StillSecure® Strata Guard™

Protects you from the cost of malicious attacks.

Features, functions, and benefits

Feature	Function	Benefit
Attack rules		
3500+ rule database	Comprehensive protection from attack.	Detects widest range of network attacks.
Automated rule updates from StillSecure Security Alert Team (SAT)	Updates rules as often as hourly.	▪ Protects against the latest vulnerabilities. ▪ SAT operates 24x7 monitoring for threats.
Utilizes Snort®* rules and format	Utilizes well-known Snort signature format.	▪ Takes advantage of most well-known and popular signature database and format.
Rules compiled and tested from multiple sources: ▪ StillSecure SAT ▪ Open Source Snort Rules Consortium (OSSRC) ▪ Bleeding Snort® ▪ SourceFire VRT ▪ Open source, GPL	Provides depth and breadth of attack coverage.	Highest level protection, highest quality rules available.
Customizable	Allows you to import custom signatures.	▪ Allows for customized signatures—write your own signatures to block attacks specific to your network in standard Snort format.
History / logging of all updates	Logs updates to rule sets on each instance creating a complete history of rule set changes.	▪ Know how your rule set is changing. ▪ Know you are current on rule updates.
Attack detection		
Multiple attack-detection methods (signature analysis, stateful packet analysis, TCP stream reassembly, protocol anomaly/behavior analysis, Layer 2 analysis)	Detects all malicious traffic.	▪ Protects against the widest variety of attacks.
DoS and DDoS detection	▪ Ensures DoS/DDoS attacks don't bring down the network. ▪ Prevents Strata Guard from contributing to a DoS attack.	▪ Warns you of a DoS condition. ▪ Regulates/terminates DoS attacks. ▪ Prevents Strata Guard from contributing to a DoS attack while still reporting on other attacks occurring on your network. ▪ Ensures resource availability/business continuity. ▪ Does not inhibit the flow of legitimate traffic.
Anomaly/behavior based attack detection	Creates models of TCP/IP protocols using their specifications/request for comments (RFCs).	▪ Ensures that events within a session conform to the proper state as defined by the protocol ▪ Detects wide range of known and unknown attacks.
Attack qualification		
Dynamic Attack Qualification™ *	A compilation of qualification methods to eliminate false-positives. Includes *Accessible Device Protection*, *Vulnerable Device Protection*, *Quick-tune*, and *Intelligent Attack Profiling*.	Ensures only legitimate attacks trigger response/alerts.
Accessible Device Protection™	▪ Displays and responds to attacks aimed at live devices and ports. ▪ Attacks aimed at non-existent devices or closed ports are safely ignored.	▪ Significantly reduces false-positives. ▪ Focuses IT resources on attacks that pose real threats. ▪ Focus attention on attacks only to live devices and ports.
Vulnerable Device Protection™	Correlates an attack with vulnerability information about the device being attacked.	▪ Protects (i.e., "shields") devices known to have vulnerabilities. ▪ Correlates attacks with vulnerable devices, thereby reducing false-positives and focusing IT resources on real threats.
Intelligent Attack Profiling™	Tailors the level of response to attacks based on user-defined attack profiles.	▪ Significantly reduces false-positives. ▪ Saves IT resources and time by providing only relevant threat information. ▪ Allows IT staff to quickly respond to verified attacks. ▪ Customize per-attack response based on selectable/definable parameters.

*Snort is a registered trademark of Sourcefire, Inc. Latis Networks, Inc. is not affiliated with, connected to, or sponsored by Sourcefire, Inc.

