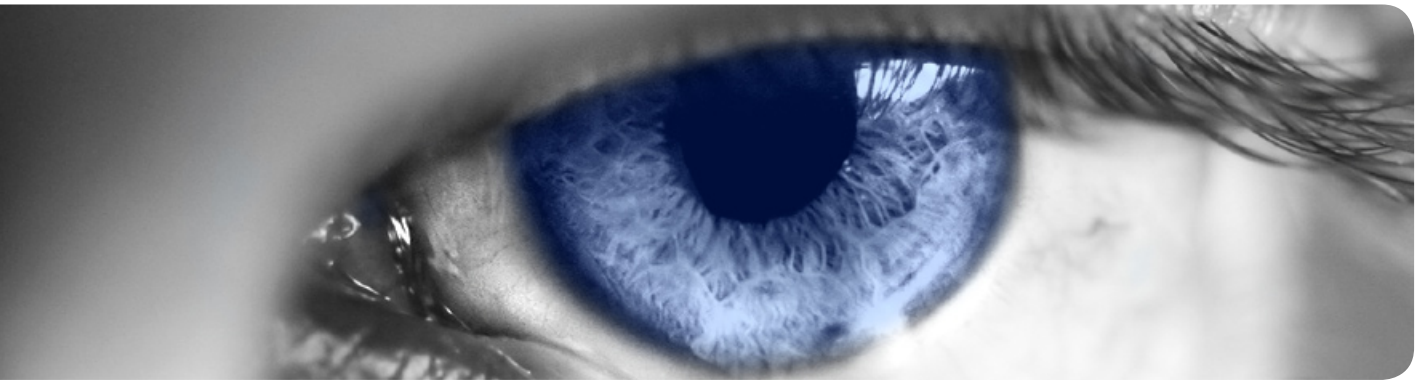
Clavister InSight™



Clavister SSP™ Security Services Platform

firewall • VPN termination • intrusion prevention • anti-virus
anti-spam • content filtering • traffic shaping • authentication

clavister™

Protecting Values

- Enterprise-wide security intelligence
- Regulation support: SOX, GLBA, HIPPA, PCI and FISMA
- Heterogeneous device support
- Real-time monitoring and correlated alerting
- Forensics and investigative root cause analysis
- Reporting and monitoring portals
- MSSP support with advanced user access controls

Clavister Insight™

Clavister Insight™ is an award-winning, easy-to-use Security Information and Event Management (SIEM) solution that provides essential real-time security intelligence to help decipher hacker/virus behavior, combat security threats and meet regulatory compliance requirements across the entire IT infrastructure.

Clavister Insight™ provides powerful security intelligence across thousands of network devices that have an impact on a company's security framework. Clavister Insight™ automatically collects and correlates event data from variety of heterogeneous multi-vendor network devices including routers, switches, firewalls, VPNs, IDS/IPS systems, proxy servers, spyware, antivirus, SPAM and content Figure 1: Clavister Insight™ Enables Advanced Security and Regulatory Compliance filtering web security appliances. This information helps to eliminate false positives, identify security breaches and corporate violations, improve security operations and delivers the necessary tools to meet Sarbanes-Oxley (SOX), Gramm-Leach-Billey Act (GLBA), Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry (PCI) and Federal Information Security Management Act (FISMA) compliance.

Clavister Insight™ helps minimize incident response time and maximize the ability to take preventative actions by providing advanced security event monitoring, correlation and historical reporting. The end result improves security operations and protects IT assets by helping organizations centrally manage information risk and take proactive steps to minimize security breaches and meet compliance mandates.

