Insurance Sector Endpoint Security Modernization

Enterprise-scale EDR deployment, compliance remediation and managed support

EXECUTIVE CONTEXT

COMnet strengthened endpoint security for one of India's largest insurance organizations by deploying Trend Micro EDR across 800 endpoints and optimizing the Apex One management environment. The engagement combined advanced endpoint controls, agent upgrades, compliance reporting, vulnerability remediation and 24x7 remote support under an SLA-driven managed services model.

1 800 ENDPOINTS

Trend Micro EDR deployed across the enterprise endpoint estate.

2 ADVANCED CONTROLS

USB blocking, application control, cookie protection, file and web scanning.

3 24x7 MANAGED SUPPORT

Remote assistance, SLA governance and continuous platform support.

IMPACT

- Deployed Trend Micro EDR across 800 endpoints, improving enterprise-wide detection, visibility and response readiness.
- Enabled USB blocking and application control to reduce unauthorized device and software risks.
- Activated cookie protection, file scanning and web scanning to strengthen layered endpoint protection.
- Fine-tuned the Apex One console and upgraded endpoint agents for consistent policy enforcement and platform stability.
- Closed auditor-identified product vulnerabilities and strengthened the organization's overall endpoint security posture.

MAJOR ISSUES

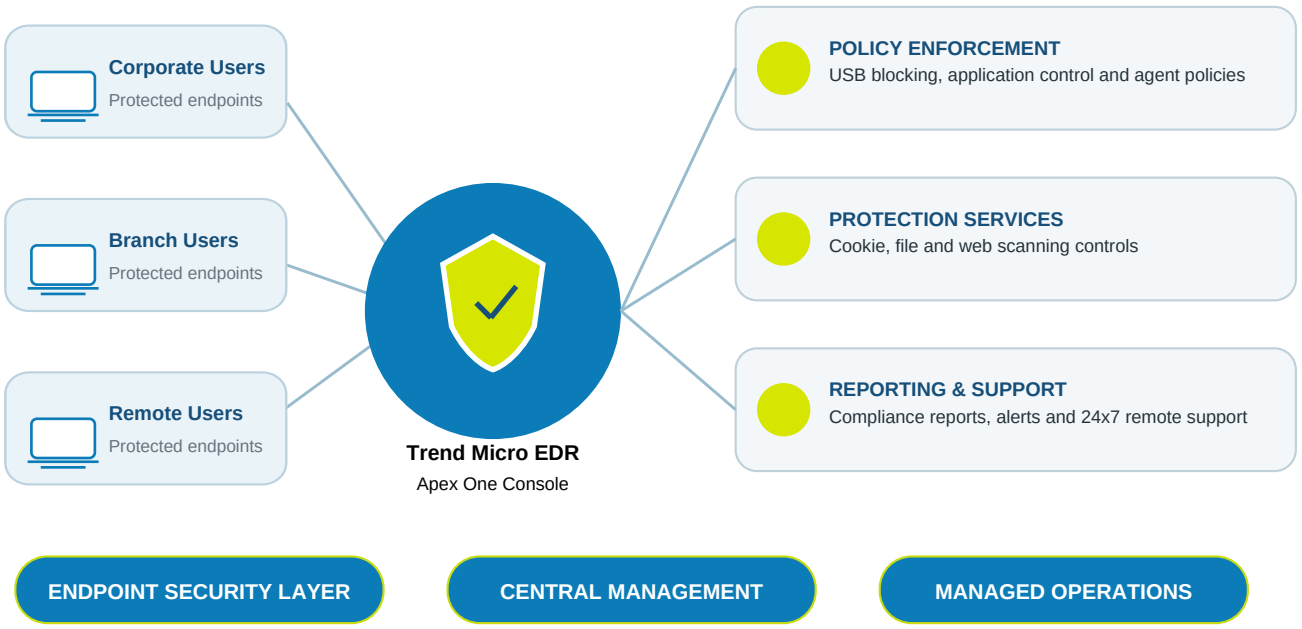
- Existing endpoint controls required advanced capabilities to address evolving threats and stricter audit expectations.
- Auditor findings identified product vulnerabilities and compliance gaps requiring structured remediation.
- Inconsistent agent versions and policy configurations reduced control consistency across the endpoint estate.
- A large-scale rollout across 800 endpoints required phased deployment, validation and minimal user disruption.
- The client required 24x7 remote support, measurable SLA performance and an accountable technology partner.

