WHITE PAPER

GFI LANguard S.E.L.M. im Einsatz

Überblick über die Funktionsweise und verschiedene Einsatzstrategien

In diesem White Paper erhalten Sie einen Überblick über die Funktionsweise von GFI LANguard S.E.L.M. Zudem werden die Themen Installation und Einsatzmöglichkeiten behandelt, damit Sie entscheiden können, wie das Produkt in Ihrem Netzwerk am besten eingesetzt werden sollte.

Einführung

In diesem White Paper erhalten Sie einen Überblick über die Funktionsweise von GFI LANguard S.E.L.M. Zudem werden die Themen Installation und Einsatzmöglichkeiten behandelt, damit Sie entscheiden können, wie das Produkt in Ihrem Netzwerk am besten eingesetzt werden sollte.

Die Struktur von GFI LANguard S.E.L.M.

GFI LANguard S.E.L.M. wurde für die Überwachung von Ereignisprotokollen entwickelt, die ohne die Installation eines Agent oder Client auf jedem zu kontrollierenden Rechner auskommt. Dieses Prinzip erspart Administratoren somit zusätzlichen Konfigurations- und Verwaltungsaufwand.

GFI LANguard S.E.L.M. bietet operative Komponenten (Dienste, die diskret im Hintergrund laufen) und eine Benutzeroberfläche mit verschiedenen Modulen. Standardmäßig werden beide Komponenten installiert, aber es ist auch möglich, nur die operativen Komponenten zu installieren (es sei denn, Sie verwenden Microsoft Access als Backend). Folgende Komponenten werden installiert:

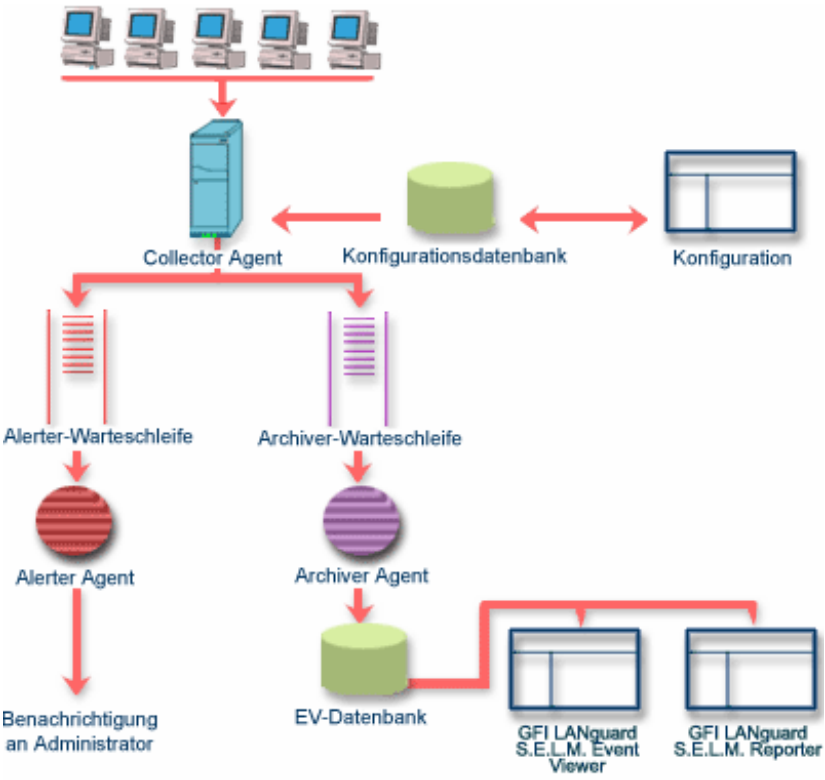
Operative Komponenten (nicht sichtbar/konfigurierbar für Anwender)

1. GFI LANguard S.E.L.M. Collector Agent
2. GFI LANguard S.E.L.M. Alerter Agent
3. GFI LANguard S.E.L.M. Archiver Agent

Komponenten der Benutzeroberfläche (sichtbar/konfigurierbar für Anwender)

1. MMC-Snap-In zur Konfiguration von GFI LANguard S.E.L.M.
2. MMC-Snap-In als Ereignis-Monitor von GFI LANguard S.E.L.M.
3. MMC-Snap-In als Berichtmodul von GFI LANguard S.E.L.M.
4. Support-Tools von GFI LANguard S.E.L.M.

