



GFI WebMonitor

for ISA Server

Echtzeit-Überwachung von HTTP/FTP-Verbindungen mit Virenschutz und Zugriffssteuerung

Studien des Marktforschers IDC zufolge nutzen Mitarbeiter ihren Firmenzugang zum Internet bis zu 40 Prozent für private Zwecke. Um einen unternehmensgerechten Web-Zugriff sicherstellen zu können, müssen Administratoren Werkzeuge zur Verfügung stehen, die das Surf-Verhalten kontrollieren und steuern sowie Datei-Downloads auf Viren und andere Malware überprüfen. GFI WebMonitor for ISA Server erlaubt es, Website-Aufrufe und Downloads in Echtzeit zu überwachen und zu regulieren – für einen produktiveren Einsatz des Internet.

GFI WebMonitor ermöglicht eine gezielte Steuerung des Website-Aufrufs: Per WebGrade Database, einer vollständig manuell gepflegten Datenbank zur Website-Kategorisierung, können Administratoren den Zugriff auf bestimmte Kategorien sperren, darunter Erotikseiten, Online-Spiele, Freemail-Anbieter, P2P-Tauschplattformen, Flugbörsen oder Social-Networking-Plattformen wie Facebook und MySpace.

Lassen Sie Datei-Downloads durch Mitarbeiter überwachen, um beispielsweise Formate wie MP3-Dateien vom Netzwerk fernzuhalten. Ebenso können sämtliche heruntergeladenen Inhalte mit mehreren Anti-Virus-Engines auf Viren, Spyware und andere Malware überprüft werden. Selbst die Gefahr des Informationsdiebstahls per betrügerische Phishing-Websites wird gemindert: Mit Hilfe einer automatisch aktualisierbaren Datenbank zu Phishing-URLs lässt sich der Zugriff auf manipulierte Sites sperren.

GFI WebMonitor for ISA Server ist in 3 Editionen erhältlich:

- **WebFilter Edition:** bietet URL-Filterung und Website-Kategorisierung
- **WebSecurity Edition:** liefert Viren- und Phishing-Schutz und spürt Spyware auf
- **UnifiedProtection Edition:** vereint die WebFilter Edition und WebSecurity Edition in einer Lösung

Alle Editionen unterstützen Microsoft ISA Server 2004 und Microsoft ISA Server 2006.

Leistungsmerkmale von GFI WebMonitor – WebFilter Edition

■ Schutz vor rechtlichen Fallstricken

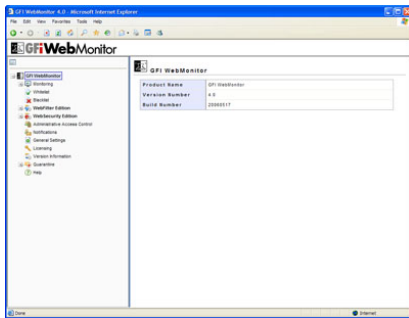
Unternehmen müssen die Möglichkeit haben, das Surf-Verhalten von Mitarbeitern zumindest ansatzweise zu kontrollieren, um sich auch rechtlich abzusichern. Sind keine Verfahren zum Schutz vor Belästigungen von Mitarbeitern durch das Internet implementiert, können Organisationen für die Vernachlässigung ihrer Sorgfaltspflicht verantwortlich gemacht werden. Der Einsatz von Tools, die den Zugriff auf Websites mit anstößigen oder rechtswidrigen Inhalten sperren oder zumindest überwachen, ist somit unerlässlich.

Vorteile

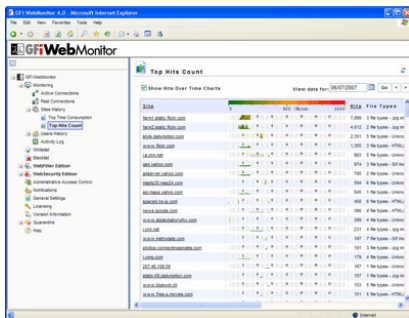
Warum GFI WebMonitor?

