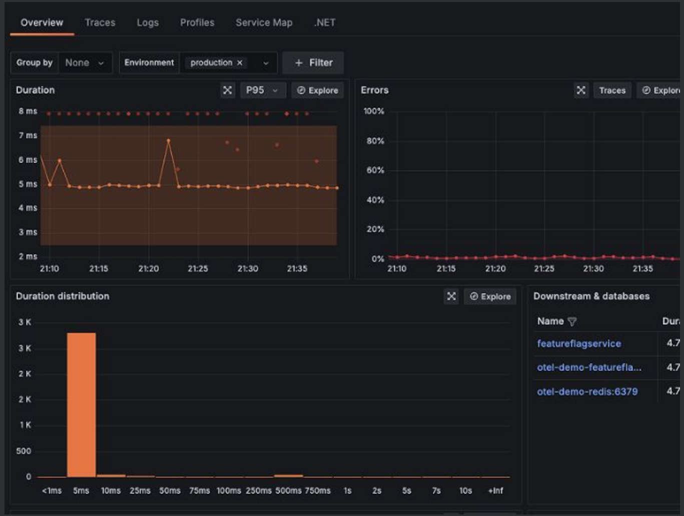
Real-Time Edge Observability:

The New Frontier of Security Monitoring and Threat Detection



Name	Dur
featureflagservice	4.7
otel-demo-featurefla...	4.7
otel-demo-redis:6379	4.7

Chintan Udeshi, Principal/Lead Product Manager

Edge Market Size and Growth

Enable near-real time Decisions

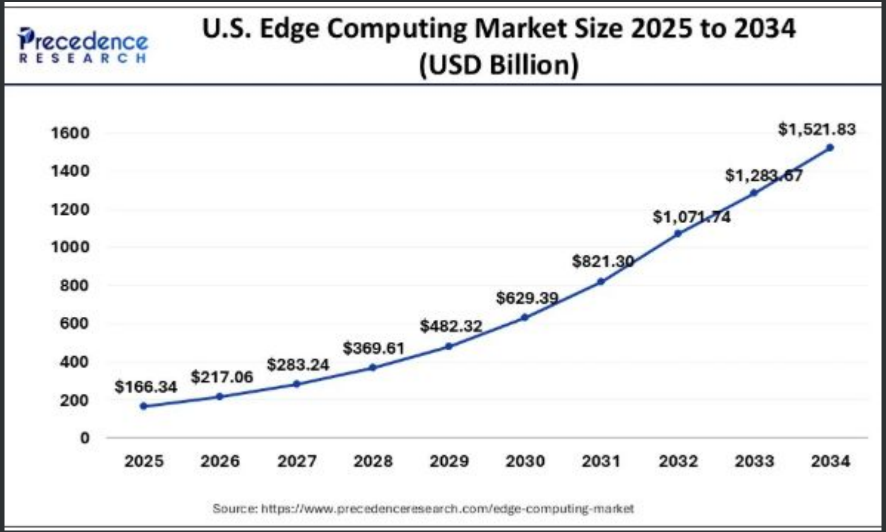
Reduce network latency to few milli-seconds to enable split second decisions

Operational Resiliency

Critical systems can continue to operate even during network outage

Reduced Bandwidth Consumption

Local data processing, reducing substantial bandwidth saving compared to cloud-only architectures



U.S. Edge Computing Market Size 2025 to 2034 (USD Billion)

