

Attack rules

- 3500+ rule set
- Rule set consolidated from multiple sources
 - StillSecure® Security Alert Team (SAT)
 - Open Source Snort Rules Consortium (OSSRC)
 - Bleeding Snort®
 - SourceFire VRT
 - Open source, GPL
- Automatic rule updates
 - Initiated by SSL request to SAT server
 - Occur up to hourly
- SAT email notification as high-profile rules released
- Custom rule creation/rule editing
- Custom IDS rule import

Attack detection

- Network-level attacks
- Application-level attacks
- Signature- and behavior-based detection techniques:
 - Stateful packet analysis
 - Signature analysis
 - TCP stream reassembly analysis
 - Protocol anomaly/behavior analysis
 - Layer 2 analysis
 - DoS and DDoS detection
- VoIP, SIP and RDP attacks
 - DoS and man-in-the-middle detection

Attack qualification

- Quick Tune™
 - Configures Strata Guard to ignore attacks not relevant to environment
- Intelligent Attack Profiling™
 - Ignore attacks that do not conform to user-specified threat profiles
- Accessible Device Protection™
 - Employs NMAP scan to identify accessible devices
 - Ignores attacks directed at inaccessible devices
 - Configure aggressive default attack response for attacks targeting accessible devices
- Vulnerable Device Protection™
 - Vulnerable device data imported from StillSecure VAM™ vulnerability management system or entered manually
 - Configure highly aggressive default attack response for attacks targeting vulnerable devices
- Tune as you go
 - Specify response for future occurrences of current attack

Attack response

- Configurable on per-rule basis
- Response options/combinations include:
 - Drop offending packet
 - Block attack source host
 - Secure TCP reset
 - Run a custom script
 - Prompt user to take action
 - DoS rules/rate-limiting response
 - Send SNMP trap
 - Send email notification(s)
 - Log attack event
- Pre-emptive attack policies (Inline deployment only)
 - Verifies packet before sending
 - Drops offending packets without restricting legitimate traffic from source
 - Ideal for email viruses, network worms, single packet attacks

- Responsive attack policies (Inline and out-of-band deployments)
 - Blocks attack source IP address for user-specified duration (e.g., 30 minutes)
 - Ideal for defending against port scans, session interruptions
- Configurable default response for new rules

Performance

- High-availability bypass unit (fail open)
- High availability (active/active serial)
- By version:
 - Strata Guard SMB: < 10 Mbps
 - Strata Guard Enterprise < 200
 - Strata Guard GigE: > 200 Mbps

Deployment

- Inline deployment
 - Two interfaces, all traffic passed through and inspected, serves as network bridge
 - Instantaneous response to offending packet
 - Fail open with bypass switch
 - Optional high availability
- Out-of-band deployment
 - Single listening interface
 - Enables port monitoring
 - Fail open passive design
 - Responsive attack policies enabled in conjunction with supported firewalls: Cisco PIX, CheckPoint, NetScreen, Linux IPTables

OS/platform/architecture

- StillSecure OS, a hardened Linux OS, installs with Strata Guard
- Open architecture; customizable, extensible
- On-board ODBC compliant database
- Design incorporates multiple open source components
- Data archiving options
 - Internal to Strata Guard
 - Configuration settings backup
 - Third-party backup tool integration
 - Offload database to other media or device

Management

- Multi-node, multi-user management capabilities
 - Unlimited number of Strata Guard nodes managed through single console
 - Ideal for MSSP and enterprise-scale deployment
 - Rule sets, response configurations shared among multiple nodes
 - Individual- and multi-node reporting
 - Read-only reporting by node for non-admin users
- Privileges/access control
 - Administrator
 - Read-only, for attack activity reporting and node monitoring
- Single Web-based console for individual- and multi-node management

Availability

- Available as:
 - Software – user-installed on dedicated host
 - Hardware appliance – custom configured per consultation with customer
- Purchasing models:
 - Annual subscription
 - Perpetual: purchase plus annual maintenance

Support

- Engineer-delivered
- Available at no charge to subscribers
- 8:00 a.m. to 6:00 p.m. MST; 24-hour support available
- Training and tuning assistance available



Strata Guard intrusion detection/prevention appliance

System requirements

1. A dedicated server for product installation with the following recommended system requirements.
 - Pentium 4 (2 GHz or above)
 - 1 GB RAM
 - 72 GB hard disk space
 - 3 NICs 10/100 (3Com or Intel) for *Gateway* mode; 2 NICs for *Standard* mode

Note: The StillSecure OS, a distribution of Linux®, installs with the product.
2. Windows workstation running Internet Explorer 6 or later with 128-bit encryption.

Firewall compatibility (*Standard* mode only)

- Check Point FireWall-1™
- Cisco PIX™
- Linux IP Tables
- NetScreen™

Hardware appliance

StillSecure custom-configures hardware appliance in consultation with customers.

Strata Guard product suite

Strata Guard is available in a variety of versions designed to meet the needs of businesses of all sizes, from small organizations to global enterprises

	SMB (small-medium business) <i>Ideal for organizations with modest throughput requirements</i>	Enterprise <i>For mid- to enterprise-sized organizations</i>	GigE <i>Designed for organizations with high throughput requirements</i>
Performance	< 10 Mbps	< 200 Mbps	> 200 Mbps
Key technologies			
<i>Dynamic Attack Detection™</i>	✓	✓	✓
<i>Dynamic Attack Response™</i>	✓	✓	✓
<i>Dynamic Attack Qualification™</i>	✓	✓	✓
<i>Accessible Device Protection™</i>	✓	✓	✓
<i>Vulnerable Device Protection™</i>	✓	✓	✓
Custom reporting	✓	✓	✓
Database	<i>Unlimited</i>	<i>Unlimited</i>	<i>Unlimited</i>
Rule updates	<i>Automated</i>	<i>Automated</i>	<i>Automated</i>
Enterprise functionality			
Multi-node manager		✓	✓
Centralized rule management		✓	✓
Centralized reporting		✓	✓
User permissions		✓	✓
Support			
Number of incidents	<i>3 incidents</i>	<i>Unlimited</i>	<i>Unlimited</i>
Training included	<i>None</i>	<i>Upon request/fee based</i>	<i>Upon request/fee based</i>
Hardware			
Optimized hardware appliance			✓
Optional hardware appliance	✓	✓	✓
Optional bypass unit	✓	✓	✓

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