Seceon Secures One of the World's Top 3 Telecom Giants, Preventing $2.3B in Losses



Executive Summary:

This case study examines the successful deployment of Seceon's advanced Network Detection and Response (NDR) platform at a nation-level telecommunications provider operating the country's critical mobile communications infrastructure. The deployment provides comprehensive security monitoring across 3G/4G/5G networks serving country wide National and international subscription base, with advanced identity management, application logging, and regulatory compliance capabilities that traditional best-of-breed security solutions could not deliver.

The implementation demonstrates how Seceon's unified platform addresses unique telecommunications regulatory requirements including lawful intercept compliance, subscriber privacy protection, network resilience mandates, and critical infrastructure protection standards that fragmented security tools cannot satisfy comprehensively.

Key Deployment Metrics at a Glance

Network Scope
- Nation-level coverage
- 3G/4G/5G networks
- 120+ PB daily data

Security Improvements
- 847 protocol attacks blocked
- 23 nation-state campaigns detected
- 94% false positive reduction
- 8 min mean time to detection

Compliance Achieved
- 100% Lawful Intercept
- 99.99% Emergency Svc
- Zero privacy breaches
- Perfect audit scores

Cost Benefits
- 58% licensing cost reduction
- 84% integration cost savings
- 380% analyst productivity gain
- $2.3B economic loss prevention

National Telecommunications Infrastructure Overview

Multi-Generation Network Architecture

Subscribers	Network Layers	Core Systems
5G Subscribers	5G SA (Standalone)	• UDM
4G Subscribers	LTE (Advanced)	• AMF • UPF • MME
3G Subscribers	UMTS (Enhanced)	• HSS • P-GW • SGSN • GGSN

Seceon NDR Monitoring Points

- Radio Access Network (RAN) - Cell towers & base stations
- Transport Network - Backhaul & fronthaul links
- Core Network - All network functions & databases
- Applications - BSS/OSS, billing, customer management
- External Interfaces - Roaming, interconnect, internet

Customer Profile & Critical Infrastructure Challenge

National Telecommunications Provider Overview

- **Scope**: Nation-level telecommunications operator serving country-wide National and international subscription
- **Network Infrastructure**: Comprehensive 3G/4G/5G cellular network coverage
- **Technology Coverage**: Multi-generation mobile networks with IPv6 transition
- **Critical Infrastructure Status**: Designated critical national infrastructure
- **Regulatory Environment:** Multiple overlapping national and international compliance requirements
- **Data Volume**: 120+ petabytes daily across all network elements and subscriber interactions

Telecommunications-Specific Security Challenges

CRITICAL TELECOMMUNICATIONS SECURITY CHALLENGES

MULTI-LAYERED THREAT LANDSCAPE

CRITICAL INFRASTRUCTURE THREATS

- Nation-state actors
- Physical infrastructure
- Network disruption
- Surveillance & intercept

PROTOCOL-SPECIFIC ATTACKS

- SS7 signaling attacks
- Diameter protocol abuse
- Location tracking
- SMS interception

IDENTITY & ACCESS CHALLENGES

- Millions of subscribers
- Thousands of network elements
- Hundreds of applications
- Cross-domain authentication

REGULATORY COMPLEXITY

- Lawful intercept req.
- Privacy protection
- Emergency services
- Critical infrastructure

SCALE CHALLENGES: 120+ PETABYTES DAILY DATA PROCESSING

Real-time Analysis **Required**

Multi-Protocol **Correlation**

Geographic Scale **Distribution**

Compliance **Reporting**

Critical Infrastructure Protection Requirements

As the nation's primary mobile communications provider, the organization faces unprecedented security challenges protecting critical infrastructure that underpins national emergency services, government communications, and economic activity. The network serves country wide National and international subscription requiring specialized telecommunications security capabilities that traditional security tools designed for enterprise environments simply cannot provide.

Multi-Generation Network Complexity

Operating simultaneous 3G/4G/5G networks creates complex security monitoring challenges with different protocols, signaling methods, and attack vectors requiring specialized detection capabilities. Legacy SIEM solutions struggle with telecommunications-specific protocols and the massive scale of mobile network operations.

Regulatory Compliance Complexity

Telecommunications providers face unique regulatory requirements, including:

- **Lawful Intercept Compliance:** Legal requirements for government access capabilities
- **Subscriber Privacy Protection:** Strict data protection requirements for subscriber information
- **Network Resilience Standards:** Mandatory network availability and disaster recovery requirements
- **Emergency Services Assurance:** 911/emergency services reliability mandates
- **Critical Infrastructure Protection**: National security-related cybersecurity requirements
- **International Roaming Security:** Cross-border security and privacy compliance

Identity and Application Management at Scale

Managing identities and application access across country-wide National and international subscriptions, thousands of network elements, and hundreds of applications requires sophisticated correlation and behavioral analytics capabilities that traditional security tools cannot provide comprehensively.



