

SENTARUS is a dynamic threat management solution that integrates the major components of network security, including NETWORK and HOST-BASED INTRUSION DETECTION AND PREVENTION, EXTENSIBLE SERVICE MONITORING, SYSTEM INTEGRITY VERIFICATION, and VULNERABILITY MANAGEMENT. This comprehensive, integrated approach eliminates the cost and complexity of managing and aggregating data from multiple point solutions. As the most powerful and comprehensive security solution available, Sentarus also enables organizations to SIGNIFICANTLY REDUCE THE COSTS associated with THREAT MANAGEMENT, RISK MITIGATION and CORPORATE COMPLIANCE.

Sentarus Threat Management Console Sentarus MCX/NSH/MCS/NSS

Sentarus features an intuitive management console that allows you to manage, control and protect global networks from a centralized location. With the ease of the Sentarus configuration system, you can readily customize your system to meet your specific network needs.

Primary Features

- Network and Host-based Intrusion Detection and Intrusion Prevention
- System Integrity Verification
- Vulnerability Management
- Extensible Service Monitoring
- Event Correlation
- False Alert Suppression Technology (FAST)
- Advanced Customized Reporting
- Self-Tuning Alert Response (STAR)
- Virtual Sensors
- Selective Sensor Permissions
- Positive Profiling

Management Console

- Linux-based Sentarus OS
- Network Sensor

Network Sensor

- Linux-based Sentarus OS
- Unlimited Network Sensors
- Up to 8 Gbps
- Virtual Sensor capabilities

Host Sensor Agents

- All major platforms

User Interface

- Secure web application
- Local control console

Number of Users

- Unlimited

Centralized Management

- Real-time event viewing
- Historical event viewing
- Policy management
- Incident management
- Aggregate sensor data view
- Individual sensor data view
- Quick Stats bar

Reporting

- Fully customizable reports
- Instant reports
- Scheduled reports
- Recurring reports
- Graphical reports
- Exportable (PDF)
- Automatic email delivery

Secure Communication

- SSL secured
- Encrypted channels
- PKI secured

Signature Updates

- Real-time updates
- Automated updates
- User customizable updates

Notification Methods

- SMTP (email)
- SNMP trap
- Pager
- SMS (mobile phone)
- Remote Syslog

Automatic Intelligent Updates

- Operating environment
- Management console
- Network sensor
- Host sensor
- IDP rule sets
- Vulnerability scanning plugins

Advanced Configuration

- Manual and assisted
- Automated network discovery
- Turnkey deployment

Data Storage

- Off-site secure back-up capability
- Redundant storage (hardware)

Help System

- Integrated
- Contextual
- Online

Third Party Integration

- Standards compliant
- SNMP traps
- Plugin ready notifications

next >

Network Intrusion Detection/Prevention Sentarus MCX/NSH/MCS/NSS

Using advanced, intelligent detection methods—including a combination of stateful signature, protocol anomaly, and traffic anomaly—Sentarus gives you the option of monitoring or proactively preventing completion of in-progress attacks before they are capable of doing harm. With Sentarus, you can choose to not only block attacks occurring on the local network, but also on company systems world-wide.

Detection Methods

- Stateful signature detection
- Protocol anomaly detection
- Traffic anomaly detection
- Backdoor detection
- IP spoofing detection
- DoS detection
- Advanced port scan detection
- Layer 2 detection

Signatures

- Stateful
- Compound
 - (stateful plus protocol anomaly)
- Automated updates
- Open signature format
- Custom, user-definable
- Parallel signature matching
- Policy conformance monitoring

Traffic Interpretation

- Reassembly
- Normalization
- Self-tuning alert response (STAR)

Active Responses

- Distributed response
- Custom actions
- Close client
- Close server
- Close connection
- IP actions
- Unlimited firewall integrations

Packet Management

- User-specified logging
- Built-in full payload viewer
- 3rd party compatibility