Insurance Sector Endpoint Security Modernization

Enterprise-scale EDR deployment, compliance remediation and managed support

HIGHLIGHTS

ARCHITECTURE AND DEPLOYMENT SCOPE



Engagement Highlights

- Assessed the existing endpoint security posture and mapped auditor findings to a structured remediation plan.
- Deployed Trend Micro EDR across 800 endpoints using phased rollout, validation and exception handling.
- Upgraded endpoint agents and fine-tuned the Apex One console to improve stability, visibility and policy consistency.
- Enabled advanced controls including USB blocking, application control, cookie protection, file scanning and web scanning.
- Established 24x7 remote support with defined SLA measurement, escalation and service governance.

Technical Deployment Scope

- **Endpoint Protection Layer:** Trend Micro EDR provided endpoint telemetry, threat detection and response capabilities across the managed estate.
- **Device and Application Control:** USB blocking and application control reduced unauthorized device use and unmanaged software exposure.
- **Web and File Protection:** Cookie protection, file scanning and web scanning strengthened layered protection against malicious content.
- **Centralized Management:** Apex One console tuning and agent upgrades improved policy consistency, visibility and administrative control.
- **Compliance and Reporting:** Reporting supported audit evidence, control validation and closure tracking for identified vulnerabilities.
- **Managed Services:** COMnet provided 24x7 remote support, incident coordination, SLA monitoring and structured escalation.

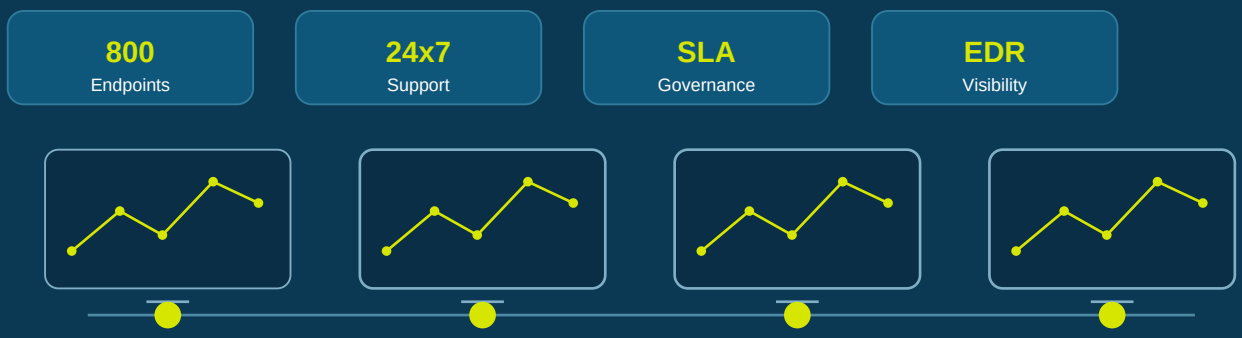
Insurance Sector Endpoint Security Modernization

Enterprise-scale EDR deployment, compliance remediation and managed support

KEY STRATEGIES

Endpoint Security Operations Assurance Model

Continuous visibility, policy governance, vulnerability closure and SLA-led support.



- **Assessment-Led Remediation:** Auditor findings and existing control gaps were translated into a prioritized technical action plan.
- **Policy-First Security:** Device, application, web and file controls were standardized through centrally governed endpoint policies.
- **Phased Deployment:** Endpoint onboarding and agent upgrades were sequenced to reduce business disruption and support rollback readiness.
- **Console Fine-Tuning:** Apex One policies, agent communication and administrative settings were optimized for stable operations.
- **Continuous Compliance:** Reporting and evidence collection supported audit closure, control validation and management visibility.
- **SLA-Driven Support:** 24x7 remote support, incident coordination and structured escalation helped sustain the environment after rollout.
- **Knowledge and Handover:** Operational guidance, issue tracking and support processes improved long-term platform maintainability.

Solution Model

- **EDR and Endpoint Protection**
  Threat visibility and response across 800 endpoints.
- **Centralized Policy Control**
  Apex One console tuning, agent upgrades and consistent enforcement.
- **Compliance and Reporting**
  Audit evidence, vulnerability closure and contrl validation.
- **Managed Security Services**
  24x7 remote support, SLA governance and escalation management.

EXECUTIVE OUTCOME

COMnet established a stronger, auditable endpoint security foundation across 800 devices, closed identified vulnerabilities and sustained the environment through 24x7 SLA-based managed support.