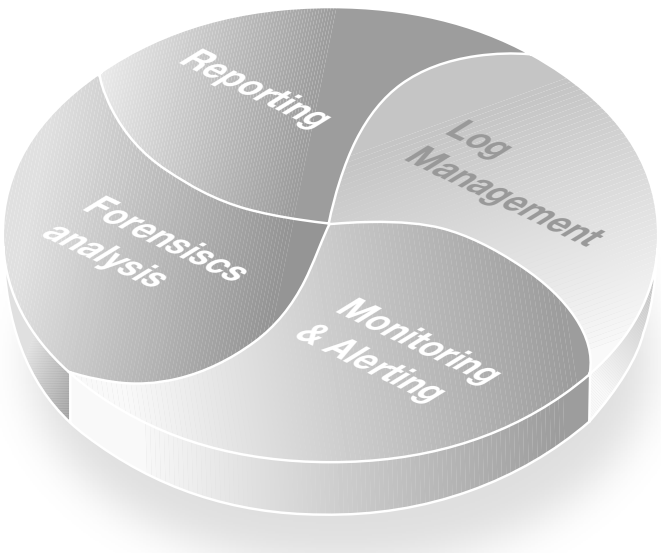


Figure 1: Advanced Security and Regulatory Compliance

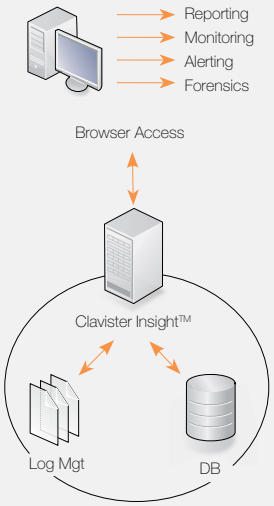
Architectural Overview

In today's environment, one of the primary key features for a security management solution is the ability to scale to large networked environments. Clavister Insight™ provides a distributed architecture for small to medium enterprises that scales to thousands of network devices. The architecture supports both a stand-alone deployment for smaller networks and a distributed deployment for larger enterprise installations.

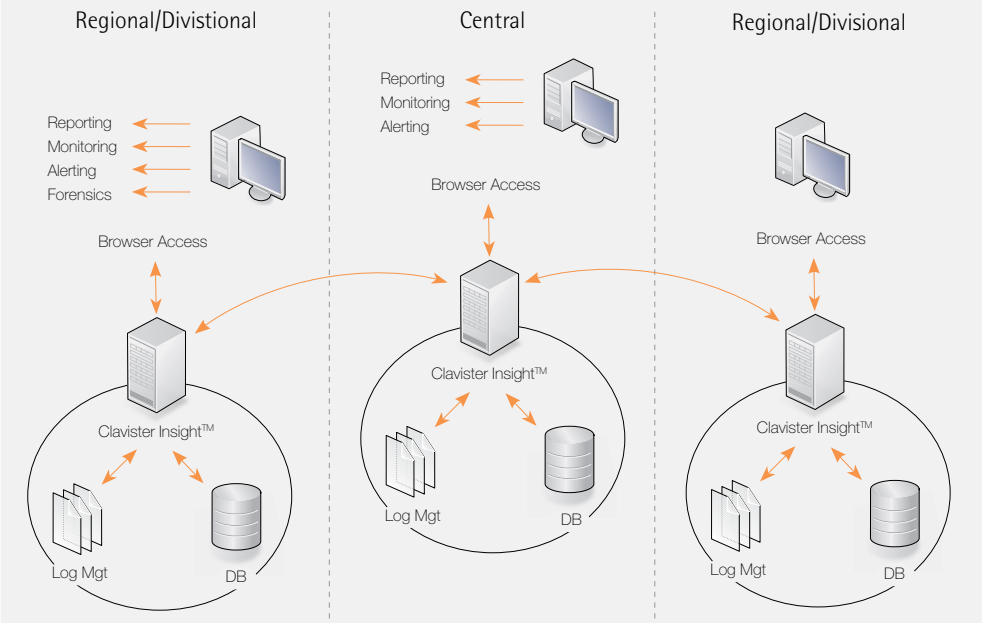
The flexibility of the Clavister Insight™ architecture allows for the creation of a SIEM solution that can adapt to any environment. The architecture allows MSSPs to take advantage of out-of-the-box reporting and monitoring portals to offer new value-added revenue generating services or expand their current remote monitoring services to include comprehensive on-demand reporting and compliance audit log management. The built-in XML-based API allows MSSPs and enterprise customers to integrate Clavister Insight™ reporting, alerting and monitoring data with other third-party portals.

Clavister Insight™ delivers all necessary tools, such as centralized log management, monitoring/alerting, reporting and forensics analysis to help meet both compliance and security operations management requirements, all in a single solution.

Standard Deployment



Distributed Deployment



Architectural Benefits

- Distributed and highly scalable
- Heterogeneous device and vendor support
- Anytime, anywhere web-based management
- All-in-one solution with log management, monitoring, correlation, reporting and forensics
- Role-based access and Active Directory/ LDAP single sign-on integration
- Out-of-the-box reporting and monitoring portals
- XML-based API for easy integration by MSSPs and enterprise customers

Advanced Security Intelligence

Event Drilldown through Workbench – Provides advanced on-the-fly event drill-down with correlation and analysis of significant security events to enable quick resolution of security incidents.

User-definable Event and Threat-Level Classifications – Classify events and threat levels based on unique requirements.