Folgende Darstellung zeigt, wie die einzelnen Komponenten von GFI LANguard S.E.L.M. zusammenarbeiten:



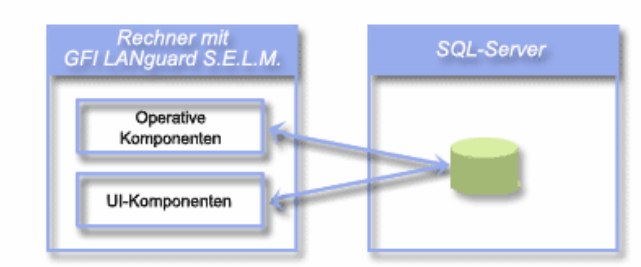
Überblick über die Funktionsabläufe von GFI LANguard S.E.L.M.

Technische Voraussetzungen für die Installation

Auswahl der Datenbank-Backends

Während der Installation müssen Sie auswählen, welches Datenbank-Backend für GFI LANguard S.E.L.M. zum Einsatz kommen soll. Zur Auswahl stehen:

1. Microsoft Access
2. SQL-Datenbank unter Verwendung von Microsoft SQL Server oder
3. SQL-Datenbank auf Grundlage von MSDE (geringe Ressourcen, kostenfreie Version von MS SQL).



Greift GFI LANguard S.E.L.M. auf Microsoft SQL Server als Datenbank-Backend zurück, muss sich dieser SQL-Server auf demselben Rechner wie GFI LANguard S.E.L.M. befinden. Ebenso können beim Einsatz von SQL oder MSDE mehrere Installationen von GFI LANguard S.E.L.M. mit demselben SQL-Backend arbeiten. Bei großen Netzwerken hat dies den Vorteil, dass sich mehrere Collector-/Analyse-Dienste mit weiterhin nur einer konsolidierten Ereignis-Datenbank verwenden lassen.

In kleineren Netzwerken, wo der Umfang der gesammelten Daten nicht sehr groß ist, kann GFI LANguard S.E.L.M. für den Einsatz einer MS Access-Datenbank als Backend konfiguriert werden.

Bei wachsendem Datenaufkommen sollte diese dann jedoch von MS SQL Server als Backend abgelöst werden. MS SQL Server bietet eine höhere Skalierbarkeit, erlaubt eine leichtere Verwaltung der Datenbank und ist zudem leistungsfähiger.

Single/Multi-Domain-Umgebungen

Wenn Sie mit mehreren Domänen arbeiten, sollten Sie aus Sicherheitsgründen und für eine optimale Bandbreite mindestens eine Installation von GFI LANguard S.E.L.M. für jede Domäne vorsehen. In diesem Fall steht dann für jede Installation ein eigenes Datenbank-Backend zur Verfügung. Mit Hilfe des Connectors von GFI LANguard S.E.L.M. können diese Datenbanken dann als eine gemeinsame Datenbank aneinander angebunden werden.

Von GFI LANguard S.E.L.M. verwendete Ports und Protokolle

GFI LANguard S.E.L.M. verwendet RPC-over-SMB, um Ereignisse zu erfassen und benötigt daher die Ports 445 und 139, um mit dem Zielrechner zu kommunizieren. (Greift GFI LANguard S.E.L.M. jedoch auf seinen WAN-Connector zurück, der Daten per DTS abruft, oder auf eine SQL Server-Datenbank, muss zudem der SQL-Port verfügbar sein, Standard: 1433.) Der Datenverkehr wird dabei standardmäßig per Windows 2000/XP Kerberos oder Windows NT LM2 abgesichert. Daher lassen sich Traffic und Ereignisdaten nicht mutwillig verändern, und die Daten des abgefragten Rechners werden an den abfragenden Rechner über den ersten Ausgangs-Port zurückgeleitet.

