Sidewinder G2 Security Appliance

Standing between you and the unknown

Consolidating all major Internet security functions in one system, the Sidewinder G2® Security Appliance from Secure Computing® is the strongest self-defending platform in the world. Built on a unique Zero-hour Attack Protections (ZAP™) technology, Sidewinder G2 defends your networks and applications from all types of Internet threats, both known and unknown. At the center of the Sidewinder G2 attack protections design are secure application pathways that allow your tightly defined and recognized traffic through at Gigabit speeds. Simultaneously, our self-defending ZAP technology has zero tolerance for all suspicious and undesirable traffic—including known threats before security patches or attack signatures are available or applied—providing you with essential 24x7 Application Defenses™ for your mission-critical operations.

A unified threat management (UTM) device as defined by IDC, Sidewinder G2 goes even further to include best-of-breed security so you gain greater manageability, more control, and stronger security than other UTM and firewall appliances provide. Sidewinder G2’s comprehensive yet flexible platform protects you instantly out of the box. It also allows you to customize and implement your security policy as you see fit using any or all of the protective features of Sidewinder G2, including over 200,000 known virus, spyware, and attack signatures, Web content filtering, and much more.

Our unique unequalled CERT advisory record and zero emergency security patches over the 11-year life of Sidewinder G2 sets us apart. Broadly deployed worldwide, the Sidewinder G2 Security Appliance is extensively used by all types of organizations from small to enterprise, and is the only security appliance to have achieved the pre- eminent EAL4+ common criteria certification for application firewalls.

The greatest challenge facing the security industry

In the first half of 2005, the average time between the disclosure of a software vulnerability and the release of an associated threat was only 6 days. On average, vendor patches are being released 54 days after a vulnerability disclosure. Most organizations require at least 30 days for routine execution of their patch management process and this opens large windows of vulnerability from unknown attacks. No one is immune.

Threats are increasingly able to spread at a frighteningly fast pace. In 2001, Code Red’s infection doubling time was about 37 minutes. In 2003, Slammer’s initial doubling rate was 8.5 seconds, on its way to infecting 90% of all susceptible hosts within 10 minutes. With the ubiquity of high-speed Internet services and evolving capabilities of attackers, “flash” threats (requiring just 30 seconds to fully spread) will soon be a reality, reducing the effectiveness of all reactive countermeasures essentially to zero. This is why the greatest challenge facing the security industry today is defending against the unknown attack before security patches or attack signatures are available or applied.

The Positive Security Model

Two defensive approaches against both known and unknown attacks exist today: The negative security model and the positive security model.

Negative security model countermeasures identify bits of traffic known to be threatening. Anti-virus and intrusion detection/prevention systems are classic examples, both of which depend upon checking traffic flows against attack signatures. With threats increasing at such a rapid pace, this results in less and less time to react to new attacks, and a steady increase of successful attacks over time.

Positive security model countermeasures understand and allow all legitimate, acceptable traffic requirements and deny everything else. This approach is highly effective at preventing unknown attacks and dramatically reduces an organization’s attack surface by automatically eliminating exposure to all sorts of attacks—unknown as well as known.

Positive-model security tools, which apply an in-depth knowledge of how a wide range of applications work, are what’s needed to face down today’s greatest security challenge (the unknown attack).

The Sidewinder G2 Security Appliance is such a leading-edge solution.
Our SecureOS operating system prevents root access and other attacks

Sidewinder G2 is built to defend itself from future unknown attacks. At its never-been-compromised core, the Sidewinder G2 Security Appliance runs on our high-speed, high-assurance SecureOS® operating system with patented Type Enforcement® technology.

Type Enforcement technology protects everything in the system; every file, every directory, every application, the hardware’s software drivers, the operating system, and more against the hacker’s dream—root access. This technology protects all software hosted on the appliance and prevents the installation of malicious software, buffer overflow attacks, and other known and unknown attacks. That’s why Sidewinder G2 has never required an emergency security patch in over 11 years on the market. In contrast to competitive security systems who have numerous emergency security patches and vulnerabilities as documented in CERT advisories.

