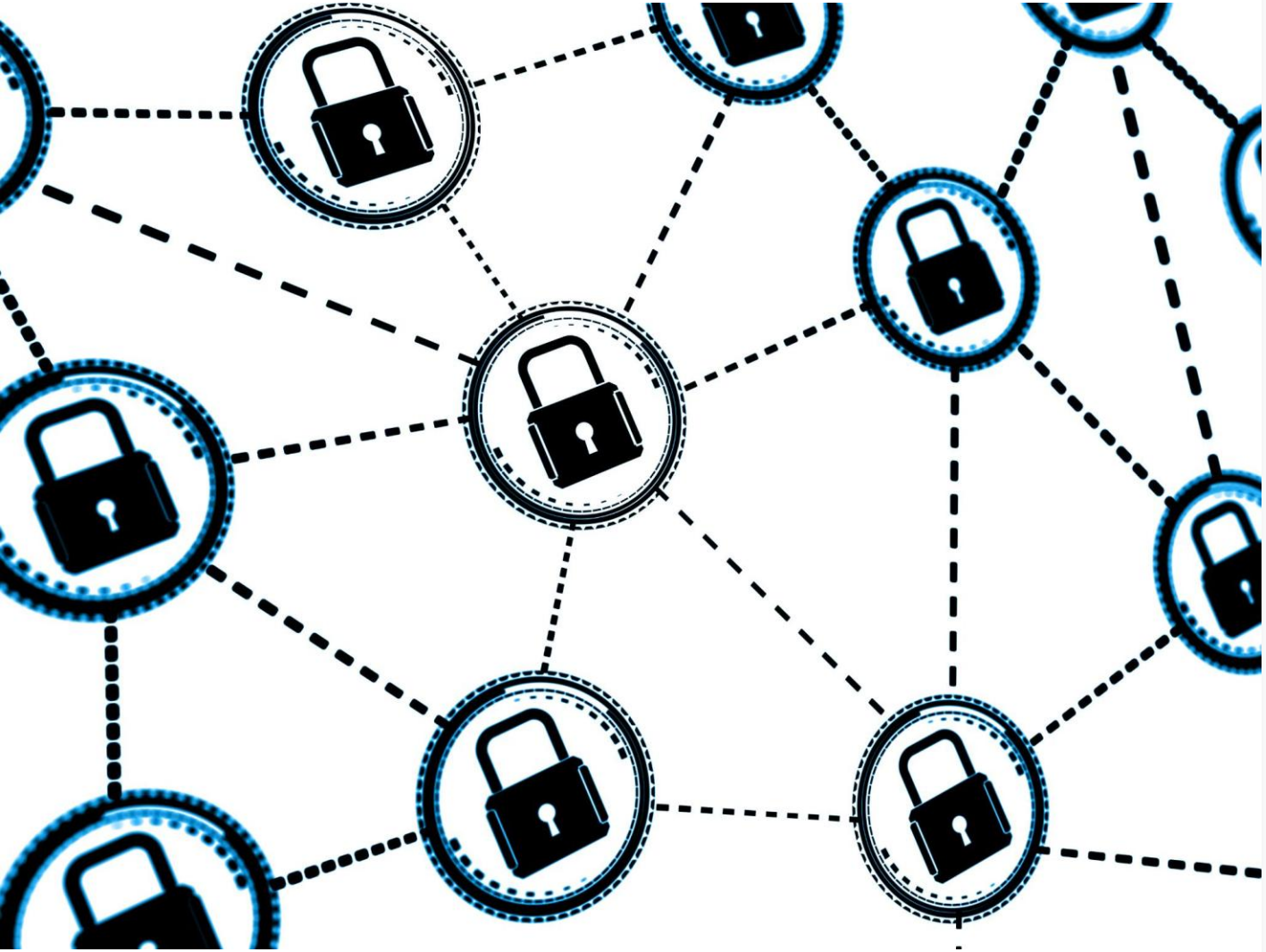
Cisco SSE Migration Project: Key Areas, Challenges, and Outcomes

Overview of strategic migration and security enhancements

Agenda Overview

- Business Impact and Affected Processes
- Project Criticality and Strategic Importance
- Challenges, Constraints, and Mitigation Strategies
- Technical Implementation Details
- Security Posture: Before and After Implementation
- Testimonials

Business Impact and Affected Processes



Business areas and processes impacted by Cisco SSE rollout

IT Infrastructure Impact

Cisco SSE rollout improves IT infrastructure by enhancing secure connectivity for remote and hybrid workforces.

