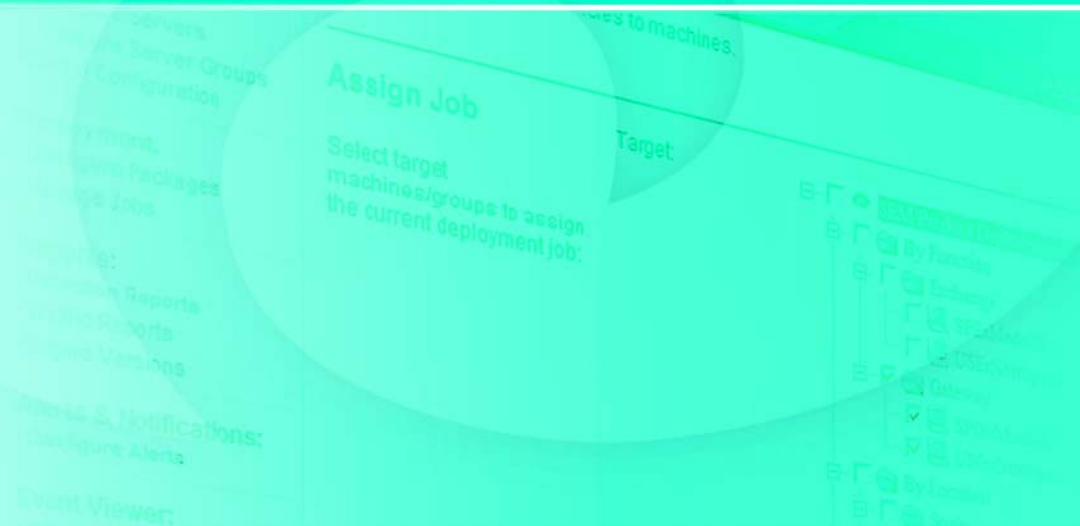


SYBARI Enterprise Manager

Der Sybari Enterprise Manager (SEM) ist ein zentralisiertes Standalone-Tool. Damit verfügen Administratoren über ein leistungsfähiges Mittel zum Managen der Sybari Softwarelösungen auf allen Servern im Unternehmen. Durch ein webbasiertes Management-UI ermöglicht SEM Administratoren zentralisiertes Deployment, Monitoring, Reporting und Konfigurationsmanagement.



Enterprise Management, Enterprise Deployment

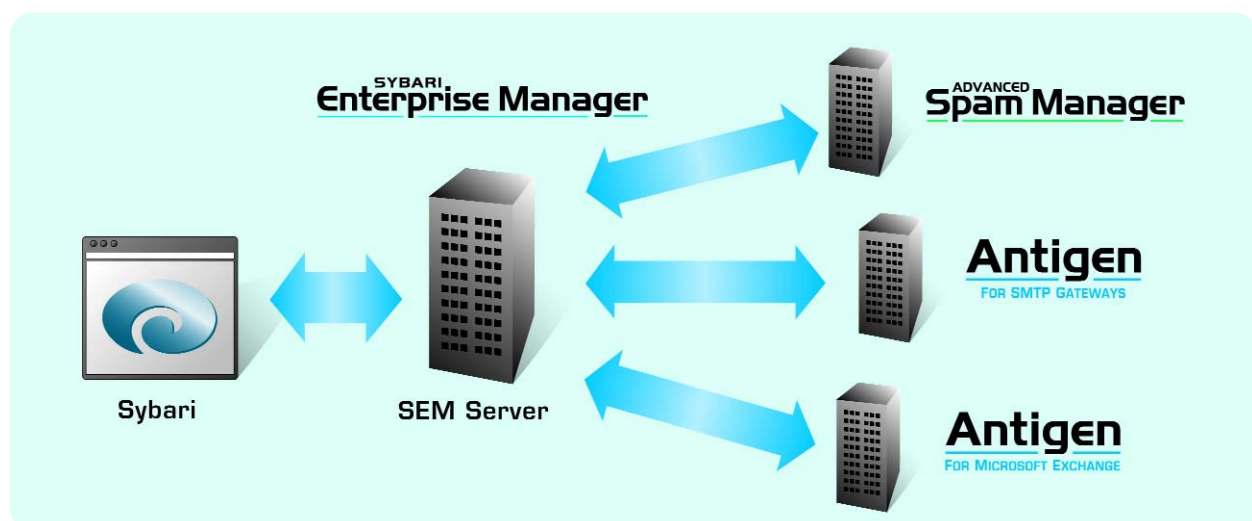
Mehr als je zuvor kommt es heute darauf an, Server-Sicherheitskonfigurationen und -strategien von einer zentralen Stelle aus zu managen. IT-Administratoren müssen von einem solchen zentralen Punkt aus umgehend auf Bedrohungen ihrer Netzinfrastruktur reagieren und gleichzeitig über die Leistungen der einzelnen Komponenten und Verkehrszahlen Bericht erstatten können. Der Sybari Enterprise Manager (SEM) bietet eine integrierte Lösung für das Überwachen und Managen von Sybari Technologien, die die Messaging- und Collaboration-Server Ihres Unternehmens schützen.

