StillSecure® Strata Guard™

Protects you from the cost of malicious attacks | Datasheet

Strata Guard™ is an award-winning family of network-based intrusion detection/prevention systems (IPS/IDS) that provide real-time, zero-day protection from network attacks and malicious traffic.

With four different models and two deployment options, Strata Guard protects your enterprise from the network perimeter to the core, including remote and internal segments *(as shown in Figure 1)*.

Strata Guard employs six distinct attack-detection technologies for comprehensive network protection. With signature-based and behavior-based attack detection, deep packet inspection, and protocol anomaly analysis, Strata Guard terminates network-, application-, and service-level attacks including worms, trojans, spyware, port scans, DoS and DDoS attacks, server exploit attempts, and viruses before they infiltrate the network and cause real damage.

Beyond blocking malicious attacks, Strata Guard enforces your network usage polices and can block peer-to-peer file sharing, instant messaging, chat, prohibited browsing activity, and worm propagation. It detects anomalous activity such as spoofed attack source addresses, TCP state verification, and rouge services running on the network.

Highly automated, Strata Guard is designed for ease of use and streamlined administration and management. Through its multi-layered *Dynamic Attack Qualification™* technologies, Strata Guard eliminates false-positives. Its multi-node, multi-user management capabilities allow for enterprise-wide deployments and provide appropriate levels of control for all users requiring access to security data.

Strata Guard is available as software or as a preconfigured hardware appliance.

SC MAGAZINE BEST OF 2004

★★★★★

Strata Guard receives a perfect five stars in all categories: "Easy to set up, comfortable to navigate, and it really streamlined the complex process of intrusion prevention without losing functionality. One of the best in terms of usage and installation."

SC Magazine

RATED EXCELLENT InfoWorld

"Installation and setup are fast and easy, the GUI is top-notch, and reporting is excellent, removing all the difficulty of navigating Snort® and displaying attacks and payloads. An excellent choice for signature-based detection and prevention."

InfoWorld Magazine

Deployment for attack detection and attack prevention

Strata Guard can be installed anywhere the potential for attack exists: at the perimeter, internally, in the DMZ, and between strategic segments (e.g., remote offices, partners) where organizations need to control direct links to un-trusted networks.

Strata Guard is deployable in both in-line and out-of-band configurations:

In-line deployment:

- True IPS functionality
- React instantaneously to attacks; drop offending packets (i.e., *Pre-emptive policies™*)
- Highest level of protection—attacks can't penetrate the network
- Allows you to move from IDS to IPS functionality at your own comfort level

Out-of-band deployment:

- Blocks attacks by inserting rules into firewall (i.e., Responsive policies)
- Provides history of attack events
- Forensic tracking