Network Security Enhancement

The rollout strengthens network security through advanced threat detection and secure web gateway operations.

User Access Management

It streamlines user access management and identity controls across multiple business units and cloud applications.

Business needs driving the migration project

Need for Scalability

The project addresses the growing demand for scalable cloud-native security solutions in modern work environments.

Support for SaaS and Remote Access

Increasing SaaS application use and remote work require secure, unified access to enterprise resources.

Unified Zero-Trust Access

Cisco SSE enables unified zero-trust access to reduce complexity and strengthen security posture across the network.

Improved Network Visibility

Enhanced visibility across the enterprise network helps in monitoring and managing security effectively.

Impact on business operations and user experience

Enhanced Security Posture

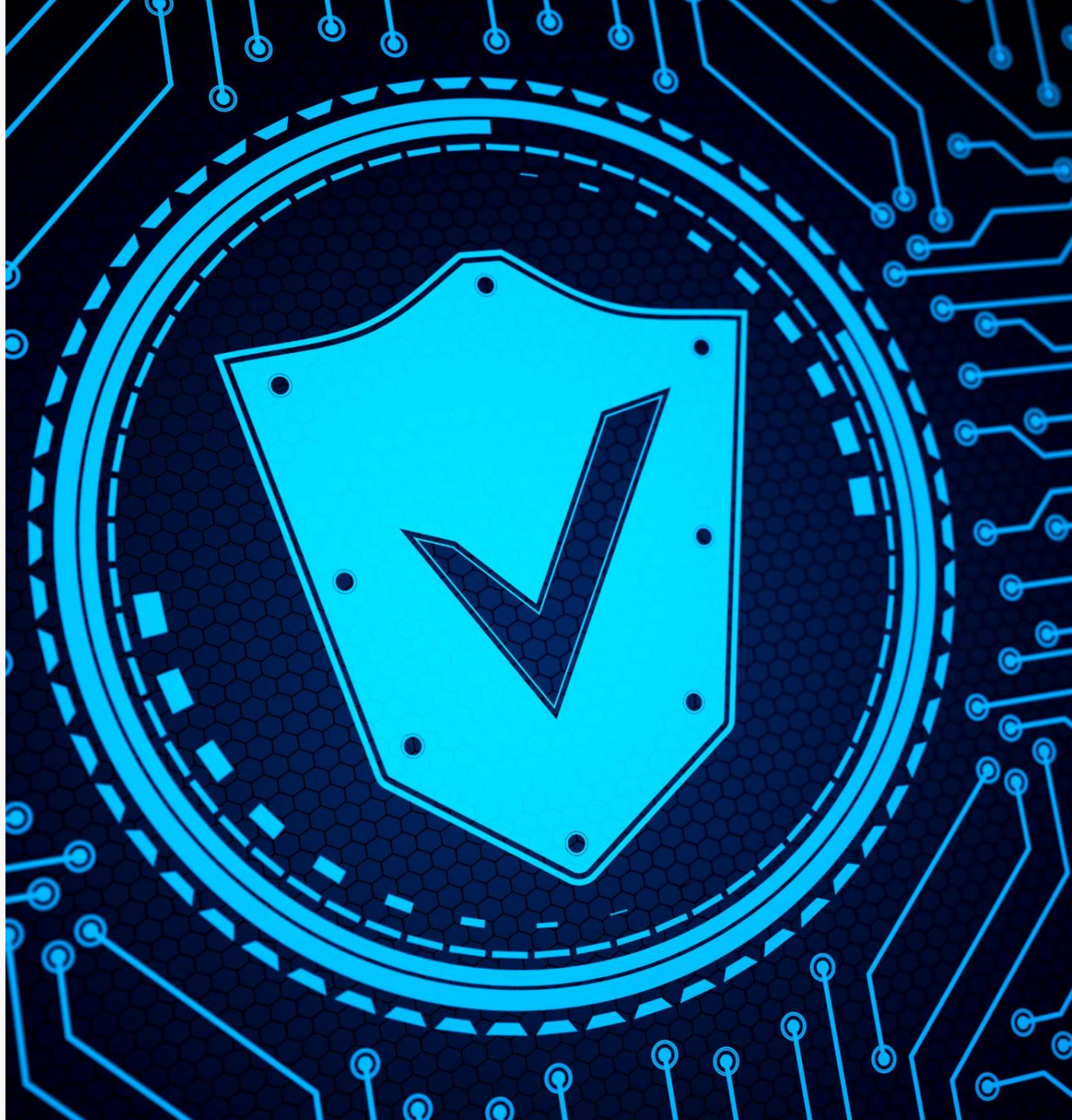
Cisco SSE rollout enforced Zero Trust security improving protection and access for over 80,000 users.

