Manual do produto GFI



Guia de avaliação - para obter os melhores benefícios da versão de avaliação o GFI LanGuard





As informações e o conteúdo deste documento são apenas informativos e fornecidos "no estado em que se encontram" sem nenhuma garantia de qualquer tipo, expressa ou implícita, incluindo, sem limitação, as garantias de comercialização, adequação a uma finalidade específica e não violação. A GFI Software não se responsabiliza por danos de qualquer natureza, incluindo danos indiretos, resultantes do uso deste documento. As informações foram obtidas de fontes disponíveis ao público. Apesar do razoável esforço para garantir a precisão dos dados fornecidos, a GFI não alega, promete ou garante que as informações sejam íntegras, precisas, recentes ou adequadas, e não se responsabiliza por falhas na impressão, informações desatualizadas ou outros erros. A GFI não oferece garantia expressa ou implícita e não assume obrigação ou responsabilidade legal pela precisão ou integridade das informações contidas neste documento.

Se você acredita que este documento contenha erros efetivos, entre em contato conosco. Analisaremos a questão assim que possível.

Todos os nomes de produtos e empresas aqui mencionados podem ser marcas de seus respectivos proprietários.

Os direitos autorais sobre GFI LanGuard pertencem à GFI SOFTWARE Ltd. - 1999-2015 GFI Software Ltd. Todos os direitos reservados.

Versão do documento: 12.0

Última atualização (dia/mês/ano): 14/04/2016

# Índice

1 Introdução	4
1.1 Visão geral do GFI LanGuard	4
1.2 Por que os clientes compram o GFI LanGuard?	5
1.3 Obtenção de uma chave de avaliação	9
2 Realizar verificações de segurança	10
2.1 Verificações de segurança sem agente	10
2.2 Auditorias com agente	14
2.3 Auditoria em smartphones e tablets	16
2.4 Perfis de verificação	17
2.5 Acionamento de verificações pelo Dashboard	18
3 Analisar resultados da verificação	20
3.1 Dashboard	20
3.2 Como exibir alterações de segurança relevantes a partir de sua rede	22
3.3 Como adicionar/exibir mais dispositivos no painel	23
3.4 Como filtrar dispositivos	24
3.5 Como agrupar dispositivos	24
3.6 Como pesquisar computadores	26
3.7 Busca de texto completo	27
3.8 Geração de relatórios	28
4 Corrigir problemas de segurança	30
4.1 Implementar atualizações de software ausentes	30
4.2 Desinstalar aplicativos não autorizados	33
4.3 Implementar software personalizado	36
4.4 Enviar notificações por email para proprietários de dispositivos móveis	37
4.5 Outras operações de correção	38
5 Automatizar tarefas	40
5.1 Descobrir automaticamente novos dispositivos na rede	40
5.2 Automatizar auditorias de segurança	41
5.3 Automatizar download de correções	43
5.4 Automatizar operações de correção	44
5.5 Automatizar geração de relatórios	49
6 Glossário	50
7 Índice	57

# 1 Introdução

Obrigado por avaliar o GFI LanGuard. O objetivo deste guia é ajudá-lo a aproveitar ao máximo sua versão de teste do GFI LanGuard.

Nas próximas seções, nossas diretrizes irão ajudá-lo a comprovar os benefícios para si mesmo e para outras pessoas que estejam envolvidas no processo de tomada de decisão.

Tópicos nesta seção:

1.1 Visão geral do GFI LanGuard	4
1.2 Por que os clientes compram o GFI LanGuard?	5
1.3 Obtenção de uma chave de avaliação	9

# 1.1 Visão geral do GFI LanGuard

O GFI LanGuard é uma solução completa de gerenciamento de rede. Ele atua como um consultor de segurança virtual, ajudando nas seguintes áreas:

- » Gerenciamento de correções
- » Avaliação de vulnerabilidade
- » Auditoria de rede e software
- » Inventário de ativos
- » Gerenciamento de dispositivo móvel
- » Análise de risco
- » Conformidade

O GFI LanGuard verifica, analisa e ajuda a corrigir sua rede.

» Não importa se sua instalação é com ou sem agente, o GFI LanGuard verifica a rede quanto a problemas de segurança e reúne informações relevantes sobre esse aspecto. Reúne informações sobre vulnerabilidades de segurança, patches ausentes, service packs ausentes, portas abertas, compartilhamentos abertos, usuários e grupos, aplicativos instalados, smartphones e tablets usados por funcionários e inventário de hardware. GFI LanGuard integra-se a mais de 4000 apli-cativos de segurança, como antivírus, anti-spyware ou firewalls, e emite relatórios sobre o status desses aplicativos.

» Com os resultados das verificações, você pode analisar o status de sua rede. O GFI LanGuard fornece um painel avançado para o usuário navegar pelos resultados da verificação e investigá-los. Os sensores de segurança são acionados caso algum problema seja detectado. O nível de vulnerabilidade é atribuído a cada computador verificado com base nos resultados da auditoria. O GFI LanGuard também fornece relatórios e comparações de resultados.

» Após a verificação e a análise, o GFI LanGuard ajuda na correção dos problemas de segurança, automatizando o processo sempre que possível.

» Depois de criar uma verificação de linha de base, você pode identificar qualquer diferença ou alteração às configurações de segurança e do computador em todos os computadores da rede. Você pode optar por tomar ações, como implementar uma atualização de segurança ausente, seja ela da Microsoft ou não, ou uma atualização não relacionada à segurança, reverter atualizações, implementar scripts e software personalizado, desinstalar aplicativos não autorizados e abrir conexões de desktop remoto em computadores verificados. Todas essas ações o ajudarão a garantir que sua rede esteja atualizada e que as correções mais recentes tenham sido aplicadas.

# 1.2 Por que os clientes compram o GFI LanGuard?

Com base em nossa experiência, os cinco principais motivos dos clientes da GFI para comprar o GFI LanGuard são:

- 1. Para minimizar os riscos de violação de segurança ao:
- » Verificar a rede quanto a problemas de segurança e vulnerabilidade
- » Detectar e desinstalar automaticamente qualquer aplicativo não autorizado
- » Examinar dispositivos de hardware e softwares (quais computadores têm quais softwares instalados) na rede
- » Receber alertas e relatórios sobre o ambiente de segurança da rede

2. Para automatizar o gerenciamento de patch, isto é, detectar e implementar correções ausentes de sistemas Microsoft, Mac OS e Linux e de outros aplicativos de terceiros

3. Para conduzir a auditoria de rede e o monitoramento do funcionamento da rede

4. Para auxiliar na conformidade com regulamentações de segurança que exigem avaliação de vulnerabilidade regular e gerenciamento de correções (por exemplo, PCI DSS, HIPAA, SOX, GLBA e PSN CoCo)

5. Para avaliar e gerenciar a segurança de smartphones e tablets usados por funcionários para acessar as informações e aplicativos da empresa

Os tópicos a seguir fornecem cenários reais com mais informações de uso prático do GFI LanGuard:

## 1.2.1 Usar o GFI LanGuard para avaliação de vulnerabilidade

O GFI LanGuard executa mais de 50 mil verificações de vulnerabilidade em seu sistema operacional, ambientes virtuais, dispositivos de rede e aplicativos instalados usando bancos de dados de verificação de vulnerabilidade, como OVAL e os Top 20 do SANS.

Esta seção traz as diretrizes de nossa recomendação sobre como abordar as avaliações de vulnerabilidade e a correção de problemas de segurança para manter seus computadores seguros e atualizados.

» Mantenha o GFI LanGuard atualizado.

» Certifique-se de que a máquina na qual o GFI LanGuard está instalado tenha acesso à Internet. O GFI LanGuard executa verificações diariamente para obter informações atualizadas sobre vulnerabilidades e correções.

- » Se um servidor proxy for usado, ele pode ser definido em Interface do usuárioGFI LanGuard > Menu principal > Configuração> Configurações de Proxy...
- » Se o acesso à Internet não estiver disponível na máquina em que o GFI LanGuard está instalado, o produto poderá ser configurado para obter as atualizações a partir de um local alternativo. Há mais detalhes disponíveis aqui.
- » Execute auditorias de segurança regularmente.

» Novos problemas de segurança são descobertos todos os dias. A correção desses problemas exige um planejamento prospectivo e recomendamos que você tome conhecimento desses problemas de segurança o quanto antes para poder planejar uma correção eficaz.

» Recomendamos também que você configure o produto para examinar automaticamente a rede todos os dias ou semanalmente.

» Implemente antes as atualizações de segurança ausentes.

» A grande maioria dos problemas de segurança podem ser resolvidos garantindo-se que todas as correções e pacotes de serviços estejam atualizados em todas as máquinas.

» Os pacotes de serviços contêm diversas correções de segurança, portanto, recomendamos que eles sejam aplicados antes.

» Depois que os pacotes de serviços forem implementados, recomendamos que você faça uma nova verificação da rede (para ter uma visão atualizada do status das correções de sua rede).

» Após a nova verificação, implemente as correções que estiverem faltando.

» O produto pode ser configurado para implementar automaticamente as atualizações de segurança ausentes, se isso for pré-aprovado pelo administrador.

» Investigue e corrija outros problemas de segurança.

» Os resultados da avaliação de vulnerabilidade são fornecidos com descrições detalhadas dos problemas de segurança detectados e com referências a Web sites externos para que você consulte outras informações.

» O GFI LanGuard vem com ferramentas que o ajudam a tratar das vulnerabilidades desinstalando softwares não autorizados de forma remota, habilitando antivírus, antispyware e firewalls, acionando atualizações de definições para antivírus e antispyware, implementando scripts e softwares personalizados ou abrindo conexões de desktop remoto em computadores.

» Como verificar o status de segurança de sua rede

» Acesse **Dashboard > Overview** para ter uma visão geral administrativa do status de segurança da rede, inclusive dos computadores mais vulneráveis, da distribuição de vulnerabilidade e das tendências de vulnerabilidade.

» O GFI LanGuard oferece um Nível de Vulnerabilidade de Rede, que é calculado com base nos níveis individuais de vulnerabilidade de cada computador. Cada máquina possui um nível de vulnerabilidade baseado nos problemas de segurança detectados nela. Os problemas de segurança são classificados como tendo gravidade Alta, Média ou Baixa, com base no sistema de pontuação CVSS, conforme calculado pelo NVD.

» Acesse **Dashboard > History** para ver a lista de novos problemas de segurança detectados, junto com uma lista de outras alterações de configuração relacionadas à segurança na rede.

» Acesse Dashboard > Vulnerabilities para obter uma visão detalhada das vulnerabilidades detectadas na rede.

» Acesse **Dashboard > Patches** para obter uma visão detalhada do status das correções da rede.

» Acesse **Reports > Network Security Overview** para obter uma visão geral administrativa do status da segurança da rede.

» Acesse **Reports > Vulnerability Status** para obter uma visão detalhada do status da segurança da rede.

» Acesse **Reports > Remediation History** para ver o histórico dos problemas de segurança corrigidos usando o GFI LanGuard.

»

Use o relatório em **Relatórios > Auditoria de dispositivos móveis** para obter uma visão geral sobre que smartphones e tablets se conectam aos servidores Microsoft Exchange da empresa e detecte se possuem sistemas operacionais obsoletos com problemas de segurança conhecidos

» Os relatórios podem ser configurados para serem gerados regularmente.

### 1.2.2 Usar o GFI LanGuard para gerenciamento de correções

O GFI LanGuard possibilita a detecção, o download e a implementação automatizados ou sob demanda de atualizações ausentes, incluindo:

- » Aplicativos e sistemas operacionais Microsoft
- » Aplicativos e sistemas operacionais Apple OS X

» Aplicativos e sistemas operacionais Linux. As seguintes distribuições Linux são compatíveis: Red Hat Enterprise Linux, Fedora, Ubuntu, Suse, OpenSuse, CentOS e Debian

» Conhecidos aplicativos de terceiros relacionados à segurança que operam em plataformas Windows, inclusive todos os principais navegadores, produtos Adobe, tempos de execução Java, e assim por diante. Para ver uma lista completa, clique aqui.