Following our heritage of products that have achieved the highest certifications, Sidewinder G2 is ICSA certified and Common Criteria EAL4+ certified against the application firewall protection profile.

Zero-hour Attack Protections and Secure Application Pathways

Secure Computing’s Zero-hour Attack Protections technology is at the heart of the multi-layered defense-in-depth design of the Sidewinder G2 Security Appliance, the strength of which is its ability to face and defeat both known and unknown attacks. Sidewinder G2’s exclusive Zero-hour Attack Protections (ZAP™) technology kills zero-hour unknown attacks automatically by cleansing unknown elements out of the data stream. Just turn on Sidewinder G2’s gigabit-speed Secure Application Pathways for out-of-the-box Zero-hour Attack Protections.

Current estimates say about 80% of all new malware is focused on application-oriented vulnerabilities. Sidewinder G2’s advanced Secure Application Pathways tightly define allowed, legitimate use of Internet-facing applications. Each pathway can be defined according to the customer’s unique use of their applications, which forms the baseline against which all traffic is checked. Sidewinder G2’s unified threat management GUI makes tightening connections to ‘legitimate use only’ a straightforward point and click process.

Sidewinder G2 comes out-of-the-box with dozens of pre-built Secure Application Pathways to securely service and protect your application traffic requirements including Web, mail, Oracle SQL, Citrix remote access, streaming media, NetMeeting, FTP, and the like.

Signature-based Application Defenses™

Sidewinder G2 excels at stopping unknown attacks but also includes best-of-breed signature-based defenses for over 200,000 known attacks! Out-of-the-box, all signature-based services are tightly integrated into the appliance software. Just switch these services on to keep signatures updated automatically at the network perimeter to ensure that known threats do not leak inside the network.

What further sets Sidewinder G2’s signature-based security services apart is our commitment to offering only best-of-breed attack signature services from industry security leaders. Compare our best-of-breed solutions to many others who use open-source, poorly updated and maintained signature services.

Comprehensive defense-in-depth

Sidewinder G2 combines multiple technologies for a full defense-in-depth strategy, including:

- Sidewinder G2 anti-virus* and anti-spyware*
- Sidewinder G2 anti-spam* and anti-fraud*
- The world’s strongest firewall that’s never been compromised
- Multi-protocol content filtering, layer 3 to layer 7
- Application and stateful inspection firewall
- Zero-hour Attack Protections for unknown attacks
- Anomaly and behavior-based detection
- Virtual “black hole” technology repels attackers
- Hardware accelerated HTTPS/SSL termination*
- Advanced network cloaking techniques
- Secure DNS gateway services
- Both IPSec and clientless SSL* VPN services
- Outbound Web access controls with IM & P2P blocking; industry-leading SmartFilter® content protection*

*Add-on modules must be purchased separately.

Both clientless SSL and IPSec VPN remote access supported

Offering both IPSec and clientless SSL VPN solutions, Sidewinder G2 accommodates every type of virtual environment. IPSec is best suited for branch office connectivity. For an e-commerce environment, Sidewinder G2’s clientless SSL VPN offers simple, reliable, anywhere access to Web applications and Outlook mail, no thick client required. For strong two-factor authentication, Secure Computing’s SafeWord® solutions positively confirm user identity before extending remote access privileges to anyone.

Why IT professionals choose the Sidewinder G2 Security Appliance

Sidewinder G2’s underlying hardware and networking technology is designed to meet the rigorous requirements of today’s IT professionals. Pre-installed and pre-tuned for ease of installation, the Sidewinder G2 line of eight high-performance, rack-mounted appliance platforms provides an out-of-box security solution that drops seamlessly into any IP network. Its all-in-one consolidation of multiple security functions greatly reduces the number of point products the IT security manager must buy, deploy, learn, administer and update, from small remote offices to high-bandwidth offices.
Ultra-fast performance and high availability

The security appliance line of 8 models ranges from the model 110 (mini-1U platform), to our most powerful 5U model 4150. Multi-gigabit stateful inspection and next generation, parallel processing algorithms for secure application pathways offer gigabit throughput.