Improved Operational Efficiency

Automation and real-time dashboards streamlined deployment and governance in business operations.

Scalable, Future-ready Infrastructure

The initiative delivered scalable infrastructure ensuring zero disruption to business continuity.



Project Criticality and Strategic Importance

Mission-critical nature and scale of the Cisco SSE rollout

Large-scale Deployment

The rollout impacted over 80,000 endpoints and more than 1,200 projects, showcasing extensive enterprise reach.

Zero Trust Enforcement

Central to the rollout was enforcing Zero Trust architecture to replace legacy proxy systems.

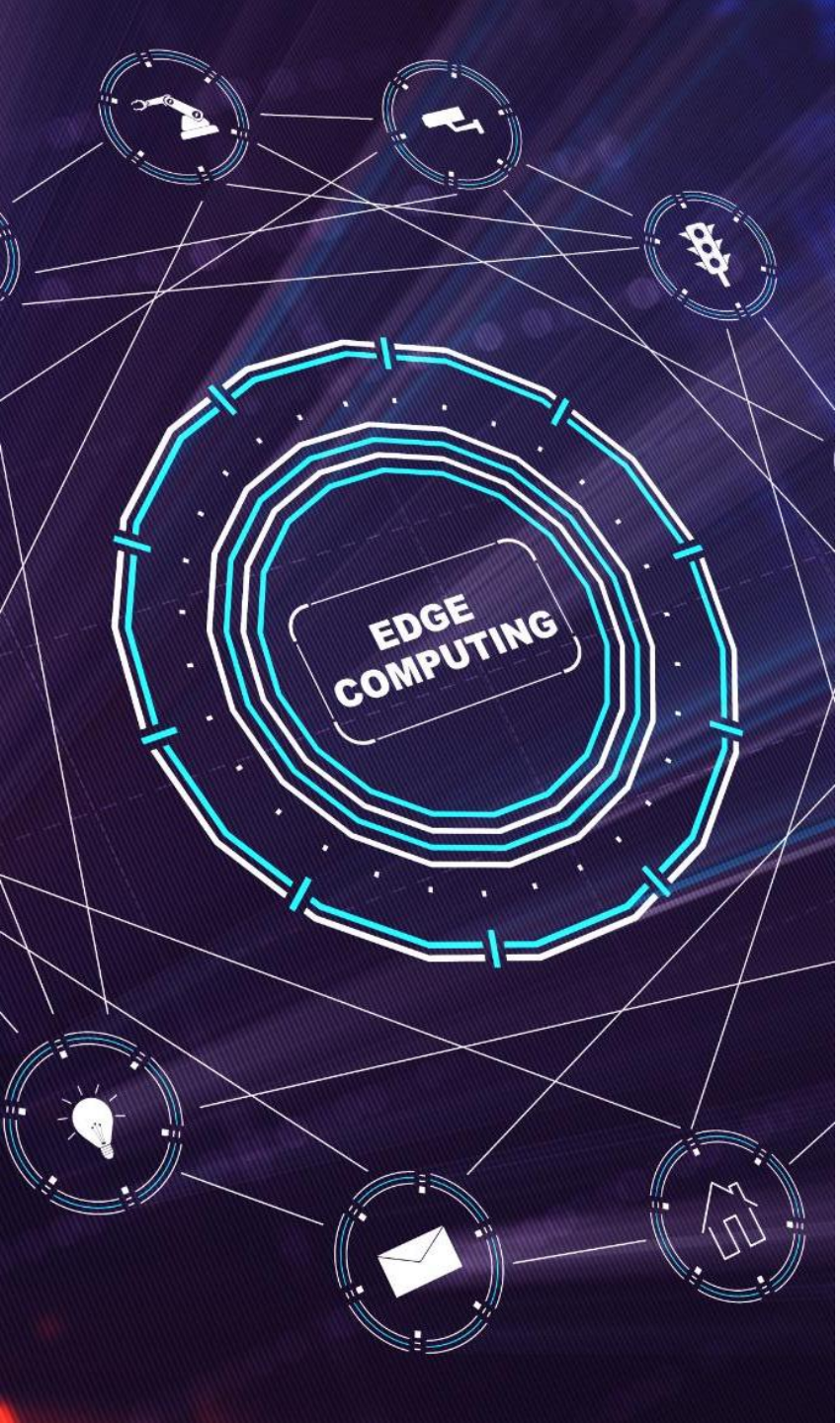
Business Unit Connectivity

Secure and scalable connectivity was established across 40+ business units ensuring uninterrupted operations during migration.