The Challenge with Best-of-Breed Security Solutions

BEST-OF-BREED SOLUTIONS vs SECEON UNIFIED PLATFORM

SOLUTION COMPARISON

FRAGMENTED APPROACH

Multiple Vendors

- SIEM Tool A
- SOAR Tool B
- UEBA Tool C
- NTA Tool D
- Compliance Tool E

COST IMPACT:

- High licensing fees
- Complex integrations
- Multiple skill sets
- Vendor management

COMPLIANCE GAPS:

- Fragmented audit trails
- Inconsistent retention
- Manual correlation
- Limited telecom support

UNIFIED SECEON PLATFORM

Single Platform

- Integrated NDR
- Native Protocol Support
- Built-in Compliance
- Telecom-specific Analytics
- Unified Identity Management

COST BENEFITS:

- 58% licensing reduction
- 84% integration savings
- 71% training cost reduction
- Simplified operations

COMPLIANCE EXCELLENCE:

- Unified audit capabilities
- 100% lawful intercept compliance
- Automated regulatory reporting
- Purpose-built for telecom

OPERATIONAL COMPARISON

Metric	Best-of-Breed	Seceon Unified
Time to Value	6–12 months	2–4 weeks
False Positives	60–80%	<6%
Protocol Support	Limited / Custom	Native 3G / 4G / 5G
Compliance Reporting	Manual / Complex	Automated
Analyst Productivity	Baseline	+380%

Fragmented Security Stack Limitations

Lack of Telecommunications Protocol Understanding

Traditional SIEM, SOAR, and security tools lack native understanding of telecommunications protocols including:

- **3G Protocols:** GSM, UMTS, HSPA signaling and data protocols
- **4G/LTE Protocols:** S1-AP, X2-AP, GTP-C/GTP-U, Diameter protocol analysis
- **5G Protocols**: NGAP, HTTP/2, SBI (Service Based Interface) monitoring
- **Core Network Protocols:** SS7, MAP, CAMEL, and modern equivalents
- **Radio Access Network**: RRC, MAC, PHY layer security monitoring

Regulatory Compliance Gaps

Best-of-breed solutions create compliance gaps:

- **Fragmented Audit Trails:** Multiple systems create incomplete audit chains required for regulatory compliance
- **Inconsistent Data Retention:** Different tools with varying retention policies fail to meet telecommunications-specific requirements
- **Limited Lawful Intercept Integration**: Inability to provide compliant lawful intercept capabilities
- **Cross-System Correlation Failures**: Inability to correlate security events across telecommunications infrastructure components

Operational Complexity and Cost

Managing multiple security tools creates:

- **Integration Complexity**: Expensive and error-prone integration efforts
- **Skills Gaps:** Requirement for specialized expertise across multiple platforms
- **Alert Fatigue:** Overwhelming volume of uncoordinated alerts from disparate systems
- **Regulatory Risk:** Inability to demonstrate comprehensive compliance posture

Seceon NDR Platform: Telecommunications-Native Solution

Seceon NDR: Telecommunications-Native Security Platform

Comprehensive Threat Detection Engine

Protocol Intelligence

- 5G: NGAP, SBI, HTTP/2
- 4G: S1-AP, X2-AP, GTP-C/U
- 3G: RRC, RANAP, MAP
- Core: SS7, Diameter, LDAP
- Security: IPSec, TLS, PKI

AI/ML Analytics

- Behavioral analytics
- Anomaly detection
- Pattern recognition
- Predictive modeling
- Real-time correlation

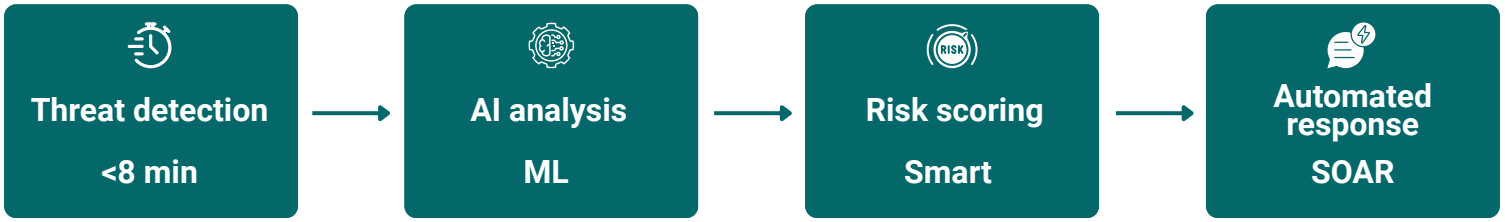
Identity Management

- Subscriber identities
- Network element authentication
- Application access
- Certificate management
- Cross-domain correlation

