GTT Greater Technology Together

Whitepaper

THE IT AND SECURITY LEADER'S GUIDE TO SECURING THE DISTRIBUTED EDGE

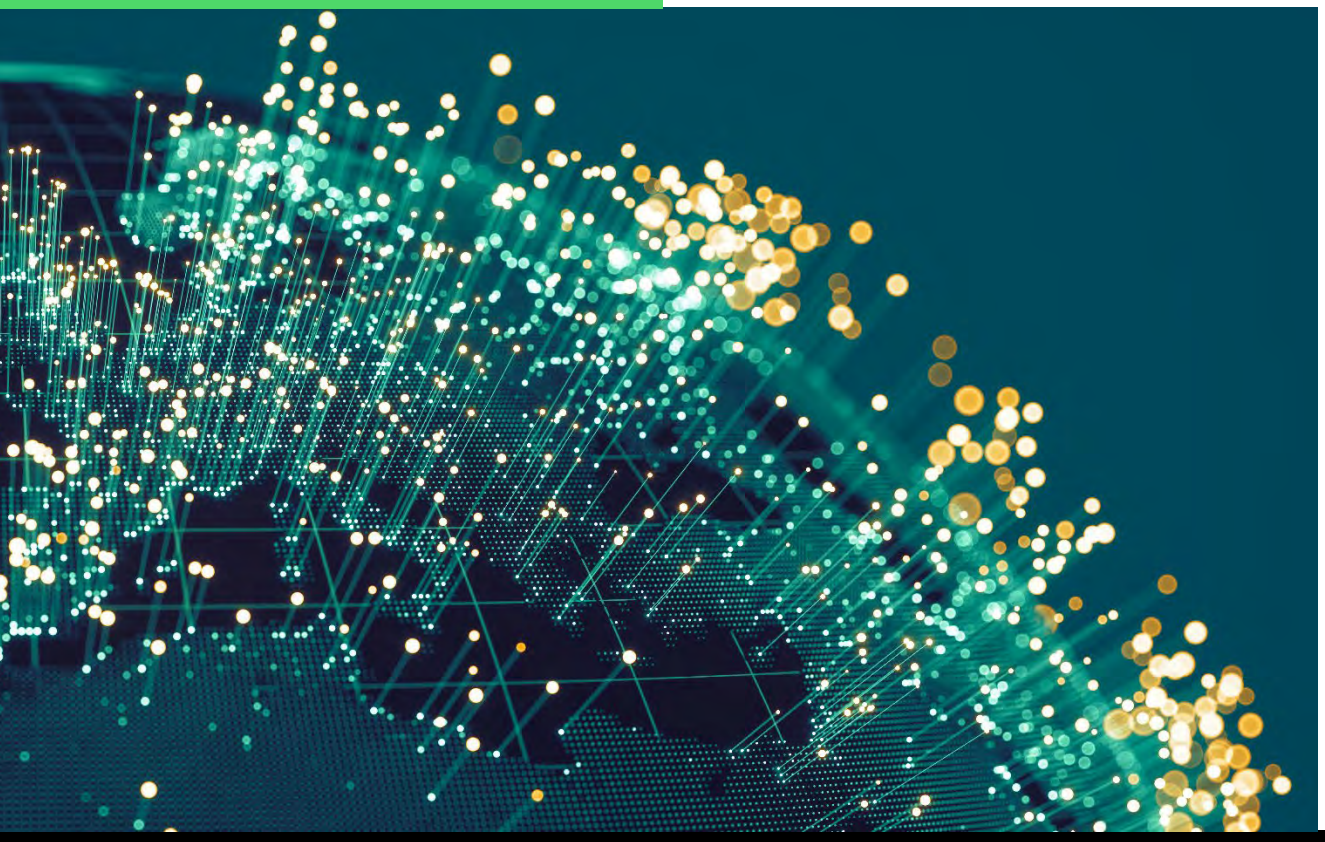
Contents

1. INTRODUCTION: THE DISTRIBUTED EDGE CHALLENGE

Enterprise perimeters no longer exist within four walls. Operations now happen at the distributed edge. Branches, remote workers and IOTdevices push computing closer to the data source. This shift drives incredible efficiency but introduces severe security demands.

Traditional security models fail in this environment. Perimeter-based defenses assume everything inside the network is safe. When your network spans thousands of global locations and endpoints, the perimeter dissolves. Backhauling traffic to a centralized data center creates latency and frustrates users. You need a strategy that secures data where it lives.