Active/Active appliances in a high-availability pair deliver the performance of two appliances performing as one, providing continuous operation 24 x 7 x 365. If you need even more power, the Sidewinder G2’s unique one-to-many cluster-management tools make scaling Zero-hour Attack Protections to multi-gigabit rates with rack-clusters as easy as managing a single appliance.

New updates are delivered to you automatically via the Internet. Sidewinder G2 authenticates, self-checks, and even self-installs upgrades for your system with just a single ‘click’ per your schedule.

Event monitoring, system management and regulatory compliance

The framework of a good security environment is its underlying policy. Sidewinder G2 facilitates the creation and administration of security policy through a variety of tools:

- Secure Windows-based graphical user interface protected with SSL or Secure SSH Telnet
- Sidewinder G2 Security Reporter (optional Windows-based central reporting solution for real-time event monitoring and reporting)
- Sidewinder G2 Enterprise Manager (optional SecureOS-based central management appliance)

Secure Computing’s Sidewinder G2 Security Appliance also meets the needs of government regulations, such as SOX, GLBA, and HIPAA. The Sidewinder G2 Security Reporter generates over 800 easy-to-understand reports, many of which are ideally suited to meet stringent regulatory requirements, including the following types of security events:

- Failed system-level and application-level login attempts
- Attempted exploitation of a system by a virus or worm or unauthorized individuals
- Failed access attempts to files or application data
- Correlating multiple system events to illicit data access

You can create and distribute policies, reuse policy objects, and modify rules for multiple security functions easily. Using the Sidewinder G2 Enterprise Manager, you can manage up to 500 appliances from a single console, making policy changes on hundreds of appliances instantly with ‘object substitution.’ Advanced central management features such as delegated administration, policy rollback, and policy adherence facilities are also included.

Operating at virtual wire speed over a Gigabit Ethernet

New updates are delivered to you automatically via the Internet. Sidewinder G2 authenticates, self-checks, and even self-installs upgrades for your system with just a single ‘click’ per your schedule.

Event monitoring, system management and regulatory compliance

The framework of a good security environment is its underlying policy. Sidewinder G2 facilitates the creation and administration of security policy through a variety of tools:

- Secure Windows-based graphical user interface protected with SSL or Secure SSH Telnet
- Sidewinder G2 Security Reporter (optional Windows-based central reporting solution for real-time event monitoring and reporting)
- Sidewinder G2 Enterprise Manager (optional SecureOS-based central management appliance)

Secure Computing’s Sidewinder G2 Security Appliance also meets the needs of government regulations, such as SOX, GLBA, and HIPAA. The Sidewinder G2 Security Reporter generates over 800 easy-to-understand reports, many of which are ideally suited to meet stringent regulatory requirements, including the following types of security events:

- Failed system-level and application-level login attempts
- Attempted exploitation of a system by a virus or worm or unauthorized individuals
- Failed access attempts to files or application data
- Correlating multiple system events to illicit data access

You can create and distribute policies, reuse policy objects, and modify rules for multiple security functions easily. Using the Sidewinder G2 Enterprise Manager, you can manage up to 500 appliances from a single console, making policy changes on hundreds of appliances instantly with ‘object substitution.’ Advanced central management features such as delegated administration, policy rollback, and policy adherence facilities are also included.

IPSec VPN compatibility

- IPSec and IKE protocol compliance verified through ICSA certification
- Extended IKE Authentication (XAUTH) Version 6.0
- X.509 version 3 certificates
- Simple Certificate Enrollment Protocol (SCEP)
- Support for Baltimore, Entrust, Verisign, Netscape, and Microsoft certificates
- Tunnel or transport mode security AES, DES, Triple-DES, MD5, SHA-1 algorithms, and CAST
- PKCS #7, #10, and #12
- FIPS PUB 46-3
- FIPS PUB 140-1
- FIPS PUB 140-2
- FIPS PUB 180-1

