Inteltel

TECHNOLOGY FOR A MORE SECURE TOMORROW

SOLUTION DATASHEET
Managed IT & Security Operations

Managed IT & Security Operations for the AI Era

Operate Smarter. Secure Continuously. Improve Proactively.

Inteltel delivers managed IT and security operations built for today's hybrid, cloud and AI-enabled environments—helping you maintain availability, strengthen security, and continuously improve performance.



- Proactive Operations
- Stronger Security
- Faster Response
- Improved Performance
- Reduced Complexity
- Aligned with Business Goals

www.inteltel.com | info@inteltel.com | (866) 466-8358

STRATEGY | SECURITY | OPERATIONS | RESULTS

EXECUTIVE OVERVIEW

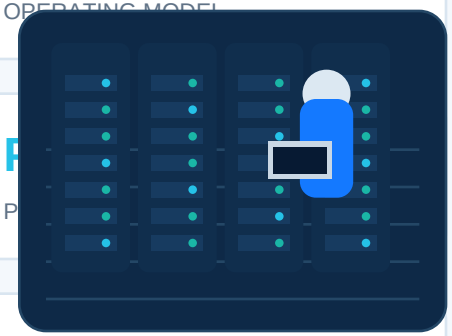
Managed IT & Security Operations for the AI Era

Modern IT operations extend across corporate networks, data centers, cloud platforms, SaaS applications, cybersecurity systems, endpoints, remote users, and increasingly AI-enabled workloads. Managing these environments requires more than responding to individual incidents - it requires continuous visibility, disciplined operations, experienced engineering, and ongoing optimization.

Inteltel brings daily support and long-term improvement into one coordinated operating model. Defined service levels, documented procedures, regular reviews, automation, analytics, and AI-assisted capabilities provide clear accountability and help align IT operations with business priorities.

24/7 + AI

OPERATING MODEL



HUMAN LED

CONTROL PRINCIPLE

THE SHIFT

Reactive Support → Proactive Operations → Predictive Improvement

AI assists with analysis and prioritization; engineering and security teams retain accountability for consequential decisions.

OVERVIEW

Why Operations Must Evolve

1 Hybrid Complexity

Infrastructure now spans branches, remote users, data centers, SaaS, public cloud, private cloud, and multiple security domains.

2 Alert Volume

Operations teams face high event volumes, fragmented tools, duplicated alerts, and growing pressure to resolve issues faster.

3 A

AI work
security
service-management requirements.



The operating challenge

Organizations need an operating model that can correlate signals across technology domains, prioritize events by business impact, automate repeatable tasks, and keep experienced people in control of architecture, security, and risk decisions.

Visibility → Context → Priority → Action → Learning

OVERVIEW

Five Operating Principles

1 Business-Aligned

Prioritize technology operations according to critical services, users, risk, and business impact.

2 Observable

Build continuous visibility across network, cloud, infrastructure, applications, identity, and security.

3 Automated with Control

Automate repeatable work while retaining approval and oversight for consequential actions.

4 Secure by Design

Integrate security operations, access controls, configuration discipline, and incident response.

5 Continuously Improving

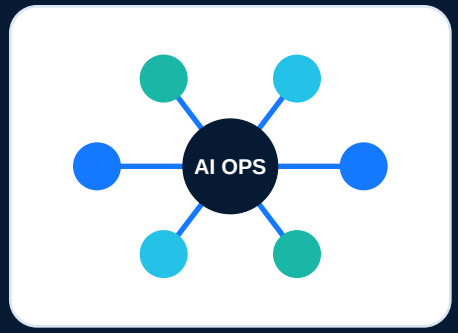
Use trends, incidents, capacity data, and service reviews to improve the environment over time.

BUSINESS BENEFITS

Operational Outcomes That Matter

Six benefits of a coordinated AI-assisted operating model

The goal is not automation for its own sake. Inteltel uses monitoring, analytics, engineering, security practices, and AI-assisted intelligence to improve service quality, reduce operational friction, and support better technology decisions.



Proactive → Secure → Faster → Available → Simpler → Aligned

BUSINESS OUTCOME

Greater resilience + stronger security + better service availability

with reduced operational complexity and clearer accountability across the enterprise.

BUSINESS BENEFITS

Benefits 1-3

1 Proactive IT Operations

Continuous monitoring and operational analytics help identify performance degradation, infrastructure issues, and potential service disruption earlier.