Innovation and Compliance

The rollout supported compliance for customer ODCs and influenced Cisco product innovations industry-wide.

Challenges, Constraints, and Mitigation Strategies



Key constraints encountered and mitigation approaches

Proxy Conflicts & VPN Issues

Transition challenges included avoiding proxy conflicts and managing VPN behavioral inconsistencies across environments.

Customer Engagement and Access

Access delays due to customer reluctance to whitelist IPs were mitigated through targeted engagement and policy alignment.

Latency and Route Optimization

Latency was addressed by conducting a route optimization exercise at data centers to improve network performance.

Visibility and Progress Tracking

Lack of rollout progress visibility was resolved by developing a real-time Power BI dashboard for proactive management.

Major risks identified and risk mitigation measures

Technical Risks and Solutions

Proxy conflicts and VPN instability were mitigated through phased deployment and dynamic proxy switching innovation.

User Disruption Mitigation

Automation and refined endpoint policies minimized user disruption during rollout with effective communication.

Latency and Customer Engagement

Latency was reduced by route optimization; customer resistance managed via proactive engagement and policy alignment.

Visibility and Feature Testing

Power BI dashboards improved rollout visibility; phase-wise testing ensured feature compatibility before production.

Technical Implementation Details

Technical deployment statistics and automation approach

Deployment Targets and Achievement

The project targeted 78K headcount with 76K achieved, reaching 97% in 4 months.

Operating Systems Used

Deployments were carried out on both Windows and Mac operating systems for diverse compatibility.

Services Provisioned

Provisioned secured internet and private access services ensuring secure connectivity.

Automation Deployment Approach

Automated deployment and rollback processes were used to ensure smooth and efficient delivery.

Platforms and solutions used for deployment and governance

Security and Network Access

Cisco Secure Service Edge Proxy provides secure network access and enforces security policies during deployment.

Automated Deployment Tools

Microsoft Intune enables automated rollout of software and policies to endpoints for efficient deployment management.

Scripting for Endpoint Transition

PowerShell and Python scripting facilitate Windows and Mac endpoint transitions with customized automation.

Governance and Monitoring

Power BI dashboards track governance metrics and deployment progress with visual analytics and reporting.

SSL Decryption and SSO Integration

Enhanced security by decrypting SSL traffic for inspection and integrating Single Sign-On for seamless user authentication

Security Posture: Before and After Implementation

Security environment and limitations prior to Cisco SSE

Existing Security Posture

LTIMindtree used Zscaler’s cloud-native platforms providing AI analytics and sandboxing for effective threat prevention.