- Sorgt für höhere Mitarbeiterproduktivität durch gezieltes Regulieren der Internet-Nutzung
- Schützt das Netzwerk vor sicherheitsgefährdenden Downloads – in Echtzeit
- Mindert die unerwünschte private Nutzung des Internet
- Verhindert Informationsdiebstahl über betrügerische Websites
- Liefert mehrere Scan-Engines für umfassenderen Schutz vor Viren und anderer Malware in heruntergeladenen Dateien

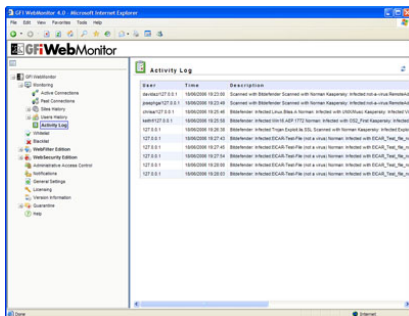
Leistungsmerkmale von GFI WebMonitor – WebSecurity Edition



Konfiguration

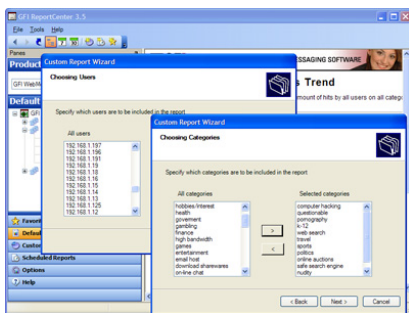


Verbindungsüberwachung und Statistiken



Überwachung der Online-Aktivitäten von Mitarbeitern

GFI WebMonitor ReportPack



Assistent zur Erstellung individueller Berichte



Übersicht zu Standardberichten

Kontrolle von Datei-Downloads mit mehreren Anti-Virus-Engines

GFI WebMonitor überprüft Dateien, die aktuell heruntergeladen werden, mit mehreren Viren-Scannern. Der Einsatz verschiedener Scanner verkürzt die durchschnittliche Wartezeit bis zum Erhalt aktualisierter Signatur-Updates und verringert die Gefahr, mit einem neuen Virus infiziert zu werden. Es gibt keinen Anti-Virus-Hersteller, der stets am schnellsten auf akute Bedrohungen reagiert. Wird ein neuer Virus bekannt, hängt ein rasches Bereitstellen entsprechender Updates z. B. davon ab, wo der Schädling entdeckt wurde. Die Verwendung mehrerer Scan-Engines erhöht die Chance, dass mindestens eine von ihnen zeitnah aktualisiert wird und rechtzeitig Schutz bietet. Zudem wendet jede Lösung ihre eigene Heuristik an und besitzt individuelle Abwehrmethoden. Einige Scanner erkennen bestimmte Virenarten samt Untergruppen besser als andere, die wiederum ihre eigenen speziellen Stärken haben. Fakt ist: Je mehr Scan-Engines eingesetzt werden, desto umfassender ist der Schutz.

Virenschutz durch Norman Virus Control und BitDefender

GFI WebMonitor wird im Bundle mit Norman Virus Control und BitDefender ausgeliefert. Norman Virus Control ist eine professionelle Anti-Virus-Engine, die bereits 19 Mal mit dem "Virus Bulletin 100% Award" ausgezeichnet wurde. Zudem hat das Produkt die ICSA- und Checkmark-Zertifizierung erhalten. BitDefender ist eine sehr schnelle und flexibel einsetzbare Anti-Virus-Engine und hebt sich durch die Anzahl der Formate hervor, die erkannt und gescannt werden. BitDefender ist ebenfalls ICASA-zertifiziert und hat für seinen hervorragenden Schutz neben zahlreichen anderen Preisen auch den "Virus Bulletin 100% Award" erhalten. Die Virendefinitionen für Norman Virus Control und BitDefender werden automatisch auf den neuesten Stand gebracht, sobald Aktualisierungen verfügbar sind. Im Produktpreis von GFI WebMonitor sind bereits Updates für 1 Jahr eingeschlossen.

Abwehr von Malware (z. B. Trojaner und Spyware) per Kaspersky-Engine – optional

Für umfassendere Sicherheit und zusätzliche Virenüberprüfungen steht die Anti-Virus-Engine von Kaspersky mit seiner SuperSecure-Datenbank als optionales Scan-Modul zur Verfügung. Die Kaspersky-Lösung erkennt böswillige Software wie Programme zur Remote-Verwaltung, Tastatur-Logger, Passwort-Späher, Dialer für kostenpflichtige Angebote, Downloader für Adware oder Erwachsenen-Inhalte u. v. m. Virendefinitionen der Scan-Engine werden von GFI WebMonitor automatisch auf den neuesten Stand gebracht, sobald Aktualisierungen verfügbar sind.

Schutz vor betrügerischen Phishing-Websites

Hacker setzen das Phishing ("password fishing") als Variante des manipulativen "Social Engineering" ein: Benutzer werden per E-Mail oder Instant Messenger auf vermeintlich echte Firmen-Websites, vorrangig von Online-Shopping-Unternehmen oder Banken, gelockt. Über diese präparierten Sites wird dann versucht, an vertrauliche Daten wie Anmelde- und Kreditkarteninformationen zu gelangen. Durch das Blockieren bekannter Phishing-Websites mindert GFI WebMonitor das Risiko, Opfer eines solchen Betrugs zu werden. Die Kontrolle erfolgt über eine automatisch aktualisierte Datenbank zu Phishing-URLs.

