Calance SOCaaS

## Making SOC-as-a-Service (SOCaaS) Simple

Our Security Operation Center (SOC) combines Artificial Intelligence and trained SOC Engineers to continuously monitor all network activity and quickly detect patterns indicative of malicious behavior.

This service delivers SOC capabilities at a simple and predictable pricing model, enabling businesses of all sizes to implement leading security operations capabilities. Our SOCaaS is SOC2 certified and our experts are trained to handle a variety of situations.

Calance SOCaaS Capabilities – Simple Install Security SME

Dedicated Security Expert | Detection & Response | SIEM Replacement | Regulatory Compliance
Behavioral Analytics | Real-time Alerting | Log Analysis With AI | Vulnerability Scans

The Security Journey
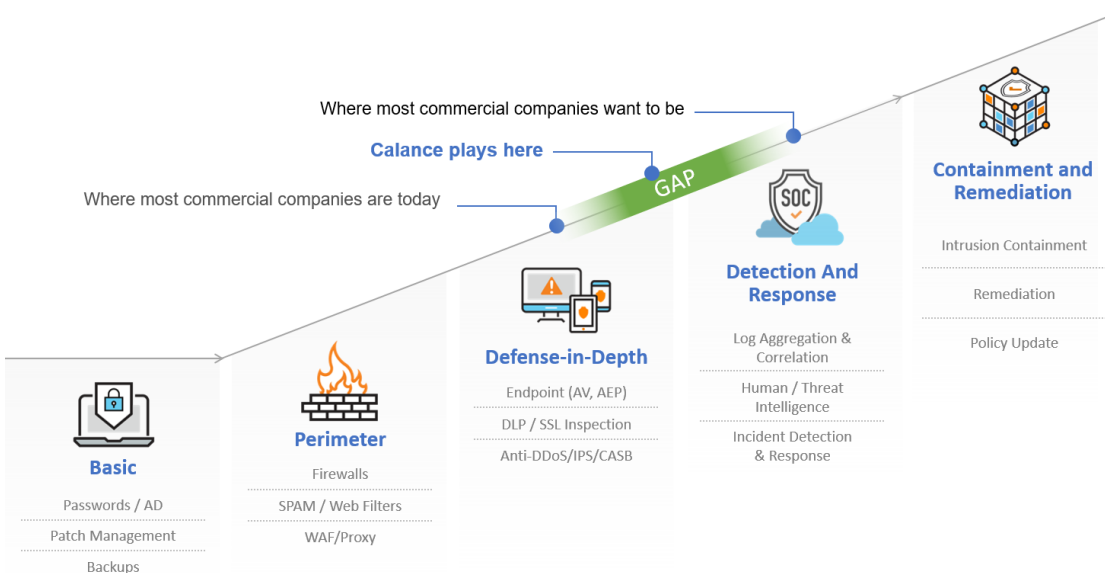
Turnkey SOC

Concierge Security Engineers

- Customer-dedicated primary point of contact
- Actionable remediation recommendations

Managed Detection & Response

- Machine learning with adaptive tuning for efficiency and scale
- Proactive hunting and remote forensic analysis

Security Incident and Crisis Support

- Prioritize security incidents with actionable intelligence
- Required steps for response and remediation
- Comprehensive log collection and retention
- No query languages to learn

Cloud Monitoring

- 360-degree visibility across customer's on-premises and cloud resources
  – Public cloud infrastructure
  – SaaS applications
  – Security services

Compliance

- Monitors user behavior and manages security incidents
- Reduces time and costs of audit preparation

Simple, Predictable Pricing

- Fixed recurring price
- Unlimited data collection

Calance SOCaaS

Concierge Security Engineer

The Concierge Security Engineer (CSE) is your single point of contact for your Arctic Wolf SOC-as-a-Service. Your CSE is your trusted security advisor and an extension of your internal team.