Dank SEM profitieren Administratoren von einem webbasierten Management-Tool, das zentralisiertes Deployment und Reporting für alle Server mit Antigen 8.0 im Unternehmen ermöglicht. SEM beinhaltet auch die Sybari Centralized Optimum Update-Technologie. Diese neue Funktion stellt Administratoren auf der Basis einer neuartigen Push-Pull-Architektur einen zentralen Mechanismus zur Aktualisierung von Scan-Engines auf mehreren Remote-Servern zur Verfügung. Vorkonfigurierte, umfassende, individuell anpassbare grafische Berichte, die die gesamte Messaging- und Filteraktivität zusammenfassen, helfen Administratoren, ihr aktuelles Environment zu optimieren und zu analysieren. Inzwischen ist auch das Überwachen und Managen von Viren- und ähnlichen Ausbrüchen zu einem Muss geworden. Die Administratoren können individuelle Virenwarnungen erstellen, die SMTP-

Meldungen und SNMP-Fallen aussenden, wenn die vorgegebenen Grenzwerte für Viren, Spam und Contentfilter überschritten werden.

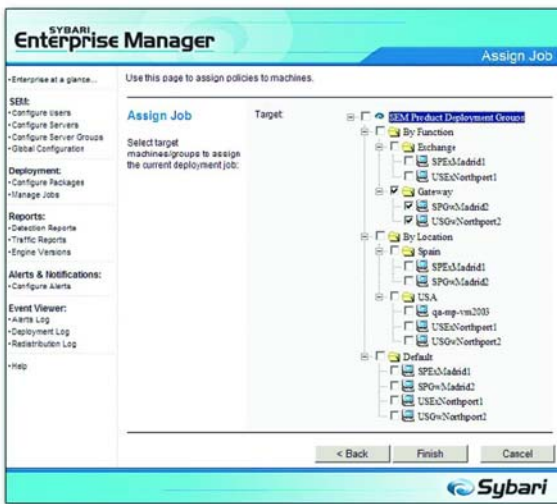
Browserbasiertes Management

SEM ermöglicht eine bessere Koordination aller Messaging- und Collaboration-Server, die durch Sicherheitslösungen von Sybari geschützt sind, durch eine kollektive Aufstellung der Server mit Antigen- und Advanced Spam Manager in Form einer hierarchisch aufgebauten Baumstruktur. Die Administratoren können Antigen und Advanced Spam Manager von einer zentralen, webbasierten Schnittstelle aus einsetzen, installieren und managen. Über seine Hub- und Spoke-Architektur kommuniziert der SEM-Server mit jedem der in die Sybari Serverprodukte integrierten SEM-Agenten.



