AI-Driven Threat Screening for 5G UPF with Automated Risk Mitigation

Securing the User Plane Function in Cloud-Native 5G Architectures

CONF42 DEVOPS 2026

Speaker Introduction

Binu Govindan

Principal SDET at Microsoft

Specializing in security testing and threat detection for cloud-native network architectures, with extensive experience in DevOps automation and AI-driven security frameworks for next-generation telecommunications infrastructure.

The presentation/slides information I share today represent my own personal views. I am speaking for myself and not on behalf of my employer, Microsoft Corporation.

CHALLENGE

The Growing Threat Landscape in 5G Networks

As 5G networks scale globally, the User Plane Function faces unprecedented security challenges. Traditional signature-based detection methods struggle with the volume, velocity, and complexity of modern threats targeting virtualized network functions.

Protocol Gaps

Vulnerabilities in signaling and data plane protocols exploited by sophisticated attackers

Virtualization Risks

Cloud-native deployments introduce new attack surfaces across containerized workloads

Slice Misconfigurations

Network slicing complexity creates opportunities for isolation breaches and resource abuse

Understanding the User Plane Function

The Data Handling Core

The UPF processes all user data traffic in 5G networks, routing packets between devices and external networks. It operates with ultra-low latency requirements while handling massive traffic volumes, making it a critical target for attackers.

Any compromise at this layer can impact service availability, data integrity, and user privacy across entire network slices.

SOLUTION OVERVIEW

AI-Driven Multi-Factor Risk Scoring Framework

Our approach moves beyond static rules to analyze traffic patterns using multiple dimensions of context, enabling real-time threat detection and classification.

01

Behavioral Analysis

Pattern recognition across protocol usage and session characteristics

02

Geographic Context

Location-based anomaly detection and geofencing policies

03

Temporal Indicators

Time-based pattern analysis for unusual activity windows

04

Volumetric Metrics

Traffic volume analysis to identify DDoS and resource exhaustion attempts

05

Historical Intelligence

Threat actor profiling and reputation scoring based on past behaviors

Beyond Signature-Based Detection

Traditional Approach

- Relies on known threat signatures
- Manual rule updates required
- High false positive rates
- Cannot detect zero-day threats
- Limited contextual awareness

AI-Driven Approach

- Identifies unknown threat patterns
- Continuous adaptive learning
- Contextual risk assessment
- Detects evasive techniques
- Multi-factor correlation analysis

Continuous Online Learning Architecture

The system continuously evolves by incorporating real-world observations and analyst feedback, ensuring models adapt to emerging threats and changing network behaviors.

Data Ingestion

Real-time traffic and telemetry collection

Model Updates

Continuous retraining and improvement

Model Inference

Risk scoring and threat classification

Response Actions

Automated mitigation execution

Analyst Review

Human validation and feedback

AUTOMATION

Tiered Automated Mitigation Pipeline

When threats are detected, the system applies graduated defensive responses based on risk severity, leveraging programmable 5G data planes for rapid enforcement.

Level 1: Enhanced Monitoring

Collecting additional telemetry and logging suspicious network sessions.

Level 2: Traffic Shaping

Limiting traffic rates and adjusting QoS for malicious flows.

Level 3: Session Isolation

Quarantining high-risk traffic by isolating it within restricted network slices.

Level 4: Full Termination

Blocking confirmed threats and terminating all associated network sessions.

Policy-Driven Enforcement at Scale

Programmable Data Plane Integration

The mitigation pipeline integrates directly with 5G UPF data planes, enabling microsecond-level policy enforcement without manual intervention. Security policies are expressed declaratively and automatically translated into data plane rules.

This approach ensures consistent, auditable responses across distributed network functions while maintaining the ultra-low latency requirements of 5G services.

Operational Benefits for DevOps Teams

Reduced Alert Fatigue

AI-driven correlation reduces false positives by 70%, allowing teams to focus on genuine threats requiring human analysis

Faster Incident Response

Automated mitigation reduces mean time to respond from hours to seconds, minimizing blast radius of security incidents

Operational Consistency

Policy-driven enforcement ensures uniform security posture across all network slices and geographic regions

Continuous Improvement

Online learning captures operational insights, making the system smarter with every incident

Strengthening UPF Resilience

By combining AI-driven detection with automated response, organizations can build UPF deployments that are resilient against both known and emerging threats.

Threat Detection

Identify unknown attacks and evasive patterns in real-time traffic flows

Rapid Response

Execute mitigation in milliseconds using programmable data planes

Adaptive Learning

Continuously improve detection accuracy through analyst feedback

Integration with Cloud-Native DevOps Workflows

Built for Modern Operations

The framework integrates seamlessly with GitOps workflows, observability platforms, and incident management tools used by SRE teams.

- Prometheus metrics for model performance tracking
- OpenTelemetry integration for distributed tracing
- API-first design for CI/CD pipeline integration
- Kubernetes-native deployment models

IMPLEMENTATION

Getting Started: Key Considerations

1

Baseline Establishment

Deploy in observation mode to establish normal traffic patterns and tune initial models

2

Telemetry Pipeline

Ensure comprehensive data collection across UPF instances and network slices

3

Policy Definition

Define graduated response policies aligned with organizational risk tolerance

4

Analyst Training

Establish feedback loops and review processes to drive continuous improvement

5

Gradual Automation

Start with monitoring, then enable automated responses as confidence grows

The Future of 5G Security Operations

AI-driven threat screening represents a fundamental shift in how we secure next-generation networks. As 5G deployments continue to grow, the combination of intelligent detection and automated response becomes essential for maintaining security at scale.

> The operational disciplines required for 5G demand security approaches that match the speed, scale, and complexity of the infrastructure itself.

By embracing these techniques, DevOps teams can build security operations that are as agile and resilient as the networks they protect.

Thank You!

Binu Govindan Principal SDET, Microsoft

CONF42 DEVOPS 2026

Questions.?
Welcome.