BUSINESS VALUE

Earlier intervention

2 Stronger Security Operations

Coordinate security monitoring, access controls, incident management, vulnerability priorities, and escalation procedures across the environment.

BUSINESS VALUE

Lower security exposure

3 Faster Incident Response

Centralized visibility, defined escalation, automation, and AI-assisted analysis help teams investigate and prioritize incidents more efficiently.

BUSINESS VALUE

Shorter time to action

BUSINESS BENEFITS

Benefits 4-6

4 Improved Performance & Availabili

Ongoing maintenance, capacity management, configuration review, and optimization help improve reliability of critical business services.

BUSINESS VALUE

More reliable services

5 Reduced Operational Complexity

Bring network, cloud, infrastructure, security, and support activities into a coordinated operational framework with consistent processes.

BUSINESS VALUE

Simpler operations

6 Continuous Business Alignment

Executive reviews, capacity forecasts, optimization recommendations, and roadmaps keep operations aligned with evolving business priorities.

BUSINESS VALUE

Better investment decisions

CAPABILITIES

Integrated Operations Capability Map



24/7 Monitoring

Integrated service domain

Network Operations

Integrated service domain

Cloud & Hybrid IT

Integrated service domain

Security Operations

Integrated service domain

AI-Assisted Operations

Integrated service domain

Incident & Problem Mgmt

Integrated service domain

Change & Configuration

Integrated service domain

Capacity & Performance

Integrated service domain

Lifecycle & Vendor Mgmt

Integrated service domain

Service Governance

Integrated service domain

CAPABILITIES

Core IT Operations

1 24/7 Monitoring & Event Management

Monitor critical infrastructure, networks, systems, cloud services, and security events with defined alerting and escalation.

2 Network & Infrastructure Operations

Support routing, switching, SD-WAN, wireless, Internet connectivity, data-center infrastructure, and critical enterprise platforms.

3 Cloud & Hybrid IT Operations

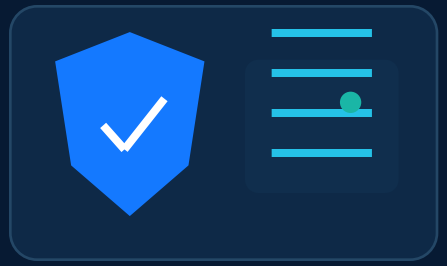
Manage and optimize infrastructure distributed across on-premises environments, private clouds, public clouds, and hybrid architectures.

4 Capacity & Performance Management

Analyze utilization, performance trends, infrastructure health, and growth requirements to support proactive planning.

CAPABILITIES

Security Operations & Control



1 Managed Security Operations

Coordinate security monitoring, firewall management, access controls, threat detection, incident escalation, and policy improvement.

2 Incident & Problem Management

Use structured processes for response, escalation, root-cause analysis, corrective action, and recurring-problem reduction.

3 Configuration & Change Management

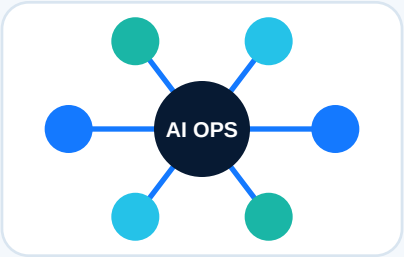
Maintain documented configurations and controlled change procedures to reduce operational risk and improve consistency.

4 Lifecycle & Vendor Management

Coordinate maintenance, upgrades, support cases, vendor relationships, lifecycle planning, and modernization.

CAPABILITIES

AI-Assisted Operations - Human-Governed by Design



Event Correlation

Connect related alerts and telemetry to improve context.

Capacity Analysis

Identify utilization trends and potential constraints.

Anomaly Identification

Surface unusual patterns for engineering review.

Recommended Remediation

Suggest next actions based on approved procedures and context.

Alert Enrichment

Add asset, service, dependency, and historical context.

Operational Summaries

Condense incidents and trends for faster review.

Ticket Classification

Assist routing, categorization, and prioritization.

Continuous Learning

Use outcomes and service reviews to refine rules and workflows.

Governance principle: AI assists with analysis and recommendations; people approve consequential security, architecture, and policy changes.

AI-DRIVEN OPERATIONS MODEL

Monitor → Detect → Analyze → Prioritize → Respond → Optimize

1 MONITOR

Continuous visibility across networks, cloud, applications, security systems, and critical services.

