

SENTINELONE IMPLEMENTATION SERVICE

Avertium's SentinelOne Implementation Service delivers expert, hands-on guidance to deploy and operationalize the SentinelOne platform across Endpoint, Identity, and AI SIEM environments. Whether you are new to SentinelOne or expanding from Singularity Endpoint to a full XDR platform, Avertium provides a structured, best practice driven implementation that enables confident ownership.

Designed for on premises, cloud, and hybrid infrastructures, this service helps organizations of all sizes move quickly from purchase to production while minimizing operational risk and ensuring long term success.

Organizations engage with us when they:

- » Are new to SentinelOne and need expert guidance to deploy correctly from day one
- » Want to expand to an XDR platform, adding Identity and AI SIEM to an existing endpoint deployment
- » Need help navigating complex, hybrid environments
- » Must meet regulatory and compliance requirements (e.g., HIPAA, PCI-DSS, GDPR)
- » Lack internal resources to plan, tune, and scale deployments efficiently

KEY CHALLENGES WE ADDRESS

- Complex deployments across diverse environments
- Limited internal expertise or overburdened IT teams
- Risk of misconfiguration, alert noise, and production impact
- Unclear rollout processes and ownership boundaries
- Difficulty scaling security while maintaining performance and compliance

IMPLEMENTATION PHASES

1. **Customer Kickoff:** Objectives alignment, discovery planning, timeline confirmation, and cadence setup
2. **Deployment:** Pilot deployment, baseline policy configuration, full deployment, initial tuning
3. **Go Live:** Readiness validation, production cutover, documentation delivery, and enablement
4. **Calibration:** Alert tuning, ingestion optimization, and exclusion refinement
5. **HyperCare:** Post-implementation support to stabilize operations and accelerate adoption

WHAT YOU GET

Avertium delivers a **phased, structured implementation**, scoped according to your organization's size, that accelerates value while reducing risk. Core capabilities include:

Tailored Deployment → Customized configuration aligned to your environment, risk profile, and compliance needs

Structured Onboarding and Rollout → Phased delivering covering planning, pilot, tuning, mass deployment, Go Live, and HyperCare

Integration Support → Enablement of marketplace integrations, API connections, syslog ingestion, and automation

Compliance Enablement → Configuration guidance to support auditability, logging, and regulatory alignment

Knowledge Transfer and Training → Hands-on enablement so your team can confidently manage SentinelOne post-implementation

Support → Short-term, high-touch support after Go Live to reinforce stability and adoption

PLATFORM COVERAGE

SINGULARITY AI SIEM

- » Log sources and syslog servers onboarding
- » Marketplace API integration guidance and configuration
- » Out-of-the-box detection enablement and tuning
- » Validation testing and ingestion optimization

SINGULARITY ENDPOINT

- » Secure deployment across servers and workstations
- » Pilot-first approach with alert review and tuning
- » Scalable rollout with defined limits for manual intervention
- » Demonstration of advanced capabilities (network control, device control, discovery)

SINGULARITY IDENTITY

- » Baseline Identity Detection and Response (IDR) policy deployment
- » Support for on-premises, cloud-only, and hybrid environments
- » Training for ongoing policy management and tuning

SERVICE OUTCOMES

With Avertium, SentinelOne deployments are completed **more quickly and securely**, enabling organizations to realize protection benefits faster while minimizing downtime.

By following best practices and a consultative approach, **operational and production risks are significantly reduced** throughout the deployment process.

Security maturity and visibility are enhanced, providing organizations with greater insight and stronger defenses across their environments.

Upon project completion, customers are equipped with the knowledge and tools necessary to **confidently manage and maintain** their SentinelOne solution.

The deployed architecture is **designed to be scalable**, ensuring it can accommodate and **support future organizational growth** and evolving security needs.

DELIVERABLES

- ✓ Kickoff meeting and architecture review
- ✓ Successful, optimally tuned protection rollout
- ✓ Documentation and knowledge transfer
- ✓ Deployed and configured SentinelOne platform
- ✓ HyperCare support post Go Live

WHY AVERTIUM?

Avertium goes beyond basic deployment. Following our Assess, Design, Protect approach, our consultative, best practice driven deployment ensures your SentinelOne investment is implemented correctly, tuned responsibly, and positioned for long term success. We combine deep SentinelOne platform expertise with real world cybersecurity program experience to deliver outcomes that fit your business.

ABOUT AVERTIUM

[Avertium](#) is a cyber fusion and MXDR leader, delivering comprehensive security and compliance services to mid-market and enterprise customers. Our unique “Assess, Design, Protect” methodology addresses and improves security strategy, reduces attack surface risk, strengthens compliance, and provides continuous threat protection. Avertium maximizes customer security investments and enables customers to focus on growth, innovation, and business outcomes, while assuring that their security infrastructure is resilient and adaptive to evolving threats. That’s why customers trust Avertium to deliver better security, improved compliance, and greater ROI.