Cybersecurity Modernization for a Leading Indian Bank

Broadcom/Symantec Endpoint Protection, NAS Malware Protection, DLP Discovery with OCR, Full Disk Encryption, and Secure Proxy Modernization

EXECUTIVE CONTEXT

COMnet partnered with one of India's largest banking-sector clients to modernize and operationalize a Broadcom/Symantec security stack. The program covered Symantec Protection Engine for NAS, SEP agent and policy expansion for 500 users, DLP Discovery with OCR, Full Disk Encryption renewal, Broadcom Proxy migration, and severity-based managed support across S1, S2, and S3 incident classes.

500
SEP users

~4 Lakh
NAS scope

24x7
Support

IMPACT

- Centralized manageability for endpoint protection, DLP, disk encryption, NAS malware scanning, and secure web access controls.
- Expanded endpoint coverage through SEP agent and policy implementation for 500 users, improving policy enforcement and endpoint posture.
- Strengthened NAS security with high-performance malware detection for large storage environments, including deployment scope around 4 lakh NAS units or files.
- Improved regulated-data discovery through DLP with OCR, enabling detection of sensitive content in scanned and image-based documents.
- Reduced data exfiltration risk by aligning secure proxy controls with DLP inspection and web traffic governance.
- Improved operational continuity through 24x7 remote support for S2/S3 incidents and onsite engineer support for S1 severity events.

MAJOR ISSUES

- The bank had multiple security renewals and platform migrations spanning endpoint, NAS, DLP, encryption, and proxy layers.
- Fragmented controls created operational complexity in policy governance, evidence generation, incident handling, and security reporting.
- NAS repositories contained high-volume unstructured content, requiring scalable malware inspection without degrading storage performance.
- Sensitive information embedded in scanned forms and image-heavy files could evade text-only discovery methods.
- Broadcom Proxy migration required policy translation, controlled cutover, authentication validation, and continuity of web access.
- The operating model required severity-based response, OEM coordination, and audit-ready documentation suited to BFSI environments.

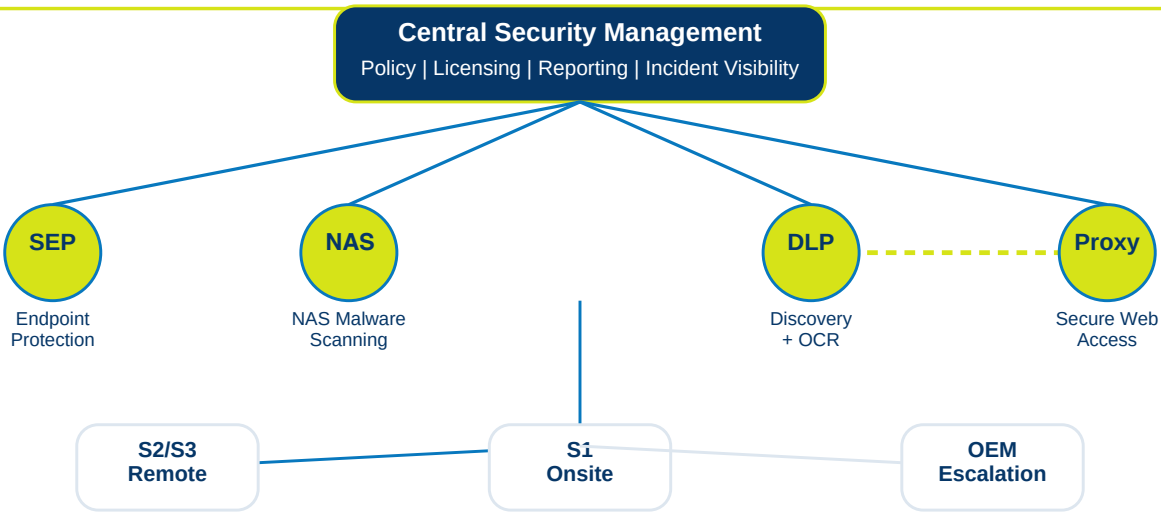
Cybersecurity Modernization for a Leading Indian Bank