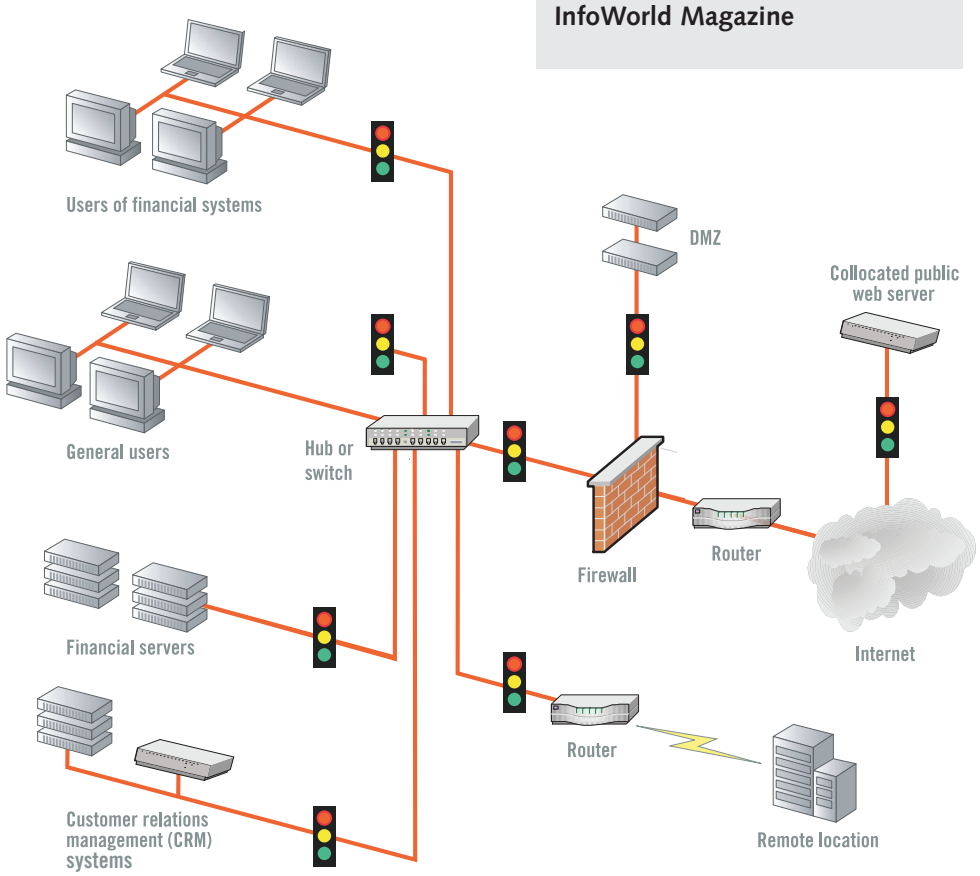

Figure 1. Strata Guard, represented by the stoplight, secures the connections that expose your organization to attack: at the perimeter, internally, and on links to remote offices, partners, and vendors. It protects and controls access to sensitive business systems and users and enables targeted compliance reporting and monitoring.

Multi-level attack detection

Strata Guard's *Dynamic Attack Detection*™ technology *(Figure 2)* applies a combination of detection methods with the goal of identifying all possible malicious traffic. *Dynamic Attack Detection* includes:

- **Layer 2 analysis** – detects invalid and malicious activity at the layer 2 level including duplicate and spoofed Ethernet addresses.
- **Protocol anomaly/behavior** – creates models of TCP/IP protocols using their specifications/request for comments (RFCs). This ensures that events within a session conform to the proper state as defined by the protocol; it is used to detect a wide range of known and unknown attacks.
- **TCP stream reassembly analysis** – reassembles packet fragments and examines complete sessions. Strata Guard maintains state on more than 64,000 simultaneous sessions, which increases accuracy and reduces IDS/IPS evasion.
- **Stateful packet analysis** – prevents IDS/IPS evasion and increases accuracy of alerts. Strata Guard's flexible rule language provides a content-matching system that can describe anomalies within application layer protocols, allowing certain anomalies to be detected, like buffer overflows, without having specific signatures for the attack.
- **Signature analysis** – provides pattern matching and content analysis to detect any known attack signatures. Strata Guard provides 3500+ signatures that are updated as often as every hour. See *Comprehensive signature database* below for more information.
- **DoS and DDoS detection** – identifies DoS and DDoS conditions automatically, and reacts appropriately. See *DoS/DDoS attack prevention* on p. 3.

Comprehensive signature database

Strata Guard attack rules—or signatures—are created, tested, and released by the StillSecure Security Alert Team (SAT), which operates on a 24x7 basis to monitor and respond to network threats. In addition to writing and releasing GPL rules in-house, SAT compiles rules from other sources including Open Source Snort Rules Consortium, Bleeding Snort, SourceFire VRT, and other sources.

Strata Guard rules conform to the industry-standard Snort* format. Strata Guard can be configured to check for updated SAT rules as frequently as every hour, or users can download rule updates on demand, ensuring up-to-the-minute protection against newly released threats. Custom rules can be easily created to address organization-specific threats and policy compliance.

SAT Security Alert Team StillSecure®

Qualifying attacks

Strata Guard qualifies attacks through its *Dynamic Attack Qualification*™ technology *(Figure 3)*. This combination of powerful qualifying techniques isolates the real threats to your network, and eliminates the overwhelming majority of attacks as false-positives. Your IT resources stay focused on responding to legitimate threats. *Dynamic Attack Qualification* includes:

- **Accessible Device Protection**™ (ADP) – Scans the network, discovering all devices and open ports; as a result, attacks aimed at inaccessible devices or ports are ignored.
- **Vulnerable Device Protection**™ (VDP) – Creates a protective, attack-blocking shield around devices with known vulnerabilities. Vulnerabilities can be imported from the StillSecure VAM™ vulnerability management platform or entered manually.
- **Quick Tune**™ – Eliminates attacks based on the types of devices and operating systems on your network.
- **Intelligent Attack Profiling**™ (IAP) – Allows you to define the attack-specific profile that qualifies an attack as a legitimate threat within your business environment. Configurable profile parameters include: attack type, attack severity, source and destination IP address, source and destination port, number of attack occurrences, attack time of day. Attacks not conforming to a given profile are ignored.