Deployment

SEM wurde entwickelt, um die Produktinstallationen zu vereinfachen und Produktaktualisierungen, Hot Fixes und Patches, Templates und Signature-Dateien von einer zentralen Stelle aus aktivieren zu können. Um Silent Remote-Installationen und Upgrades noch effizienter zu machen, brauchen dank der Sybari Hot Upgrade-Technologie einzelne Dienste oder ganze Server wie Exchange, IMC und SMTP Services nicht mehr neu gestartet zu werden. Der SEM-Server steht im ständigen Austausch mit den lokalen SEM-Agenten, damit die Administratoren zentral einen einzelnen Remote-Server mit Sybari-Sicherheitsprodukten oder eine ganze Gruppe von Remote-Servern zentral konfigurieren können.

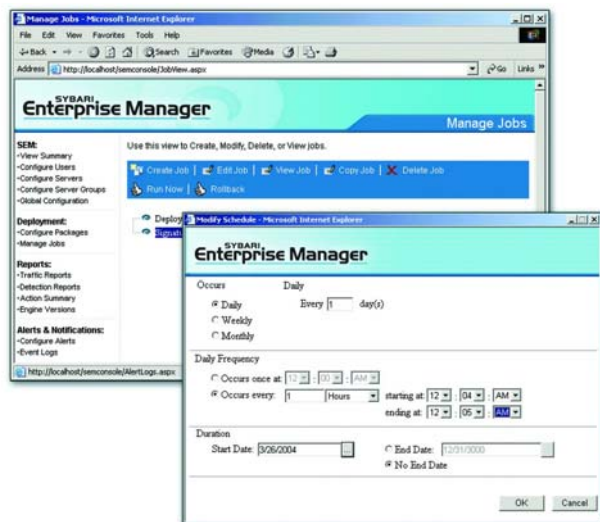


Die Sybari Centralized Optimum Update-Technologie

Die Sybari Centralized Optimum Update-Technologie wurde konzipiert, um das so genannte Window of Exposure, d.h. die Sicherheitslücke, die entsteht, wenn aktualisierte Motoren und Virus-Signaturen während eines Virenausbruchs verwendet werden, zu automatisieren und zu reduzieren. Die Administratoren können den integrierten Scheduler so konfigurieren, dass Sybari's sichere Sites regelmäßig abgerufen werden können. Sobald er auf eine neue Scan-Engine-Aktualisierung stößt, löst SEM die Aktualisierung aller Remote-Server mit Sybari-Sicherheitsprodukten aus.

Umfassende Berichterstattung

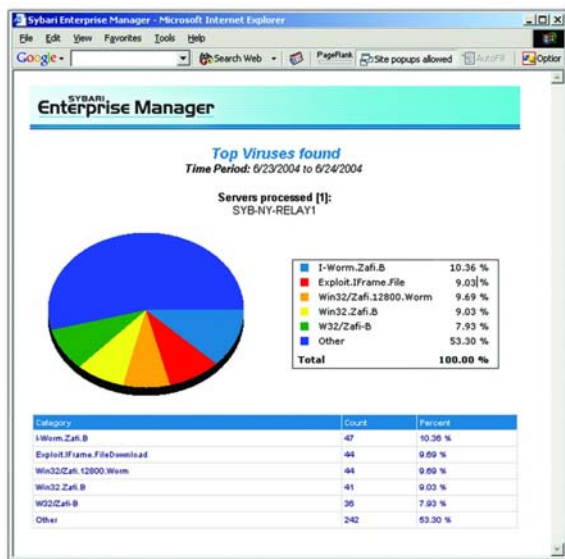
SEM erfasst Daten bezüglich Nachrichtenverkehr, ungewöhnliche Erfassungsaktivitäten, Zusammenfassung der Aktionen und Engine-Versionen aus allen mit Sybari-Sicherheitsprodukten ausgestatteten Servern und generiert grafische Berichte. 14 der über 25 Berichte, die verwendet werden können, um die Sicherheitsaktivitäten in einem Unternehmen darzustellen, sind Traffic Reports, die Nachrichtenverkehrsdaten wie Viren, Dateifilterung, Spam und Contentfilterung sammeln und grafisch darstellen. Zusätzliche Verkehrsberichte können Daten über SMTP-Messages und Bytes liefern, die zu fest vorgegebenen Zeiten in einem Server oder einer Servergruppe bearbeitet werden. Die Administratoren können auch Erfassungsberichte konfigurieren, die Daten bezüglich Virenanzahl, Anwendung von Suchfiltern und Spam-Zwischenfällen, die über eine bestimmte Zeitspanne an bestimmten oder multiplen Servern erfasst werden, zusammenfassen und grafisch darstellen.