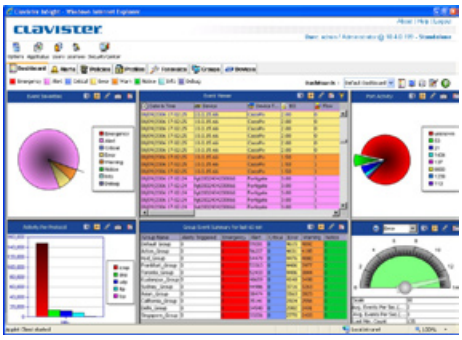


Figure 3: Dashboard

Security Reporting

Reporting Portal with Powerful Drilldown – Access to over 1,000 interactive reports.

Correlated Reporting – Offers a holistic view and understanding of hacker and virus activity by correlating data across all network devices instead of looking at each device data separately.

Intrusion and Rules-based Reporting – Attack and rules-based reports provides a comprehensive understanding of the intrusions and rule violations.

Protocol and Web Usage Reporting – Provides a firm handle on protocol and web usage patterns.

SPAM, Spyware and Antivirus Reporting – Generates reports on malware activities.

Vulnerability Reporting – Integrates and reports on vulnerability data derived from your network.

Content Categorization Reporting – Generates reports to help understand employee web usage patterns.

Automated Report Generation and Distribution – Automatic e-mail distribution of reports in HTML, MHTML, PDF, Word, Excel and Text formats.

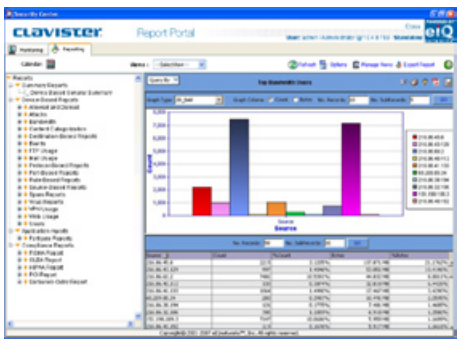


Figure 4: Security intelligence and Compliance Reports

Real-time Monitoring and Alerting

Heterogeneous Real-time Monitoring – Monitors security event data across the entire network in real-time.

Real-time Correlated Alerting – Allows the creation and definition of any number of alerts to reduce false positives and identify blended attacks.

Real-time Event Manager – Presents a view of security event data from thousands of heterogeneous and multi-vendor network devices. Prioritizes the actions based on business impact of each event, allowing for corrective actions before an incident occurs.

Monitoring Dashboard – Provides a quick, consolidated view of the environment. Create and view any number of user specific monitoring views and toggle between the different views.

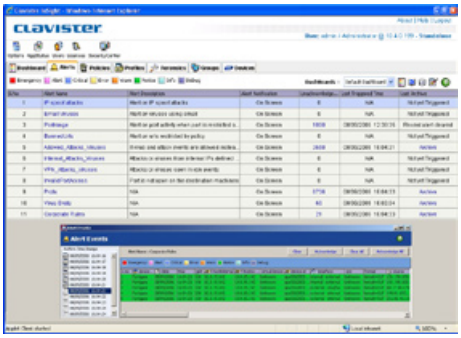


Figure 5: Alerting center

Compliance Management

Log Archiving for Compliance – Automatically compresses, encrypts and archives log files for investigative analysis and regulatory compliance.

Compliance Monitoring – Provides centralized monitoring and alert correlation for real-time investigation of security incidents with regulatory compliance implications.

Compliance Reports – Offers detailed reports specific to SOX, HIPAA, GLBA, PCI and FISMA.

Scalable Search – Searches hundreds of GB of log data across multiple devices to aid in investigative analysis.

Activity Investigation – Identifies anomalies and employee corporate policy violations.

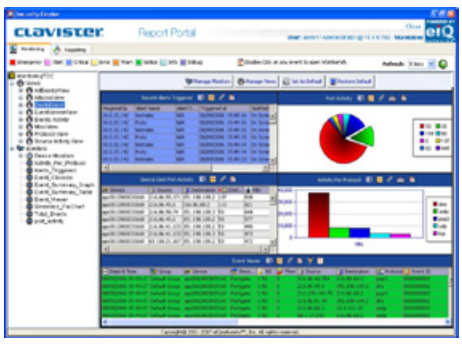


Figure 6: Security Monitoring Portal

Awards

System Requirements

- **Processor – Pentium 4 – 2.8 GHz or higher**
- **Disk Space – 100 GB or higher**
- **RAM – 2 GB or higher**
- **Operating System – Windows Server 2000 / 2003**
- **Fast IO**
- **Internet Explorer 6.0 with Java**

Clavister SSP™ Security Services Platform

firewall • VPN termination • intrusion prevention • anti-virus
anti-spam • content filtering • traffic shaping • authentication

clavister™

Protecting Values

Part number: clavister-dts-insight-a004