This playbook provides actionable guidance for it and security directors and managers. We focus on transforming your edge security posture through intelligent frameworks and centralized control. You will learn how to connect people to applications, secure your global infrastructure and simplify IT operations.



2. KEY PRINCIPLES FOR SECURING THE DISTRIBUTED EDGE

Effective edge security requires a fundamental shift in architecture. The foundation rests on three pillars:

Zero-trust security

Assume breach. A zero-trust approach operates on the principle of "never trust, always verify."

- Identity verification: you must authenticate every user, device and application attempting to access the network.
- Least privilege access: limit users to the resources they need to perform their jobs.
- Micro-segmentation: divide the network into secure zones. If a breach occurs in one zone, the threat cannot move laterally to other areas.

Ai-driven analytics

Human teams cannot process the sheer volume of alerts generated by a distributed network. Ai-enabled transformation is necessary.

- Real-time threat detection: machine learning algorithms analyze traffic patterns instantly to identify anomalies.
- Automated responses: systems can isolate compromised endpoints without waiting for human intervention.
- Predictive insights: ai identifies vulnerabilities before attackers exploit them to help you prevent breaches.

Unified management

Visibility is your biggest asset. You cannot protect what you cannot see.

- Centralized control: manage policies across all edge locations from a single platform.
- Consistent policy enforcement: ensure every remote branch and device adheres to the exact same security standards.

3. BEST PRACTICES FOR EDGE SECURITY

Translating principles into action requires a structured approach. Implement these core practices to secure your infrastructure.

Conduct a comprehensive security audit

Start by mapping your entire edge environment. Identify all connected devices, applications and users. Assess your current security posture to find visibility gaps and vulnerabilities. A thorough audit establishes the baseline for your modernization efforts.

Implement strong identity and access management (IAM)

Deploy strict IAM protocols across the organization. Require multi-factor authentication for all access requests. Tie access privileges directly to user roles and business needs.

Use micro-segmentation to isolate critical assets

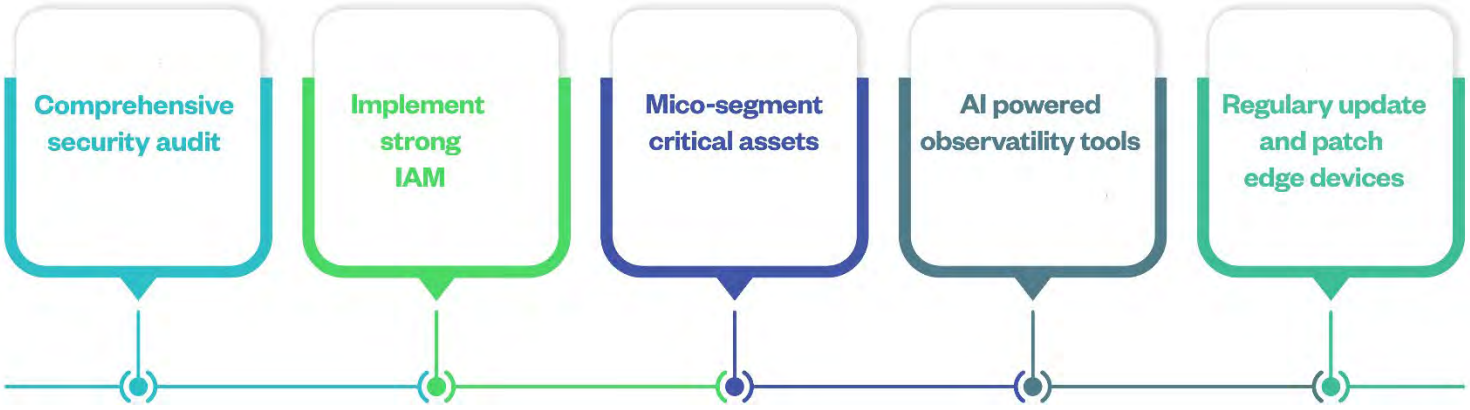
Apply micro-segmentation policies at the edge. Group workloads and devices based on their function. This containment strategy minimizes the blast radius of any potential security incident.

