THE ARCHON

TECHNOLOGY INTELLIGENCE

EXECUTIVE BRIEF

GTT Unveils AI-Native Defense Platform for Real-Time Network Threat Neutralization

GTT announced a purpose-built platform that leverages generative AI and proprietary threat models to scan every packet, flag anomalies, and trigger corrective actions without human intervention.

CONTROL FRAMEWORK

Platform Architecture – Core Building Blocks

The solution consists of five tightly coupled modules: (1) Telemetry Ingest Engine pulls NetFlow, sFlow, and packet-level data; (2) AI Inference Engine runs lightweight models at the edge; (3) Threat Correlation Layer maps alerts to MITRE ATT&CK tactics; (4) Automated Remediation Engine executes device-level playbooks; (5) Policy Engine enforces compliance and risk thresholds.

→ Zero-trust data pipelines with TLS-1.3 encryption

→ Extensible model marketplace for industry-specific threats

CONTROL FRAMEWORK

AI-Driven Detection Pipeline

Raw traffic is normalized, enriched with contextual metadata, and streamed to the AI Inference Engine where ensemble models evaluate risk scores in milliseconds. High-scoring events are forwarded to the Correlation Layer for contextual enrichment.

→ Feature extraction includes protocol anomalies, flow entropy, and payload signatures

→ Models are continuously retrained using federated learning across GTT's global footprint

CONTROL FRAMEWORK

Automated Remediation Loop

When a threat is confirmed, the Remediation Engine selects a predefined playbook, authenticates to the target device via NETCONF/RESTCONF, and pushes a configuration change (e.g., ACL update, quarantine VLAN). The platform then validates the outcome and logs the action for audit.

- → Playbooks are version-controlled in Git and can be customized per customer policy
- → Rollback is automatic if post-change health checks fail

CONTROL FRAMEWORK

Seamless Integration with Existing Network Fabric

The platform exposes open APIs (REST, gRPC) and native plugins for SD-WAN controllers, MPLS routers, and 5G edge nodes, allowing enterprises to protect legacy and cloud-native assets from a single pane of glass.

→ Supports Cisco IOS-XE, Juniper Junos, and Nokia SR-Linux via standard YANG models

→ Zero-touch onboarding through DHCP option 43 or NETCONF discovery

CONTROL FRAMEWORK

Operational Impact – Faster Detection & Fewer Manual Interventions

By moving analytics to the data plane and automating response, organizations can shrink detection latency from minutes to sub-second intervals and reduce manual incident-response effort.

→ Mean Time to Detect (MTTD) drops dramatically

→ Mean Time to Respond (MTTR) approaches real-time

→ Security staff can focus on strategic threat hunting

EXECUTIVE TAKEAWAY

Executive Takeaway

GTT's AI-native defense platform delivers a unified, real-time security fabric that aligns with modern networking architectures. Enterprises gain instant threat visibility, automated containment, and a future-proof foundation for AI-enhanced operations.