

MUSI system

A new generation of unified security



Manage All Security Functions Through a CCTV-Like Window

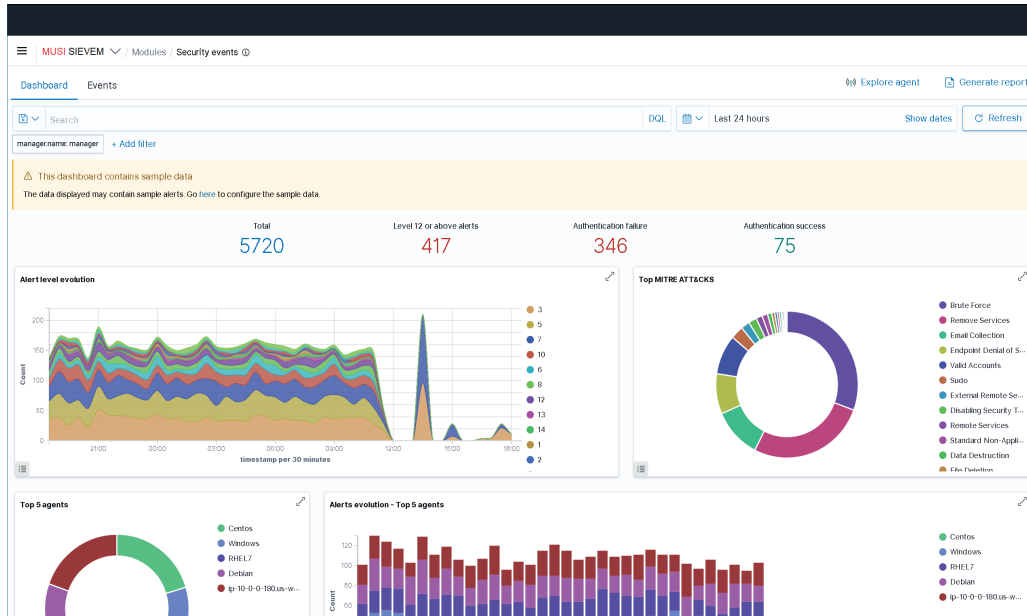
MUSI 3000

For successful businesses and large organizations. In compliance with cyber-industry' best practices, and standards, such as NIST, PCI-DSS, HIPPA, & GDPR, fulfilling your organization' growth and promising expansion, your emerging technological needs, MUSI 3000 is the optimal solution to secure digitalized business operations, capable of protecting multiple data centers, headquarters ICT environment, to connect your branches, and to keep an eye on every little detail in your digital environment. MUSI 3000 has a powerful forensics engine, huge archives, it covers IoT security such as datacenter monitoring solutions, AI devices, in addition to its main features that include all next generation firewall functions, vulnerability management, secure network management, along with to its powerful AI-driven SIEM system, all of which securing your datacenters, computer systems, and even IoT devices, in a very cost-effective manner.





MUSI Dashboards



AUDITING AND POLICY MONITORING

Policy monitoring

Verify that your systems are configured according to your security policies baseline.

System auditing

Audit users behavior, monitoring command execution and alerting on access to critical files.

OpenSCAP

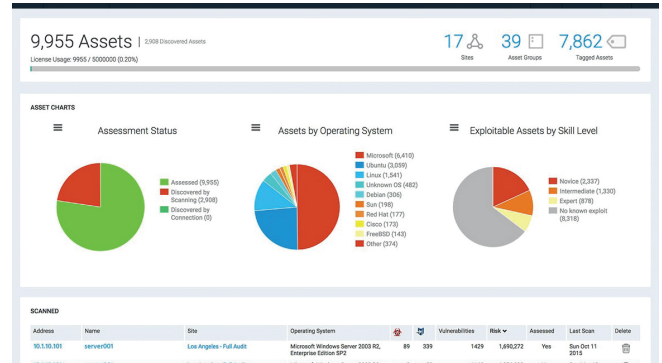
Configuration assessment and automation of compliance monitoring using SCAP checks.

CIS-CAT

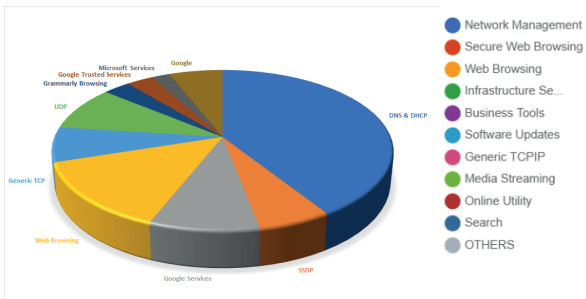
Configuration assessment using Center of Internet Security scanner and SCAP checks.