Source: https://www.precedenceresearch.com/edge-computing-market

CAGR over 28% from 2025 to 2034

The Edge Security Challenge

Operating Outside Traditional Boundaries

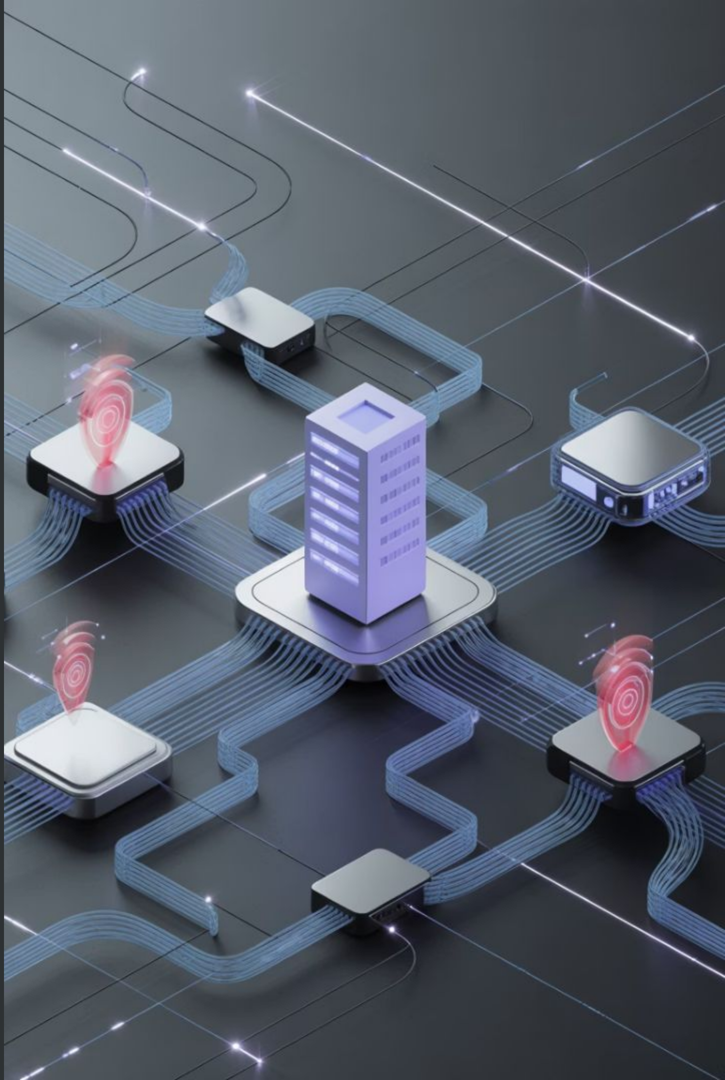
Creation of dangerous blind spots in visibility and enforcement.

Limited Visibility

Legacy monitoring solutions lack capabilities to detect edge-specific threats, compromises, and anomalous behavioral patterns.

Increased Attack Surface

Exponential expansion of threat landscape, offering attackers numerous potential entry points and vulnerabilities



Threat Landscape at the Edge

45% of organizations have experienced at least one significant edge security incident in the past 12 month

Network Infiltration

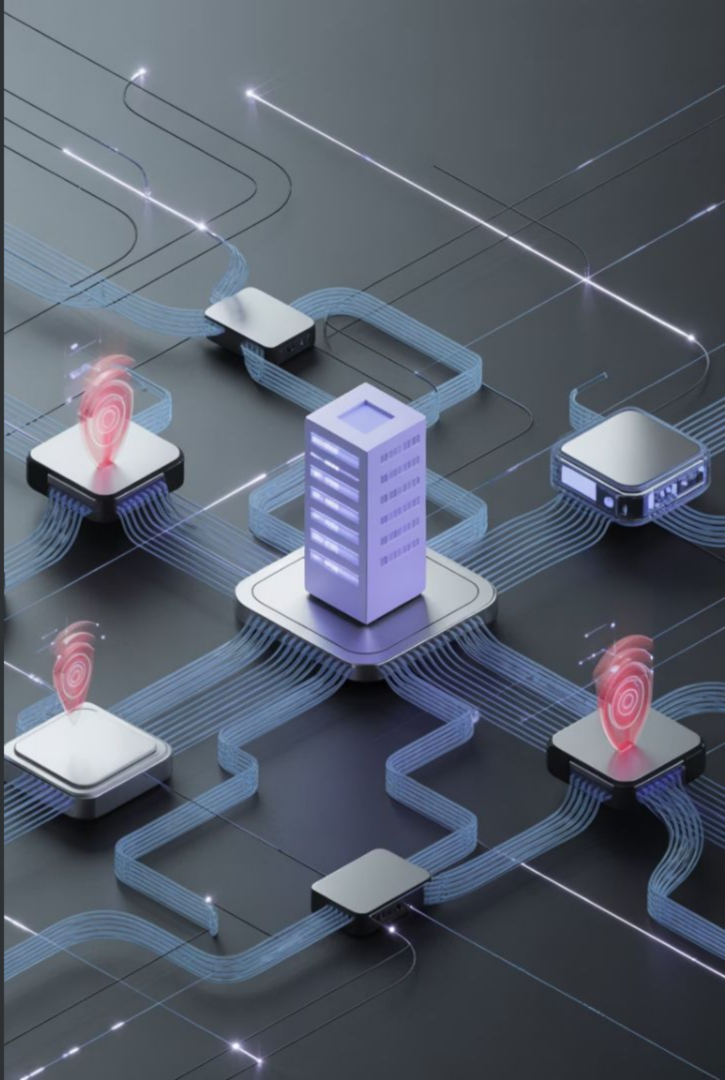
Edge acts as entry points to critical core systems. Attackers exploit established trust relationships to spread malware to the rest of the network

Data Breaches

Systematic extraction of confidential information through compromised edge nodes, targeting vulnerable, unencrypted data

DDoS Attacks

Strategic hijacking of edge infrastructure to orchestrate massive distributed attacks; Botnet devices hijack vulnerable devices



Real-Time Monitoring Architecture

Edge Collection

Distributed micro-agents capture comprehensive telemetry with minimal CPU and memory footprint impact.