Administration system requirements

- OS - MS Windows 2000 or XP
- CPU - Intel (1 GHz minimum)
- Memory - 512 MB minimum
- Drives - 300 MB of available disk space, 3.5” 1.44 MB floppy disk drive, CD-ROM drive
- Monitor - 1024 x 768 or higher
- Network interface card - access to your firewall network
- Browser - Internet Explorer 4 or later; Netscape 4.x or later

Model 110 & 210 - Mini 1U platform
Model 410 & 510 - small 1U platform
Model 1100 - enterprise 1U platform
Model 2100 & 2150 - 2U platform
Model 4150 - 5U platform

Real-time attack monitoring dashboard
### Performance

<table>
<thead>
<tr>
<th>Highlight</th>
<th>Power supply</th>
<th>Max. # of concurrent connections</th>
<th>Concurrent connections</th>
<th>IPSec VPN throughput</th>
<th>Concurrent connections</th>
<th>Signature-based Application Defenses (SAP)</th>
<th>Performance upgrades</th>
<th>Max. # of concurrent connections</th>
<th>Concurrent connections</th>
<th>Performance upgrades</th>
<th>Signature-based Application Defenses (SAP)</th>
<th>Concurrent connections</th>
<th>Performance upgrades</th>
<th>Signature-based Application Defenses (SAP)</th>
<th>Concurrent connections</th>
<th>Performance upgrades</th>
<th>Signature-based Application Defenses (SAP)</th>
<th>Concurrent connections</th>
<th>Performance upgrades</th>
<th>Signature-based Application Defenses (SAP)</th>
<th>Concurrent connections</th>
<th>Performance upgrades</th>
<th>Signature-based Application Defenses (SAP)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Next-business-day, onsite parts replacement warranty included with models 410, 510, 1100, 2100, and 2150. Advanced replacement hardware warranty included with models 410, 510, and 1100.</td>
<td>RAID 5</td>
<td>2</td>
<td>2</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td></td>
</tr>
<tr>
<td>Advanced replacement hardware warranty included with models 410, 510, and 1100.</td>
<td>RAID 5</td>
<td>2</td>
<td>2</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td></td>
</tr>
<tr>
<td>High-speed operating system with patented Type Enforcement technology.</td>
<td>RAID 5</td>
<td>2</td>
<td>2</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td></td>
</tr>
<tr>
<td>High-speed operating system with patented Type Enforcement technology.</td>
<td>RAID 5</td>
<td>2</td>
<td>2</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td></td>
</tr>
<tr>
<td>Firewall, 24 x 7 live monitoring and reporting.</td>
<td>RAID 5</td>
<td>2</td>
<td>2</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td></td>
</tr>
<tr>
<td>SecureOS™, Self-Defending Platform</td>
<td>RAID 5</td>
<td>2</td>
<td>2</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td></td>
</tr>
<tr>
<td>High-speed operating system with patented Type Enforcement technology.</td>
<td>RAID 5</td>
<td>2</td>
<td>2</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td></td>
</tr>
<tr>
<td>FireWall, 24 x 7 live monitoring and reporting.</td>
<td>RAID 5</td>
<td>2</td>
<td>2</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td></td>
</tr>
<tr>
<td>SecureOS™, Self-Defending Platform</td>
<td>RAID 5</td>
<td>2</td>
<td>2</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td></td>
</tr>
<tr>
<td>High-speed operating system with patented Type Enforcement technology.</td>
<td>RAID 5</td>
<td>2</td>
<td>2</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td></td>
</tr>
<tr>
<td>Firewall, 24 x 7 live monitoring and reporting.</td>
<td>RAID 5</td>
<td>2</td>
<td>2</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td></td>
</tr>
</tbody>
</table>

### Highlights

- Three-year warranty included with models 410, 510, 1100, 2100, and 2150.
- Advanced replacement hardware warranty included with models 410, 510, and 1100.
- High-speed operating system with patented Type Enforcement technology.
- Firewall, 24 x 7 live monitoring and reporting.
- SecureOS™, Self-Defending Platform.
- High-speed operating system with patented Type Enforcement technology.
- Firewall, 24 x 7 live monitoring and reporting.
- SecureOS™, Self-Defending Platform.
- High-speed operating system with patented Type Enforcement technology.