Security configuration assessment

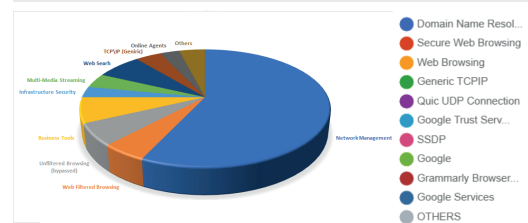
Scan your assets as part of a configuration assessment audit.



App Categories Breakdown



Apps Breakdown





MUSI Structure

Next generation firewall

- 01 Classical firewall rules for traffic access
- 02 Intrusion prevention
- 03 SSL and SSH inspection
- 04 Deep-packet inspection
- 05 Reputation-based malware detection
- 06 Application awareness

Log heaven

(Future SIVEM) Replacing Legacy SIEM technologies

Availability Monitoring Powerful and Scalable Analytics
 Baselining and Statistical Anomaly Detection External
 Technology Integrations Real-Time Configuration Change
 Monitoring Device and Application Context Scalable and
 Flexible Log Collection Notification and Incident Manage-
 ment Rich Customizable Dashboards External Threat
 Intelligence Integrations Simple and Flexible Administration
 Easy Scale Out Architecture

Cryptosystem

All logs encrypted.

**Network Management,
 Storage Management,
 & Remote Backups**

Secure,VPN,DNS,DHCP and Routing Services

- Identifies and Categorizes All Applications, on All Ports, All the Time, with Full Layer 7 Inspection
- Enforces Security for Users at Any Location, on Any Device, While Adapting Policy Based on User Activity
- Prevents Malicious Activity Concealed in Encrypted Traffic
- Offers Centralized Management and Visibility
- Maximize Your Security Investment and Prevent Business Disruption with AIOps
- Detect and Prevent Advanced Threats with Cloud-Delivered Security Services
- Enables SD-WAN Functionality
- Delivers a Unique Approach to Packet Processing with Single-Pass Architecture

Vulnerability Scanner Manager

- With our AI-driven VM, applying multiple vulnerability assessment tools that concurrently provide:
- 1automated patch management,
 - 2Web server hardening
 - 3Security Configuration management
 - 4High-risk software audit
 - 5Compliance with CIS benchmarks



Compliance

Real-time reports, summarized assessment against NIST
Viewable in the Security Highlights part



