Sécuriser les applications liées à la Convergence (SIP) et la messagerie

Garantir la confidentialité et assurer la conformité aux réglementations

Focus sur SIP pour l’OSSIR (Groupe SUR)
A proven market leader

- Founded in 1993, headquartered in Toronto, Canada
- 8,000 Customers in 65 countries
- 500 Channel Partners
- Leading Alliance Partners
- Continuous innovation & vision
- Multiple EAL4+ certifications
- Security, Privacy & Compliance
<table>
<thead>
<tr>
<th>Product/Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>S-Core™ Operating System</td>
<td>UNIX-based hardened operating system that has never been breached</td>
</tr>
<tr>
<td>BorderWare Security Network (BSN)</td>
<td>Proactive gathering global data from over 8,000 customers and multiple protocols for real-time threat prevention &amp; behavioral analysis</td>
</tr>
<tr>
<td>SIPassure - First SIP application firewall</td>
<td>Only security company to offer application security for VoIP, IM, Video Conferencing and other converging applications</td>
</tr>
<tr>
<td>MXtreme Intercept™ Engine</td>
<td>Blocks 98% of unwanted inbound email by detecting and blocking in real-time</td>
</tr>
<tr>
<td>MXtreme Privacy &amp; Compliance Engine</td>
<td>Unprecedented granular content management integrated with secure content delivery and archiving integration capabilities</td>
</tr>
<tr>
<td>Infinity - Unified Messaging Security Platform</td>
<td>First truly converged security platform, securing Web, FTP, email, Instant Messaging &amp; blogs with single Management system &amp; Policy</td>
</tr>
<tr>
<td>EAL4+ certification</td>
<td>Passed through several EAL4+ certification processes - Highest level of 3rd party certification for network security devices</td>
</tr>
</tbody>
</table>
IP applications are converging – New challenges
BorderWare portfolio of solutions

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>BSN</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SIPassure</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Infinity</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MXtreme</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SteelGate</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>S-Core</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

EAL4+ Certified Operating System
Recognition

BorderWare named Hot Company by Info Security
Selected from more than 600 info security vendors around the world, this prestigious honor comes to BorderWare based upon the company’s market success and a stern selection criteria of 4Ps - Products, People, Performance and Potential.

MXtreme Named Best Email Security Product
MXtreme beat out competitive solutions from Ironport, Barracuda Networks & Symantec during an in-depth bakeoff held by Swedish IDG Publication, Nätverk & Kommunikation. MXtreme received top marks for its anti-spam accuracy, effectiveness and general ease of administration.

BorderWare wins "Innovation Driver" Award @ Security Zone 2005
A panel of judges reviewed applicants for innovation and for applicability to solving real-world problems. Eight winners were selected including Borderware’s SIPassure™ SIP Firewall.

BorderWare wins "Fierce 15 VoIP" Honor
This distinction honors BorderWare as one of the top 15 emerging VoIP companies in 2005 for its leadership role in securing VoIP and for the release of SIPassure™, the first Session Initiation Protocol (SIP)-based turn-key security platform.

EAL4+ Certified

VoIP Magazine Top 20 Companies to Watch in 2006
The VoIP Magazine 20 features the companies that are best positioned in the coming year to spur IP communications adoption and innovation while, at the same time, delivering on the immediate needs of the marketplace. This distinction honors BorderWare for its leadership role in securing VoIP and for the release of SIPassure™, the first Session Initiation Protocol (SIP)-based firewall.

BorderWare named to Deloitte & Touche Fast 50 "Companies To Watch"
The Deloitte Fast 50 is a prestigious annual awards program honouring technology companies that rally behind innovation, break down obstacles and systematically defy the odds.

MXtreme Named "Anti-Spam E-mail protection Product of the Year"
An independent panel of judges chose MXtreme for its outstanding anti spam capabilities, comprehensive protection against other threats to email and overall assurance of security with a certification of Common Criteria EAL4+.

"The holy grail for a security manager is a centralised mechanism to address all the threats as they change, protect customer data and finally to demonstrate compliance to all the regulatory authorities”
John Pescatore - VP, Distinguished Analyst, Gartner

Best in tests!
BorderWare World Class Customers’ sample (1)
PostX is the leading provider of secure messaging and delivery for enterprises with the largest customer deployments and most diverse solution-lines in the secure email and messaging industry. PostX solves several critical business applications, including compliance, document delivery, and interactive customer relations, with one single Messaging Application Platform. PostX has been granted several patents for its secure delivery, platform, and authentication techniques.