- » Correções de segurança e não relacionadas à segurança
- » Reversão de correções

» Implementação em toda a rede de scripts e softwares personalizados (qualquer software que possa ser executado silenciosamente pode ser implementado usando o GFI LanGuard)

## 1.2.3 Usar o GFI LanGuard para controle de ativos

Dispositivos não gerenciados ou esquecidos são um risco à segurança. Use o GFI LanGuard para localizar dispositivos sobre os quais você não tem conhecimento:

- » Servidores e estações de trabalho
- » Máquinas virtuais
- » Dispositivos baseados em IP, como roteadores, impressoras, pontos de acesso, switches, etc.
- » Dispositivos móveis, como iPads, iPhones e dispositivos Android

Para obter mais informações, consulte Implementar software personalizado (página 36).

### 1.2.4 Usar o GFI LanGuard para auditoria de rede e software

O GFI LanGuard fornece uma análise detalhada do que está acontecendo em sua rede, isto é, quais aplicativos ou configurações padrão estão apresentando riscos de segurança e todas as informações que você precisa saber sobre sua rede, como:

- » Sistemas operacionais
- » Máquinas virtuais
- » Hardware e software instalados
- » Informações da CPU
- » Espaço em HD
- » Dispositivos sem fio
- » Adaptadores de rede
- » Serviços
- » Políticas de auditoria
- » Grupos e usuários
- » Compartilhamentos
- » Portas abertas TCP e UDP

» Smartphones e tablets que se conectam aos serviços da empresa, como Microsoft Exchange, Office 365, Google Apps e Apple Profiles Manager

Acesse Dashboard > Software para obter uma visão detalhada de todos os aplicativos instalados na rede.

Acesse **Dashboard > Hardware** para verificar o inventário de hardware da rede.

Acesse **Dashboard > System Information** para exibir detalhes relacionados à segurança dos sistemas presentes na rede.

Acesse **Dashboard > History** para obter uma lista de alterações relacionadas à segurança que foram realizadas na rede.

Acesse **Reports > Software Audit** para gerar um relatório completo dos aplicativos instalados na rede.

Use o relatório em **Reports > Mobile Device Audit** para obter uma visão geral sobre que smartphones e tablets se conectam aos serviços Microsoft Exchange, Office 365, Google Apps ou Apple Profiles Manager da empresa e detecte se possuem sistemas operacionais obsoletos com problemas de segurança conhecidos.

O GFI LanGuard pode ser usado para indicar, detectar e remover aplicativos não autorizados da rede.

O GFI LanGuard integra-se a mais de 4000 aplicativos de segurança essenciais dentro das seguintes categorias: antivírus, anti-spyware, firewall, anti-phishing, cliente de backup, cliente VPN, filtragem de URL, gerenciamento de patches, navegador da Web, mensagens instantâneas, P2P, criptografia de disco, prevenção contra a perda de dados e controle de acesso do dispositivo. Ele gera relatórios sobre o status desses aplicativos e corrige problemas ao permitir operações como: habilitar antivírus ou firewall, acionar atualizações de definições para antivírus ou antispyware e desinstalar aplicativos P2P.

# 1.2.5 Usar o GFI LanGuard para conformidade regulamentar

Há cada vez mais leis e regulamentações que impõem práticas específicas de segurança às empresas. Instituições governamentais, empresas que oferecem serviços financeiros e o setor de saúde estão entre os mais afetados por essas regulamentações, mas a tendência é que todas as empresas em algum momento precisem ter segurança o suficiente para proteger a privacidade e os dados de seus funcionários, clientes e parceiros. O não cumprimento dessas regulamentações pode resultar em perda de oportunidades, penalidades financeiras e jurídicas e, em casos extremos, fechamento da empresa.

Esta é uma lista dos itens de segurança mais comuns exigidos pelas regulamentações e com os quais o GFI LanGuard pode ajudá-lo:

- » Executar regularmente avaliações de vulnerabilidade
- » Manter os sistemas com todas as correções aplicadas

» Garantir que softwares antispyware e antivírus estejam instalados, atualizados e funcionando em todos os sistemas da rede

- » Garantir que um firewall pessoal esteja instalado e ativado em cada sistema da rede
- » Garantir que um software de criptografia esteja instalado em toda a rede

O GFI LanGuard pode ser combinado com outros produtos do GFI Software para formar um conjunto de produtos dedicado à conformidade:

- » GFI EventsManager<sup>®</sup> solução de gerenciamento de log
- » GFI EndPointSecurity<sup>™</sup> solução de bloqueio de dispositivo

O GFI LanGuard é fornecido pronto para o uso com um conjunto de relatórios predefinidos dedicados à conformidade com a PCI DSS, HIPAA, SOX, GLBA e PSN CoCo, dentre outras normas. Há mais detalhes sobre a PCI DSS aqui.

Esta é uma lista com algumas das normas mais importantes relacionadas à segurança da infraestrutura de TI:

» Norma de Segurança de Dados do Setor de Cartões de Pagamento (PCI DSS - Payment Card Industry Data Security Standard)

» Lei de Portabilidade e Responsabilidade de Seguro Saúde (HIPAA - Health Insurance Portability and Accountability Act)

- » Lei Sarbanes–Oxley (SOX Sarbanes–Oxley Act)
- » Lei Gramm–Leach–Bliley (GLB/GLBA Gramm–Leach–Bliley Act)
- » Lei de Gestão da Segurança de Informações Federais (FISMA Federal Information Security Management Act)
- » Lei de Privacidade e Direitos Educacionais da Família (FERPA Family Educational Rights and Privacy Act)

»

- Lei de segurança na Internet para crianças (CIPA Children's Internet Protection Act)
- » Rede do Setor Público Código de Conexão (PSN CoCo)

- » Diretriz de Proteção de Dados da União Europeia
- » Diretriz da União Europeia sobre a Privacidade e Comunicações Eletrônicas

### 1.2.6 Usar o GFI LanGuard para gerenciamento de dispositivos móveis

O GFI LanGuard consegue detectar smartphones e tablets que se conectam aos serviços da empresa, como servidores do Microsoft Exchange, Office 365, Google Apps ou Apple Profiles Manager e:

» Detalha dispositivos por usuário, fabricante, modelo do dispositivo, sistema operacional, hora da última conexão

» Executa uma avaliação de vulnerabilidade do sistema operacional do dispositivo. Compatível com Android, iOS e Windows Phone.

- » O recurso de geração de relatório sobre as atualizações do sistema operacional está disponível.
- » Envia notificações personalizadas por email aos proprietários dos dispositivos.

# 1.3 Obtenção de uma chave de avaliação

Caso você ainda não tenha baixado o GFI LanGuard, antes de começar, baixe a versão de avaliação aqui.

Para começar a avaliação do GFI LanGuard insira sua chave de avaliação gratuita. A chave de avaliação permite que você tenha acesso a todas as funcionalidades do produto, limitando-se a 25 endereços IP e 25 dispositivos móveis por um período de 30 dias. A chave é enviada para o endereço de e-mail registrado ao fazer o download do produto.

Caso você não tenha acesso ao e-mail que contém a chave, solicite uma nova chave de avaliação gratuitamente clicando aqui.

Se precisar avaliar durante um período mais longo ou com mais de 25 endereços IP e 25 dispositivos móveis, é possível submeter seu pedido aqui.

# 2 Realizar verificações de segurança

Em sistemas Windows, o GFI LanGuard pode executar verificações de segurança com e sem agente. Neste momento, somente estão disponíveis verificações sem agente para sistemas que não sejam Windows (Linux, Mac OS, dispositivos de rede, smartphones e tablets). A seguir indicamos alguns pontos a serem considerados para escolher um método de verificação:

Verificações sem agente:

- » Não há instalações nas máquinas do cliente.
- » Todo o processamento é feito pelo servidor central. Não é preciso usar recursos das máquinas do cliente.
- » Devem ser feitas em sistemas que não oferecem suporte a agentes.

Verificações com agente:

» Melhor desempenho devido à distribuição de carga entre clientes.

» Funcionam melhor em ambientes de baixa largura de banda, visto que a comunicação entre o servidor e os clientes é muito menos intensa do que no caso de verificações sem agente.

» Melhor suporte para notebooks, visto que os agentes continuam a executar a tarefa quando se está off-line. Ao ficar on-line, eles apenas sincronizam com o servidor.

» Melhor precisão nos resultados devido ao fato de que as verificações locais têm acesso a mais informações do que as verificações remotas.

Tópicos nesta seção:

2.1 Verificações de segurança sem agente	10
2.2 Auditorias com agente	14
2.3 Auditoria em smartphones e tablets	16
2.4 Perfis de verificação	17
2.5 Acionamento de verificações pelo Dashboard	18

# 2.1 Verificações de segurança sem agente

### 2.1.1 Acionamento de verificações e acompanhamento do progresso em tempo real

Acesse a guia **Scan** para acionar imediatamente verificações sem agente e acompanhe o progresso em tempo real. O destino da verificação pode ser qualquer uma das seguintes combinações:

- » Nomes de computador
- » Arquivos de texto contendo nomes de computador
- » Um único endereço IP ou intervalos de endereços IP
- » Domínio ou grupos de trabalho e unidades organizacionais

#### Nota:

O acesso administrativo às máquinas remotas é necessário para a obtenção de resultados completos da auditoria de segurança.

۰			GFI LanG	iuard					×
-	🔹 📀   🔶   🔿 🔹 Dashboard	Scan Remediate	Activity Monitor	Reports	Configuration	Utilities	۰ 🥲	Discuss this version	
Laun	ch a New Scan								
Scan	ch a New Scan Target:  Target: Target:  Target: Targ	Ptofile: Full Scan Username: root et properties ters. e following rules: Clear rule following rules:		word:	General General Computer name Computer or ra	Scan Add new rule les for custom target. omputer name is omputer file lat is ompute		V Bemove Select Import Export	
		ОК	Cancel						
Scan	ner Activity Window								*
							_		

Captura de tela 1: Verificações de segurança sem agente

## 2.1.2 Verificações agendadas

1. Para agendar verificações sem agente periodicamente, clique em **Configuration > Scheduled Scans** e selecione os tipos de destinos a serem verificados.