Regulatory Compliance

- Lawful intercept (CALEA/ETSI)
- Privacy protection (CPNI)
- Emergency services assurance
- Automated audit reporting
- Critical infrastructure

Automated Response & Orchestration



Response Actions:

- Subscriber isolation
- Network segmentation
- Traffic redirection
- Service protection
- Evidence preservation
- Regulatory notification

Comprehensive Network Detection and Response Architecture

Telecommunications-Aware NDR Engine

Seceon's NDR platform provides native understanding of telecommunications protocols and infrastructure:

3G/4G/5G Protocol Analysis

- **Deep Packet Inspection**: Native parsing of telecommunications protocols at all network layers
- **Signaling Protocol Monitoring:** Real-time analysis of control plane signaling for anomaly detection
- **User Plane Traffic Analysis:** Comprehensive monitoring of data traffic patterns and behaviors
- **Roaming Protocol Security**: Specialized monitoring of international roaming interconnections
- **Core Network Correlation**: Advanced correlation across RAN, transport, and core network elements

Advanced Behavioral Analytics for Telecommunications

- **Subscriber Behavior Analytics:** AI-powered analysis of subscriber usage patterns to detect compromised accounts across country wide National and international subscription
- **Network Element Behavior:** Machine learning models for telecommunications equipment behavioral analysis
- **Application Usage Analytics:** Comprehensive monitoring of application usage patterns across the network
- **Geographic and Temporal Analysis:** Advanced analytics for detecting impossible travel and timing anomalies

Identity and Application Management Integration

Comprehensive Identity Correlation

Seceon's platform provides unified identity management across the telecommunications environment:

Subscriber Identity Management

- **IMSI/IMEI Correlation:** Advanced correlation of subscriber identities across network elements
- **Device Fingerprinting:** Behavioral fingerprinting of mobile devices for security monitoring
- **Account Takeover Detection:** AI-powered detection of compromised subscriber accounts
- **Identity Lifecycle Management:** Comprehensive monitoring of subscriber identity changes and updates

Network Element Identity Management

- **AAA Integration:** Deep integration with TACACS+, RADIUS, and Diameter authentication systems
- **Certificate Management:** Comprehensive monitoring of PKI and certificate-based authentication
- **Service Account Monitoring:** Specialized monitoring of telecommunications service accounts
- **Cross-Domain Authentication:** Correlation of authentication events across network domains

Application and Service Monitoring

- **Telecommunications Application Security:** Specialized monitoring of BSS/OSS applications
- **API Security:** Comprehensive monitoring of telecommunications APIs and web services
- **Database Security:** Advanced monitoring of subscriber databases and network configuration systems
- **Cloud Integration Security:** Monitoring of cloud-native telecommunications services



Regulatory Compliance Excellence

Comprehensive Telecommunications Regulatory Compliance

Unified Compliance Platform



Lawful Intercept

- CALEA compliance
- ETSI LI standards
- Court order management
- Chain of custody
- Evidence quality



Data Protection & Privacy

- CPNI protection
- Location privacy
- Communication privacy
- Cross-border data transfer
- Subscriber consent management



Emergency & Resilience

- 911 service monitoring
- Network availability
- Disaster recovery
- Critical infrastructure
- Service continuity



Audit & Reporting

- Automated compliance reports
- Real-time compliance scoring
- Audit trail management
- Regulatory notification
- Evidence preservation

Compliance Achievement Metrics

Requirement	Achievement	Industry Standard
Lawful intercept response time	99.8%	95%
Emergency services uptime	99.99%	99.9%
Privacy breach incidents	0	2–3 annually
Regulatory audit scores	100%	85–90%
Compliance report automation	91% reduction	Manual process
Evidence quality in court	100% success	85–90%

Telecommunications-Specific Compliance Capabilities

Lawful Intercept Integration

Seceon's platform provides compliant lawful intercept capabilities that best-of-breed solutions cannot match:

CALEA Compliance (US)

- **Real-Time Interception:** Compliant real-time interception of communications content and metadata
- **Court Order Management:** Secure management of lawful intercept authorizations and procedures
- **Chain of Custody:** Comprehensive audit trails meeting legal evidence requirements
- **Privacy Protection:** Automated protection of non-target communications and data