Voraussetzungen für die Identifikation der Computer

GFI LANguard S.E.L.M. identifiziert Computer anhand des Rechnernamens oder der IP-Adresse. Wenn NetBIOS-kompatible Rechnernamen verwendet werden, müssen Sie sicherstellen, dass Ihr DNS-Dienst für eine Namensauflösung entsprechend konfiguriert ist. Eine unzuverlässige Namensauflösung führt zu einer bedeutenden Schwächung der Systemleistung. Beachten Sie bitte, dass bei einer Deaktivierung von NetBIOS-over-TCP/IP GFI LANguard S.E.L.M. dennoch weiterhin verwendet werden kann – Sie müssen jedoch den Rechnernamen über die IP-Adresse festlegen.

Erforderliche Bandbreite für GFI LANguard S.E.L.M.

Der Abruf eines einzelnen Ereignisses von einem Rechner erzeugt ein Datenaufkommen von ca. 300 Bytes. Ein Rechner, der mit den empfohlenen Überwachungsrichtlinien von GFI LANguard S.E.L.M. konfiguriert ist, erzeugt ungefähr zehn Ereignisse pro Tag. Bei einem mit S.E.L.M. überwachten Rechner, auf dem keine besonderen Ereignisse eintreten, fallen somit 3 KB an täglichem Datenverkehr im Netzwerk an. Bei modernen Netzwerken ist diese Datenmenge unerheblich.

HINWEIS: Obwohl die Ereignisprotokoll-Einträge sehr viel Text enthalten, werden nur die Parameter zwischen dem Host- und Zielrechner übertragen, die für das Erstellen der jeweiligen Mitteilung notwendig sind. Sprachunabhängige Zeichenketten werden nicht übertragen. Dadurch wird die übertragene Datenmenge bei der Verbindung zwischen den beiden Rechnern erheblich reduziert.

Einsatzbeispiele

1. Kleinere Netzwerke mit einer einzelnen Domäne

Bei Netzwerken von bis zu 300 Rechnern, z. B. mit 10 Servern und 290 Arbeitsplatzrechnern, ist eine einzige Installation von GFI LANguard S.E.L.M. mit einem Access- oder SQL-Backend vollkommen ausreichend.

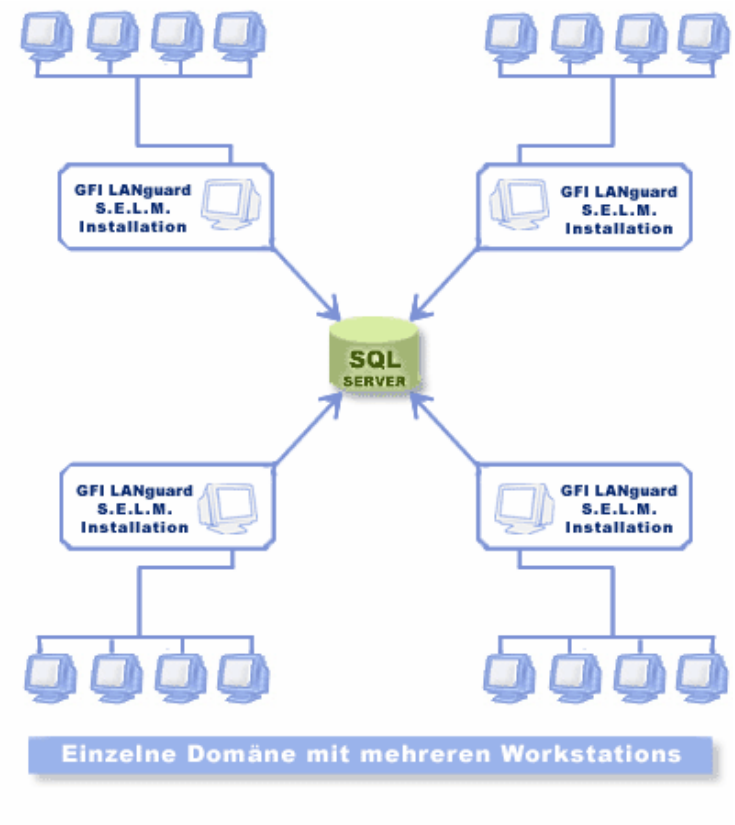
Wenn Sie Server in Echtzeit überwachen möchten, ist allgemein zu empfehlen, eine Installation von GFI LANguard S.E.L.M. pro 15 Server zu verwenden. Sie können Arbeitsplatzrechner dann einmal pro Stunde kontrollieren lassen. In diesem Fall kann eine Installation von GFI LANguard S.E.L.M. bis zu 200 Arbeitsplatzrechner überwachen, solange einem Server eine höhere Überwachungspriorität zugewiesen wird als einem Arbeitsplatzrechner.

