Web Intelligence
Protection for the entire Web environment

YOUR CHALLENGE
One fact of life is very clear—businesses increasingly rely on the Internet. Legacy client-server applications once only available on the corporate LAN are now accessible on the Web. However, rapid adoption of the Internet, intranets, and extranets also increases the risk of exposing mission-critical data to attackers and other unauthorized visitors.

A complete Web environment includes the network, operating systems, Web servers, and backend systems. Many software applications built for the Web have not been designed with security as a priority. As a result, Web applications often include security flaws ranging from Unicode decoding to various forms of buffer overflows. Hackers continually arm themselves with innovative ways to exploit vulnerable parts of the Web environment. So as Web applications become more popular, they have become a primary target of attackers.

Even as organizations struggle to find solutions to protect their Web investments and valuable data, they find the majority of today’s solutions ineffective. At best, they provide a partial solution—none can provide a complete solution—to protect the entire Web environment.

OUR SOLUTION
Web Intelligence™ is the only Web application firewall technology to provide complete protection for the entire Web environment. Check Point gateways such as VPN-1® Power, VPN-1 UTM, UTM-1, and Connectra™ are equipped with Stateful Inspection, Application Intelligence™, and Web Intelligence™ technologies to provide a multi-layer defense for the network, operating systems, Web servers, and backend systems. Web Intelligence is supported by SmartDefense™ Services, which protect against new threats by providing real-time defense updates and configuration advisories.

PRODUCT DESCRIPTION
Web Intelligence™ is a set of advanced capabilities that detects and prevents attacks against the Web infrastructure. It provides comprehensive protection when using the Web for business and communication.

PRODUCT FEATURES
- Malicious Code Protector™
- Advanced streaming inspection
- Simple deployment and management
- Seamless integration with Check Point products

PRODUCT BENEFITS
- Establishes strongest protection against buffer-overflow attacks
- Offers application-level Web security at wire-speed
- Improves end-user experience by inserting helpdesk Web pages
- Provides quick deployment for mission-critical applications
- Protects against new threats through SmartDefense™ Services

Each layer of a Web infrastructure has multiple vulnerabilities.
WEB INTELLIGENCE FEATURES

Malicious Code Protector

Check Point’s patent-pending Malicious Code Protector™ offers a revolutionary way of identifying buffer overflow, heap overflows, and other malicious executable code attacks that target Web servers and other applications without the need of signatures. It offers another strong layer of protection on top of Check Point’s existing Application Intelligence. Malicious Code Protector can detect malicious executable code within Web communications by identifying not only its existence within a data stream but its potential for malicious behavior.

Malicious Code Protector performs four important actions:

- Monitors Web communication for potential executable code
- Confirms the presence of executable code
- Identifies whether the executable code is malicious
- Blocks malicious executable code from reaching a target host

Malicious Code Protector identifies both known and unknown attacks, offering preemptive attack protection. Recent experimental lab testing confirmed it operates at the highest degree of accuracy with a very low rate of false positives. Moreover, this level of protection does not come at the price of performance degradation because Malicious Code Protector is offered at the kernel level, delivering wire-speed throughput.

Advanced streaming inspection

Advanced Streaming Inspection is a Check Point kernel-based technology that processes the overall context of communication. As with Stateful Inspection and Application Intelligence, Advanced Streaming Inspection is based upon Check Point’s INSPECT™ engine. This technology can make real-time security decisions based on session and application information. And it allows Web Intelligence to understand Web communication even when it spans multiple TCP segments. Starting in Web Intelligence, process-intensive application inspections are now offloaded to the kernel level, dramatically improving throughput and connection rates.

Protection on the fly

Advanced Streaming Inspection introduces Active Streaming in Web Intelligence, with the capability to modify content of a Web connection on the fly. This important capability offers several unique advantages to Check Point customers.

Active Streaming introduces HTTP-header-spoofing capability, providing a first level of defense by hiding important site-specific properties about the Web environment. These properties often include the names and versions of operating systems and identities of Web servers and backend servers. This information is typically useless to end users, but extremely valuable to attackers who are trying to gather information about their target. Web Intelligence can intercept a Web response that contains a server’s identity and gives the administrator the option to either completely hide such disclosure or optionally change the stream to confuse attackers.

Enhanced usability

Administrators can improve the end-user experience with Active Streaming by predefining custom error pages. To most users, generic error status codes are meaningless. Active Streaming redirects the end user to a custom-defined error page with meaningful helpdesk hints. This feature dramatically improves the end-user experience and reduces helpdesk costs.

Web Intelligence Performance*

Throughput: 1.9 Gbps
Connections rate: 8,300 HTTP connections/sec

*Performance measured with default Web Intelligence settings.
Protection for the entire Web environment

Simple deployment and management
The management of Web Intelligence within VPN-1 and UTM-1 is fully integrated into the SmartCenter™ security management GUI. This user interface is preconfigured with protections to counter known common attacks—each with attack and defense descriptions. As shown in the screenshot on the above right, “Web Server View” is the command center for all Web servers within the enterprise, which offers a summary of types of protections applied to various servers. Because each Web application server is different from others in its security requirements, Web Intelligence offers the capability to configure granular security for different Web applications and Web servers. First-time configuration of Web Intelligence takes just minutes.

Web Intelligence also introduces Monitor-only mode, allowing smooth security deployment without the risk of rejecting connections to a mission-critical application due to misconfiguration of a security policy.