1				GFI LanG	uard				- D ×
💷 🔹 🧄 I 🔶 I -	Dashboard	Scan Rer	ediat	e Activity Monitor	Reports	Configuration	Utilities	100	Discuss this version
Configurations:		8 II II		•					
Agents Management     Agents Management     Scanning Profiles     Scheduled Scans     Mobile Devices		Scan Ta	get	Last Scanned	Next S	can	Profile	Remediation	n Description
Software Categorie     Applications Invent     G. Auto-Uninstal	_			New scheduled	scan			×	
Software Updates     Software Updates     Age Patch Auto-De     Software Updates     Patch Auto-De     Software Updates     Alertino Options	Step 1 of 9: Def Select the ty	1 of 9: Define target type elect the type of targets to be scanned and describe this scan.							
-B Database Mainteni	Scan type				Desc	ription		_	
General	🖲 Scan a gir	ngle computer			Scan	a single computer.			
- Consider the second s	⊖ Scan a ra	nge of computers			Choo	se the local computer ame or IP address of	r or specify the f a remote		
6	⊖ Scan a  s	t of computers			comp	uter.			
Common Tasks:	O Scan dom	ains or organizati	nalun	its					
Go to: Alerting options	Scan inh des	cription:							
Actions:									
Start scheduled scan no Edit scheduled scan's pr Delete scheduled scan									
Enable selected scans Disable selected scans									
	1 Tel me more.				< <u>B</u> ac	k Next >	Cancel	1	
		_							
									.:

Captura de tela 2: Nova verificação agendada

2. O progresso das verificações agendadas pode ser acompanhado em Activity Monitor > Security Scans:

٠				GFI LanG	Guard					- 🗆 🗙
	Dashboard	Scan	Remediate	Activity Monitor	Reports	Configuration	Utilities	6	) * Discuss th	is version
Activity Monitor:	Dray	Provi	curity Scar des visibility to the eader here to gro	<b>NS</b> requeue, progress an up by that column	d status of all s	cans.				
	D	Target		Profile	Start time		Status	Remaining time	Errors	Remediation enable
Common Tasks:		ex2013ins	5	Mobile Devices	7/17/2013 1	1:58:13 AM	completed	N/A	0 errors	No
Filter security scans Go to: Scheduled scans Befreah Actions: Stop selected scans Vew remediation details Vew scan results details	000000000000000000000000000000000000000	CRISTI 192.168.5 fictouster 192.168.9 193.17 1	7.74 sroup 2013 7 . 7.251 7.249 5 5 5 5 5 5 5 5 5 5 5 5 5	Full Scan Full Scan Full Scan Full Scan Full Scan Full Scan Mobile Devices Mobile Devices Mobile Devices Full Scan Full Scan Full Scan Full Scan	7/16/2013 3: 7/16/2013 2: 7/16/2013 2: 7/16/2013 2: 7/16/2013 2: 7/16/2013 1: 7/16/2013 1: 7/16/2013 1: 7/16/2013 1: 7/16/2013 1: 7/15/2013 2:	04:21 PM 04:01 PM 25:47 PM 19:56 PM 13:59 PM 11:01 PM 1:59:47 AM 1:51:48 AM 1:51:48 AM 1:50:37 AM 1:51:48 AM 20:25 AM 20:02 FM 20:00 PM	completed completed completed completed incompleted completed completed completed completed completed completed completed completed completed	N(A N(A N(A N(A N(A N(A N(A N(A N(A N(A	0 errors <u>3 errors</u> <u>3 errors</u> <u>3 errors</u> <u>6 errors</u> 0 errors <u>10 errors</u> <u>2 errors</u> 0 errors <u>10 errors</u> 0 errors	No No No No No No No No

Captura de tela 3: Verificações de segurança

# 2.1.3 Verificações da linha de comando

1. Para executar verificações da linha de comando, use a ferramenta **Insscmd.exe**.

Administrator: Command Prompt
C:\Program Files (x86)\GFI\LanGuard 11>lnsscmd
You didn't specify the scan target!
Usage:
<pre>Insscmd {Target&gt; [/profile=profileName] [/report=reportPath] [/reportnam e=reportName] [/output=pathToXmlFile] [/user=username /password=password] [/emai 1 [/EmailAddress=emailAddress]] [/DontShowStatus] [/UseComputerProfiles] [/Wake] [/Shutdown [/ShutdownIntervalStart=<hh:mm:ss>] [/ShutdownIntervalEnd=<hh:mm:ss> ]] [/?]</hh:mm:ss></hh:mm:ss></pre>
Lnsscmd.exe [/?] for more details.
C:\Program Files (x86)\GFI\LanGuard 11>lnsscmd localhost
STARTING SECURITY SCAN FOR MACHINE/RANGE: localhost Profile: Full Scan
[Network discovery]: Validating targets [Network discovery]: Building computers list [Network discovery]: Resolving hosts [Network discovery]: Determining computers that are alive

Captura de tela 4: Verificações da linha de comando

# 2.2 Auditorias com agente

O processo para habilitar agentes é simples. Basta definir uma lista de computadores, domínios ou unidades organizacionais nas quais os agentes precisam ser implementados e fornecer as credenciais com acesso administrativo às máquinas remotas.

O GFI LanGuard fará a operação de implementação.

O que os agentes fazem:

- » O GFI LanGuard instala automaticamente os agentes nos computadores selecionados.
- » Os agentes são instalados apenas em sistemas operacionais Microsoft Windows.

» Por padrão, os agentes executam uma verificação completa da máquina host uma vez por dia, mas é possível configurar a frequência, o tempo de verificação e o perfil de verificação.

» Os agentes precisam de cerca de 25 MB de RAM e 600 MB de espaço em disco

» Os agentes consomem a CPU apenas quando realizam uma auditoria no computador host. Isso normalmente leva alguns minutos por dia e a prioridade do processo é abaixo da faixa normal, portanto, ele não irá interferir no trabalho da máquina.

» Os agentes podem ser desinstalados diretamente do GFI LanGuard. Por padrão, os agentes serão automaticamente desinstalados se não tiverem contato com o servidor por 60 dias. O número de dias pode ser configurado.

» Os agentes do GFI LanGuard comunicam seu status para o servidor do GFI LanGuard usando a porta TCP 1070. Esse número de porta pode ser configurado.

» O GFI LanGuard pode ser configurado para descobrir redes automaticamente em domínios e unidades organizacionais e instalar agentes automaticamente em máquinas recém-detectadas.

» O GFI LanGuard também lida automaticamente com situações em que os agentes tenham sido removidos por engano ou precisem ser atualizados.

#### Importante:

Um agente pode ser chamado de Agente de Relé, que permite que as correções sejam realizadas de forma mais eficiente e usando menos largura de banda da rede para redes grandes ou com diversos locais. O Agente de Relé armazena uma cópia local dos dados da correção (normalmente armazenados no servidor do GFI LanGuard) e essa cópia é usada para corrigir computadores próximos.

#### Nota:

Para saber mais sobre os Agentes de Relé, consulte o Guia do administrador que pode ser baixado aqui.

Para habilitar agentes:

1. Clique em Configuration > Manage Agents.

۲		GFI LanG	uard		- • ×
	Dashboard Scan Remed	liate Activity Monitor	Reports Configu	uration Utilities	😢 * Discuss this version
Configurations: Agent's Management Agent's Management Configurations: Configurations Conf	ons Manage Enable agents  Manage Enable agents  GFI LanGuard is able to au information on a regular ba  Deploy Age Instate agent  Agents Se Vew and mo	Agents to automate network security ditentire networks in just few sis, making sure that you alw ents ts deployment on specified tay timos dify general agents settings, th corresponding agent status	audit and to distribute so minutes through the use sys have an up-to-date n get computers.	anning load across client machin of agents. When deployed on a etwork security status every tim	tes. computer, the apent will start collecting syste the application is opened. <u>Tell me more</u>
Version Information	Drag a column header her	e to group by that column	Public	Land out the	
Common Tasks:	Computer name	Agent status	Detais	Last results	Is relay C
Deploy Agents	CR LINSSWIN7X64	Not installed		10000037, 5037 107 2	No
Agents Settings	2 LNSSWIN2003X64	Not installed			No
	UNSSWINVISTAX86	Not installed			No
	LNSSWIN2008X64	Not installed			No
	LINSSWIDK86	Not installed			No
	LINSSWINVISTAX64	Not installed			No
	LNSSWIN2008X86	Not installed			No
	LNSSWINK64	Not installed			No
	LNSSWIN2003X86	Not installed			No
	UNSSWIN2008R2	Not installed			No
	CNSSWIN7X86	Not installed			No
	192.168.97.180	Not installed			No
	OPENSUSEX64	Not installed			No
	di CISCO	Not installed			No
	Count: 19				
	<				
	Co. Use Death and a	A Anti-the Manifester Inc.	ante activito		
	Use Lasincoard ar	e Activity matrice to view as	ena acenty.		

Captura de tela 5: Gerenciamento de agentes

# 2.2.1 Solução de problemas de erros de implementação de agentes

Para ver uma lista das possíveis causas pelas quais o GFI LanGuard apresenta falhas na implementação de agentes em determinadas máquinas, clique aqui

Para habilitar e configurar agentes, clique em **Dashboard > Overview** e selecione **Deploy agent...** na seção **Common Tasks**:

8	GFI LanGuard 2	014		- 🗆 🗙
🔲 🕶 🚷   🗲   🔿 🖉 Dashboard	Scan Remediate Activity Monitor Rep	orts Configuration	Utilities 🥹 -	Discuss this version
Image: Pilter         Image: Search	Overview Computers	rabilities Patches	Ports Software	Hardware Information
Entire Network     Locahost : CRISTI     E Local Domain : WORXGROUP	LNSSWIN2003X64 Proper	ies 🔹	x mputer Details	ą.
<ul> <li></li></ul>	Agent deployment status Agent status: Not installed Dgploy agent Disallow a	pent installation	Name IP Address MAC Address Manufacturer	LNSSWIN2003X64 A 192.168.102.174 00-15-5D-01-2F-08 (Microsoft Microsoft Corporation
	Agent activity settings There is no scan schedule defined.		) Model an Activity	Vitual Machine 🗸
UNSSWEWNESTAX64     UNSSWEWG64     WE Other computers     Mobile Devices	Change scan schedule Scanning profile: Full Scan	v		12/2013 2/12/2013 2/12/2013
	Auto remediation settings Auto remediation is: OFF Charge settings		Last Scan: 7/16/2013 11	:45:24 AM Activity
			stics ecurity Updates: 59 (54 Crit Ion-Security Updates: 17 'acks and Update Rollups:	ہ ical/High) ^ 7
Common Tasks: Manage agents		OK Cancel	aion Linnades: 9	v a
Add more computers	nuew refe		<u>_</u>	
R.M. A. BOLLES		15/2013 7/16/2013	7/16/2013	7192013 71172013

Captura de tela 6: Implementação de agentes

# 2.2.2 Acionamento de verificações com agente sob demanda

As verificações com agente normalmente são automaticamente executadas em segundo plano em máquinas remotas, de acordo com o agendamento de auditorias definido (por padrão, os agentes fazem a verificação uma vez por dia).

#### Nota:

Se você precisar atualizar as informações de segurança, pode acionar verificações com agentes sob demanda pela opção **Scan and refresh now** no **Dashboard**.

# 2.3 Auditoria em smartphones e tablets

O GFI LanGuard pode fazer auditoria a smartphones e tablets que se conectam aos serviços da empresa (como o Microsoft Exchange, o Office 365, o Google Apps ou o Apple Profiles Manager). Use este recurso para saber que dispositivos móveis são usados por seus funcionários, que problemas de segurança têm e se existe alguma atualização dos sistemas operacionais que podem corrigir esses problemas de segurança.

#### Nota:

A auditoria dos dispositivos móveis é efetuada sem agente. Os sistemas compatíveis são: Google Android, Apple iOS e Windows Phone.

Use **Configuration > Mobile Devices** para adicionar ou editar origens de gerenciamento de dispositivos móveis.

*				GFI LanG	uard 2014				- 🗆 🗙
💷 🔹 🚷 i 🗧 i 🔿 🗋	Dashboard	Scan	Remediate	Activity Monitor	Reports	Configuration	Utilities	<b>0</b> -	Discuss this version
Configurations: Agents Management Scanning Profiles Scheduled Scans Mobile Devices Software Categories Applications Inventory Auto-Uninstall Validation Software Updates Patch Auto-Deployment Patch Auto-Deployment Patch Auto-Download Patch Auto-Download Software Updates Program Updates General Updates	See 1d	GFIL	Mobile Manage mo nGuard can dete Add Mode Provide Manage Configure Add N	Devices     bile phones, tablets ar     text mobile devices while     text mobile devices while     text of the device Management     details and of the device Management     text of the device Management	id other mobili th connect to I t. Source or connecting anagement	e devices. Microsoft Exchange to a Microsoft Excha h did not connect re t Source	Server for email acces inge Server. rwrth	is. <u>Tell me n</u>	ore_
Common Tasks: Add Management Source Manage Retention Policy	Skep 1 of Con Source D Jype: Server Credentia Provide and has User ni Passwo Use	2: figure a mo betails Name: sis credentials : the log o ame: ard: per compu	bile device mana Microsoft Microsoft Geogle A Apple Pro a user which n as a service' rij der credentials w	igement source. Exchange Server Exchange Server Office 365 pops for Business offie Manager his a member of the To ght.	xchange Organ	nization Administrato	rs' domain group	Delet	e selected configurations

Captura de tela 7: Gerenciar dispositivos móveis

É possível monitorar as verificações de dispositivos móveis usando **Monitor de atividade > Verificações de segurança**. É possível visualizar os resultados de verificação dos dispositivos móveis no painel ou gerar relatórios. O relatório de auditoria de dispositivos móveis é dedicado aos resultados de verificação recuperados dos smartphones e tablets.