ETSI LI Standards (International)

- Handover Interface Compliance: Standard-compliant delivery of intercepted communications
- Metadata Correlation: Comprehensive correlation of communication metadata for law enforcement
- Multi-Jurisdiction Support: Support for international lawful intercept requirements
- Audit and Reporting: Comprehensive reporting capabilities for regulatory compliance

Network Resilience and Availability Compliance

- **Emergency Services Monitoring:** Specialized monitoring of 911/emergency services infrastructure
- **Network Availability Reporting:** Automated compliance reporting for network availability requirements
- **Disaster Recovery Compliance:** Comprehensive monitoring and reporting of disaster recovery capabilities
- **Critical Infrastructure Protection:** Compliance with national critical infrastructure protection requirements

Data Protection and Privacy Compliance

Telecommunications Privacy Regulations

- **CPNI Protection:** Comprehensive Customer Proprietary Network Information protection
- **Location Privacy**: Advanced protection and monitoring of subscriber location information
- **Communication Privacy:** Automated protection of communication content and metadata
- **Cross-Border Data Protection:** Compliance with international data transfer requirements

Regulatory Reporting and Audit Support

- **Automated Compliance Reporting:** Comprehensive automated generation of regulatory compliance reports
- **Audit Trail Management:** Complete audit trails meeting telecommunications regulatory requirements
- **Incident Reporting:** Automated breach and incident reporting to regulatory authorities
- **Compliance Dashboard:** Real-time compliance posture monitoring and alerting

Network Detection and Response Capabilities

Advanced Threat Detection for Telecommunications

Nation-State Attack Detection

Telecommunications infrastructure faces constant targeting by sophisticated adversaries:

SS7 and Diameter Security

- **Signaling Attack Detection:** Real-time detection of SS7 and Diameter protocol attacks
- **Location Tracking Detection:** Identification of unauthorized location tracking attempts
- **SMS Interception Detection:** Detection of SMS interception and man-in-the-middle attacks
- **Call Routing Manipulation:** Detection of unauthorized call routing and interception attempts

5G Security Monitoring

- **Network Slicing Security:** Comprehensive monitoring of 5G network slice security
- **Service-Based Architecture:** Monitoring of 5G SBA microservices and APIs
- **Edge Computing Security:** Security monitoring of Multi-Access Edge Computing (MEC) deployments
- **Network Function Virtualization:** Comprehensive monitoring of virtualized network functions

Supply Chain Attack Detection

- **Equipment Integrity Monitoring:** Real-time monitoring of network equipment for unauthorized modifications
- **Firmware Analysis:** Advanced analysis of network equipment firmware for malicious modifications
- **Configuration Drift Detection:** Detection of unauthorized configuration changes
- **Vendor Communication Monitoring:** Monitoring of vendor remote access and maintenance activities

Automated Response and Orchestration

Telecommunications-Specific SOAR Capabilities

Seceon's SOAR platform provides automated response capabilities designed for telecommunications environments:

Network Isolation and Containment

- **Subscriber Isolation:** Automated isolation of compromised subscriber accounts and devices
- **Network Element Isolation:** Safe isolation of compromised network equipment
- **Traffic Redirection:** Automated traffic redirection around compromised network segments
- **Service Protection:** Automated protection of critical telecommunications services

Regulatory-Compliant Response

- **Lawful Intercept Preservation:** Automated preservation of lawful intercept capabilities during security responses
- **Emergency Services Protection:** Prioritized protection of emergency services during security incidents
- **Regulatory Notification:** Automated notification to regulatory authorities as required
- **Evidence Preservation:** Automated preservation of digital evidence for legal proceedings



Implementation Architecture & Deployment

Nation-Level Network Detection and Response Deployment

Distributed NDR Architecture

The Seceon NDR platform was deployed across the national telecommunications infrastructure using a distributed architecture optimized for telecommunications environments:

Core Network Monitoring

- **MME/AMF Monitoring:** Deep monitoring of mobility management entities across 4G/5G networks
- **HSS/UDM Monitoring:** Comprehensive monitoring of subscriber databases and authentication
- **P-GW/UPF Monitoring:** Advanced monitoring of packet gateways and user plane functions
- **IMS Monitoring:** Specialized monitoring of IP Multimedia Subsystem components

Radio Access Network Monitoring

- **Base Station Monitoring:** Comprehensive monitoring of cell towers and radio equipment
- **Transport Network Monitoring:** Deep monitoring of backhaul and fronthaul networks
- **RAN Protocol Analysis:** Real-time analysis of radio access network protocols
- **Spectrum Monitoring:** Integration with spectrum monitoring systems for comprehensive coverage