Seamless integration with Check Point products
Due to its tight integration with VPN-1 Power, VPN-1 UTM, UTM-1, and Connexta gateways, Web Intelligence does not require installation on additional devices. For VPN-1 and UTM-1, Web Intelligence is managed by the award-winning SmartCenter. This means there is little learning effort for administrators already familiar with the user interface. Security and audit logs are integrated with the rest of VPN-1 and UTM-1 security logs, providing administrators a powerful tool to centrally analyze any security violation.

Integration with SmartCenter also provides full, rich, enterprise-level reporting, auditing, and real-time monitoring capabilities. Web Intelligence is supported by SmartDefense Services, which maintain the most current preemptive security for the Check Point security infrastructure. To help you stay ahead of new threats and attacks, SmartDefense Services provide real-time updates and configuration advisories for defenses and security policies.

Logs of Web Intelligence are integrated with SmartCenter.
**WEB PROTECTIONS**

Malicious code
- Malicious Code Protector™
- General HTTP Worm Catcher

Application layer
- Cross Site Scripting protection
- LDAP Injection protection
- SQL Injection protection
- Command Injection protection
- Directory Traversal protection

Information disclosure
- Header Spoofing enforcement
- Directory Listing prevention
- Error concealment

HTTP Protocol inspection
- HTTP Format Size enforcement
- ASCII-only Request enforcement
- ASCII-only Response Header enforcement
- Header Rejection definitions
- HTTP Method enforcement

**ENFORCEMENT OPTIONS**

Active
- Block and track
- Block, track, and send HTML error page

Monitor-only mode

Disabled

**CONFIGURATION GRANULARITY**

Individual servers protected by Web Intelligence

Attack protections enabled for each server

For each attack protection, apply to individual servers or inspect all HTTP traffic

Customizable SmartDefense profiles associated with specific Check Point gateways

**REAL-TIME SAFEGUARD AND DEFENSE UPDATES**

SmartDefense™ Services subscription

**LICENSE REQUIREMENTS**

Web Intelligence licensed on a per gateway basis (based on number of servers protected by Web Intelligence: three, 10, or unlimited)

**SYSTEM REQUIREMENTS**

Web Intelligence shares the same system and configuration requirements as the related Check Point gateways:

- Supported gateway versions: R55W or R60 or higher
- Supported enforcement points
  - FireWall-1®
  - VPN-1® Power™
  - VPN-1 UTM
  - UTM-1
  - Connectra™ (Web Intelligence included with purchase)

Web Intelligence can be managed using SmartCenter™ Power or SmartCenter UTM™

---

**March 7, 2007**
P/N 502431

©2003–2007 Check Point Software Technologies Ltd. All rights reserved. Check Point, AlertAdvisor, Application Intelligence, Check Point Express, Check Point Express CI, the Check Point logo, ClusterXL, Confidence Indexing, ConnectControl, Connectra, Connectra Accelerator Card, Cooperative Enforcement, Cooperative Security Alliance, CoSa, DefenseNet, Dynamic Shielding Architecture, Eventia, Eventia Analyzer, Eventia Reporter, Eventia Suite, FireWall-1, FireWall-1 GX, FireWall-1 SecureServer, FloodGate-1, Hacker ID, Hybrid Detection Engine, IMsecure, INSPECT, INSPECT XI, Integrity, Integrity Clientless Security, Integrity SecureClient, InterSpect, IPS-1, IQ Engine, MailSafe, NG, NGX, Open Security Extension, OPSEc, OSFirewall, Policy Lifecycle Management, Provider-1, Safe@Home, Safe@Office, SecureClient, SecureClient Mobile, SecureKnowledge, SecurePlatform, SecurePlatform Pro, SecureRemote, SecureServer, SecureUpdate, SecureXL, SecureXL Turbocard, Sentivist, SiteManager-1, SmartCenter, SmartCenter Express, SmartCenter Power, SmartCenter Pro, SmartCenter UTM, SmartConsole, SmartDashboard, SmartDefense, SmartDefense Advisor, Smarter Security, SmartLSM, SmartMap, SmartPortal, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartViewTracker, SofaWare, SSL, SSL Network Extender, Stateful Clustering, TrueVector, Turbocard, UAM, UserAuthority, User-to-Address Mapping, VPN-1, VPN-1 Accelerator Card, VPN-1 Edge, VPN-1 Express, VPN-1 Express CI, VPN-1 Power, VPN-1 Power VSX, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecureRemote, VPN-1 SecureServer, VPN-1 UTM, VPN-1 UTM Edge, VPN-1 VSA, Web Intelligence, ZoneAlarm, ZoneAlarm Anti-Spyware, ZoneAlarm Antivirus, ZoneAlarm Internet Security Suite, ZoneAlarm Pro, ZoneAlarm Secure Wireless Router, Zone Labs, and the Zone Labs logo are trademarks or registered trademarks of Check Point Software Technologies Ltd. or its affiliates. ZoneAlarm is a Check Point Software Technologies, Inc. Company. All other product names mentioned herein are trademarks or registered trademarks of their respective owners. The products described in this document are protected by U.S. Patent No. 5,606,668, 5,835,726, 6,496,935, 6,873,988, and 6,850,943 and may be protected by other U.S. Patents, foreign patents, or pending applications.