SEM kann außerdem Daten präsentieren, die auf den Aktionen von Sybari's Antigen oder Advanced Spam Manager im Zusammenhang mit der Erfassung von Viren, Anwendung von Suchfiltern oder Spam basieren. Diese Berichte können genauer ausgeführt werden, indem Messages gestrichen, entfernt, gefiltert oder gelöscht werden. Die Administratoren können zudem Informationen über Lösungen von Sybari und jede einzelne ihrer integrierten Antivirus- und Antispam-Engines einschließlich Version und Aktualisierungsdetails erfassen und darüber Bericht erstatten.

Outbreak Management

SEM wurde konzipiert, um Administratoren proaktiv Viren oder Junk Mail zu melden, oder sie zu warnen, wenn die Grenzwerte für Datei- oder Contentfilter überschritten werden. Abhängig von den Anforderungen des Unternehmens können die Administratoren spezifische Grenzwerte (in Zahlen oder Prozent) definieren und konfigurieren. SEM benachrichtigt die Administratoren via Meldungen und SNMP-Fallen. Network Management-Lösungen, die Daten von SNMP-Fällen erfassen, z.B. Tivoli, NetIQ AppManager und HP OpenView usw., können Antigen und Sybari Advanced Spam Manager in ihren Berichten und auf den Konsolen überwachen.



Erweiterte Überwachungs- und Warnungsfunktionen

SEM kann die Administratoren auch per SMTP E-Mail-Meldungen und SNMP-Warnungen benachrichtigen, die davon abhängen, ob die Antivirus- oder Spam-Scan-Engines richtig aktualisiert wurden oder nicht. Damit wird sichergestellt, dass alle mit Sybari-Sicherheitsprodukten ausgestatteten Server mit den neuesten verfügbaren Scan-Engines und Signature-Dateien arbeiten.

Wichtige Merkmale und Vorteile

- ▶ Zentrales Deployment
- ▶ Virenwarnung
- ▶ Browserbasierte Managementkonsole
- ▶ Hot Upgrade-Technologie
- ▶ Umfassende Berichterstattung
- ▶ Sybari Centralized Optimum Update-Technologie

Systemanforderungen

Kompatibilität:

- Antigen 8.0 for Exchange
- Antigen 8.0 for SMTP Gateways
- Antigen 8.0 for SharePoint
- Antigen 8.0 for Instant Messaging
- Advanced Spam Manager 8.0

Mindestanforderungen an den Server:

- Windows 2000, Windows 2000 Server/Advanced Server oder Windows 2003
- 128 MB verfügbarer Speicherplatz
- 183 MB verfügbarer Speicherplatz auf der Festplatte für die weiter unten angeführten Voraussetzungen
- 65 MB verfügbarer Speicherplatz auf der Festplatte für den SEM

Voraussetzungen:

- IIS 5.0 oder darüber
- .net Runtime v. 1.1
- ASP.net v. 1.1
- Microsoft Message Queue und MSMQ Triggers
- MSDE oder SQL Server



Sybari Software Germany

Mühlweg 2 B. 82054 Sauerlach. Germany
Phone: +49 (0) 8104 6493 0 · Fax: +49 (0) 8104 6493 34
e-mail: sales-de@sybari.com