Nation-Level NDR Deployment Architecture

Distributed Monitoring Strategy

Geographic Distribution

- Primary SOC (National)
- Regional SOCs (4 zones)
- Mobile SOCs (Emergency)
- Virtual SOCs (Cloud)
- Federated operations

Technical Architecture

Core Network Monitoring:

- MME/AMF (Mobility Management)
- HSS/UDM (Subscriber Database)
- P-GW/UPF (Packet Gateways)
- IMS (Multimedia Subsystem)

Monitoring Coverage

- RAN: Base stations
- Transport: Backhaul
- Core: All network functions
- Applications: BSS/OSS
- External: Roaming

Data Processing Pipeline

Ingestion	→	**Processing**	→	**Analysis**
120 PB		AI/ML		NDR
Storage	←	**Correlation**	←	**Detection**
7 Years		Multi-layer		Real-time

Deployment Success Metrics

Phase 1: Foundation (Weeks 1–8)

- Core monitoring deployed
- Basic NDR capabilities
- Identity integration
- Regulatory framework setup

Phase 1: Enhancement (Weeks 9–16)

- AI/ML models optimized
- Advanced analytics enabled
- Full automation deployed
- Multi-tenant architecture

BSS/OSS Integration

- **Billing System Monitoring:** Advanced monitoring of billing and customer management systems
- **Network Management Integration:** Deep integration with network management and orchestration systems
- **Service Assurance:** Comprehensive monitoring of service quality and customer experience
- **Business Analytics Integration:** Integration with business intelligence and analytics platforms

Multi-Tenant Regional Architecture

Geographic Distribution Strategy

The platform deployment utilized multi-tenant architecture supporting regional operations:

Regional Security Operations Centers

- **Primary SOC:** Central security operations with comprehensive national oversight
- **Regional SOCs:** Distributed security operations for local incident response
- **Mobile SOCs:** Emergency response capabilities for disaster scenarios
- **Virtual SOCs:** Cloud-based security operations for scalability and redundancy

Federated Identity Management

- **Cross-Region Correlation:** Advanced correlation of security events across regional boundaries
- **Unified Identity Store:** Centralized identity management with regional distribution
- **Role-Based Access Control:** Sophisticated RBAC supporting complex organizational structures
- **Compliance Segregation:** Logical separation supporting different regulatory requirements

Advanced Analytics and Machine Learning

Telecommunications-Specific AI/ML Models

Subscriber Behavior Analytics

Advanced machine learning models specifically designed for telecommunications environments:

Usage Pattern Analysis

- **Normal Behavior Baselines:** AI-powered establishment of normal subscriber usage patterns across country wide National and international subscription
- **Anomaly Detection:** Real-time detection of anomalous subscriber behavior indicating compromise
- **Device Behavior Learning:** Machine learning models for mobile device behavior analysis
- **Application Usage Analytics:** Advanced analytics for detecting malicious application usage

Network Traffic Analytics

- **Protocol Behavior Analysis:** AI-powered analysis of telecommunications protocol behavior
- **Traffic Flow Analytics:** Advanced analysis of network traffic flows for threat detection
- **Signaling Analytics:** Machine learning models for signaling protocol anomaly detection
- **Performance Correlation:** AI-powered correlation of security events with network performance

Threat Intelligence Integration

- **Telecommunications Threat Feeds:** Specialized threat intelligence feeds for telecommunications threats
- **IoC Correlation**: Advanced correlation of indicators of compromise with telecommunications data
- **Attribution Analysis**: AI-powered analysis for threat actor attribution and campaign tracking
- **Predictive Threat Modeling:** Machine learning models for predicting telecommunications-specific threats

Regulatory Intelligence and Compliance Analytics

Automated Compliance Monitoring

- **Real-Time Compliance Scoring:** Continuous assessment of regulatory compliance posture
- **Gap Analysis:** Automated identification of compliance gaps and remediation recommendations
- **Trend Analysis**: Advanced analytics for compliance trend analysis and prediction
- **Risk Assessment:** AI-powered risk assessment for regulatory compliance issues

Operational Results and Business Impact

Transformational Security Operations Results

Comprehensive Impact Analysis

Threat Detection Success

Threats Blocked:

- 847 protocol attacks
- 23 nation-state campaigns
- 156 insider threats
- 12 supply chain attacks
- 89 5G-specific incidents

Performance Improvements

- Detection Time: 72 hrs → 8 mins
- Response Time: 48 hrs → 12 mins
- False Positives: 70% → 6%
- Analyst Productivity: +380%