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

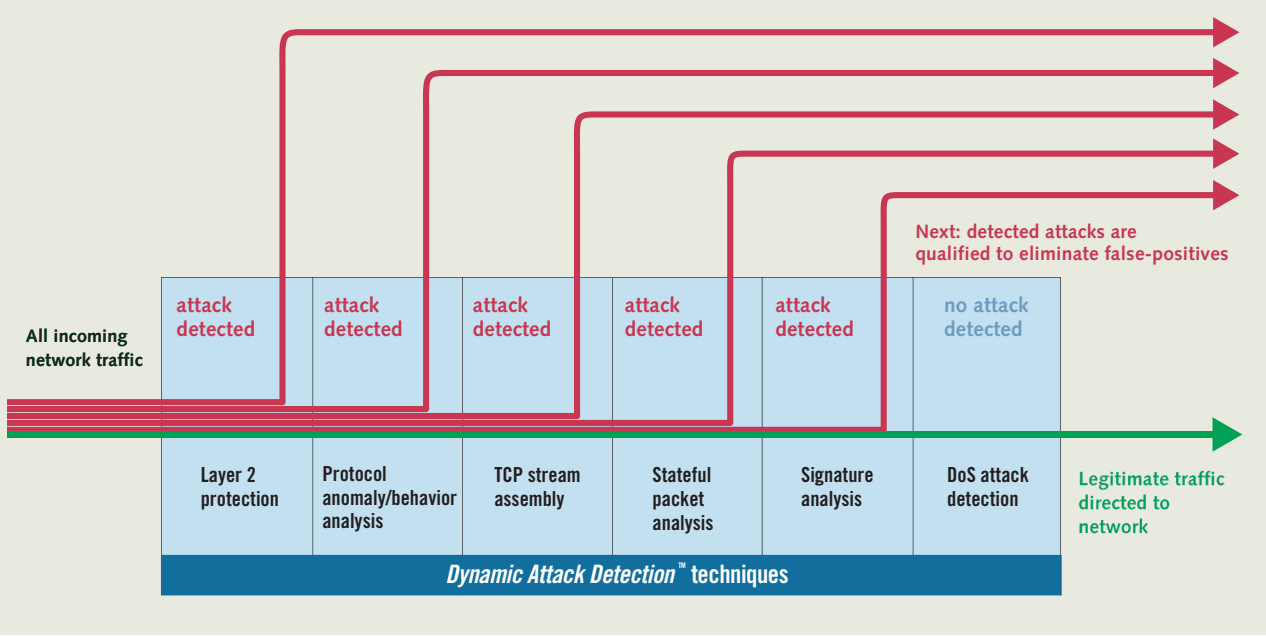

Figure 2. Multiple, complimentary attack detection techniques provide the highest level of protection against the range of malicious traffic.

Flexible attack response options

Strata Guard's multiple attack-blocking options provide flexibility and control over how you respond to attacks. You can implement a default blocking strategy to ensure a base level of protection, and create custom blocking strategies for specific attacks. Strata Guard can be set to automatically block attacks upon detection, or it can prompt you, allowing you to investigate the attack before committing to a specific course of action. Attack blocking techniques include:

- **Dropping attack packets** (in-line deployment only) – Prevents any part of an attack from infiltrating the network. Combines packet payload analysis with traditional packet header analysis at the kernel level.
- **Block attack source IP/ port** – Blocks the current attack from progressing and ensures that the attacker cannot launch future attacks. Traffic from the source IP / port or session is temporarily prohibited from entering the network.
- **Secure TCP reset** – Terminates traffic without letting it pass through to the target and resets the offending session. Unlike other IPS tools, Strata Guard does not send a reset command back to the originating host, so the attacker receives no indication that the session has been actively terminated.
- **Execute a custom command script** – Allows administrators to create custom responses for specific attack types.
- **Notifications** – Alerts users of an attack via SNMP trap and/or email; logs the attack event

DoS/DDoS attack prevention

Strata Guard takes a multi-tiered approach to defending against DoS/DDoS attacks. Strata Guard's onboard stateful IPS firewall continually monitors all incoming and outgoing traffic for anomalous conditions that indicate a DoS/DDoS attack. Using a threshold-based detection mechanism, the onboard IPS firewall will apply two levels of DoS/DDoS suppression. In the first level, traffic is regulated. In the second, traffic is rate-limited to a pre-defined level for the duration of the attack. Valid sessions are unaffected by the IPS firewall's actions and are given priority over the offending DoS/DDoS attack.

