SentinelOne Endpoint & Server Security Transformation for Banking

SentinelOne Endpoint and Server Security Transformation with XDR, Device Control, Centralized Management, and 24x7 Remote Support

EXECUTIVE CONTEXT

COMnet partnered with a major Indian banking institution to strengthen endpoint and server cyber defense using the SentinelOne platform. The engagement covered endpoint deployment with device control and XDR capabilities, server protection architecture design, centralized management through a single console, and a five-year 24x7 remote support model aligned to banking-sector resilience and operational continuity requirements.

XDR
Telemetry led detection

Single
Mgmt console

5 Yrs
24x7 support

IMPACT

- Unified endpoint and server protection under a single management plane, improving operational visibility and policy consistency.
- Strengthened threat detection and response through SentinelOne XDR, enabling deeper telemetry correlation and faster analyst investigation.
- Reduced exposure from unauthorized peripherals and removable media by enabling device control on endpoint devices.
- Improved security operations efficiency by consolidating alerts, response actions, and protection policies into a centralized console.
- Established long-term operational resilience with a five-year 24x7 remote support model for ongoing monitoring and incident handling.

MAJOR ISSUES

- The client needed stronger endpoint protection against advanced malware, ransomware, and post-compromise lateral movement.
- Server workloads required a protection architecture that improved detection without compromising uptime or application availability.
- Fragmented visibility across endpoints and servers limited rapid investigation, cross-domain correlation, and centralized governance.
- The organization required tighter control over peripheral usage and endpoint policy enforcement to reduce insider and device-borne risk.
- A long-duration support construct was required to sustain platform performance, operational continuity, and continuous security tuning.

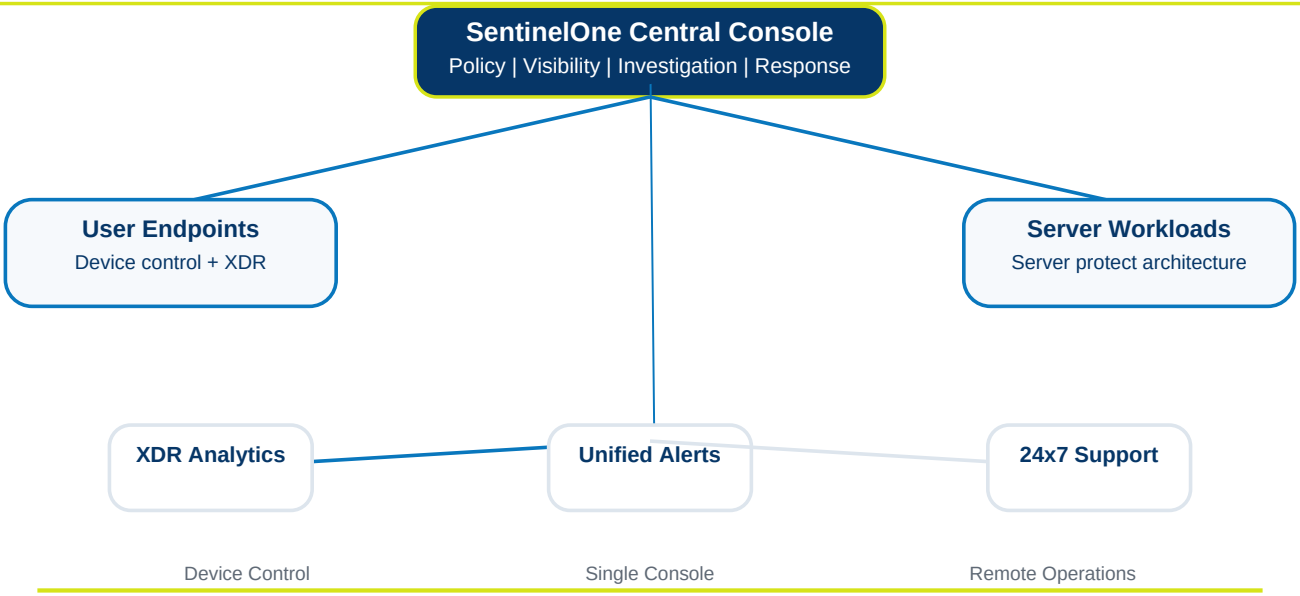
SentinelOne Endpoint & Server Security Transformation for Banking

SentinelOne Endpoint and Server Security Transformation with XDR, Device Control, Centralized Management, and 24x7 Remote Support

HIGHLIGHTS

ARCHITECTURE AND DEPLOYMENT SCOPE

REFERENCE SECURITY ARCHITECTURE



- Designed and deployed SentinelOne on endpoint devices with advanced features including device control and XDR.
- Designed server protection architecture using SentinelOne to extend security coverage across critical server workloads.
- Enabled a single console for both server and endpoint protection to improve visibility, response coordination, and policy administration.
- Established a five-year support construct backed by 24x7 remote support for platform continuity and issue resolution.
- Created an enterprise security posture foundation suitable for regulated BFSI operations and evolving threat conditions.

- Endpoint Protection Layer: SentinelOne agents deployed on user devices to provide behavioral detection, automated protection, and device control enforcement.
- Server Security Layer: Server protection architecture designed to extend SentinelOne coverage to critical compute workloads and improve workload resilience.
- Centralized Management Layer: A single console provided unified administration for endpoints and servers, including policy management, alert review, and response actions.
- XDR and Telemetry Layer: Security telemetry from protected assets supported investigation workflows, detection enrichment, and broader incident context.
- Operational Support Layer: 24x7 remote support enabled continuous service oversight, health monitoring, troubleshooting, and operational assistance.
- Deployment Scope: Enterprise endpoint devices, critical servers, central administration, and sustained support services over a five-year lifecycle.

SentinelOne Endpoint & Server Security Transformation for Banking

SentinelOne Endpoint and Server Security Transformation with XDR, Device Control, Centralized Management, and 24x7 Remote Support

KEY STRATEGIES

- Platform Consolidation: Standardized endpoint and server protection on a common security platform to reduce tooling fragmentation and simplify governance.
- Behavioral Detection and XDR Adoption: Leveraged advanced detection and response capabilities to improve visibility beyond signature-based controls.
- Policy-Led Endpoint Hardening: Implemented device control and unified policy enforcement to reduce attack surface and strengthen endpoint hygiene.
- Workload-Centric Server Protection: Designed server security architecture with operational stability, uptime sensitivity, and threat containment in mind.
- Centralized Visibility and Response: Used a single management console to improve analyst efficiency, accelerate triage, and streamline protection operations.
- Long-Term Support Assurance: Structured five-year 24x7 remote support to sustain platform performance, issue resolution, and ongoing optimization.
- Resilience for BFSI Environments: Aligned the security model to the needs of regulated banking operations, where availability, detectability, and governance are critical.

EXECUTIVE TAKEAWAY

COMnet transformed a focused endpoint-security requirement into a more comprehensive endpoint-and-server protection program built on SentinelOne. By combining XDR-enabled protection, centralized management, and a long-term support model, the engagement strengthened cyber resilience while simplifying security operations for a regulated banking environment.

OUTCOME SNAPSHOT

- Higher confidence in endpoint and server security posture across the environment.
- Improved detection visibility and more consistent operational control through centralized management.
- A scalable foundation for ongoing cyber defense supported by continuous remote operations.

TRANSFORMATION SUMMARY

SentinelOne endpoint + server security | XDR | device control | single console | 5-year 24x7 support