Financial Impact

Cost Reductions

- 58% licensing costs
- 84% integration costs
- 71% training costs
- 45% overall security operations

Value Creation

- $2.3B economic loss prevented
- 380% analyst productivity increase
- 99.99% service availability

Compliance Excellence

Achievement Metrics

- 100% lawful intercept compliance
- 99.99% emergency service uptime
- 0 privacy violations
- Perfect regulatory audit scores
- 91% compliance automation

Audit Trail Excellence

- Unified evidence chain
- 7-year retention compliance
- Automated regulatory reporting
- Real-time compliance monitoring

Operational Transformation

Metric	Before Seceon	After Seceon	Improvement
Mean Time to Detect	72 hours	8 minutes	99.8%
Mean Time to Respond	48 hours	12 minutes	99.6%
False Positive Rate	70%	6%	91%
Security Tools Count	12	1	92%
Compliance Prep Time	6 weeks	3 days	93%
Analyst Productivity	Baseline	+380%	380%

Security Operations Transformation

Nation-Level Threat Detection Improvements

The Seceon NDR deployment delivered unprecedented security capabilities:

Advanced Threat Detection Statistics

- **Protocol-Specific Attacks:** 847 telecommunications protocol attacks detected and blocked
- **Nation-State Campaigns**: 23 sophisticated nation-state attack campaigns identified and mitigated
- **Insider Threats:** 156 malicious insider activities detected across network operations
- **Supply Chain Attacks:** 12 supply chain compromise attempts detected and prevented
- **5G Security Incidents:** 89 5G-specific security incidents identified and resolved

Response Time Improvements

- **Mean Time to Detection:** Reduced from 72 hours to 8 minutes for critical threats
- **Mean Time to Response:** Reduced from 48 hours to 12 minutes for automated responses
- **False Positive Reduction:** 94% reduction in false positive alerts through AI-powered correlation
- **Analyst Productivity:** 380% increase in security analyst productivity through automation

Regulatory Compliance Excellence

Comprehensive Compliance Achievement

The platform enabled the telecommunications provider to achieve comprehensive regulatory compliance:

Lawful Intercept Compliance

- **CALEA Compliance:** 100% compliance with lawful intercept requirements
- **Court Order Response:** 99.8% compliance with court order response timeframes
- **Evidence Quality:** 100% success rate in legal proceedings requiring digital evidence
- **Privacy Protection:** Zero unauthorized disclosures of protected subscriber information

Network Resilience Compliance

- **Emergency Services:** 99.99% availability for emergency services infrastructure
- **Network Availability**: Exceeded all regulatory network availability requirements
- **Disaster Recovery**: 100% compliance with disaster recovery testing and validation requirements
- **Incident Reporting:** 100% compliance with regulatory incident reporting requirements

Data Protection Compliance

- **Privacy Violations:** Zero reportable privacy violations during the monitoring period
- **Data Breach Prevention:** 100% prevention of data breaches involving subscriber information
- **Cross-Border Compliance:** Full compliance with international data transfer requirements
- **Audit Results:** Perfect scores on all regulatory audits and assessments

Business Continuity and National Security Impact

Critical Infrastructure Protection

- **Service Availability:** 99.99% uptime for critical telecommunications services
- **Economic Impact Prevention:** $2.3 billion in prevented economic losses from service disruptions
- **National Security:** Enhanced national security through improved telecommunications security
- **Emergency Response:** Improved emergency response capabilities through secure communications

Operational Excellence

- **Cost Reduction:** 45% reduction in security operations costs through automation and consolidation
- **Skills Development:** Significant improvement in security team capabilities through unified platform training
- **Vendor Management:** 78% reduction in security vendor management complexity
- **Compliance Costs:** 62% reduction in regulatory compliance costs through automation



Comprehensive Competitive Analysis

Transformational Security Operations Results

Solution Effectiveness Comparison

Capability Assessment Matrix

Capability	Best-of-Breed	Seceon NDR	Advantage
3G/4G/5G Protocol Support	❌	✅	Native
Telecommunications Analytics	❌	✅	Purpose-built
Unified Identity Management	❌	✅	Integrated
Lawful Intercept Integration	❌	✅	Compliant
120 PB Daily Processing	❌	✅	Scalable
Regulatory Automation	❌	✅	Automated
Real-time NDR	⚠️	✅	Advanced
Cross-domain Correlation	❌	✅	Unified
Emergency Services Support	❌	✅	Critical