Additional approaches leverage Strata Guard's Snort IPS engine. Strata Guard maintains more than 60 rules for identifying and blocking DoS/DDoS attacks, the majority of which have been custom-authored by SAT security engineers. These rules detect specific attacks—such as Ping of Death, Tear Drop, LAND, and other TCP-based malicious traffic—and prohibit them from entering the network and impacting the flow of traffic.

Strata Guard business benefits

In today's heightened threat environment Strata Guard delivers tangible benefits to security-focused organizations:

- Ensures availability of resources in today's escalating threat environment
- Maintains detailed compliance audit trail for attack and attack-response activities
- Mitigates risk of attack and risk from noncompliance with regulations and policies
- Reduces security administration through automated defense and enterprise-scale security management
- Identifies highest criticality of attacks through correlation with device vulnerability data *(integration with StillSecure VAM)*
- Integrates with the StillSecure suite of network security solutions for comprehensive layered security.

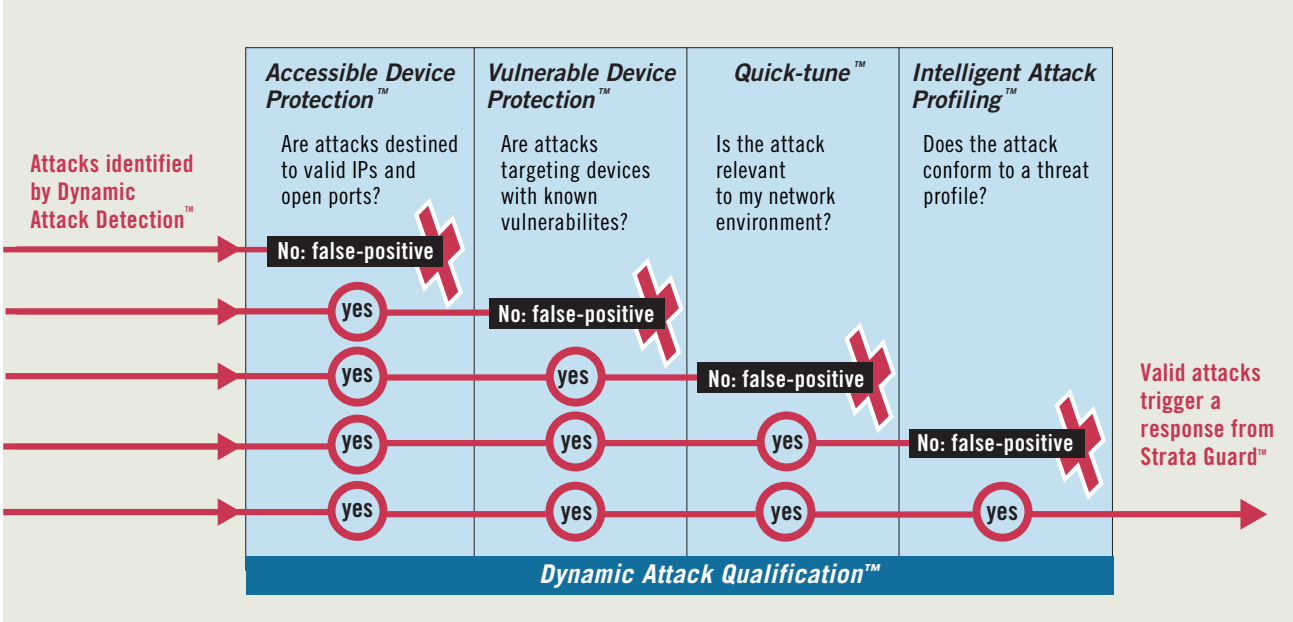

Figure 3. Dynamic Attack Qualification eliminates false-positives, which constitute the majority of detected threats. Only valid attacks trigger a response from Strata Guard.

Multi-node, multi-user management

Strata Guard's Multi-node manager centrally manages an unlimited number of Strata Guard instances, making it an ideal solution for managed security service providers (MSSPs) and for enterprise networks of any size and complexity.

Through the Multi-node manager *(Figure 4)*, attack rules can be shared among all or a subset of managed nodes, thereby simplifying administration and ensuring a consistent security posture network wide. Likewise, reporting can be consolidated across multiple Strata Guard nodes, or reports can be run on individual nodes to view segment-specific attack data. Users can be assigned read-only access to specific nodes, allowing them to monitor and report activity but not alter node configuration.

Multi-node manager is included with Strata Guard Enterprise and GigE at no additional charge.