Dateityp- und benutzerspezifische Download-Blockierung

Über benutzer-, gruppen- und IP-spezifische Richtlinien zur Download-Kontrolle lässt sich das Herunterladen einzelner Dateitypen wie JavaScript, MP3, MPEG, EXE u. Ä. differenziert unterbinden. Sicherheitsgefährdende Programme (wie Trojaner-Downloader) versuchen oftmals, als harmlose Dateien getarnt in ein System einzudringen. Mit Hilfe des in GFI WebMonitor integrierten Dateisignatur-Scanners lässt sich jedoch der tatsächliche Dateityp von heruntergeladenen HTTP-/FTP-Dateien erkennen.

Leistungsmerkmale von GFI WebMonitor UnifiedProtection Edition (allgemeine Merkmale)

Die folgenden Leistungsmerkmale stehen in allen Editionen zur Verfügung.

■ Überwachung und Abbruch von Downloads oder Seitenbesuchen in Echtzeit

Systemverantwortliche behalten jederzeit den Überblick über aktuell aufgerufene Websites und laufende Downloads. Aktive Verbindungen, Seitenbesuche und Downloads können mit nur einem Mausklick blockiert werden. Beispielsweise lässt sich das Herunterladen einer übergroßen Datei umgehend unterbrechen.

■ Überwachung und Blockierung von versteckten Downloads durch Anwendungen

Einige Software-Anwendungen erstellen automatisch eine HTTP-Tunneling-Verbindung zur Website ihres Herstellers, um nach Updates zu suchen. Als Erleichterung für den Administrator gedacht, stellt diese Unterstützung jedoch auch ein Sicherheitsrisiko dar: Unbekannte Anwendungen und Trojaner können mit dieser Methode unbemerkt schädliche Dateien, darunter auch Spyware, Adware und Pornware, auf den PC herunterladen. GFI WebMonitor erlaubt es Ihnen festzulegen, von welchen Sites Updates bezogen werden dürfen (z. B. Microsoft).

■ Überwachung der Bandbreiten-Nutzung

Die Überwachung der Bandbreiten-Nutzung je Benutzer oder Website erlaubt es Administratoren, Upload- und Download-Aufkommen sowie URL-Aufrufe über einen längeren Zeitraum hinweg nachzuverfolgen. Die detaillierte Berichterstellung mit anschaulichen Grafiken unterstützt eine Überwachung in Echtzeit.

■ Erstellung von Whitelists und Blacklists für Filterausnahmen

URLs, Benutzer und IP-Adressen lassen sich vorübergehend oder dauerhaft auf eine Whitelist oder Blacklist setzen, um von der Kontrolle durch Richtlinien zur Web-Filterung und -Sicherheit ausgenommen zu sein. Beispielsweise ist es hierdurch möglich, einem einzelnen Mitarbeiter befristeten Zugang zu seinem privaten Webmail-Konto zu gewähren.

■ Zugriffskontrolle für die Konfigurations- und Überwachungskonsole

Der Zugriff auf die Konfigurations- und Überwachungsoberfläche von GFI WebMonitor kann auf einzelne Anwender beschränkt werden. Zugriffsrechte lassen sich unter anderem unter Berücksichtigung der Rechner-IP erteilen. Nur Anwender, die in der Liste autorisierter Benutzer/IPs stehen, erhalten Zugang.

Systemanforderungen

- Microsoft Windows 2000 (SP4), 2003
- Microsoft ISA Server 2004 oder neuer
- Microsoft Internet Explorer 6 oder neuer
- Microsoft .NET Framework 2.0

Auszeichnungen



Ihre Testversion steht unter <http://www.gfisoftware.de/de/webmon/> zum Download bereit!

GFI Software
Magna House, 18 – 32 London Road
Staines, Middlesex
TW18 4BP
UK
Tel +44 (0) 870 770 5370
Fax +44 (0) 870 770 5377
sales@gfi.co.uk

GFI Software
15300 Weston Parkway
Suite 104
Cary, NC 27513
USA
Tel +1 (888) 243-4329
Fax +1 (919) 379-3402
sales@gfiusa.com

GFI Asia Pacific Pty Ltd
83 King William Road
Unley 5061
South Australia
Tel +61 8 8273 3000
Fax +61 8 8273 3099
sales@gfiap.com

GFI Software
GFI House
San Andrea Street
San Gwann SGN 1612
Malta
Tel +356 21 382418
Fax +356 21 382419
sales@gfi.com

Microsoft
GOLD CERTIFIED
Partner

GFI
www.gfi.com