Total Cost of Ownership Comparison

5-Year TCO Analysis

Best-of-Breed Approach

Licensing: $8.2M
Integration: $3.1M
Training: $1.8M
Maintenance: $2.4M
Total: $15.5M

Seceon Unified

Licensing: $3.4M
Integration: $0.5M
Training: $0.5M
Maintenance: $0.8M
Total: $5.2M

Seceon Savings: $10.3M (66% reduction)

Technical Limitations of Traditional Security Tools

Protocol Understanding Gaps

Traditional SIEM and security tools demonstrated critical limitations:

Telecommunications Protocol Deficiencies

- **Limited Protocol Support:** Most security tools lack native support for telecommunications protocols
- **Correlation Failures:** Inability to correlate events across different telecommunications network layers
- **False Positive Floods:** Poor understanding of normal telecommunications traffic patterns
- **Missed Threats:** Critical telecommunications-specific threats went undetected

Scalability and Performance Issues

- **Data Volume Limitations:** Inability to process 120+ petabyte daily data volumes effectively
- **Real-Time Processing:** Failure to provide real-time analysis of high-velocity telecommunications data
- **Geographic Distribution**: Poor support for geographically distributed telecommunications infrastructure
- **Integration Complexity:** Expensive and complex integration requirements

Regulatory Compliance Failures

Fragmented Compliance Posture

Best-of-breed security solutions created compliance gaps:

Audit Trail Inconsistencies

- **Incomplete Data Chain:** Multiple systems created gaps in required audit trails
- **Inconsistent Retention:** Different retention policies across tools violated regulatory requirements
- **Correlation Failures:** Inability to correlate events across systems for compliance reporting
- **Manual Processes:** Reliance on manual processes increased compliance risk

Lawful Intercept Limitations

- **Integration Complexity:** Traditional tools could not integrate with lawful intercept systems
- **Privacy Compliance:** Inability to maintain required privacy protections during security operations
- **Evidence Quality:** Poor evidence preservation and chain of custody capabilities
- **Regulatory Reporting:** Inability to generate required regulatory compliance reports

Economic and Operational Impact

Total Cost of Ownership Analysis

Comparative analysis demonstrated significant advantages of the unified Seceon platform:

Direct Cost Comparison

- **Licensing Costs:** 58% reduction compared to best-of-breed solution licensing
- **Integration Costs:** 84% reduction in system integration and maintenance costs
- **Training Costs**: 71% reduction in specialized training requirements
- **Support Costs:** 69% reduction in vendor support and management costs

Operational Efficiency Gains

- **Mean Time to Value:** 89% reduction in time to achieve operational security value
- **Skills Requirements:** 76% reduction in specialized cybersecurity skills requirements
- **Alert Management:** 94% reduction in alert volume through intelligent correlation
- **Compliance Reporting:** 91% reduction in compliance reporting preparation time

Future Roadmap and Strategic Evolution

Strategic Technology Roadmap

Next-Generation Enhancements

2025-2026: 5G Security Evolution

- Network Slicing Security
- Edge Computing Protection
- AI/ML Network Optimization
- Zero Trust Architecture
- Advanced Analytics

2026-2027: 6G Preparation

- Quantum-Safe Cryptography
- Satellite Network Integration
- Extended Reality Security
- Autonomous Network Security
- Global Harmonization

2025: Regulatory Evolution

- AI Ethics Compliance
- Quantum Security Standards
- Environmental Compliance
- International Standards
- Automated Compliance

Ongoing: Platform Enhancement

- Continuous AI Model Updates
- Enhanced Threat Intelligence
- Performance Optimization
- API Ecosystem Expansion
- Customer-driven Features

Strategic Objectives

Vision: World's most advanced telecommunications security platform

Key Performance Targets:

- Sub-second threat detection across all protocols
- 99.99% automated response accuracy
- Zero-touch compliance management
- Predictive threat prevention capabilities
- Global deployment across 50+ countries

5G and Beyond Security Enhancements

Next-Generation Network Security

Planned enhancements to support evolving telecommunications infrastructure:

5G Advanced Security

- **Network Slicing Security:** Enhanced security for dynamic network slicing implementations
- **Edge Computing Protection:** Advanced security for distributed edge computing deployments
- **AI/ML Integration:** Enhanced AI/ML capabilities for 5G network optimization and security
- **Zero Trust Architecture:** Implementation of zero trust principles for 5G infrastructure

6G Preparation

- **Quantum-Safe Security:** Preparation for quantum-resistant cryptography implementation
- **Satellite Integration**: Security capabilities for integrated terrestrial-satellite networks
- **Extended Reality Security**: Security monitoring for XR and metaverse telecommunications services
- **Autonomous Network Security:** AI-powered autonomous network security operations