Regulatory compliance and reporting

Strata Guard plays a key role helping organizations comply with the information security provisions of regulations such as Sarbanes-Oxley, HIPAA, GLBA, FISMA, Safe Harbor, and others. Strata Guard contributes to compliance on multiple levels:

- Provides access compliance checking
- Monitors and verifies adherence to encryption and privacy policies
- Produces a range of actionable reports for auditors, managers, and IT staff
- Deployment of an IDS/IPS is considered a best practice and demonstrates an organizational commitment to safe-guarding sensitive data

Strata Guard includes a comprehensive, full-featured reporting and analysis engine for insightful views into the state of security across your network. Sorting by types, frequencies, source and destination of attacks, and actions taken, these actionable reports are appropriate for all stakeholders. With both on-demand and automated scheduled reporting, Strata Guard satisfies compliance guidelines and enables efficient security monitoring and management.

Integration within the StillSecure suite

Strata Guard is part of the integrated StillSecure suite of layered security solutions for the network. In addition to Strata Guard, the suite includes:

- StillSecure VAM™ – vulnerability management platform
- StillSecure Safe Access™ – network access control solution

Through the StillSecure *Enterprise Integration Framework*™ (EIF) security data is shared among suite solutions and with existing IT systems, greatly enhancing network protection and operational efficiencies. The EIF enables data import/export and process integration with a wide-range of security and IT systems including trouble ticketing, third-party vulnerability scanners, patch managers, asset management systems, security information managers (SIMs), etc.

The suite offers organizations the following benefits:

- Layered security from a single provider
- Enhanced security through solution integration/data correlation
- Leveraging of existing security investments through open architecture
- Simplified administration with suite-wide common functionality, usability, and data management

We invite you to try a free demonstration. Contact 303-381-3830, sales@stillsecure.com, or visit www.stillsecure.com.

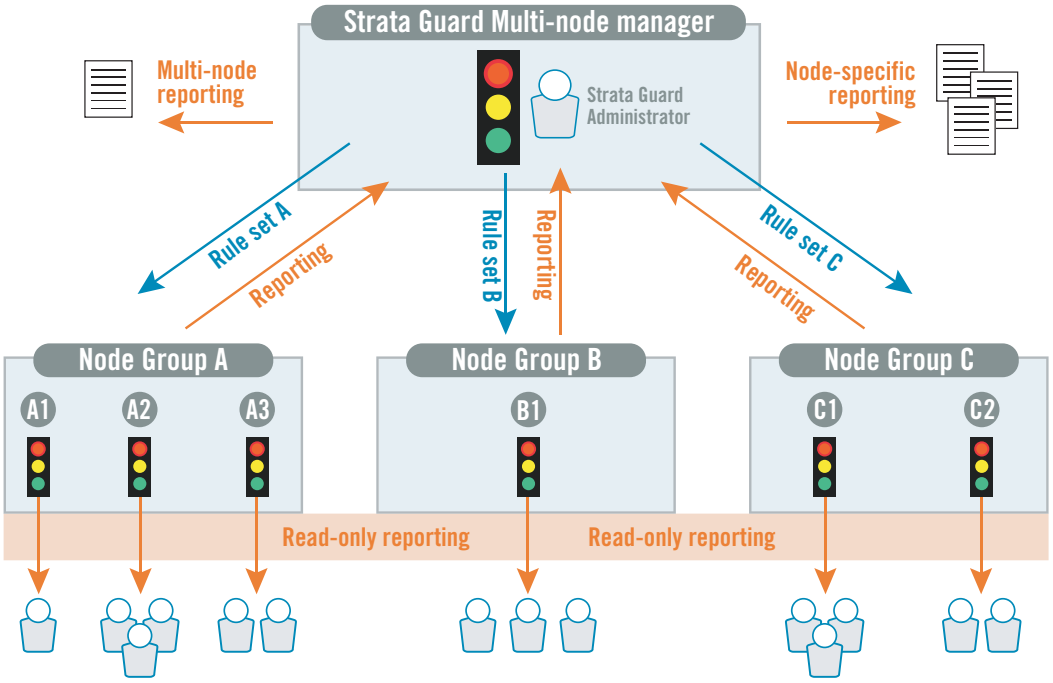

Figure 4. The Multi-node manager controls all Strata Guard instances form a single, centralized management console where custom rule sets are managed and distributed and reporting is consolidated. Users, such as security administrators, auditors, network administrators, and others can be granted read-only access and reporting to specific Strata Guard nodes.

StillSecure
100 Superior Plaza Way
Suite 200
Superior, CO 80027

P: [303] 381-3800
F: [303] 381-3880
www.stillsecure.com