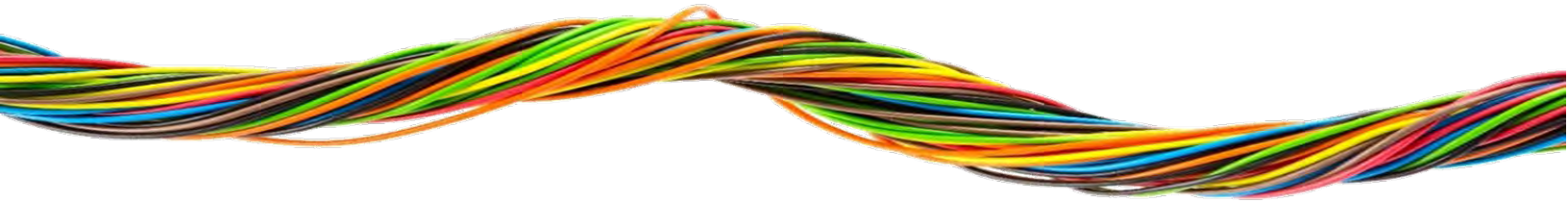
Deploy AI-powered observability tools

Integrate AI-native platforms to achieve continuous threat detection. These tools provide the context needed to separate critical threats from background noise. This reduces alert fatigue and allows your team to focus on strategic initiatives.

Regularly update and patch edge devices

Unpatched devices represent massive vulnerabilities. Establish automated patching schedules for all edge hardware and software. Maintain strict version control to ensure compliance across your entire footprint.





4. TOOLS AND TECHNOLOGIES TO CONSIDER

Modernizing your security posture requires the right technological investments. Focus on solutions that drive digital scalability and demonstrate clear ROI

Ai-native security platforms

Invest in platforms that process massive datasets in real time. Gtt envision, a platform that provides the visibility and orchestration needed to manage secure networks. It uses ai-driven insights to optimize performance and enforce security policies globally.

Zero-trust frameworks

Adopt zero trust network solutions. For example, ZTNA replaces outdated VPNS by connecting users directly to applications rather than the broader network. This secures remote workforces without sacrificing performance.

Unified management solutions

Consolidate your security stack. Look for solutions that integrate SD-WAN and security services for a SASE framework. Unified management platforms simplify global network operations and reduce administrative overhead.

5. OVERCOMING COMMON CHALLENGES

Transformation requires careful planning. IT leaders must anticipate obstacles and manage change effectively.

Addressing system sprawl with phased implementation

Do not attempt a complete overhaul overnight. Replace legacy systems in manageable phases. Start with high-priority locations or critical user groups. Validate the success of each phase before scaling the solution globally.

Integrating edge security with legacy systems

Many organizations rely on older systems that lack native security features. Use edge gateways and API integrations to bridge the gap. Apply modern security controls over legacy traffic to protect older infrastructure until you can fully retire it.

Training teams to manage distributed environments

New technology requires new skills. Invest in training your it and security staff on ai-enabled networking and zero-trust concepts. Partner with managed service providers to fill immediate knowledge and resource gaps to support your internal teams.

6. CONCLUSION: BUILDING CONFIDENCE IN EDGE SECURITY

Securing the distributed edge is a strategic business mandate. It protects your organization, enables hybrid work and ensures compliance.

Success requires moving away from outdated perimeter defenses. Embrace zero-trust principles to verify every connection. Implement ai-driven analytics to detect threats in real time. Adopt unified management to regain control over your global network.

Start by developing a strategic roadmap. Assess your current state, align your security goals with business outcomes and deploy platforms like gtt envision to simplify your transformation.

7. GLOSSARY OF TERMS

- **Zero-trust:** a security framework requiring all users to be authenticated and authorized continuously.
- **Micro-segmentation:** the practice of splitting a network into isolated segments to limit lateral movement.
- **AI -enabled networking:** the use of artificial intelligence to optimize network performance and security.
- **ZTNA** (zero trust network access): a technology that provides secure remote access to applications based on defined access control policies.
- **Distributed edge**: the decentralized locations where data is processed close to the end user or device.
- **GTT Envision:** a single platform delivering visibility, orchestration and control across network and security, built on the GTT global tier 1 backbone.
- **Identity and access management** (IAM): the policies and tools used to verify user identities and control access to network resources.

ABOUT GTT

GTT is a leading networking and security as a service provider for multinational organizations, simply and securely connecting people and agents to data and applications anywhere in the world. We serve thousands of organizations, bringing together the right people, partners and technology to reduce the burden on IT teams and solve the most pressing networking and security challenges. Built on our top-ranked global Tier 1 network, GTT Envision is a single global technology platform to connect, orchestrate, virtualize and automate enterprise networks, enabling customers with consumable solutions to achieve business missions and meet ongoing demand when, where and how needed. Our portfolio includes SASE, SD-WAN, security, internet, voice and other connectivity options, complemented by a suite of professional services and sales and support teams in local markets around the globe. We partner with our customers to deliver Greater Technology Together. For more information, visit www.gtt.net.

EnEdge_secur_dist_EdgeWtPaper_GGMCM-4483_v1_08102026