Operational Modes

- Sniffer (passive)
- Bridge
- Proxy-ARP
- Transparent

Enterprise Networking

- 802.1QVLAN Support
- SNMPMIB-II Support

Network Forensics/Incident Response

- Application (L7) information/awareness
- Network (L2-L4) information/awareness
- Policy violation visibility/awareness
- Incident correlation
- Policy refinement
- Event cross correlation

Incident Management

- Investigative Tools
- Detailed packet capture
- Consolidated threat analysis

Network Awareness

- Automatic configuration
- Passive host discovery
- OS fingerprinting
- Active discovery available
- Event correlation
- Asset discovery

System Integrity Verification Sentarus MCX/NSH/MCS/NSS

Sentarus enables you to maintain the integrity of your business and information systems by monitoring your systems for unusual activity at the host level. Granular changes such as such as improper file access, unapproved privilege escalation, disallowed system processes, or other alterations of system settings can be monitored and prevented.

Monitoring Ability

- Local file system
- Remote web pages
- Customized

Rule Capabilities

- Wildcard rules
- Recursive rules
- Prioritized rules
- Policy-based rules
- Advanced exclusion policies
- Intelligent exclusions

Attributes Monitored

- Fully customizable
- Created time
- Modified time
- Accessed time
- Size
- Links
- Blocks
- Inode
- Owner
- Group
- Permissions
- Cryptographic checksums

Cyptographic Hashes

- Redundant algorithms
- MD5
- SHA1

Reporting Data

- Multiple views
- Exportable baselines
- Baseline comparison reports
- Historical trending

next >

Vulnerability Management Sentarus MCX/NSH/MCS/NSS

To proactively identify previously undetected threats to your network, Sentarus allows you to schedule regular security audits of the hosts residing on your network. Unpatched systems, new network devices, routers, firewalls and other network-connected devices can all be monitored and reviewed to help you prevent potential new threats from adversely impacting your entire network.

Scanning Techniques

- Automated scanning
- Distributed scanning
- Intelligent identification
- Non disruptive probing
- Automatic host discovery
- Automatic service discovery
- Automatic network application discovery
- Network discovery-based blocking

Scan Types

- One-time network scans
- Recurring network scans

Scan Configurability

- Host level
- Port level
- Plug-in level
- Intensity level

Scan Modules

- Automatic updates
- Open module format
- Custom, user-definable
- Policy conformance monitoring

Data Displayed

- Vulnerabilities detected
- Priority level
- Resolution hints
- 3rd party resource links

Scan History

- Archived scans
- Established baselines
- Scan search functionality

Extensible Service Monitoring Sentarus MCX/NSH/MCS/NSS

Unplanned downtime can be catastrophic for any business. Sentarus proactively monitors network and host services, allowing immediate discovery of compromised services from both internal and external threats. Automatic process and service regeneration and Unix log and Windows event log monitoring means you can easily monitor and maintain thousands of hosts without having to expand your current infrastructure.

Local Host Monitoring

- Agent-based
- Host health monitoring
- Unlimited host agents
- All major operating systems supported

Process/Service Monitoring

- Windows and Unix platforms
- Service availability assurance
- Process regeneration
- Windows service regeneration

Log Monitoring

- Customizable monitoring
- Windows event log
- Syslog
- Text logs

Remote Service Monitoring

- Extensible monitoring
- Distributed monitoring
- Protocol-based
- Service-based
- Response-based
- Customized plug-ins

Advanced Configuration

- Manual and assisted
- Automated discovery
- Active host lookup
- Service Sensor classifications

Reporting Data

- Regulatory compliance
- Historical trending
- Graphical daily view
- SLA level reporting

About Demarc

Demarc is a global provider of dynamic threat management solutions. Demarc's Sentarus product line provides a complete portfolio of fully integrated network and host-based security solutions for small businesses, government entities, multi-national corporations and service providers. Available in both hardware and software editions, Sentarus products ensure efficient, intelligent IT risk mitigation. Demarc customers include Fortune 500 and Global 1000 enterprises, and military and global government agencies in more than 25 countries around the world. Demarc is headquartered in Carpinteria, CA. Please visit the Demarc website at www.demarc.com for more information.

Specifications subject to change without notice.