Secure Access and Policy Enforcement

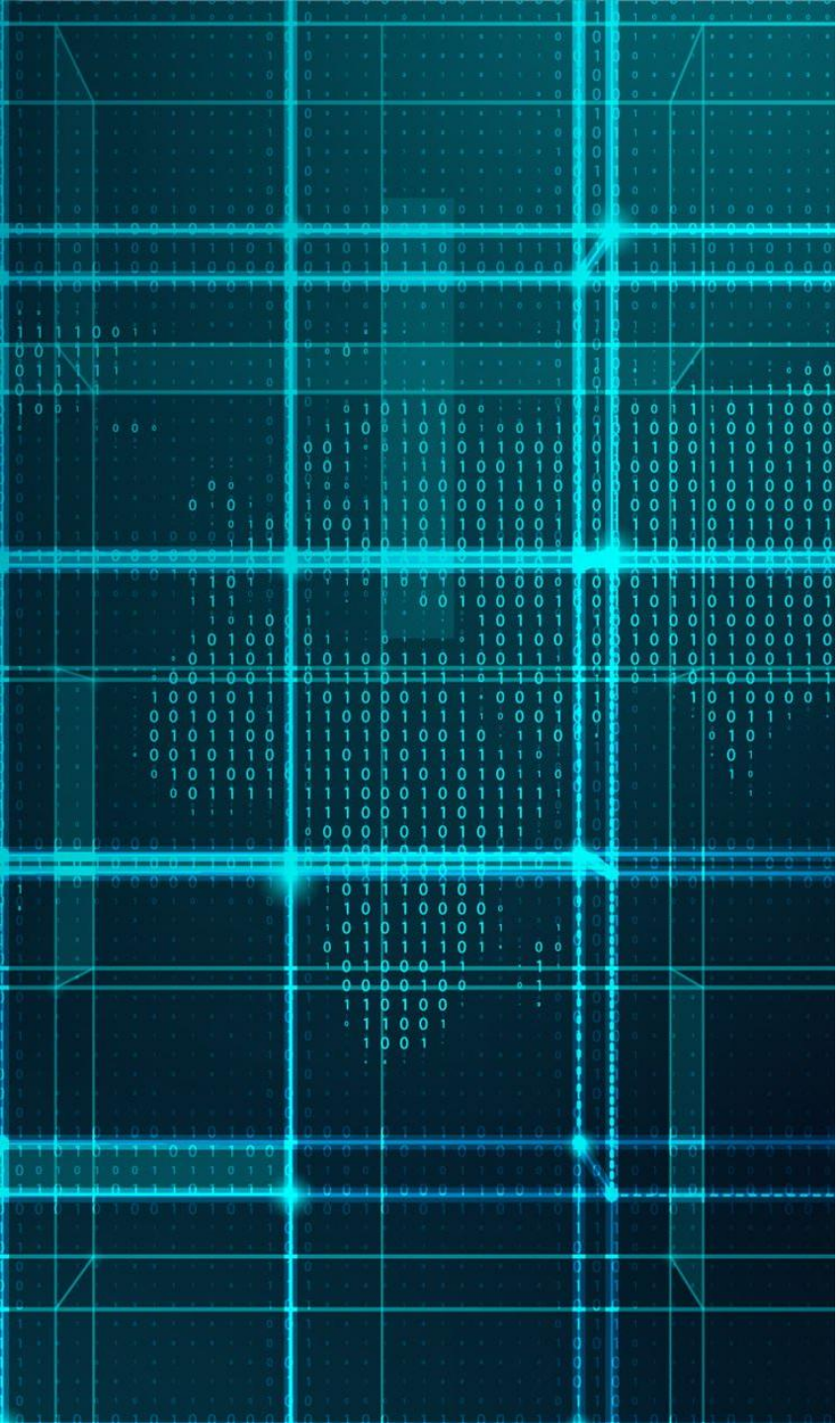
Zscaler’s ZIA and ZPA ensured secure access and policy enforcement across a widely distributed enterprise environment.

Limitations and Challenges

Diagnostic precision was limited and threat intelligence lacked global telemetry, creating gaps in proactive defense.

Need for Integrated Security Model

Evolving enterprise needs highlighted the opportunity for a more integrated and advanced security solution.



Enhanced security and operational efficiency post-implementation

Improved Security Posture

Deployment enhanced security using policy-driven access, SSL decryption, and SSO aligned with Zero Trust principles.

Advanced Threat Prevention

Integration with global telemetry enabled proactive blocking of malicious URLs and detection of sophisticated threats.

Enhanced Network Visibility

ThousandEyes offered deep network traffic insights, improving user experience and application performance monitoring.

Operational Efficiency Gains

Advancements led to reduced incidents and improved endpoint compliance, positioning the organization as an early adopter.

The Results

The Results

Improved Security Posture:

AI enhanced security with zero trust principles is providing granular access control. Users access only permissioned resources, reducing risks from unauthorized access and cyber threats. The integrated solution improved network visibility, enabling faster threat detection and mitigation

Streamlined IT Operations:

The unified cloud-managed console simplified IT management, reducing administrative overhead and enabling strategic initiatives. A single client replaced four legacy security tools, simplifying complexity and improving manageability.

Scalability and Performance:

LTIMindtree secured its global hybrid workforce of 84,000+ employees efficiently, accommodating their dynamic remote and on-site teams. Modern protocols like MASQUE and QUIC enhanced network performance, delivering low-latency access to applications.

Enhanced User Experience:

Users enjoy seamless connectivity with a unified client that intelligently guides them to the right application security level, reducing credential prompts and boosting productivity. DEM has optimized user performance by identifying and resolving potential issues.

Operational Efficiency and Cost Savings:

Faster deployment and simplified operations have resulted in measurable efficiency gains. Secure Access eliminated redundancies and reduced operational costs by simplifying policy management and onboarding

Testimonials

Testimonials

- A short video on Cisco's Video Portal highlights how LTIMindtree is securing its remote workforce
- An article on Cisco Systems website details the partnership and benefits of the implementation
- Cisco Press Release
- Thank you email from IT head

Adobe Acrobat Document

- Feedback from project

Outlook Item