#### Nota:

É possível enviar notificações por email para os proprietários de dispositivos móveis para informá-los sobre a disponibilidade de atualizações de segurança para o sistema operacional de seus dispositivos.

# 2.4 Perfis de verificação

Os perfis de verificação determinam como as verificações de segurança são realizadas: quais problemas de segurança devem ser procurados e quais dados de rede serão coletados. Pronto para o uso, o GFI LanGuard vem com uma lista ampla de perfis de verificação predefinidos.

Para exibir, modificar ou criar perfis de verificação personalizados:

#### Em Configuration, selecione Scanning Profiles.



Captura de tela 8: Perfis de verificação

# 2.5 Acionamento de verificações pelo Dashboard

Uma maneira fácil de acionar auditorias de segurança é usando o **Dashboard**. Basta selecionar a lista de computadores/domínios/unidades organizacionais na árvore do **Dashboard** e clicar na opção **Scan and refresh information now** ou **Custom scan**. Ambas as opções estão disponíveis na área **Common Tasks** ou clicando com o botão direito do mouse nos computadores selecionados.

٠			GFI L	anGuard 201	4		- 🗆 🗙											
- I 🔹 🔷 i 🗲	-> Dashboard	Scan Rem	ediate Activity Mon	itor Reports	Configuration	Utilities	😢 * Discuss this version											
Filter Grou	p Search	Overview	Computers	ory Vulnerab	Ities Patches	Ports Softwar	re Hardware System											
4 💐 Entire Network	-		П (192.168.30.1)															
Localhost : CRI	Add more com	puters	L .			a Complexity Database												
Local Domain : Local Domain :	Scan	•	Refresh informati	ion now	rs	4 Computer Details	*											
END TEST	Deploy Agent		Custom scan		re Updates	Name Name	CRISTI											
UNSS1	Network discov	ery	Hedium	Service	Packs and Update	IP Address	192.168.30.1 00.50.55.00.00.08.0.00.uses											
Other compute	Assign attribute	5		Rollups		MAL Address	DECOURSE (VMWare,											
Mobile Devices (gro	Remove			Vulnera	bilities	Operating System	Windows 8 x64 (SP: Gold)											
Alcatel OT-918	Export	÷	Address 9	Mahwai	e Protection Issue	s Scan Activity	a											
Apple Phone 5	Setup as a relay	agent	Malainus Calhuran		e r retecten 1339e													
HTC Windows P	Assign a relay		Tool for Windows 8	🔒 🕑 Firewa	Issues	6												
> 👰 Samsung Galax	y Remediate		Systems - July 2013	🕢 Unauth	orized Application													
🕨 👰 Samsung Galax	Wake up comp	uter	0) • Security Update for			2												
🕨 💇 Samsung Galax	y Open Remote D	esktop	epiorer 10 for Windows	Audit S	tatus													
Samsung 19000	G Shut down com	down computer	71)	Creder	tials Setup	7/6/2013 7/8/2013 7/10	201 7/12/201 7/14/201 7/16/201 7/16/201 3 3 3 3 3 3											
Samsung 19070 Samsung 19070	G Send email noti	fication	date for Internet sh Player for	pdate for Internet ash Player for	pdate for Internet ash Player for	pdate for Internet ash Player for	pdate for Internet ash Player for	pdate for Internet ash Player for	pdate for Internet ash Player for	pdate for Internet ash Player for	pdate for Internet ash Player for	pdate for internet ash Player for	pdate for Internet ash Player for	pdate for Internet			Last Scan: 7/16/20	13 3:04:25 PM
<ul> <li>Samsung 19100</li> <li>Samsung 19300</li> </ul>	G Expand		8 for X54-based (82857645)	x X64-based V Agent Health Issues			ation Activity											
Samsung P6210	Collapse				a Resu	its Statistics												
Unmanaged mo	bil Expand all		batallad															
	Collapse all		ristalled	2	an Now	assing Security Updates: 15 (1 Assing Non-Security Lindates:	12											
	Rules Manager		un every day at 12:00:00 PM.			ervice Packs and Update Rol	lups: 1											
Common Tasks:	Properties		wed on:7/16/2013 3:13:2	2 PM	✓ ▲ F	otential Vulnerabilities: 2	v											
Manage agents	repetites	vunerability in	end Over Time				4											
Add more computers.		al Her			• •	•	• •											
Scan and refresh infor Custom scan	nation now	25 Vedum	/ <b>t</b>	/														
Set credentials		n In																
Deploy agent		7620	19 762019	71	020+3	7122013 714201	13 7/16/2013											

Captura de tela 9: Acionamento de verificações pelo Dashboard

Recurso	Descrição
Verificar e atu- alizar infor- mações agora	Esta opção aciona imediatamente uma auditoria de segurança que é executada em segundo plano nos com- putadores selecionados. Nos computadores em que o agente está instalado, a verificação será realizada pelo agente e usando o perfil de verificação definido para ele. Para computadores nos quais o agente não está disponível, uma verificação sem agente é agendada para ser executada em segundo plano usando o perfil <b>Full Scan</b> . Acesse <b>Activity</b> <b>Monitor &gt; Security Scans</b> para monitorar verificações com agente e verificações agendadas sem agente.
Verificação personalizada	Esta opção selecionará a guia <b>Scan</b> com o destino de verificação já pré-selecionado na lista de computadores que foram selecionados no <b>Dashboard</b> .

# 3 Analisar resultados da verificação

Tópicos nesta seção:

3.1 Dashboard	20
3.2 Como exibir alterações de segurança relevantes a partir de sua rede	22
3.3 Como adicionar/exibir mais dispositivos no painel	23
3.4 Como filtrar dispositivos	24
3.5 Como agrupar dispositivos	24
3.6 Como pesquisar computadores	26
3.7 Busca de texto completo	
3.8 Geração de relatórios	

# 3.1 Dashboard

O **Dashboard** reúne resultados de todas as verificações, não importa em qual perfil de verificação elas são feitas, ou se são verificações com ou sem agente. O objetivo é mostrar instantaneamente uma visão geral completa do status de segurança da rede.

O resumo administrativo mostra, dentre outras informações, os computadores mais vulneráveis, problemas de segurança proeminentes e tendências de vulnerabilidade. Os usuários também podem detalhar informações de computadores ou problemas específicos.

A árvore de computadores, à esquerda, mostra uma lista organizada de domínios e unidades organizacionais e dispositivos móveis agrupados por usuários. No lado direito, a seção do Dashboard mostra diversas exibições com informações de segurança completas com base nos dados adquiridos durante as auditorias. Dentre outras configurações, o Dashboard permite que você determine o nível atual de vulnerabilidade da rede, os computadores mais vulneráveis e o número de computadores no banco de dados.

- » Overview,
- » Computers, History,
- » Vulnerabilities,
- » Patches,
- » Ports,
- » Software,
- » Hardware,
- » System Information.



#### Captura de tela 10: Dashboard

Seção	Descrição
•	Esta seção fornece informações sobre: Filtrar os dispositivos na árvore de acordo com diversos critérios, incluindo sistemas operacionais, nível de vulnerabilidade, hora da última verificação, etc. Agrupar computadores por domínios e unidades organizacionais, sistemas operacionais ou outros atributos com definição personalizada. É possível agrupar dispositivos móveis por usuário, sistema operacional ou modelo de dispositivo. Pesquisar dispositivos por nome ou procurar os resultados de verificação que contenham palavras-chave específicas
2	<ul> <li>Esta seção fornece informações sobre como visualizar e gerenciar dispositivos verificados e protegidos pelo GFI LanGuard:</li> <li>Os servidores e as estações de trabalho estão listados no nó Toda a rede, bem como as máquinas virtuais e os dispositivos de rede com base em IP, como roteadores, interruptores, impressoras, etc.</li> <li>Os smartphones e tablets que se conectam aos servidores Microsoft Exchange da empresa para verificar emails de trabalho estão listados no nó Dispositivos móveis</li> <li>O ícone no lado direito da árvore indica o nível de vulnerabilidade ou se uma auditoria está em curso</li> <li>Os computadores com texto azul são máquinas virtuais</li> <li>Use <ctrl> + clique para selecionar vários computadores</ctrl></li> </ul>
3	Esta seção permite ao usuário acionar ações para dispositivos selecionados na árvore.
4	Esta seção permite ao usuário selecionar diferentes exibições com estatísticas ou resultados de verificação para dispositivos selecionados na árvore.
5	Esta seção permite ao usuário ver a seleção atual de dispositivos.

#### Seção Descrição

6

- Esta seção fornece informações sobre a exibição de estatísticas e detalhes de resultados de verificação para os dispositivos selecionados na árvore:
- » Os sensores de segurança indicam como muitos dispositivos são afetados por diferentes problemas de segurança
- » Clique nos sensores de segurança ou nos gráficos da área de visão geral do painel para obter dados mais específicos

# 3.2 Como exibir alterações de segurança relevantes a partir de sua rede

O GFI LanGuard notifica o usuário quando:

- » Novos dispositivos são detectados
- » Novas vulnerabilidades de segurança são detectadas
- » Aplicativos são instalados ou removidos
- » Serviços são iniciados ou interrompidos
- » Novas portas são abertas
- » Novos compartilhamentos são criados
- » Novos usuários são criados
- » Alterações no hardware são detectadas

Para verificar alterações de segurança relevantes em sua rede:

#### 1. Clique em Dashboard > History.



Captura de tela 11: Exibição de alterações de segurança em sua rede

#### Nota:

Se um destinatário de e-mail válido for configurado em **Alerting Options**, o GFI LanGuard envia, por padrão, um relatório Daily Digest com o histórico de toda a rede das últimas 24 horas.

# 3.3 Como adicionar/exibir mais dispositivos no painel

A menos que seja filtrada, a árvore do painel mostra todos os dispositivos gerenciados pelo GFI LanGuard. Isso significa que todos os dispositivos foram detectados ou totalmente verificados pelo produto.

Para exibir computadores no **Dashboard**, é preciso executar uma das seguintes operações:

1. Verificar os computadores sem agentes, clicando na guia Scan, Configuration > Scheduled Scans ou nas verificações da linha de comando.

2. Habilitar agentes nos computadores, clicando em Configuration > Agents Management.

3. No **Dashboard**, clique em **Add more computers...** na área **Common Tasks** para adicionar domínios/grupos de trabalho e unidades organizacionais inteiros ou uma lista de computadores específicos.



Captura de tela 12: Adição e exibição de computadores no Dashboard

Para efetuar uma auditoria dos smartphones e tablets, use **Configuração > Dispositivos móveis** para adicionar ou editar as origens de gerenciamento de dispositivo móvel (forneça detalhes dos servidores Microsoft Exchange).

# 3.4 Como filtrar dispositivos

Use a área de filtragem, disponível nas exibições **Painel, Corrigir** e **Relatórios** para filtrar os dispositivos mostrados na árvore no lado esquerdo da tela:



Captura de tela 13: Filtragem de computadores

# 3.5 Como agrupar dispositivos

Os computadores da árvore podem ser agrupados de acordo com critérios predefinidos, como domínios e unidades organizacionais (agrupamento padrão), sistemas operacionais, a função da rede, a distribuição de relés ou atributos personalizados definidos pelos usuários. É possível agrupar dispositivos móveis por usuário (agrupamento predefinido), sistema operacional, modelo de dispositivo e atributos personalizados.