• Conducts daily triage and forensics

• Customizes service to your needs

• Provides actionable remediation recommendations
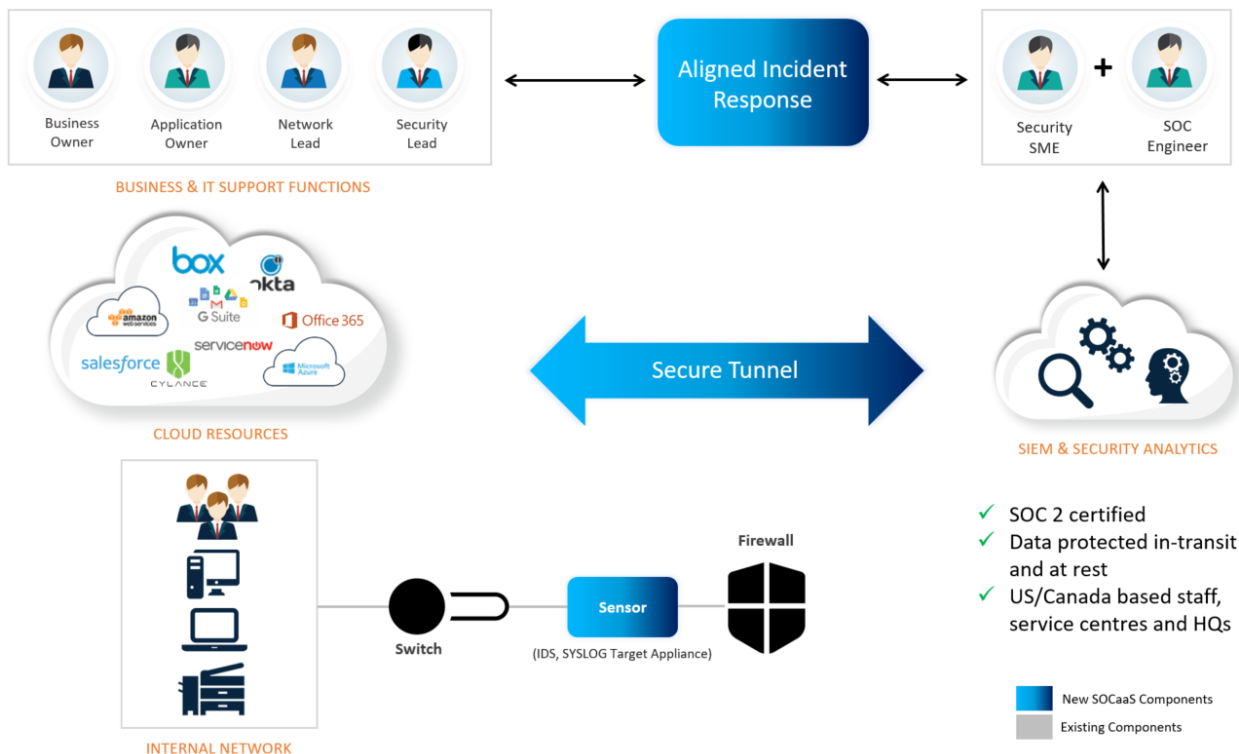
Hybrid AI

Hybrid AI demonstrably identifies attacks, reduces false positives, and speeds up the time between detection and response. It augments a security engineer's expertise with the efficiency and productivity of artificial intelligence.

• 10X better threat detection

• Human intelligence and intuition

• Machine scale and efficiency

Customized Rule Engine (CRulE)

CRulE provides unlimited flexibility to tailor our services to the specific needs of every customer. It allows the Concierge Security Engineer to apply your exact security and operational policies and update them as needed to align expeditiously with your changing business needs.

• Unlimited security policy customization

• Unlimited rules granularity or generalization

• Unlimited situational rules customization

Security Optimized Data

SODA unifies the ingestion, parsing, and analysis of network traffic and log data. It provides the foundation for the security analytics that give our security engineers deep pervasive visibility into your security posture.

• On-demand access to the relevant security data for incident investigation

• Instrumented for cybersecurity data science

• Immediately operational with zero setup time