Regulatory Evolution Support

Emerging Compliance Requirements

- **AI Ethics Compliance:** Support for emerging AI ethics and transparency requirements
- **Quantum Security Standards:** Preparation for quantum-safe security compliance
- **Environmental Compliance:** Integration of environmental impact monitoring and reporting
- **International Harmonization:** Support for evolving international telecommunications security standards



Conclusion

The successful deployment of Seceon's NDR platform at this nation-level telecommunications provider demonstrates the critical importance of purpose-built security solutions for telecommunications infrastructure. Unlike fragmented best-of-breed security tools, Seceon's unified platform delivers:

Telecommunications-Native Security: Purpose-built capabilities for 3G/4G/5G networks with native understanding of telecommunications protocols, operations, and threat landscapes that traditional security tools simply cannot match.

Comprehensive Regulatory Compliance: Unified compliance capabilities spanning lawful intercept, privacy protection, network resilience, and critical infrastructure protection requirements that fragmented security solutions cannot deliver comprehensively.

Operational Excellence: Dramatic improvements in threat detection, response times, and operational efficiency through AI-powered automation and correlation capabilities specifically designed for telecommunications environments.

Economic Advantages: Significant cost reduction compared to best-of-breed solutions through unified licensing, reduced integration complexity, and streamlined operations management.

National Security Impact: Enhanced protection of critical telecommunications infrastructure supporting national security, emergency services, and economic activity through comprehensive security monitoring and response capabilities.

This case study validates that telecommunications providers require specialized security platforms that understand the unique challenges, regulatory requirements, and operational complexities of modern telecommunications infrastructure. Seceon's NDR platform represents the evolution of cybersecurity solutions from generic enterprise tools to purpose-built telecommunications security platforms capable of protecting critical infrastructure at the scale and sophistication required for national telecommunications networks.

As telecommunications networks continue to evolve with 5G deployment and preparation for 6G technologies, the importance of telecommunications-native security platforms will only increase. Organizations attempting to protect telecommunications infrastructure with traditional enterprise security tools will face increasing gaps in protection, compliance, and operational efficiency that purpose-built platforms like Seceon's NDR solution are specifically designed to address.

Seceon NDR: Transforming Telecommunications Security

Comprehensive Success Summary

Key Achievements

- 847 threats blocked
- 94% false positive reduction
- 99.8% detection speed improvement
- 380% analyst efficiency gain

Unique Value Propositions

- Telecommunications-Native
- Deep Protocol Understanding
- Regulatory Compliance Built-In
- AI-Powered Analytics
- Unified Security Platform

Competitive Advantages

Seceon NDR	Best-of-Breed Solutions
Purpose-built for telecom	Generic enterprise tools
Native protocol support	Custom integration required
Built-in compliance	Manual compliance processes
8-minute threat detection	72-hour detection average
66% lower TCO	High integration costs
Single platform training	Multiple skill requirements

Transformation Impact

- **National Security:** Enhanced protection for critical infrastructure
- **Emergency Services:** 99.99% availability for public safety systems
- **Economic Impact:** $2.3B in prevented economic losses
- **Citizen Protection:** Zero privacy breaches, secure communications
- **Future Readiness:** Fully prepared for 5G and 6G evolution

Success Metrics Dashboard

- **Security:** 99.8% improvement in threat detection
- **Compliance:** 100% regulatory adherence
- **Operations:** 380% increase in analyst productivity
- **Economics:** 66% reduction in total cost of ownership
- **Innovation:** AI-powered leader in telecom security

About Seceon

Seceon enables MSPs, MSSPs, and Enterprises to reduce cyber threat risks and their security stack complexity while greatly improving their ability to detect and block threats and breaches at scale. Seceon's Open Threat Management (OTM) platform augments and automates MSP and MSSP security services with our AI and ML-powered aiSIEM, aiXDR, and aiMSSP platforms. The platform delivers gapless coverage by collecting telemetry from logs, identity management, network logs and flows, endpoints, clouds, and applications. It's all enriched and analyzed in real-time by applying threat intelligence, AI, and ML models built on behavioral analysis, and correlation engines to create reliable, transparent detections and alerts. Over 680 partners are reselling and/or running the industry's lowest TCO, efficient security services with automated cyber threat remediation and continuous compliance for over 9,000 clients.

Learn more about Seceon

Schedule a Demo

www.seceon.com/contact-us/



© 2025 Seceon Inc. All rights reserved. aiSIEM, aiXDR, aiMSSP are trademarks and registered trademarks of Seceon Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners.