THE ARCHON

TECHNOLOGY INTELLIGENCE

EXECUTIVE BRIEF

Autonomous Security Operations, Now On-Premises

Enterprises demand AI-driven SOC automation without sacrificing data sovereignty or latency. An on-premises appliance delivers both.

CONTROL FRAMEWORK

The Legacy SOC Challenge

Traditional security operations centers face alert overload, long mean-time-to-respond, and reliance on cloud-only tools that expose sensitive telemetry.

→ High false-positive volume

→ Latency from cloud round-trip

→ Regulatory limits on data export

CONTROL FRAMEWORK

Strike48 Introduces an On-Premises Appliance

Strike48's appliance embeds its autonomous security engine inside the data center, delivering real-time AI triage, automated containment and continuous model learning without sending raw logs to the cloud.

→ Hardware-validated, rack-mount form factor

→ Zero-trust integration with existing SIEMs

→ Local model training for privacy

CONTROL FRAMEWORK

Autonomous SOC Process Flow

The appliance follows a closed-loop workflow: ingest telemetry → AI triage → policy-driven playbook execution → automated remediation → feedback to model.

CONTROL FRAMEWORK

Core Capabilities Delivered On-Prem

Strike48's on-prem solution provides three pillars of autonomous security:

- → AI-driven threat detection with sub-second scoring
- → Automated containment actions integrated with firewalls and endpoint agents
- → Continuous model refinement using only internal data

CONTROL FRAMEWORK

Integration Landscape

The appliance connects to existing security stacks through standard APIs, enabling seamless orchestration with SIEM, SOAR and ticketing platforms.

→ REST and gRPC endpoints for log streaming

→ Native connectors for Splunk, QRadar, ServiceNow

→ Policy sync via Open Policy Agent

CONTROL FRAMEWORK

Business Benefits

Deploying the appliance yields measurable operational improvements while preserving data control.

- → Reduced mean-time-to-respond through automated actions
- → Full data residency for regulated industries
- → Predictable capital and operating expense model

CONTROL FRAMEWORK

Step-by-Step Implementation

A repeatable rollout minimizes disruption and accelerates value delivery.

→ 1. Site preparation and network segmentation

→ 2. Physical installation and power-up

→ 3. Connect to telemetry sources and configure data pipelines

→ 4. Run baseline model training with internal logs

→ 5. Enable automated playbooks and handoff to SOC analysts

CONTROL FRAMEWORK

Governance and Compliance Alignment

On-prem deployment satisfies internal policies that restrict cloud data movement and supports audit-ready logging for regulatory reviews.

→ Immutable audit logs stored locally

→ Role-based access control enforced at the appliance

→ Export controls configurable per jurisdiction

EXECUTIVE TAKEAWAY

Executive Takeaway

Strike48's on-premises appliance gives enterprises autonomous SOC capabilities with zero-latency response, full data sovereignty and a clear, low-risk deployment path. The process-oriented rollout aligns security, IT and compliance teams for rapid, measurable impact.