## 3.5.1 Definição de atributos personalizados

Captura de tela 14: Definição de atributos personalizados



# 3.5.2 Exibição de computadores por atributos definidos

Captura de tela 15: Exibição de computadores por atributos definidos

# 3.6 Como pesquisar computadores

Se muitos dispositivos estiverem sendo gerenciados, pode ser difícil localizá-los na árvore. Use a área de pesquisa disponível nas exibições **Painel, Corrigir** e **Relatórios** para localizar dispositivos instantaneamente.



Captura de tela 16: Busca por computadores

# 3.7 Busca de texto completo

Acesse a área das exibições **Dashboard, Remediate** e **Reports** para localizar informações instantaneamente nos resultados da verificação com base em palavras-chave.



Captura de tela 17: Busca de texto completo

Os resultados de busca podem ser agrupados por categorias específicas. Também é possível excluir resultados encontrados em outras categorias.

# 3.8 Geração de relatórios

O GFI LanGuard oferece um amplo conjunto de relatórios administrativos, técnicos e estatísticos predefinidos. Todos eles podem ser personalizados, receber sua marca, serem agendados para gerar periodicamente e serem exportados para diversos formatos comuns, como PDF, HTML, RTF e XLS.

Além disso, o GFI LanGuard é fornecido com um amplo conjunto de relatórios dedicados à conformidade com diversas leis e normas, dentre as quais estão a PCI DSS, HIPAA, SOX, GLBA e PSN CoCo.



Captura de tela 18: Geração de relatórios

# 4 Corrigir problemas de segurança

Tópicos nesta seção:

4.1 Implementar atualizações de software ausentes	
4.2 Desinstalar aplicativos não autorizados	
4.3 Implementar software personalizado	
4.4 Enviar notificações por email para proprietários de dispositivos móveis	
4.5 Outras operações de correção	

# 4.1 Implementar atualizações de software ausentes

Para implementar atualizações de software ausentes relacionadas à segurança ou não:

#### 1. Clique em Remediate > Remediation Center > Deploy Software Updates.

2. Na árvore de computadores, à esquerda da tela, selecione os computadores ou grupos de computadores nos quais as correções precisam ser implementadas.

#### Nota:

» É possível selecionar vários itens na árvore de computadores com <CTRL> + clique.

» Para localizar os computadores com mais facilidade em grandes redes, os computadores da árvore podem ser filtrados por diversos critérios. Para obter mais informações, consulte <u>Como filtrar dispositivos</u> (página 24).

٠			G	FI LanGuard	2014			- 🗆 🗙	
💷 🔹   🔶   🔶 🛛 Da	shboard Scan	Remediate	Activity N	Ionitor Rej	ports Config	uration Utilities	🥹 - Di	iscuss this version	
	S 🖉 N	Aultiple se	election - 2	computer	s				
Y 👼 C		Remediation	Cantas 🛤		2.4.				
Filter Group Sear	rdh 🔤 🗫 '	Remediation	Center	Remediation	Jobs				
Sentre Network     Cristin     Cocahost : CRISTI     Deploy Software Updates     Use this option to deploy missing software updates detected on your network.     Use this option to deploy missing software updates detected on your network.     List of missing updates for current selection (Multiple selection - 2 computers)									
CRISTI						Find Clea	ar	<u>^</u>	
UNSSWIN7X64				_				1	
		😸 🗅 E	Suletin	Severity 🔤	Date posted ∇	Tide			
		🛛 🔄 Secur	ity Update (1	29)					
DANR			VP5813-17	Critical	2013-07-09	Adobe Flash Player 11.8.800.	.94 msi for Firefox,	Safari, Opera	
INUX-TEST			PS813-17	Critical	2013-07-09	Adobe Flash Player 11.8.800.	.94 exe		
CENTO563			₽5813-18	Critical	2013-07-09	Adobe Shockwave Player 12.0	0.3.133 msi		
CPENSUSEX64			6513-056	Critical	2013-07-09	Security Update for Windows	XP (KB2845187)	A for 111 of 110 A	
C UBUNTU 1004			013-055	Critical	2013-07-09	Cumulative Security Update to	or Internet Explorer	a for Windows XP (KE	
A PUNSS1			613-057	Critical	2013-07-09	Security Update for Windows	Media Format Runs	me 9.5 for Windows X	
ar LNSSWIN2003X64			1010-009	Critical	2013-07-09	Security update for Windows	XP (KB2834886)		
LINSSWIN2003X86			1010-0010-0	Critical	2013-07-09	security opdate for windows	AP (602050051)		
S LNSSWIN2008R2			WEA-2013-0	Critical	2013-06-25	frafox-17.0.7-1.60_4.x00	2_04		
S LNSSWIN2008X64			HEA.2013-0	Moderate	2013-06-25	ord.7 10 7.37 el6 4 v96 64			
S LNSSWIN2008X86		A A A A	HSA-2013-0	Moderate	2013-06-25	lbox1-7.19.7-37.66 4 v96 4			
UNSSWINVISTAX64			Brd 17.0.7	Critical	2013-06-25	Mozila Thunderbird 17.0.7			
AL UNSSWINK64	<b>—</b> .		irefox 22.0	Critical	2013-06-25	Mozila Firefox 22.0			
Common Tanlari	×		4513-048	Important	2013-06-18	Security Update for Windows	XP (KB2839229)		
Common Tasks:	Ť	0 0 0 0 0	PS813-16	Critical	2013-06-11	Adobe Air 3.7.0.2090	( ( ( ( ( ( ( ( ( ( ( ( ( ( ( ( ( ( (		
Manage agents		0	Count=522						
Add more computers		(						>	
Scan and refresh information now Custom scan						Total extends 107 cm		Remadute	
Set credentials Deploy agent						rotal selected: 137 soft	ware updates	2. Dementare	

Captura de tela 19: Implementar atualizações de software

Na tela **Deploy Software Updates** é possível ver todas as atualizações ausentes para os computadores selecionados com os detalhes de qual computador cada atualização deve ser implementada. É possível ajustar a implementação marcando ou desmarcando correções ou computadores.

🛷 GFI LanGuard 20	014 _ 🗆 🗙
💼 💿 🔷 I 🗲 I 🔿 🛛 Dashboard Scan Remediate Activity Monitor Repor	ts Configuration Utilities 😢 🕲 Discuss this version
Y See Computers	Remediation options
Filter Group Search 😪 Remediation Center 🌄 Remediation Jo	Before Deployment After Deployment Advanced
Entre Network Deploy Software Updates	Reboot/shut down options:
Local Domain : WORKGROUP	plates detected of Babort the tarret computers
A 192.168.97.180	tion (Multiple Stut down the target computers
Deploy software updates	Reboot/shut down schedule:
	Immediately after deployment
Market Compared Antiperson Antipe	osted V Tit O & the rest occurrence of 2.29.34 PM Q
	on Sunday, Mon V
Deploy immediately     Deploy immediately     Deploy immediately	7-09 Ad When between 2:29:34 PM 0 and 2:29:34 PM 0
	7-09 Ad on Sunday, Mon V
Credentials: Qustomize	7-09 Se Let the user decide Preview
- currently logged on user	7-09 Cu
- use per computer credentials when available	7-09 Se Show notification before thut down for 5 0 minutes with message:
Before deployment options: Qustomize	7-09 Se
- wam user before deployment (show a message)	6-25 xu
<ul> <li>copy software to deploy to target computers via administrative share</li> </ul>	6-25 fre 🗸
After deployment options: Quatomize	Delete copied files from remote computers after deployment
- do not reboot/shut down the computers	6-25 Mc Run a patch verification scan after deployment
delete copied files from remote computers after deployment	6-25 Mc
	6-18 Se Hemember settings OK Cancel
Advanced options OK Cancel	Total selected: 137 software updates
Deploy agent	

Captura de tela 20: Opções de correção

Para iniciar a operação de implementação:

- 1. Em Remediate, selecione Remediation Jobs.
- 2. No assistente **Deployment software options** configure o agendamento da implementação.
- 3. No assistente **Remediation options** selecione as opções de reinicialização e clique em **OK**



Captura de tela 21: Nova verificação das máquinas

4. Faça uma nova verificação nas máquinas para ver o status de segurança após a implementação.

#### Nota:

» Se muitas atualizações forem implementadas, a máquina de destino precisará ser reiniciada para que a implementação seja concluída.

» Se aparecer uma atualização ausente mesmo depois da operação de implementação, certifique-se de que a máquina tenha sido reinicializada.

#### Nota:

O GFI LanGuard pode ser configurado para implementar atualizações ausentes de forma automática. Para obter mais informações, consulte <u>Automatizar operações de correção</u> (página 44).

# 4.2 Desinstalar aplicativos não autorizados

Execute uma auditoria completa ou uma auditoria de software na rede par obter um inventário dos aplicativos instalados. Para obter mais informações, consulte <u>Realizar verificações de segurança</u> (página 10).

#### Nota:

É possível adicionar aplicativos não autorizados mesmo que eles não tenham sido detectados como instalados na rede. Para isso, basta usar o botão "**Add…**".

Para indicar aplicativos não autorizados:

1. Clique em **Configuration > Applications Inventory.** 

*		GFI LanG	Guard 2014				- 🗆 🗙	
💷 🔹 i ሩ i 🔿 🛛 Dashboard	Scan Remediate	Activity Monitor	Reports	Configuration	Utilities	🥴 - 🛛	Discuss this version	
Configurations:     Agents Management     Scheduled Scans     Scheduled Scans     Scheduled Scans     Scheduled Scans     Scheduled Scans     Scheduled Scans     Schware Categories     Schware Categories     Schware Updates     Schware Updat	Scan Remediate Applic Use this lis Drag a column header Drag a column header Application name SOFREE MP26 + Fie2lia Client 3: Fie2lia Clie	Yourd 2014						
Add a new application Go to . Applications auto-uninstall Actions: Configure selected application Remove selected application	Fast Reader Fast Reader Fast Reader Fast Reader Fost Reader POFCreator POFCreator POFCreator POFCreator Count=6490	n pplication for auto-unin	(9) <u>Tel ny</u> 8	a more	lation node.	<u>844</u>	< Back Njext >	Cancel

Captura de tela 22: Indicação de aplicativos não autorizados

2. Acesse **Configuration > Auto-Uninstall Validation** para testar se o GFI LanGuard consegue desinstalar com sucesso um aplicativo não autorizado de forma silenciosa.

#### Nota:

Alguns aplicativos não oferecem suporte à desinstalação silenciosa e não podem ser removidos pelo GFI LanGuard porque o processo de instalação mostrará caixas de diálogo aos usuários das máquinas de destino, esperando que eles tomem ações e interferindo em seus trabalhos.