McAfee, Inc., headquartered in Santa Clara, Calif., and the global leader in Intrusion Prevention and Security Risk Management, delivers proactive and proven solutions and services that secure systems and networks around the world.

Ubiquity Software Corporation plc develops and markets SIP-based communications software to service providers, ISVs and OEMs around the world. Its award-winning SIP Application Server (SIP A/S) is both a carrier-class deployment platform and a programmable, standards-based application creation environment (ACE) that allows customers to develop and deploy next-generation converged communications services.

FaceTime Communications is the leading provider of solutions enabling businesses to secure, manage and extend the use of instant messaging (IM) and real-time communications in the enterprise.

Sun can be found in more than 100 countries and on the World Wide Web. Sun's iForce Mail Firewall is powered by BorderWare Technology.

Brightmail currently serves many of the largest service providers, including AT&T WorldNet, EarthLink, MSN, Verizon Online, as well as a number of Global 2000 corporations. BorderWare offers Symantec/Brightmail Anti-Spam as an optional add-on to the MXtreme Mail Firewall.

BorderWare is a member of the Cisco AVVID Partner Program as a Security and VPN member. The Cisco AVVID Partner Program sets criteria for interoperability testing by independent third parties and enables leading product and services firms to deploy innovative business solutions.

F5 Networks keeps IP-based traffic flowing and business information always available to any user from any device, anywhere in the world.

Kaspersky Labs is an international software-development company offering advanced products for protection against viruses, hackers and spam.

SurfControl filtering is available for BorderWare's Firewall Server and SteelGate Firewall & VPN Appliance.

Cryoserver is the world's leading forensic archiving and compliance solution for email, instant messaging and other electronic records. Enterprises, businesses and governments rely on Cryoserver for assurance surrounding the retention and access of critical business, operational and publicly held information.

Research In Motion (RIM) is a leading designer, manufacturer and marketer of innovative wireless solutions for the worldwide mobile communications market.

PGP Alliance Partners are top-tier, security-oriented software and hardware vendors with products that are either integrated with or highly complementary to PGP product offerings.
Borderware Integrated Security Architecture

- Messaging Applications: VoIP, Video, Instant Messaging, Email, Web
- Shared Administration tools: Reporting, Management, Policy control
- Shared Platform Services: BorderWare Security Network, Clustering, Fail-Over, Archiving / Encryption I/F

BorderWare S-Core hardened Operating System
SIPassure Firewall
Security for VoIP and other SIP services

Ingmar Schraub
International SIP Expert
Demonstration

VoIP Applications and Protocols

- VoIP applications use a mix of standards based and proprietary protocols including:
  - H.323 Legacy protocol used in Microsoft’s NetMeeting and in some commercial VoIP products
  - Skinny, Cisco proprietary protocol, used by Call Manager
  - Skype, proprietary protocol designed to use a number of transports to find a way through Firewalls
  - Session Initiation Protocol, emerging as the Internet Standard
    - Implemented in new products
    - Implemented in virtually all legacy products for interoperability
    - Scope is much wider than VoIP
What role does SIP Play

- SIP is responsible primarily for session control
  - Device registration,
  - Call setup
  - Call termination
  - Advanced features such as call transfer

- VoIP and Video conferencing use other protocols for call data, typically RTP (real-time transport protocol)

- Call data parameters negotiated via SDP (Session Description Protocol)

- Instant Messaging and related services use SIP directly for message transfer
SIP Protocol Details

- Text based protocol, similar to Web (HTTP) and Email (SMTP) protocols
- Shares many of the same security risks and vulnerabilities
- Easy to monitor/spoof

```
REGISTER sip:sip.borderware.co.uk SIP/2.0
Via: SIP/2.0/UDP 192.168.19.12:5060;branch=z9hG4bK927ec13a8c04928
Max-Forwards: 70
To: <sip:johnsmith0@borderware.co.uk>
From: <sip:johnsmith0@borderware.co.uk>;tag=9600645
Call-ID: 1d21@192.168.19.12
Cseq: 20482 REGISTER
Contact: <sip:johnsmith0@192.168.19.12>
User-Agent: SIP desktop phone
Content-Length: 0
```
SIP Security Risks and Attacks (1)

- SPAM and its variants
  - Spam over Instant Messaging (SPIM)
  - Spam over Internet Telephony (SPIT)
- SIP does not automatically verify origin of messages
- Easy to fake source and send unsolicited calls/messages
  - Highly disruptive, imagine a voice mailbox full of Spam
  - Conventional filtering techniques don’t apply
  - VoIP messages carried via RTP as an audio or audio/video stream
SIP Security Risks and Attacks (2)