Quick-tune™	Tunes Strata Guard to respond only to the attacks relevant to your network.	▪ Significantly reduces false-positives. ▪ Reduces administration and improves performance.
Highlight attacks to accessible and vulnerable devices and tailor responses	Provides a visual indicator that tells you which attacks are directed toward accessible devices, a vulnerable devices, or toward devices that are accessible and vulnerable.	Helps to prioritize remediation efforts and greatly reduces false-positives by flagging attacks that are the most likely to cause damage.
Attack response		
Dynamic Attack Response™ **Active responses:** ▪ Drop attack packet ▪ Block source IP/session ▪ Secure TCP reset ▪ SNMP trap **Passive responses:** ▪ Email notification ▪ Pager notification ▪ Event logging ▪ Run custom script	Provides multiple methods to respond to attacks, including both active and passive responses.	▪ Secures your network from intrusions. ▪ Provides a variety of methods to prevent damage.
Pre-emptive Policies™ (In-line deployment only)	Drops malicious traffic before it enters the network.	Stops attacks from infiltrating the network, including difficult-to-stop single-packet attacks.
WHOIS lookups	Looks up IP addresses in ARIN directory.	Tells you who is attacking your network.
Attack research	Research attacks by accessing the StillSecure SAT attack database as well as CERT, Arachnids, and BugTraq.	Educates by providing detailed information about attacks and attack types.
Performance		
Gigabit level scalability	Strata Guard GigE: Ships as network appliance including a hardened, high-performance hardware platform. Also available as software.	Allows you to reach enterprise-level speeds cost-effectively.
Multi-segment monitoring capabilities	Monitor multiple network segments from a single Strata Guard instance.	Saves time and money by managing multiple nodes from a single console.
Runs in promiscuous mode	Strata Guard runs invisibly on the network.	▪ Prohibits hackers from detecting Strata Guard. ▪ Prohibits Strata Guard from experiencing DoS attack.
Deployment		
HA bypass switch (In-line deployment only)	▪ Allows network traffic to continue flowing in the event of a hardware failure. ▪ Does not require HA configuration to keep traffic flowing.	▪ Allows traffic to flow through in the event of a hardware failure. ▪ Ensure there is no single point of failure.
Proxy support	Allows license validation and rule updates through a proxy server.	Saves time; eliminates need for manually initiating rule updates.
Easy to install, configure, and use	Installs in minutes and requires minimal time to administer.	▪ Improves the efficiency/productivity of available IT resources. ▪ Requires minimal learning curve and ramp-up time.
Easy configuration back-up and restore	Saves configuration settings.	Saves time responding to misconfiguration or configuration data loss.
Management		
User privileges	Provides authorized users with specific read, write, and system-wide privileges.	Allows you to effectively manage your IT resources by simplifying each user's access.
Multi-node management from a single console	▪ Manages multiple instances of Strata Guard from a Web-based console. ▪ Each Strata Guard instance can be a manager of or can be managed by other Strata Guard instances.	▪ Scales across enterprises. ▪ Protects all Internet connections and optimizes resources. ▪ Centralizes security management to a single workstation.
Read-only access and reporting	Allows auditors, managers, IT staff, etc. to view report on attack activity.	Provides access without jeopardizing node configuration.
Centralized rule management across Strata Guard nodes	▪ All or any subset of Strata Guard instances can share the same rule set. ▪ Updates to a "master" rule set can be automatically pushed all instances within that group.	▪ Allows control of your rule settings across the enterprise from one master console. ▪ Avoids leaving an open path to the network by inconsistency of rules. ▪ Saves time managing multiple instances.

Data archiving—selectable settings	Archive historical data by using Strata Guard's internal archiving capability, offloading to external media, or installing a commercial back-up client on the Strata Guard machine.	▪ Stores appropriate amount of historical data. ▪ Easily keep historical data for compliance / audit purposes.
Comprehensive diagnostic displays	Displays system information for troubleshooting without an OS shell.	Effectively manage Strata Guard platforms without learning Linux.
Throughput statistics display	Displays throughput performance data.	Saves time troubleshooting and validating system performance.
Comprehensive glossary of attacks	Provides details on and educates you about each attack.	Displays information about specific attacks in real time so you can make an educated decision about how to respond.
Search active rule set	Search names and descriptions of active rules on a Strata Guard instance by keyword or phrase.	Allows you to easily search for rules among the rule set in use.
Co-brand interface and reports	Allows your logo to be placed on the main interface screen and on reports.	▪ Reinforces end-user brand in the interface. ▪ Allows resellers to co-brand in managed services environment.
Nested group management capabilities	Use *Groups* and *User accounts* to organize your network.	Allows you to logically define large network and assign responsibilities, saving time and IT resources.
Import/export device list	Allows you to import devices from the command line and indicate if they are "vulnerable" devices.	▪ Allows you to import accessible and / or vulnerable devices. ▪ Provides additional protection for weakest points on the network. ▪ Streamlines administration.
Managed through only SSL or SSH connections	StillSecure management console accesses Strata Guard via only SSL or SSH.	Prohibits Strata Guard from being compromised.
Reporting		
Customizable, comprehensive reports	Enables a wide variety of reporting capabilities at all system levels.	▪ Reports on criteria important to your business. ▪ Allows you to manipulate and present data in your preferred format. ▪ Easy to read/understand printed reports and data.
Scheduled reporting	Automatically generates and emails reports to designated recipients.	Reduces administration time and keeps stakeholders informed.
Save reports to a file	Saves reports directly to a file.	Allows you to manipulate and present data in your preferred format.
Exportable	▪ Exports reports/data to CSV or tab-delimited format. ▪ Provides printer-friendly formatting.	Allows you to use your preferred reporting package to analyze data.
ODBC / SQL access to database	Provides for custom queries and reports via standardized protocol.	Allows you to customize reports and queries.
Packet payload capture (customizable)	▪ Captures and presents attack payload data. ▪ Payload size can be varied to focus on the attack as well as the data before and after.	▪ Provides easy analysis of attacks and what is causing them—understand the attack better in order to provide a more complete response. ▪ Lets you further examine attack details.
Centralized reporting	Consolidates reporting across multiple Strata Guard nodes.	▪ Improves and simplifies data collection for managing and auditing network security. ▪ Create highly focused reports for all Strata Guard nodes.
Availability		
Software appliance	Provides implementation option as a software solution.	Flexible delivery options.
Hardware appliance	Provides implementation option as high-performance hardware appliance.	▪ Pre-configured and standardized. ▪ 3-year hardware warranty. ▪ Highly tuned solution for high-performance deployment. ▪ Quick and easy installation.
Secure locked-down OS with software and hardware appliance versions	Includes version of Linux customized for Strata Guard.	Creates no additional vulnerabilities on your network.

StillSecure
361 Centennial Parkway
Suite 270
Louisville, CO 80027
P: [303] 381-3800
F: [303] 381-3880
www.stillsecure.com

Reducing your risk has never been this easy.