٠					GFI Li	anGuard 2014				×
- E • - 🏠	←	-> Dashboard	Scan	Remediate	Activity Monit	tor Reports	Configuration	Utilities	100-	Discuss this version
Configurations: Agents Management Scanning Profiles Scheduled Scans Mobile Devices Software Categories Auto-Uninstall Validation Software Categories Patch Auto-Deployment Patch Auto-Deployment Patch Auto-Download Meeting Options Auto-Uninstall Validation Software Lipdates Validation status Meeting Options Auto-Download Meeting Options Auto-Download Meeting Options Auto-Download Meeting Options Auto-Download Meeting Options Auto-Download Meeting Options Auto-Download Meeting Options Auto-Download Meeting Options Auto-Download						Version 9.20.00.0	Publisher Egor Pavlov	by GFI LanGuard.		
e Welcom	e to ti	Aut e 'Auto-uninstall v	validatik	stall validatio	n wizard		×			
Ci Valida This w	te by un rizard wil	instaling <b>7-Zip 9.20 (</b> xi Il guide you through the v	64 editio	<ul> <li>n) from a test ma process. The appl</li> </ul>	achine! Ication validation p	process has 4 step	81			
), Step Step	1: 2:	Select validation target Specify remote logon or	edentials							
Step	3:	Launch validation								
NOTE	<b>4</b> : :	Venty validation results The test machine needs a Remote Desktop Com the uninstall requires us	to be che nection if t ler input.	cked directly or ti he validation fails	trough and			Lated unaut	horized applicatio	Validate
🕑 Tel me	more					Next >	Cancel	Applications	Inventory node.	
								-		.1

Captura de tela 23: Validação da desinstalação automática de aplicativo

3. Faça uma nova verificação da rede para detectar todos os aplicativos não autorizados.

4. Acesse **Remediate > Remediation Center > Uninstall Applications** para remover aplicativos não autorizados de sua rede.

8		GFI LanG	uard 2014					×
💷 📀   🗲   🔿 🛛 Dashboard	Scan Remediate	Activity Monitor	Reports	Configuration	Utilities	۰ (9	Discuss this version	
9 🌆 🔿	CRISTI (19)	2.168.30.1)						
Filter Group Search	Nemediation	Center 🍢 Remedi	ation Jobs					
	ſ							
A St Entre Network	Uninsta	II Applications	detected on net	work			-	0
A 💽 Local Domain : WORKGROUP	Chinistan u	autorized appreasors	devected on net	MUTR.				
🗢 192. 168. 97. 180 🔳	List of installs	d applications for (	current selec	tion (CRISTL)	192 168 30 10			
192.168.97.251	Cist of mistaire	a applications for t	current serec	aon (chiori (	132.100.30.10			n
CRISTI	I				Find Clear			
CISSWER7/64		alization come	A Manalan	D. blob us	University	abies	1 hours	
		pication name	4 Version 9, 20, 00, 0	Publisher	Uninstal	string	locestar	
K UNSSWID0386			512510010	- igor i onor	- Aller and a second seco	eve Idaec		1.11
🕨 🔮 DANR 🗧								
A T LINUX-TEST								
CENTOS63								
4 🗣 UNSS1 📲								
2 LNSSWIN2003X64								
🥂 LNSSWIN2003X86 🛛 🖉								
Sunsswin20088.2								
S LNSSWIN2008X64								
O LNSSWINVISTAX64								
CIESSWI70064								
Common Tasks: ¥								
Manage agents								
Add more computers	CC	unt=1						
Scan and refresh information now Custom scan							0	
Set credentials					Total selected: 1 ap	plication	Minstal	
Deploy agent								

Captura de tela 24: Desinstalar aplicativos

5. Faça uma nova verificação nas máquinas para ver o status de segurança após a desinstalação.

#### Nota:

O GFI LanGuard pode ser configurado para detectar e remover qualquer aplicativo não autorizado de sua rede. Para obter mais informações, consulte <u>Automatizar operações de correção</u> (página 44).

# 4.3 Implementar software personalizado

O GFI LanGuard pode implementar scripts e softwares personalizados em toda a rede. Praticamente qualquer software que possa ser executado em silêncio pode ser implementado pelo GFI LanGuard.

Para implementar scripts e softwares personalizados em sua rede:

#### 1. Clique em Remediate > Remediation Center > Deploy Custom Software.

2. Na árvore de computadores, à esquerda da tela, selecione os computadores ou grupos de computadores nos quais as correções precisam ser implementadas.

#### Nota:

Os softwares personalizados precisam ser especificados manualmente, junto com os parâmetros de instalação silenciosa e arquivos de configuração, se necessário.

٠				GFI Lan	Guard 2014	•			- 🗆 🗙
	<b>≥   ←   →</b> ]	Dashboard	Scan Remedia	te Activity Monitor	Reports	Configuration	Utilities	🥴 * Discur	is this version
9	8. s	Q	CRISTI (1	92.168.30.1)					
Filter	Group	Search	Nemediatio	n Center 🍢 Remed	liation Jobs				
<ul> <li>✓ Sentire Ne</li> <li>Sentire Ne</li> <li>Sentire Ne</li> <li>Local</li> <li>✓ Sentire Ne</li> <li>Local</li> <li>✓ Sentire Ne</li> </ul>	etwork host : CRISTI   Domain : WORKGRC 92. 168.97. 180	oue 📲	Deplo Use this Specify the	option to deploy third part software to be deploy	are ty scripts and a oyed for cu	applications.			۲
		Add	custom software		× <				j êdd
5	General								<u>E</u> dt
2	Specify th	he location of the	file to deploy on the tar	get machines;					Remove
4									jmport
> 🔮 D	Deploy the file at	location:							Egport
Common	Auxiliary (fe Auxiliary files configuration With the following No parameter Parameters n Cugtom Notes: N	are deployed, but files for non-auxil g parameters: rs required comaily used for w comaily used for in Mapped network d	i not executed. They ar any files. indows patches itemet Explorer patche	e usually used as	1				
Manage Add.mon Scan.an Custom.s		when targeting file: \aerver\ahare\file	s on network shares (e. todeploy.bat).	g.	E				
Set cred Deploy a				Add Cancel				iii	Deploy

Captura de tela 25: Implementar software personalizado

# 4.4 Enviar notificações por email para proprietários de dispositivos móveis

Os administradores de TI podem usar o GFI LanGuard para enviar notificações de email personalizadas aos proprietários de smartphones e tablets que se conectam aos serviços da empresa, como o Microsoft Exchange, o Office 365, o Google Apps ou o Apple Profiles Manager. É possível usar um modelo de email predefinido para notificar os proprietários dos dispositivos sobre as últimas atualizações do sistema operacional instalado em seus dispositivos.

Clique com o botão direito em um dispositivo móvel ou um grupo de dispositivos móveis na árvore do Painel e selecione a opção **Enviar notificação por email** para enviar mensagens de email aos proprietários dos dispositivos móveis.



Captura de tela 26: Enviar notificações por email

# 4.5 Outras operações de correção

Para ver todas as operações de correção disponíveis no GFI LanGuard:

#### 1. Em Remediate, selecione Remediation Center.

O GFI LanGuard possibilita operações de correção, como:

» Reverter correções – esta opção é muito importante quando são instaladas atualizações de segurança que interferem em seu ambiente.

- » Acionar atualizações de definições de softwares antivírus e antispyware.
- » Acionar verificações de antivírus e antispyware nas máquinas remotas.
- » Habilitar proteção em tempo real para soluções de antivírus e antispyware.
- » Ativar firewalls.

» Abrir uma conexão de desktop remoto nas máquinas de destino para solucionar rapidamente problemas de segurança que não podem ser automaticamente corrigidos.

۰	GFI LanGuard 2014 -	- 🗆 🗙
💶 🔹 l 🔶 🛛 🔿 🖉 Dashboard	Scan Remediate Activity Monitor Reports Configuration Utilities 😢 * Discuss this ver	sion
💡 🛃 🔍	Entire Network - 19 computers	
Filter Group Search	Remediation Center 🌄 Remediation Jobs	
Se Entre Network     Entre Network     Localhost : CRISTI     ELocal Domain : WORKGROUP	Deploy Software Updates           Use this option to deploy missing updates detected on selected computers.	۲
→ 😰 DANR 📲 → 😰 LINUX-TEST 📲	Use this option to uninstall software updates currently deployed on network.	۲
Other computers      Mobile Devices (grouped by Operating System      Mobile Devi	Use this option to deploy third party scripts and applications.	۲
Android 2.2.1      Android 2.2.6      Android 4.0.3      Android 4.0.4	Uninstall Applications Uninstall unauthorized applications detected on network.	۲
Android 4.1.1	Use this option to fix problems identified with malware protection software in your network.	۲
	Remote Support via Remote Desktop Connection Use this option to remotely connect to specific targets for maintenance purposes.	۲
Common Tasks: ¥		
Manage agents Add.more.computers		
Scan and refresh information now Custom scan		
Set credentials Deploy agent		
		.4

Captura de tela 27: Outras operações de correção

# 5 Automatizar tarefas

Tópicos nesta seção:

5.1 Descobrir automaticamente novos dispositivos na rede	40
5.2 Automatizar auditorias de segurança	41
5.3 Automatizar download de correções	43
5.4 Automatizar operações de correção	
5.5 Automatizar geração de relatórios	49

# 5.1 Descobrir automaticamente novos dispositivos na rede

#### Nota:

» Todas as tarefas importantes do GFI LanGuard podem ser configuradas para serem executadas automatica e periodicamente.

» Para monitorar novos dispositivos ativos na rede, agende uma verificação para ser executada regularmente no perfil Network Discovery.

Para detectar automaticamente quando novos computadores são adicionados a determinado domínio ou unidade organizacional:

1. No **Dashboard**, clique com o botão direito do mouse no domínio ou unidade organizacional na árvore de computadores e selecione **Network Discovery**...

Image: Status       Dashbadid       Scan       Remediate       Activity Monitor       Reports       Configuration       Utilities       Image: Status       Image: St	8		GFI LanGuard 2014	X
Where Oracional Overview Oracional Overview Oracional Overview O	💼 🔹 😓 🖌 🔶 Dashboard	Scan Remediate	Activity Monitor Reports Configuration Utilities	Ø * Discuss this version
Briter Hetwork     Common Tasks:     Render Jackson org     Second Lagers     S	Filter Group Search	Overview Compu	ers History Winerabilities Patches Pots :	Software Hardware
Leokoy sperk	Section Tasks:     Section	WORKGRO Application Category finity is cations (152 ofized applicat is (1) ware (1) of (2) of (2) ware (1) of (2) of	WORKGROUP Properties	X       No. of computers       3       1

Captura de tela 28: Detectar dispositivos

2. Em **Dashboard**, selecione **History** para investigar quais novos dispositivos foram detectados na rede e quando eles foram vistos pela primeira vez.

#### Nota:

Os novos dispositivos móveis são automaticamente detectados regularmente assim que a origem de gerenciamento de dispositivo móvel for definida. Para mais informações, consulte a seção Auditoria de smartphones e tablets.

# 5.2 Automatizar auditorias de segurança

As auditorias de segurança podem ser automatizadas de duas formas:

1. Definindo verificações agendadas sem agente para serem executadas em segundo plano periodicamente.

2. Implementando agentes nas máquinas de destino. Por padrão, os agentes fazem a auditoria da máquina host uma vez por dia, mas o agendamento das auditorias pode ser personalizado.

# 5.2.1 Personalizar agendamento de auditoria ao implementar agentes

<b>v</b>	GFI LanGuard 2014		- 🗆 💌
💷 🔹 i 🗧 i 🔿 🛛 Dashboard	Scan Remediate Activity Monitor Reports	Configuration Utilitie	es 😢 * Discuss this version
Configurations: Accurate Management Scheduled Scans Mobile Devices Mobile Devices Acto-United Waldation Software Utgotates Software Utgotates Configuration Software Utgotates Software Utgotates Software Utgotates Acto-United Deviced Software Utgotates Database Martenance Options	Manage Agents Enable agents to automate network security audi GFI LanGuard is able to audit entire networks in just few mir collecting system information on a regular basis, making sur collecting system information o	and to distribute scanning I des through the use of ager that you always have an up mputers.	Ioad across client machines. nts. When deployed on a computer, the agent will start hor-date network security status every time the application is Manage Agents: Advanced Settings
Step 1 of 3: Define target Select the agent deployment target.	A		How often the agent will audit the host computer to refresh security information:
Computers Select target comput Credentails © Local domain Pinish © Cystom: Add new rule	na: Cear rule 1	-	Run the audit every day at 1200 PM. Becumence pattern: daily v at; 120000 PM (2) Daly recumence pattern Bivery 1 (2) days Every meekday
Advanced Settings (Detong)	< Back Next > Ca	cel	Scan profile Aggrts scan using the profile: Full Scan V

Captura de tela 29: Personalizar agendamento de auditoria - Implementar agentes



## 5.2.2 Personalizar o agendamento de auditorias para agentes pelo Dashboard

Captura de tela 30: Personalizar o agendamento de auditorias - Pelo Dashboard

# 5.3 Automatizar download de correções

Use **Configuration > Patch Auto-Download** para configurar o produto para baixar atualizações automaticamente de forma a estarem disponíveis no arranque da operação. As opções disponíveis são:

- » Auto-download all patches
- » Auto-download only patches detected as missing by GFI LanGuard
- » Auto-download patches for specific vendors, products or languages.