NIST SP 53-800



GDPR



HIPPA



PCI-DSS

Regional Anatomy Flexible Topology



MUSI system

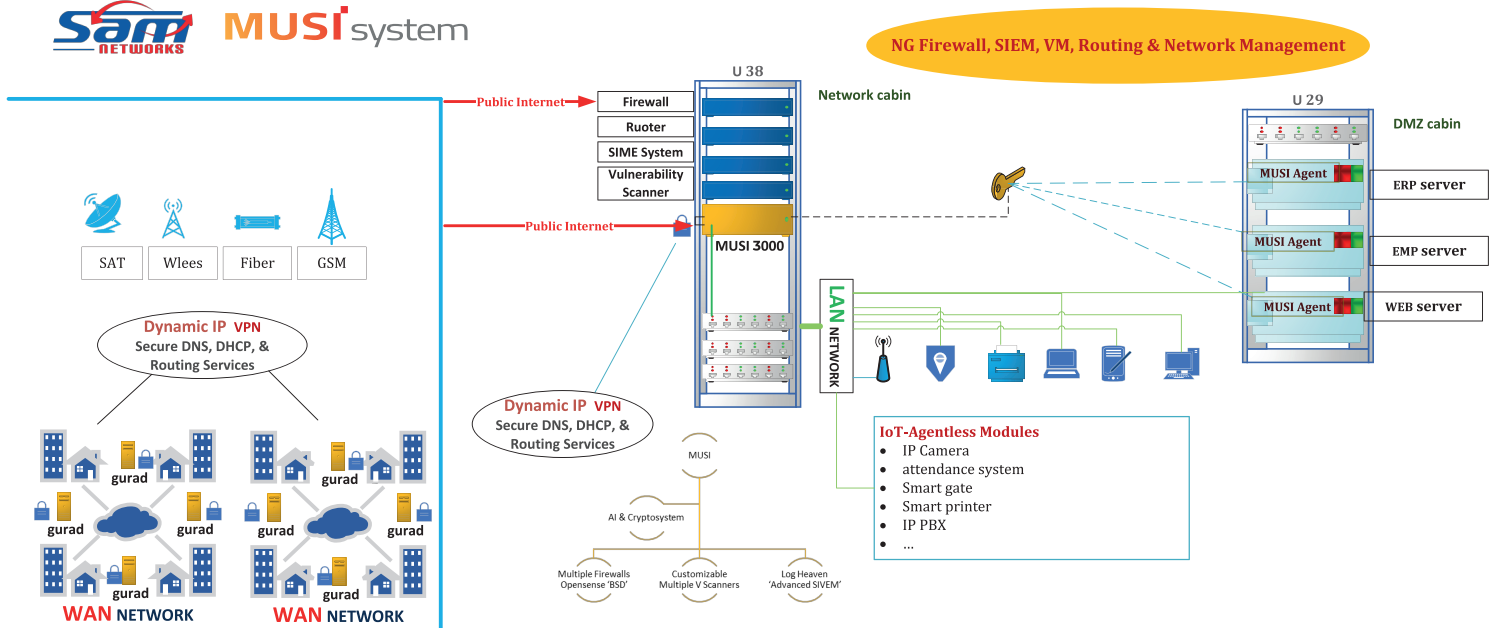


Table of technical specifications

Technical Specifications

MUSI 3000

Secure Backups	10T
Dual CPU	Yes
Firewall Throughput	12 Gbps
IPsec VPN Throughput (512 byte) 1	4 Gbps
IPS Throughput (Enterprise Mix)	4Gbps
NGFW Throughput (Enterprise Mix)	8 Gbps
Threat Protection Throughput	13Gbps
SIVEM Throughput(Event per second)	180 MEPS
SIVEM Logs (Giga bytes)	860
Indexing Volume (Mega per day)	Unlimited
Alerts per day	8 G
Vulnerability Scans (per IP)	900
VM Throughput (Mbps)	800
Security Highlights Events (daily)	300
Main Features	
Training Voucher	10
Warranty	2 yaer
Annual Fees \$	1750
Branch per device	40\150
MUSI Agent	25\120
Agentless Modules (IoT)	50\200

ROI & TCO

Return on Investment & Total Cost of Ownership

- 1 Single license for: all cyber-security functions, and network management.
- 2 Reducing HR fees, low skills needed by system admins according to ease of use.
- 3 All features included 'no extra license needed for using embedded features!'
- 4 Optimized cost for throughput, no throughput waste when using features 'Client can use IPS, IDS, without losing 80% or more of the throughput like other solutions.
- 5 Long-time investment, minimum time between two failures counted or estimated to be in years not months nor weeks!
- 6 Centralized procurement means the client will only buy one MUSI device, in a single engagement, instead of all routine procurement for three or more systems, single project, single SLA, single contract.



Fast and Efficient Installations

- ▶ Squeeze time, efforts, and costs of installing multiple systems (SIEM sizing is a separate project for some competitors)
- ▶ Quick installation for HQs with high VPN and secure connectivities deployment for branches.
- ▶ Single training approach for all security functions.
- ▶ AI- Installation implemented upon best-practices and standards (default installation includes NIST, GDPR, PCI-DSS, & HIPPA).
- ▶ MUSI experts understand all environmental needs, cooperate with client team to make success stories upon best standards mentioned earlier.



Added Values & Functionalities

- ▶ Storage, backups, and BCM
- ▶ Support of IoT, integration with AI solutions
- ▶ Perfect for Multiple locations installations
 - ▶ Securing all branches
 - ▶ Connecting all branches to the HQ
 - ▶ Domesticating:
 - ▶ Managing all remote computers
 - ▶ just like being in the same HQ building
 - ▶ Monitor all computers
 - ▶ Scan all vulnerabilities of all workstations
 - ▶ Apply same policies and same firewall rules
 - ▶ Network management, throughput management,...
 - ▶ Attach more branches easily and effectively to the HQs
 - ▶ More agents, more agent-less modules can be effortlessly added
- ▶ Ideal for double-NATting, dynamic IP with stable connectivity among branches\multiple locations.

Warranty + Updates

Hardware warranty (two years)
System updates included during warranty period
Single annual license after end of warranty

Address: Kemp House, 152 City Road London EC1V 2NX UK

info@samnetworks.co.uk Phone: 7054 3355 20 44+ www.samnetworks.co.uk