



Endpoint Security Management for Healthcare Division of a Fortune 100 Company

Client Profile

The client provides new age medical technologies and services that are giving an edge to modern patient care. It has its presence in patient monitoring systems, medical imaging and information technology, drug discovery, medical diagnostics, performance improvement, and a biopharmaceutical manufacturing technology, that is helping clinicians to predict, diagnose, inform and treat diseases.

Client Context

The onsite management of 55,000+ end clients spread across 450 locations globally proved to be a challenge in terms of effectiveness and cost. The client needed a cost effective remote IT infrastructure vendor who could securely manage the volume and also bring down its costs for the monitoring and management without comprising on the high levels of security.

Microland Approach

Microland manages the centralized endpoint security for more than 55,000 users across USA, EMEA and APAC. This service is delivered remotely from India using Terminal services over Citrix farm to connect to client's infrastructure.

Key Deliverables

Remote monitoring and management of security

Infrastructure across the 450 locations from a dedicated NOC located in Bangalore, India.

Technology Coverage

- Symantec Antivirus (SAV)
- Black ICE/Site-protector personal firewall
- Microsoft Windows Server Update Services (WSUS)
- Sophos Network Access Control (NAC)

A 24x5 basis L2 support for:

- Remote vulnerability management
- Remote SAV management
- Remote patch & Black ICE management
- Vendor management
- Remote Sophos management

Key processes managed:

- Monitoring Process
- Incident Management
- Problem Management
- Change Management
- Daily Security Upkeep Process
- Crisis Management
- Configuration Management
- Vulnerability Management
- Server Reboot Process
- Critical ISS Updates Process

Benefits

- Infections reduced for the managed clients from 10% to 1.28% within 6 months to current levels at 0.67%
- Old Definition Count reduced from 10% to 0.5%
- Vulnerability Management per client reduced from 6% to 2%
- Automation initiatives (e.g. Client Security Portal) undertaken to reduce the time for remediation of infected machines
- Processes implemented as per ITIL standard and effective monitoring ensures timely publishing of reports and management dashboards