Captura de tela 31: Automatizar download de correções

# 5.4 Automatizar operações de correção

O GFI LanGuard pode ser configurado para corrigir automaticamente determinados problemas de segurança, por exemplo, a implementação de atualizações e a desinstalação de aplicativos não autorizados, visto que eles são detectados por verificações com agente e verificações agendadas sem agente.

#### Nota:

Antes de continuar, defina aplicativos não autorizados e aprove atualizações de segurança para a implementação automática.

Para aprovar atualizações de segurança:

- 1. Em Configuration, selecione Patch Auto-Deployment.
- 2. Selecione as correções na lista.

4) ()		GFI Lan	Guard 20	)14					
💷 🔹 🗧 🔶 Dashboard	Scan Remediate Activity	Monitor	Repor	ts Configurati	ion Utilities	۷	* Discuss this version		
Configurations:	Patch Auto-Deployment     The Patches Auto-Deployment option enables you to select which patches are approved for automatic patch deployment.     Manual Approval     Select which patches are approved for automatic deployment.								
Patch Auto-Deployment     Patch Auto-Download	Group by: Vendor	× 1				Find	Clear Options		
-S Alerting Options -B Database Maintenance Options	Al Matches		Drag a co	umn header here ti	o group by that col	umn	la la la		
E- Contral	E-N Apple		D App	roval	Bulletin ID	Date posted	♥ Title		
- Version Information	E-W AudacityTeam.org		0 -	to configure	Not Available	2013-08-13	Update for Root Certific		
🗆 🐞 Licensing	Box, Inc.		0 a	to configure	Not Available	2013-08-13	Update for Root Certific		
Common Tarka:	E-19 Canneverbeltd.		0 Cc	to configure	Not Available	2013-08-13	Update for Root Certific		
Common Tasks:	E-W Canonical Inc.		0 Co	to configure	Not Available	2013-08-13	Update for Root Certific		
Options	E-D CoveFTP		0 a	to configure	Not Available	2013-08-13	Update for Root Certific		
	E-10 Decho Corporation		0 Co	to configure	Not Available	2013-08-13	Update for Root Certific		
Actions:	E-W Don Ho		0 a	to configure	Not Available	2013-08-13	Update for Root Certific		
Annous selected patches	0-10 dotPDN LLC		0 Co	to configure	Not Available	2013-08-13	Update for Root Certific		
Disapprove selected patches	B- V Foxt Corporation		0 Co	to configure	Not Available	2013-08-13	Windows Malicious Soft		
Clear approval configuration	B-Q Google Inc.		0 Co	to configure	Not Available	2013-08-13	Windows Malicious Soft		
Show Bulletin Info	E-W Igor Pavlov		0 Co	to configure	Not Available	2013-08-13	Windows Malicious Soft		
	E-W IngBum		O Co	to configure	Not Available	2013-08-13	Windows Malicious Soft		
	Malwarehotas Como	ration	0 Co	to configure	Not Available	2013-08-13	Windows Malicious Soft		
	B-Q Matin Priced	0.001	O Co	to configure	Not Available	2013-08-13	Update for Windows XP		
	B-10 Microsoft		0 Co	to configure	Not Available	2013-08-13	Update for Windows XP		
	🗊 🛺 Mozila		0 Co	to configure	Not Available	2013-08-13	Update for Windows Vis		
	- Nulsoft, Inc.		A	to confirm	Mat Auslishia	2012/08/12	Lindaka fine Mindauna Me		
	E-Q Open Source		Cou	nt: 14362			¥		
	ELLIS coop SLISE	×	<				15		

Captura de tela 32: Aprovação de atualizações de segurança

Para habilitar a autocorreção em uma nova verificação agendada sem agente:

1. Em Configuration > Scheduled scans > Common tasks, selecione New scheduled scan.

2. Selecione as opções de configuração de autocorreção no assistente e clique em Finish.



Captura de tela 33: Habilitação de autocorreção em novas verificações de segurança sem agente

Para habilitar a autocorreção em uma verificação agendada sem agente existente:

1. Em **Configuration > Scheduled scans**, selecione o destino da verificação.

2. Clique com o botão direito do mouse no destino selecionado e clique em **Properties**. Isso abre a caixa de diálogo **Pro-perties**.

3. Na guia Auto Remediation, selecione as opções na área After scan completes e clique em OK.

*		GFI LanG	uard 2014		- D ×
💶 🔹 🗧 🔶 🕹 Dashboard	Scan Remediat	e Activity Monitor	Reports Configuration	Utilities	1 Discuss this version
Configurations:	🐮 🛣 🚳	0			
Agents Management	<ul> <li>/ Scan Target</li> </ul>	Last Scanned	Next Scan	Profile	Remediation Description
Scheduled Scans	- localhost	8/20/2013 9:19:47 P	New 9:04 PM	Full Scan	No
localhost Prop	erties	× 4	Disable		
General Logon Credentials Power Saving Au	uto Remediation Repo	rting	Scan Now		
Auto-Remediation enables GFI LanGua install missing updates, service packs a unauthorized applications on the scan	ard to automatically dow and update rollups, and ned computers.	nload and uninstal	Delete Properties		
After eran completer:					
Qownload and deploy missing updates					
Download and deploy missing service pac	dis and update rollups				
Quinstal unauthorized applications					
Configure auto-remediation options	tal				
There are security updates that are no	t approved for auto-de	ployment.			
OK	Cancel	Apply			

Captura de tela 34: Habilitação de autocorreção em verificações de segurança sem agente existentes

Para habilitar a autocorreção para agentes na implementação:

- 1. Em Configuration > Agents Management, selecione Deploy agents.
- 2. No assistente **Deploy Agents**, selecione **Advanced Settings**.

3. Clique na guia Auto Remediation, selecione as opções da área After scan completes e clique em OK

<del>ب</del>			GFI LanG	uard 2014			- D ×
- <b>⊡</b> •	-> Dashboard	Scan Remediate	Activity Monitor	Reports	Configuration	Utilities	🕖 * Discuss this version
Configurations: Account in Manager Scanning Parlies Mobile Devices Account in Manager Account in Mana	s ory Validation ployment writoad ance Options	GFI LanGuardia abi collecting system int copened. I cil me mor intere intere Ver a Deploy Agents	age Agents pents to automate networks or to autile entire networks commation on a regular ber immation on a regular ber weather the weather the second secon	k security aud i in just few mi is, making su pecified target ( i settings.	it and to distributes inutes through the u re that you always h computers.	scanning los se of agents save an up-9	ad across client machines. a. When deployed on a computer, the agent will start to-date network security status every time the application is Manage Agents: Advanced Settings
Step 1 of 3: Define ta Select the agent dep	rget koyment target.			1			Auto-Remediation enables GFI LanGuard to automatically download and install missing updates, service packs and update rollups, and uninstall unauthorized applications on the scanned computers.
Computers Credentials Pinah	Select target compute Local domain Cystom: Add new rule	a:		GearnJe	ld.		After scan completes: Download and deploy missing updates Download and deploy missing service packs and update rolups Uninstal unsubnoteed applications Configure auto-remediation options the target computers.
Advanced Settings Date			< Back	· C	POL		Remediation actions are conducted from the GFI LanQuard console computer where the updates are downloaded and distributed to remediation fargets.     There are updates that are not approved for auto-deployment.     OK Cancel

Captura de tela 35: Habilitação da autocorreção para agentes durante a implementação

Para habilitar a autocorreção para auditorias com agente pelo Dashboard:

1. No Dashboard, clique com o botão direito em um agente e clique em Properties.

2. Na caixa de diálogo **Properties**, selecione a guia **Agent Status**.

3. Clique em **Change settings** e selecione as opções na área **After receiving scan results from the agent**. Clique em **OK**.



Captura de tela 36: Habilitação da autocorreção pelo Dashboard

# 5.5 Automatizar geração de relatórios

Todos os relatórios do GFI LanGuard podem ser agendados para serem gerados periodicamente e para serem salvos automaticamente no disco em um local especificado ou enviados para um destinatário de e-mail.



Captura de tela 37: Automatização da geração de relatórios

# 6 Glossário

#### A

#### Access™

Sistema de gerenciamento de banco de dados relacional da Microsoft® incluso no pacote Microsoft® Office. O Access™ costuma ser usado para pequenos bancos de dados.

#### Active Directory™ (AD)

Tecnologia que proporciona diversos serviços de rede, incluindo serviços do diretório similar a LDAP.

#### Agente de patch

Serviço de segundo plano que lida com a implantação de patches, service packs e atualizações de software nos computadores de destino.

#### Antispyware

Medida defensiva de software que detecta spyware instalado em um computador sem o consentimento do usuário.

#### Antivírus

Medida defensiva de software que detecta malware instalado em um computador sem o consentimento do usuário.

#### Arquivo de lote

Arquivo de texto contendo uma compilação de instruções a serem realizadas pelo sistema operacional ou aplicativo.

#### В

#### Banco de dados do Microsoft® Access™

Sistema de gerenciamento de banco de dados relacional da Microsoft® incluso no pacote Microsoft® Office. O Microsoft® Access™ costuma ser usado para pequenos bancos de dados.

#### Bluetooth

Protocolo de interface e comunicação sem fio que habilita a troca de dados entre dispositivos.

#### С

#### Cavalos de Troia

Tipo de malware que contém um aplicativo oculto que danifica o computador.

#### Correção automática

Tecnologia GFI LanGuard que baixa automaticamente patches ausentes. Se um aplicativo está na lista de exclusão do GFI LanGuard, a correção automática o desinstalará do computador de destino durante as operações agendadas.

#### D

#### deploycmd.exe

Ferramenta de linha de comando do GFI LanGuard usada para implantar patches da Microsoft® e software de terceiros nos computadores de destino.

#### Depurador de script

Módulo do GFI LanGuard que permite escrever e depurar scripts personalizados usando uma linguagem compatível com VBScript.

#### DMZ

Seção da rede que não é parte da rede interna, mas não é diretamente uma parte da Internet. Normalmente serve como gateway entre as redes internas e a Internet.

#### DNS

Banco de dados usado pelas redes TCP/IP que habilita a tradução dos nomes do host em números IP e o fornecimento de outras informações relacionadas ao domínio.

#### Download automático

Tecnologia GFI LanGuard que baixa automaticamente os service packs e patches ausentes em todos os 38 idiomas.

#### F

#### Ferramenta de auditoria do SQL Server

Ferramenta usada para testar a vulnerabilidade da senha da conta "sa" (ou seja, do administrador raiz) e das outras contas de usuário do SQL configuradas no SQL Server<sup>®</sup>.

#### Ferramenta de auditoria SNMP

Ferramenta que relata cadeias da comunidade SNMP frágeis fazendo um ataque de dicionário que usa os valores armazenados em seu dicionário padrão.

#### Ferramenta de pesquisa DNS

Utilitário que converte o nome de domínio do endereço IP correspondente e recupera informações particulares do domínio de destino.