2. Größere Netzwerke mit einer einzelnen Domäne

Wenn Sie ein größeres Netzwerk mit z. B. 50 Servern und 1000 Arbeitsplatzrechnern überwachen möchten, ist der Einsatz mehrerer Installationen von GFI LANguard S.E.L.M. zu empfehlen. Um die Daten zentral zu speichern und zu verwalten, sollte ein einzelner SQL-Server als Backend eingerichtet werden und jede Installation von GFI LANguard S.E.L.M. auf

diesen SQL Server-Backend schreiben.

Bei 50 Servern und 1000 Arbeitsplatzrechnern können Sie z. B. fünf Installationen von GFI LANguard S.E.L.M. einsetzen, von denen jede einzelne zehn Server und 200 Arbeitsplatzrechner überwacht und auf eine gemeinsame SQL-Datenbank schreibt.



Installation in größeren Netzwerken

3. Große WANs mit mehreren Sites und Domänen

Wenn Sie ein Netzwerk mit mehreren (geographischen) Sites und daher wahrscheinlich auch mit mehreren Domänen betreiben, sollten Sie für jede Site eine eigene Installation von GFI LANguard S.E.L.M. einrichten. Optional kann die jeweilige Installation über den S.E.L.M.-Connector als Satelliten-Server für die übergeordnete Installation von S.E.L.M. betrieben werden.

So kann z. B. ein Netzwerk mit 4370 Rechnern, die über vier Sites verteilt sind und von denen jede wiederum eine eigene Domäne ist, die Überwachung wie folgt aussehen:

- München – 250 zu überwachende Rechner
- Hannover – 100 zu überwachende Rechner
- Berlin – 4000 zu überwachende Rechner

- Würzburg – 20 zu überwachende Rechner

In diesem Fall würden sie mindestens vier Installationen benötigen, eine für jede Domäne. Die Domäne in Berlin umfasst jedoch sehr viele Rechner. Es ist zu empfehlen, maximal 300 Computer von einer Installation überwachen zu lassen. Dies bedeutet, dass Sie in Berlin 14 Installationen von GFI LANguard S.E.L.M. einrichten sollten. Jede Installation würde dann eine eigene Gruppe von Computern überwachen. Die Anzahl der Installationen sieht daher wie folgt aus:

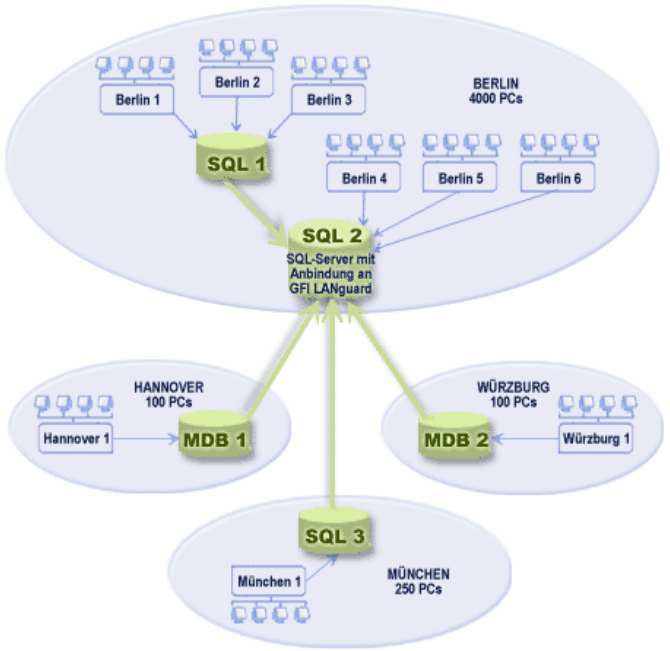
- München – 1 Installation
- Hannover – 1 Installation
- Berlin – 14 Installationen
- Würzburg – 1 Installation

Ist am Standort Berlin ein schnelles Netzwerk vorhanden, schreiben alle Installationen in dieselbe Datenbank. Bei einem langsameren Netzwerk hingegen sollte der Einsatz zweier SQL-Datenbank-Backends in Betracht gezogen werden.

Bei kleineren Sites wie Würzburg und Hannover kann auch MS Access problemlos als Datenbank-Backend eingesetzt werden. Hierdurch lassen sich die Lizenzierungskosten für den SQL-Server einsparen.

HINWEIS: Der Einsatz von GFI LANguard S.E.L.M. wirkt sich kaum auf die Leistung des Rechners aus, auf dem das Programm installiert ist. Auch die benötigte Bandbreite ist minimal.

Die sich ergebenden Installationen sehen dann wie in der folgenden Abbildung aus, mit 14 Installationen am Standort Berlin (in der Abb. als sechs Installationen dargestellt) und jeweils einer in Hannover, München und Würzburg.



Einsatz von GFI LANguard S.E.L.M. in einem großen WAN mit mehreren Domänen

Da Ihnen GFI LANguard S.E.L.M. auch die Möglichkeit bietet, nur die "operativen Komponenten" zu installieren, kann die Software in einigen Netzwerk-Bereichen auch transparent installiert werden – nicht nur, um den Administrationsaufwand zu verringern, sondern eventuell auch aus Sicherheitsgründen. Eine Installation von GFI LANguard S.E.L.M. ohne Konfigurations- oder Bericht-Tools erschwert es Unbefugten, die Konfiguration oder gesammelten Daten zu verändern.

Der Connector von GFI LANguard S.E.L.M.

Der Connector von GFI LANguard S.E.L.M. wurde speziell für den Einsatz des Produkts für mehreren Domänen/geografische Sites entwickelt. Der Connector verbindet die verschiedenen Datenbank-Backends zu einer einzigen Datenquelle. Dies ermöglicht es Ihnen, sämtliche Sicherheitsdatenbestände oder Teile davon in einer einzigen, übergreifenden Datenbank zu konsolidieren, zu deren Einträgen dann Berichte erstellt werden können.

Der S.E.L.M.-Connector kann auch so eingerichtet werden, dass andere Installationen von GFI LANguard S.E.L.M. als Satelliten-Server für den übergeordneten Haupt-Server dienen. Der Connector ruft alle wichtigen Daten aus den Datenbanken dieser Satelliten-Server ab und konsolidiert sie dann in einer Datenbank. Dies kann mit Hilfe von Filtern geschehen, sodass Sie nur die benötigten Daten erhalten und weniger Bandbreite und Speicher in Anspruch nehmen müssen.

FAQs zur Installation

Kann ich MS Access- und SQL-Datenbank-Backends gemeinsam einsetzen und dann zudem die Daten in einer zentralen Datenbank konsolidieren?

Ja, dies ist möglich. Der S.E.L.M.-Connector kann Ereignisse von den Satelliten-Servern abrufen und in einer zentralen S.E.L.M.-Datenbank zusammenführen. Sie können den Connector so konfigurieren, dass er nur die von Ihnen gewünschten Ereignisinformationen filtert.

Unter welchen Betriebssystemen kann GFI LANguard S.E.L.M. installiert werden?