Real-time Threat Detection

Identify suspicious activities and behavioral patterns that might indicate security breaches

Central Analysis

ML-powered correlation engine identifies subtle threat patterns across thousands of distributed edge nodes in real-time.

Response Automation

Autonomous defense mechanisms execute containment protocols within milliseconds, isolating compromised nodes before lateral movement.

Key Performance Metrics

MTTD reduction from 197 hours to Mere 4 hours

78%

Reduce incidents Escalation

Continuous access monitoring reduces incident escalation

84%

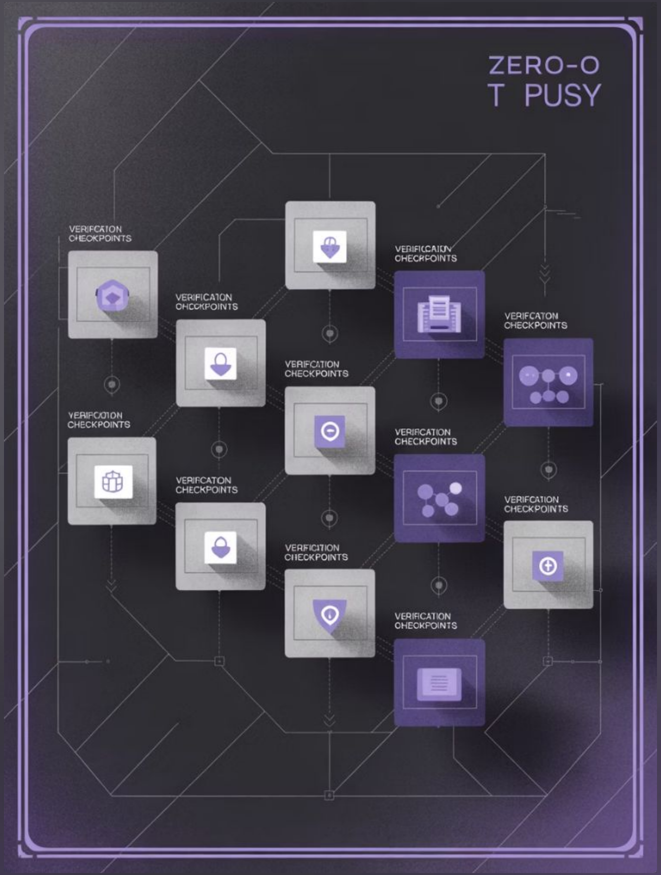
Proactive Threat Identification

Critical security anomalies detected within the first hour of emergence

89%

Lateral Movement Detection

Identify unauthorized access attempts between edge nodes and core systems



Observability in Zero-Trust

Continuous Authentication

Rigorous multi-factor verification of device identity and behavioral signatures at millisecond intervals.

Micro-segmentation

Prevent the spread of vulnerabilities to rest of the infrastructure even if some of the edge devices are affected by vulnerabilities

RunTime Security Protection

Deep packet analysis with cryptographic verification of all data exchanges across distributed edge nodes.

Least Privilege Enforcement

Adaptive permission frameworks that automatically constrict access pathways when behavioral anomalies are detected.

End-to-End Visibility

Cloud Infrastructure

Scalable architecture supporting mission-critical applications and data storage with comprehensive monitoring capabilities

On-Premises Systems

Enterprise hardware infrastructure with legacy integration and enhanced security controls for sensitive workloads

Network Fabric

Secure transmission pathways with end-to-end encryption and redundant routing to ensure reliable data flow across environments

Edge Compute

Localized processing units that minimize latency and enable real-time analytics at distributed geographical locations

IoT Endpoints

Smart devices and industrial sensors providing continuous telemetry data with embedded security protocols

ROOAD-MAP
Edge Observabilty Security System
"Boure copatwmer: couy miistuie Yoe edlecti youprone
Seay Stoicsbulv" peciur nestotkens coauicdtiies"
Assessmentent.
Cassessment · Pdhnest
Deassiviect
Delloyment
Conse & ishinnc Caton
Depitent rapetaeres
Calntmotiant as
Threened toeutuse
Cuttiaue tochone soon
"epiineat bount" cpiorazotattur prptoieizotte"

Implementation Roadmap

Assessment

- Identify all edge devices and critical security vulnerabilities
- Prioritize monitoring requirements based on risk exposure and business impact

Pilot Deployment

- Implement observability solutions in highest-risk operational segments
- Evaluate performance overhead and quantify security enhancement metrics

Platform Integration

- Seamlessly connect existing security infrastructure through APIs
- Establish consolidated dashboards for visibility across entire environment

Full Implementation

- Methodically expand deployment across all edge environments
- Develop automated incident response workflows and implement continuous optimization processes

Thank you