- Denial of Service Attacks
  - Call flooding (attacker hangs up on answer)
  - De-registration attacks (device can’t receive calls)
  - Call termination by 3rd party
- Attacks possible because of
  - Optional authentication service
  - No automatic message verification

REGISTER sip:borderware.co.uk SIP/2.0
Expires: 3600

REGISTER sip:borderware.co.uk SIP/2.0
Expires: 0
SIP Security Risks and Attacks (3)

- All Internet connected application servers face a common set of threats
- Network level attacks
  - Malformed packet attacks
  - Syn floods
  - Ping of death
  - Etc.
- Buffer Overflow attacks
  - Every other application server hides buffer overflow vulnerabilities
  - SIP is no different!
## SIP Security Requirements

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAT Traversal Services:</td>
<td>Needed to enable SIP applications to pass through perimeter Firewalls</td>
</tr>
<tr>
<td>Firewall Grade Perimeter Security:</td>
<td>Needed to protect VoIP application servers against Internet attacks</td>
</tr>
<tr>
<td>Network Level Threat Protection:</td>
<td>Needed to defend against malformed packet attacks, connection floods etc</td>
</tr>
<tr>
<td>Application Level Security:</td>
<td>Needed to protect against VoIP and SIP specific attacks (e.g. Spam, Denial of service attacks)</td>
</tr>
<tr>
<td>Stack and buffer overflow protection:</td>
<td>Required to prevent exploit of any latent vulnerability in SIP applications</td>
</tr>
<tr>
<td>Content Filtering:</td>
<td>Needed to enforce corporate usage policy</td>
</tr>
</tbody>
</table>
VoIP Security Options

- SIP enabled Firewalls
  - Provide NAT Traversal services
  - Provide good perimeter security
  - Lack in-depth application level protection
  - Lack stack and buffer overflow protection
  - Lack Content Filtering

- Session Border Controllers
  - Provide NAT Traversal services
  - Moderate Perimeter security
  - Limited application level protection
  - Lack stack and buffer overflow protection
  - Limited Content Filtering
SIPassure – Specialist SIP application level Firewall

- Combines the best of SIP enabled Firewalls and SBCs
- Offers incremental features
  - In-depth application level protection
  - Stack and buffer overflow protection
  - Content Filtering
  - Policy control

Email and web warrant their own dedicated security products

VoIP services are more complex than either
# Technology Comparison

<table>
<thead>
<tr>
<th>Feature</th>
<th>SIP enabled Firewalls</th>
<th>Session Border Controllers</th>
<th>SIPassure</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAT Traversal</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Far-end NAT Traversal</td>
<td>Limited</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Firewall enabling</td>
<td>N/A</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Firewall Grade Perimeter Security</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>Network Level threat protection</td>
<td>✓</td>
<td>Limited</td>
<td>✓</td>
</tr>
<tr>
<td>Application Level security</td>
<td>✗</td>
<td>Limited</td>
<td>✓</td>
</tr>
<tr>
<td>Stack and buffer overflow protection</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>Content Filtering</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>Policy Control</td>
<td>✗</td>
<td>Limited</td>
<td>✓</td>
</tr>
</tbody>
</table>
SIPassure Enterprise Deployment

- SIPassure Appliance deployed in conjunction with exiting Firewall
- Handles calls to/from external SIP users
- Single or multiple appliances depending on volume and resilience requirements
SIPassure Service Provider Deployment

- SIPassure Appliance deployed in conjunction with exiting Firewall
- Handles calls to/from external SIP users and/or SP customers
- Multiple appliances for resilience and volume needs
SIPassure Demo Configuration

Internet

SIPassure

SIP User Agents
(soft phones/SIP phones)

IP PBX
Asterisk/Linux

SIP Trunk (optional)

PSTN Gateway (optional)

PSTN

Internet Communications Made Safe™
Compléments:

Sébastien Bonnotte
Directeur Europe du Sud
BorderWare Technologies
Tel : + 33 689 080 595
Email : sbonnotte@borderware.com
Web : www.borderware.com

*** Sécurisez aisément vos applications convergentes: Web, FTP, email, Messagerie Instantanée, VoIP et autres applications métier ***

Demandez une évaluation gratuite sur http://www.borderware.com/fr/eval
Découvrez la démonstration de SIPassure sur

Ingmar Schraub, International SIP Expert
ingmar@borderware.com