GFI LANguard S.E.L.M. kann unter folgenden Betriebssystemen installiert werden:

- Windows 2000 Professional
- Windows 2000 Server
- Windows 2003 Server
- Windows XP Professional.

Benötigt GFI LANguard S.E.L.M. einen dedizierten Rechner?

Nein, dies ist nicht zwingend notwendig. GFI LANguard S.E.L.M. kann problemlos im Hintergrund arbeiten und Daten von bis zu 250 Computern sammeln. GFI LANguard S.E.L.M. benötigt nur wenige Ressourcen. Anstatt einen eigenen Rechner zu verwenden ist es besser, bei größeren Netzwerken die Belastung auf mehrere Installationen von GFI LANguard S.E.L.M. zu verteilen.

Über GFI LANguard Security Event Log Monitor (S.E.L.M.)

GFI LANguard Security Event Log Monitor (S.E.L.M.) bietet Eindringlingserkennung mit Hilfe der Ereignisprotokolle, die netzwerkweit verwaltet werden können. GFI LANguard S.E.L.M. archiviert und analysiert die Event-Logs aller Netzwerk-Rechner. Bei Sicherheitsproblemen, Angriffen und anderen kritischen Ereignissen erfolgt die Alarmierung in Echtzeit. Dank der intelligenten Analysetechnik von GFI LANguard S.E.L.M. sind keine Expertenkenntnisse notwendig, um Benutzer zu überwachen, die versuchen, auf geschützte Freigaben und vertrauliche Dateien zuzugreifen. Sicherheitskritische Server lassen sich effizient kontrollieren, und auch das Erstellen von Warnhinweisen für einzelne Netzwerk-Ereignisse und Bedingungen ist problemlos möglich. Zudem können Ereignisprotokolle auf Remote-Rechnern automatisch gelöscht oder gesichert werden. Angriffe über lokale Benutzerkonten lassen sich ebenfalls schnell erkennen und bekämpfen.

Weitere Informationen zu GFI LANguard S.E.L.M. und eine kostenfreie Testversion finden Sie unter http://www.gfisoftware.de/de/lanselm/.

Über GFI

GFI (www.gfisoftware.de) ist ein führender Entwickler und Anbieter von Produkten für Netzwerk- und Inhaltssicherheit sowie von Kommunikationslösungen. Das Produktportfolio von GFI umfasst unter anderem den Netzwerk-Fax-Server GFI FAXmaker for Exchange/SMTP, die Sicherheitslösung GFI MailSecurity for Exchange/SMTP zur Überprüfung von E-Mail-Inhalten und zum Schutz vor E-Mail-basierten Exploits und Viren, die Server-basierte Anti-Spam-Software GFI MailEssentials for Exchange/SMTP, GFI LANguard Network Security Scanner (N.S.S.) für Sicherheits-Scans und Patch-Management, GFI Network Server Monitor zum automatischen Versand von Warnmitteilungen und zur Fehlerbehebung bei Netzwerk- und Server-Problemen, GFI LANguard Security Event Log Monitor (S.E.L.M.) zur Ereignisprotokoll-basierten Eindringlingserkennung und netzwerkweiten Verwaltung von Ereignisprotokollen sowie GFI LANguard Portable Storage Control (P.S.C.) zur netzwerkweiten Kontrolle wechselbarer Speichermedien. GFI-Produkte sind im Einsatz bei Microsoft, Telstra, Time Warner Cable, Shell Oil Lubricants, NASA, DHL, Caterpillar, BMW, der US-Steuerbehörde IRS und der USAF. GFI unterhält Niederlassungen in den USA, Großbritannien, Deutschland, Zypern, Rumänien, Australien und Malta und wird von einem weltweiten Netzwerk von Distributoren unterstützt. GFI ist "Microsoft Gold Certified Partner" und erhielt die Auszeichnung "Microsoft Fusion (GEM) Packaged Application of the Year". Weitere Informationen erhalten Sie unter http://www.gfisoftware.de.