Broadcom/Symantec Endpoint Protection, NAS Malware Protection, DLP Discovery with OCR, Full Disk Encryption, and Secure Proxy Modernization

HIGHLIGHTS

ARCHITECTURE AND DEPLOYMENT SCOPE

ARCHITECTURE VIEW



- Implemented Broadcom/Symantec Protection Engine for NAS to inspect file activity and reduce malware risk on storage repositories.
- Executed SEP add-on license implementation, agent rollout, and policy configuration for 500 users.
- Deployed security solution coverage for NAS at large scale, including approximately 4 lakh NAS scope units or files.
- Implemented and renewed DLP Discovery with OCR to detect confidential and regulated content across structured and unstructured repositories.
- Supported Full Disk Encryption renewal to maintain endpoint confidentiality and device-level protection.
- Implemented Broadcom Proxy migration to strengthen secure web access and support integration with DLP controls.
- Provided 24x7 remote support for S2/S3 incidents and onsite engineer visits for S1 severity response.

- Endpoint Security Layer: SEP agents, policies, and full disk encryption strengthened endpoint defense, device confidentiality, and compliance posture.
- NAS Protection Layer: Symantec Protection Engine enabled malware scanning and protection for network-attached storage repositories at enterprise scale.
- DLP and OCR Layer: DLP Discovery with OCR expanded sensitive-data detection across text, scanned documents, image-based files, and regulated records.
- Secure Web Proxy Layer: Broadcom Proxy migration enabled controlled internet access, policy enforcement, traffic inspection, and web-DLP integration readiness.
- Central Management Layer: Centralized consoles supported policy administration, reporting, licensing governance, audit evidence, and operational visibility.
- Support and Escalation Layer: S2/S3 incidents were handled remotely on a 24x7 basis, while S1 severity events were supported through onsite engineering response.

Cybersecurity Modernization for a Leading Indian Bank

Broadcom/Symantec Endpoint Protection, NAS Malware Protection, DLP Discovery with OCR, Full Disk Encryption, and Secure Proxy Modernization

KEY STRATEGIES

- Risk-Controlled Migration: Used phased migration waves, validation checkpoints, and rollback readiness to reduce operational risk during renewal and cutover activities
- Policy Normalization: Standardized policies across SEP, DLP, NAS, encryption, and proxy domains to reduce configuration drift and improve auditability.
- Data-Centric Security Design: Combined DLP, OCR, encryption, NAS protection, and secure proxy controls to protect regulated banking data across users, repositories, and web channels.
- Performance-Aware NAS Security: Tuned scanning policies and operational workflows to balance malware protection with storage performance requirements.
- Integrated Proxy and DLP Governance: Aligned web proxy controls with DLP workflows to support inspection and control of sensitive outbound traffic.
- Severity-Based Service Delivery: Mapped support response to S1, S2, and S3 criticality to improve incident handling while optimizing remote and onsite support economics.
- OEM Lifecycle Governance: Managed licensing, renewals, version alignment, and OEM escalations to maintain platform supportability and reduce technology risk.

EXECUTIVE TAKEAWAY

The engagement converted a fragmented renewal and migration requirement into an integrated security modernization program. COMnet improved governance, supportability, and cyber resilience across endpoint protection, NAS security, data loss prevention, encryption, and proxy control layers for a highly regulated banking client.

OUTCOME SNAPSHOT

- More unified visibility across endpoint, NAS, DLP, encryption, and web proxy security domains.
- Stronger protection for regulated and confidential information in a banking operating environment.
- Improved service continuity through severity-based operations, OEM coordination, and on site support for critical incidents.

TRANSFORMATION SUMMARY

Broadcom/Symantec SEP + NAS protection + DLP OCR + FDE + Proxy migration + 24x7/S1 support