2 DETECT

Identify anomalies, service degradation, failures, and potential threats earlier.

3 ANALYZE

Correlate operational and security information to understand context and likely cause.

4 PRIORITIZE

Rank events using severity, service impact, security risk, and business importance.

5 RESPOND

Use procedures, automation, escalation, and engineering expertise to restore and protect.

6 OPTIMIZE

Use trends, incident history, capacity data, and reviews to continuously improve.

AI-DRIVEN OPERATIONS MODEL

From Reactive to Predictive Operations



A continuous improvement loop

Each operating cycle produces new telemetry, incident knowledge, performance history, and service insight. That information feeds the next cycle, helping teams improve detection quality, operational procedures, capacity decisions, and automation over time.

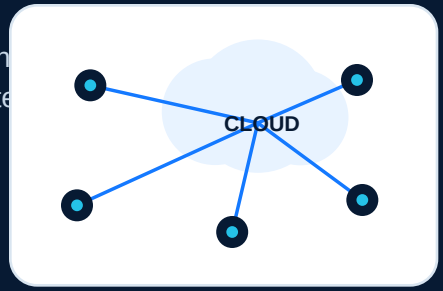


Target state: proactive, secure, data-driven operations with AI assistance and human accountability.

IMPLEMENTATION ROADMAP

Assess → Design → Integrate → Automate → Operate → Optimize

Inteltel uses a phased implementation approach designed to modernize operations while minimizing disruption to existin
establishes the foundation required for the next stage and can be adapted to organizational maturity, risk, budget, and te



Assess → Design → Integrate → Automate → Operate → Optimize

IMPLEMENTATION PRINCIPLE

Modernize progressively - prove value - expand with control.

The roadmap supports staged adoption rather than a disruptive all-at-once transformation.

IMPLEMENTATION ROADMAP

Phases 1-3: Foundation & Visibility

1

1. Assess & Discover

Assess network, cloud, applications, security systems, tools, processes, service dependencies, and existing automation. Identify visibility gaps, recurring incidents, manual work, risk, and capacity constraints.

OUTCOME

Current-state assessment + prioritized requirements

2

2. Design & Plan

Define the target operating model, monitoring requirements, telemetry, integrations, escalation, automation opportunities, governance, service levels, and performance indicators.

OUTCOME

Target architecture + implementation plan

3

3. Integrate & Establish Visibility

Connect critical infrastructure, cloud platforms, applications, security systems, and operational tools. Establish dashboards, alerts, telemetry, baselines, and event correlation.

OUTCOME

Unified operational visibility

Phases 4-6: Intelligence & Continuous Improvement

4. Automate & Apply AI

Introduce event correlation, anomaly identification, alert enrichment, ticket classification, capacity analysis, and recommended remediation with defined controls.

OUTCOME

Reduced manual workload + better intelligence

5. Operate & Respond

Transition into structured monitoring, incident management, escalation, maintenance, security operations, and service-management processes.

OUTCOME

Consistent and measurable operations

6. Optimize & Evolve

Review performance, incident trends, capacity, security conditions, automation effectiveness, service levels, and emerging business requirements.

OUTCOME

Continuous improvement + roadmap evolution

SERVICE GOVERNANCE

Measure, Review, Improve

1 Service Levels

Availability, response, resolution, escalation, and support commitments.

2 Operational KPIs

Incident trends, alert quality, recurring problems, performance, and capacity.

3 Security KPIs

Security events, control effectiveness, exposure, response, and remediation.

4 Executive Reviews

Business impact, service performance, risk, priorities, and investment decisions.

5 Optimization

Automation opportunities, architecture improvements, lifecycle actions, and cost efficiency.

6 Roadmap

Near-term actions and longer-term modernization aligned with business strategy.

INTELTEL MANAGED IT & SECURITY OPERATIONS

Operate Smarter.
Secure Continuously.
Improve Proactively.

Inteltel helps organizations transform technology operations from reactive support into a proactive, secure, data-driven, and AI-assisted operating model - providing the visibility, expertise, accountability, and continuous improvement required for the AI era.



OPERATIONS OBJECTIVE

Keep Systems Available. Keep Security Active. Keep Business Moving.

Start the conversation

www.inteltel.com
info@inteltel.com
1-888-676-6261