#### Ferramenta de rota de rastreamento

Ferramenta usada para identificar o caminho que o GFI LanGuard seguiu para chegar ao computador de destino.

#### Ferramenta para enumerar computadores

Utilitário que identifica domínios e grupos de trabalho de uma rede.

#### Ferramenta para enumerar usuários

Ferramenta que permite que você recupere usuários e informações de usuário do seu domínio/grupo de trabalho.

#### Ferramenta SNMP Walk

Ferramenta para examinar os nós da sua rede e recuperar informações SNMP.

#### Ferramenta Whois

Uma ferramenta que permite que você pesquise informações sobre determinado domínio ou endereço IP.

#### FTP

Protocolo usado para transferir arquivos entre computadores da rede.

### G

#### Gerenciamento automático de patch

Tecnologia GFI LanGuard que baixa automaticamente as atualizações Microsoft<sup>®</sup> ausentes e implanta-as pela rede.

#### GFI EndPointSecurity

Solução de segurança desenvolvida pela GFI que ajuda as organizações a manterem a integridade de dados prevenindo o acesso e transferência não autorizados de dispositivos removíveis.

#### GPO

Sistema centralizado de gerenciamento e configuração do Active Directory que controla o que os usuários podem ou não fazer em uma rede de computadores.

#### Н

#### Host local

Na rede, o host local é o computador que você usa atualmente. É possível consultar o host local usando o endereço IP reservado 127.0.0.1. Neste manual, o host local é a máquina onde o GFI LanGuard está instalado.

#### L

#### ICMP pings

O Protocolo ICMP é um dos principais protocolos da suíte de protocolo de Internet. É usado por sistemas operacionais de computadores em rede para enviar mensagens de erro indicando, por exemplo, que o serviço solicitado não está disponível ou que não é possível alcançar o host ou roteador. O ICMP também pode ser usado para retransmitir mensagens de consultas.

#### impex.exe

Ferramenta de linha de comando usada para importar e exportar perfis e vulnerabilidades do GFI LanGuard.

#### Informações do boletim

Contém uma compilação de Informações sobre um patch ou atualização da Microsoft<sup>®</sup>. Usado no GFI LanGuard para proporcionar mais informações em um patch ou atualização instalado. As informações abrangem: ID, título, descrição, URL e tamanho do arquivo do boletim.

#### Instalação automática de aplicativos

Ação de habilita a instalação automática de aplicativos que oferecem suporte à desinstalação silenciosa do GFI LanGuard.

#### Interface de gateway comum (CGI)

Script de comunicação usado por servidores Web para transferir dados a um navegador da Internet cliente.

#### L

#### Linguagem de marcação extensível (XML)

Padrão de texto aberto usado para definir formatos de dados. O GFI LanGuard usa esse padrão para importar ou exportar os resultados e configurações salvas das verificações.

#### Linux

Sistema operacional de fonte aberta que compõe a família de sistemas operacionais Unix.

#### Lista de exclusão

Lista com os nomes dos dispositivos de rede ou USBs considerados perigosos. Quando o nome do dispositivo de rede/USB corresponde a uma entrada da lista de exclusão, ao verificar a rede, o GFI LanGuard relatará tal dispositivo como ameaça à segurança (alta vulnerabilidade de segurança).

#### Lista de permissões

Lista com os nomes dos dispositivos de rede ou USBs que não são considerados perigosos. Quando o nome do dispositivo de rede/USB corresponde a uma entrada da lista de permissões, ao verificar a rede, o GFI LanGuard ignora tal dispositivo e considera-o uma fonte segura.

#### Insscmd.exe

Ferramenta de linha de comando do GFI LanGuard que permite executar verificações de vulnerabilidade em relação a destinos de rede.

#### Localizador uniforme de recursos (URL)

O localizador uniforme de recursos é o endereço de uma página na World Wide Web.

#### Μ

#### Malware

Palavra feita a partir dos termos "software" e "mal-intencionado", malware é um termo genérico para todos os softwares desenvolvidos para danificar e prejudicar um sistema de computador. Vírus, worms e cavalos de Troia são tipos de malware.

#### Microsoft® IIS

Conjunto de serviços baseados na Internet criado pela Microsoft® Corporation para servidores de Internet.

#### Microsoft® WSUS

Sigla de Microsoft<sup>®</sup> Windows Server Update Services. Esse serviço habilita o administrador a gerenciar a distribuição das atualizações da Microsoft<sup>®</sup> aos computadores de rede.

#### Módulo SSH

Módulo que determina o resultado das verificações de vulnerabilidade pelos dados do console (texto) produzidos pelo script executado. Isso significa que você pode criar verificações de vulnerabilidade Linux/UNIX personalizadas usando qualquer método de script suportado pelo SO Linux/UNIX do destino e que emita resultados para o console em texto.

#### Ν

#### NETBIOS

Sigla de Network Basic Input/Output. Esse sistema oferece serviços para permitir que os aplicativos de diversos computadores de uma rede se comuniquem entre si.

#### Netscape

Navegador da Web desenvolvido originalmente pela Netscape Communications Corporation.

#### 0

#### Objeto da política de grupo (GPO)

Sistema centralizado de gerenciamento e configuração do Active Directory que controla o que os usuários podem ou não fazer em uma rede de computadores.

#### OVAL

Padrão que promove conteúdos de segurança abertos e disponíveis ao público, e padroniza a transferência dessas informações por todas as linhas de ferramentas e serviços de segurança.

#### OVAL (Open Vulnerability and Assessment Language)

Padrão que promove conteúdos de segurança abertos e disponíveis ao público, e padroniza a transferência dessas informações por todas as linhas de ferramentas e serviços de segurança.

#### Ρ

#### Painel

Representação gráfica que indica o status das diversas operações que podem estar atualmente ativas, ou estão programadas.

#### Perfis de verificação

Compilação de verificações de vulnerabilidade que determina quais vulnerabilidades são identificadas e quais informações serão recuperadas dos destinos de verificação.

#### Portas TCP

Sigla de Transmitting Control Protocol. Protocolo desenvolvido para permitir que os aplicativos transmitam e recebam dados pela Internet usando as portas conhecidas do computador.

#### Portas UDP

Sigla de User Datagram Protocol, usado aqui para transferir dados UDP entre os dispositivos. Nesse protocolo, os pacotes recebidos não são reconhecidos.

#### Programa backdoor

Método alternativo usado para acessar um computador ou seus dados por uma rede.

#### Protocolo de desktop remoto

Protocolo desenvolvido pela Microsoft<sup>®</sup> para habilitar os clientes a se conectarem com a interface do usuário de um computador remoto.

#### Protocolo ICMP

O Protocolo ICMP é um dos principais protocolos da suíte de protocolo de Internet. É usado por sistemas operacionais de computadores em rede para enviar mensagens de erro indicando, por exemplo, que o serviço solicitado não está disponível ou que não é possível alcançar o host ou roteador. O ICMP também pode ser usado para retransmitir mensagens de consultas.

#### Protocolo TFTP

Protocolo usado para transferir arquivos entre computadores da rede.

#### S

#### SANS

Sigla da organização System Administration, Networking and Security. Instituto que compartilha soluções referentes a alertas de sistema e segurança.

#### Scripts Python

Linguagem para scripts de programação de computador de alto nível.

#### Service Packs do Microsoft® Windows

Compilação de atualizações e correções fornecida pela Microsoft<sup>®</sup> para melhorar um aplicativo ou sistema operacional.

#### Serviços de Informações da Internet (IIS)

Conjunto de serviços baseados na Internet criado pela Microsoft® Corporation para servidores de Internet.

#### Serviços de terminal

Serviço que permite se conectar a um computador de destino e gerenciar os aplicativos instalados e os dados armazenados nele.

#### Servidor da Web

Um servidor que fornece páginas da Web ao navegador cliente usando o protocolo HTTP.

#### Servidor de email

Servidor que gerencia e armazena emails do cliente.

#### Servidor Web Apache

Projeto de servidor HTTP de fonte aberta desenvolvido e mantido pela fundação do software Apache.

#### Simple Network Management Protocol (SNMP)

O protocolo SNMP é uma tecnologia usada para monitorar dispositivos de rede como roteadores, hubs e switches.

#### Sistema de nomes de domínio

Banco de dados usado pelas redes TCP/IP que habilita a tradução dos nomes do host em números IP e o fornecimento de outras informações relacionadas ao domínio.

#### SNMP

Sigla de Simple Network Management Protocol, tecnologia usada para monitorar dispositivos de rede como roteadores, hubs e switches.

#### Spyware

Tipo de malware voltado a coletar informações de um computador sem notificar o usuário.

#### SQL Server®

Sistema de gerenciamento de banco de dados relacional da Microsoft<sup>®</sup>. A Microsoft<sup>®</sup> incluiu recursos adicionais ao SQL Server<sup>®</sup> (controle de transações, manuseio de exceções e segurança) para que o Microsoft SQL Server<sup>®</sup> ofereça suporte a organizações maiores.

### U

### Universal Serial Bus (USB)

Um padrão de barramento universal amplamente usado para conectar dispositivos em um computador host.

### URL

O localizador uniforme de recursos é o endereço de uma página na World Wide Web.

### V

### VBScript

A linguagem de Visual Basic Scripting é uma linguagem de programação de alto nível desenvolvida pela Microsoft<sup>®</sup>.

#### Vírus

Tipo de malware que infecta o computador. A meta do vírus é danificar o computador corrompendo arquivos e aplicativos. Um vírus é um programa que consegue replicar a si próprio, copiando a si mesmo por todo o sistema do computador.

### Vulnerabilidades e exposições comuns (CVE)

Lista de nomes padronizados de vulnerabilidades e outras informações sobre exposições de segurança. A meta do CVE é padronizar os nomes de todas as vulnerabilidades e exposições de segurança conhecidas.

### W

### Wi-Fi/LAN sem fio

Tecnologia normalmente usada em redes de área local. Os nós da rede usam dados transmitidos por ondas de rádio, em vez de cabos, para se comunicarem.

### Х

### XML

Padrão de texto aberto usado para definir formatos de dados. O GFI LanGuard usa esse padrão para importar ou exportar os resultados e configurações salvas das verificações.

### Ζ

### Zona desmilitarizada (DMZ)

Seção da rede que não é parte da rede interna, mas não é diretamente uma parte da Internet. Normalmente serve como gateway entre as redes internas e a Internet.

# 7 Índice

### A

Agente 4, 10, 14, 16, 19, 44

## Á

Árvore de computadores 20, 30, 36, 40 Atividade 17 Atributos 21, 24 Atualizações de segurança 5, 38, 44 Atualizar 16, 19 Auditoria 4-5, 7, 10, 16, 21, 23, 33, 41 Avaliação de vulnerabilidade 4-5, 9

### В

Busca de texto completo 27

### С

Cliente 8, 10 Compartilhamentos 7, 22 Computador 4, 10 Conformidade 4-5, 8, 28

### D

Desinstalar 5, 34 Desinstalar aplicativos 33 Dispositivos de rede 5, 21

### G

Grupos 7, 10, 23

#### Н

Hardware 5, 7, 20, 22

#### I

Instalar 14

#### L

Insscmd.exe 13

#### Μ

Mensagens 37

Monitor 12, 19

## Ν

Nível 21 Notificações 9, 17, 37

#### Ρ

Painel 4, 22-24, 26, 37 PCI DSS 8 Perfis de verificação 17 Personalizar 42 Portas 22 Portas abertas 7 Proxy 5 **S** 

Servidor 5, 10, 14 Software 7, 20, 30, 36

### Т

Tempo real 10, 38

#### U

Usuários 20, 22, 34

### V

Verificação 4, 6, 12, 14, 17, 19-20, 27, 33, 35, 40, 45 Verificações agendadas 11, 19, 41 Verificações de segurança 10, 17, 46 Vulnerabilidades 4-5, 22