

GFI product comparison:
GFI LanGuard® 12
VS
BeyondTrust Retina CS 5.2

General features

| Features | GFI LanGuard 12 | BeyondTrust Retina CS |
|--|-----------------|-----------------------|
| Scheduled scans | ✓ | ✓ |
| Agent-less | ✓ | ✓ |
| Agent-based | ✓ | ✓ |
| Integration with Active Directory | ✓ | X |
| Asset tracking | ✓ | ✓ |
| Installs on workstations | ✓ | ✓ |
| Network utilities (DNS lookup, traceroute, SNMP walk, etc.) | ✓ | X |
| Flexible scan target (single machine, list of computers, IP ranges, domains, etc.) | ★★★★★ | ★★★★★ |
| Power management options (Wake-on-LAN, shut down) | ✓ | X |

Vulnerability management

| Features | GFI LanGuard 12 | BeyondTrust Retina CS |
|--|---------------------|-----------------------|
| Scan for Windows vulnerabilities | ✓ | ✓ |
| Scan for Linux/Apple OS X vulnerabilities | ✓ | ✓ |
| Scan for application vulnerabilities | ✓ | ✓ |
| Scan for network device vulnerabilities | ✓ | ✓ |
| Scan for mobile device vulnerabilities | ✓ | ✓ |
| CVE-certified | ✓ | ✓ |
| Custom vulnerability checks | ✓ | ✓ |
| Scripting support | ✓ (VB, Python, SSH) | X |
| Vulnerability remediation | ✓ | ✓ |
| Integrated with remote desktop connections | ✓ | X |

Patch management

| Features | GFI LanGuard 12 | BeyondTrust Retina CS |
|---|-----------------|-----------------------|
| Manage Microsoft updates | ✓ | ✓ |
| Manage application updates | ✓ | ✓ |
| Manage Apple OS X updates | ✓ | X |
| Manage Linux updates | ✓ | X |
| Manage non-security updates | ✓ | X |
| Deploy major upgrades | ✓ | X |
| Deploy custom software and scripts | ✓ | X |
| Automatic detection, download and deployment of patches | ✓ | X |
| Rollback patches | ✓ | X |
| Post patch deployment reboot control | ✓ | X |

Network and software audit

| Features | GFI LanGuard 12 | BeyondTrust Retina CS |
|--|-----------------|-----------------------|
| Port scanning | ✓ | ✓ |
| Retrieve computer network role | ✓ | X |
| Retrieve list of shares | ✓ | ✓ |
| Retrieve users and groups | ✓ | ✓ |
| Retrieve installed services | ✓ | ✓ |
| Retrieve logged-on users | ✓ | X |
| Retrieve password and security audit policies | ✓ | ✓ |
| Hardware audit | ✓ | ✓ |
| Virtual machine detection | ✓ | ✓ |
| Get email notifications on system changes | ✓ | ✓ |
| Installed software | ✓ | ✓ |
| Integration with over 4,000 critical security applications (antivirus, antispyware, firewalls, backup, etc.) | ✓ | X |
| Uninstall or get notified on unauthorized applications | ✓ | X |

Reporting

| Features | GFI LanGuard 12 | BeyondTrust Retina CS |
|---|-----------------|-----------------------|
| Technical reports | ✓ | ✓ |
| Dashboard | ✓ | ✓ |
| Results comparison and baselining | ✓ | ✓ |
| Scheduled reports | ✓ | ✓ |
| Email reports | ✓ | ✓ |
| Export reports to various formats (PDF, DOC, HTML, XML, etc.) | ✓ | ✓ |
| Full text search support | ✓ | X |
| PCI DSS, HIPAA and other compliance dedicated reports | ✓ | ✓ |
| Report branding | ✓ | ✓ |
| Advanced result filtering options | ✓ | X |

| BeyondTrust Retina CS Weaknesses | GFI LanGuard 12 Strengths |
|--|---|
| <p>Weak support for third party applications Supports less 3rd party applications (14 applications supported) for patch management than LanGuard. No integration with critical security applications and no full text search.</p> | <p>Strong support for third party applications GFI LanGuard automates detection, download and deployment of patches for 70+ third party applications.</p> |
| <p>WSUS disadvantages apply to patch management offered by Retina Patch management functionality implemented in Retina is based on Microsoft WSUS. WSUS installs only on Windows servers; it is hard to manage computers that are not part of the domain and customers have less control because the server does not push patches (clients contact the server).</p> | <p>Easy to install and get running Installs on both servers and workstations and it is easy to manage computers no matter how they are organized as long as administrative access to them is provided.</p> |
| <p>Patch management limited to Windows systems Based on Microsoft WSUS, Retina patch management only works for Windows operating systems</p> | <p>Patch management for Windows, Mac OS and Linux systems Manage mixed environments of Windows, Mac OS and Linux systems from a single central console.</p> |
| <p>Pricing More expensive than GFI LanGuard while offering less functionality (customers need to pay a yearly fee per IP address).</p> | <p>Low total cost of ownership Competitive price due to centralized vulnerability management, patch management and network and software audit.</p> |

A Flexible Solution

GFI LanGuard combines both patch management and vulnerability management at a fixed price for Windows, Linux, Mac OSX and mobile devices. For Windows based platforms GFI LanGuard supports both Microsoft and over 80 3rd party applications. A Web Based Central Management console offers easier management of different network sites, which could potentially also be installed in remote office locations. This makes GFI LanGuard the most flexible solution for organizations of any size from those with a hundred devices to larger ones with thousands of devices.

Conclusion

BeyondTrust Retina CS is a vulnerability assessment solution with basic patch management functionality provided through integration with WSUS, while GFI LanGuard is much more than that: It is a complete network security audit solution that supports patching for Windows, Linux, Apple OS X, third party applications, it is easy to install and get running and sells at a highly competitive price.

GFI LanGuard is your own virtual security consultant: easy, always available and affordable!



For a full list of GFI offices/contact details worldwide,
please visit <http://www.gfi.com/contactus>

Disclaimer

© 2016. GFI Software. All rights reserved. All product and company names herein may be trademarks of their respective owners.

The information and content in this document is provided for informational purposes only and is provided "as is" with no warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, and non-infringement. GFI Software is not liable for any damages, including any consequential damages, of any kind that may result from the use of this document. The information is obtained from publicly available sources. Though reasonable effort has been made to ensure the accuracy of the data provided, GFI makes no claim, promise or guarantee about the completeness, accuracy, recency or adequacy of information and is not responsible for misprints, out-of-date information, or errors. GFI makes no warranty, express or implied, and assumes no legal liability or responsibility for the accuracy or completeness of any information contained in this document.

If you believe there are any factual errors in this document, please contact us and we will review your concerns as soon as practical.