IBM Protocol Analysis Module

The protection engine inside the IBM Security Intrusion Prevention System technologies.

Highlights

- Stops threats before they impact your network and the assets on your network such as servers, desktops and network infrastructure.
- Protects end users against exploits hidden in applications used everyday such as document formats, spreadsheets, presentations, multimedia files and web browsers.
- Modular extensible framework that allows the addition of new security technology and functionality as threats evolve.

Staying ahead of the threat—stopping Internet threats before they impact your business.

The IBM Security Intrusion Prevention System (IPS) technologies stop Internet threats before they impact your business. The basis for our unique form of security lies in our engine, the IBM Protocol Analysis Module (PAM), which enables preemptive protection against a wide variety of Internet threats. PAM is built upon years of security intelligence gathered by the IBM X-Force® research and development team. The X-Force is a world-renowned security research organization dedicated to proactive examination of threats and the underlying software vulnerabilities they seek to exploit.

With its modular extensible framework, PAM is constantly evolving to block your most challenging security threats, eliminating the need to purchase additional point solutions. Backed by the world-renowned IBM X-Force research and development team, PAM is regularly—and automatically—infused with new security intelligence to keep you ahead of the latest threats. Other solutions can only hope to match individual protection signatures with exploits—a process that is too slow to stop evolving threats and results in higher rates of false positives and false negatives.

IBM Protocol Analysis Modular Technology

IBM Protocol Analysis Modular Technology	What It Does:
Virtual Patch	Shields vulnerabilities from exploitation independent of a software patch and provides the security you need to eliminate the patching fire drills for new threats. Critical systems should still be patched, but now you can execute your own tested processes for patch management. If your patch management process doesn't live up to best practices, IBM can help integrate endpoint management into a holistic approach to security that includes network, servers and clients.
Client-side Application Protection	Protects end users against attacks targeting applications used everyday such as Microsoft Office files, Adobe PDF files Multimedia files and Web browsers.
Web Application Protection	Protects web servers against sophisticated application-level attacks such as SQL Injection, XSS (Cross-site scripting), PHP file-includes, CSRF (Cross-site request forgery).
Threat Detection and Prevention	Detects and prevents entire classes of threats as opposed to a specific exploit or vulnerability.
Data Security	Monitors and identifies unencrypted personally identifiable information (PII) and other confidential information for data awareness. Also provides capability to explore data flow through the network to help determine if any potential risks exist.
Application Control	Manages control of unauthorized applications and risks within defined segments of the network, such as ActiveX fingerprinting, Peer To Peer, Instant Messaging, and tunneling.

PAM has the ability to monitor, detect or prevent the following classes of network threats:

Classes of Threats	Monitor	Detect	Prevent
Application Attacks	✓	✓	✓
Attack obfuscation	✓	✓	✓
Buffer overflow attacks	✓	✓	✓
Cross-site scripting attacks	✓	✓	✓
Data leakage	✓	✓	✓
Database attacks	✓	✓	✓
DoS and DDoS attacks	✓	✓	✓
Drive-by downloads	✓	✓	✓
Insider threats	✓	✓	✓
Instant messaging	✓	✓	✓
Malicious document types	✓	✓	✓
Malicious media files	✓	✓	✓
Operating system attacks	✓	✓	✓
Peer to peer	✓	✓	✓
Protocol tunneling	✓	✓	✓
SQL injection attacks	✓	✓	✓
Web browser attacks	✓	✓	✓
Web server attacks	✓	✓	✓

In order to address these attack categories, PAM employs multiple intrusion prevention technologies working in tandem, including:

- *Port assignment*
- *Port following*
- *Protocol analysis*
- *Protocol tunneling*
- *Pattern matching*
- *Content Analysis*
- *Injection Logic Engine*
- *Shellcode Heuristics*
- *RFC compliance checking*
- *TCP reassembly*
- *Flow assembly*

Primary network threats stopped by the IBM Protocol Analysis Module

While Internet threats continue to evolve, older attack methods cannot be discounted and many attackers build upon known intrusion techniques to evade detection. The IBM Protocol Analysis Module is dedicated to stopping the following list of Internet threats:

Internet Attack Types	What Makes It Dangerous	PAM Module That Stops It
Backdoors	Provides system entry points that bypass traditional login verification.	Threat Detection and Prevention
Botnets	Collections of compromised computers that perform tasks at the behest of a controller—usually with malicious intent to spread spam and/or malware.	Threat Detection and Prevention
Client Side Attacks	Exploits affecting the operating system or applications running on personal computers. Exploits could target e-mail clients, Web browsers, document viewers, and multimedia applications.	Client Side Application Protection
Cross-site scripting	A Web-based exploit used to embed malicious code into a supposedly legitimate link that can execute on a user's computer, typically in an attempt to steal information.	Web Application Protection
Distributed Denial of service (DDoS)	Utilizes a multitude of compromised systems to attack a single target with a flood of messages to shut the target system down	Threat Detection and Prevention

Internet Attack Types	What Makes It Dangerous	PAM Module That Stops It
Insider threats	Internal users can introduce viruses, worms and Trojans into a network, or attempt to steal proprietary data	Threat Detection and Prevention
Instant Messaging	Can be used to introduce Trojans, viruses and other malware into the network.	Application Control
Malicious content	Malicious multimedia and shell code attackers embed in documents.	Client Side Application Protection
Malicious e-mail	A common carrier for spyware and phishing scams that entice users to visit malicious Web sites, and then potentially introduce malware to the network.	Client Side Application Protection
Peer to Peer (P2P) networks	Facilitates the transfer of files infected with Trojans and viruses designed to introduce denial of service attacks and corrupt data.	Application Control
Protocol tunneling	Layers malicious data usually within a higher level protocol, allowing it to traverse network segments where lower level protocols might be blocked.	Application Control
Reconnaissance	A collection of threats including brute force, enumeration, password guessing and port scans	Threat Detection and Prevention
Root kits	A collection of tools or programs that provide hackers with administrator level privileges or root access to a network or system.	Threat Detection and Prevention
Spam	Unsolicited email usually sent in bulk messages across the Internet.	Client Side Application Protection
Spear Phishing	A carefully crafted attack targeting high value targets with the purpose of stealing confidential information.	Data Security
SQL injection	Piggybacks malicious SQL code on intended commands through the dynamic logic layer of a Web application in order to trick the application into providing database access	Web Application Protection
Trojans	Harbor dangerous code inside apparently harmless programming or data.	Threat Detection and Prevention
Worms	Virus that self-replicates by resending itself as an e-mail attachment or part of a network message.	Threat Detection and Prevention
Zero Day Attacks	Threats that attempt to exploit undisclosed vulnerabilities before software vendors are able to provide a patch.	Virtual Patch

Multilayered prevention technologies within the IBM Protocol Analysis Module

PAM combines the power of multiple threat prevention technologies—all working in concert to stop Internet threats. PAM utilizes the following attack prevention methods:

Attack Prevention Methods	What It Means	PAM Module That Supports It
Browser Exploit Prevention	Prevents attacks to Web browsers using JavaScript™ obfuscation.	Client Side Application Protection
Content Analysis	Inspects and blocks unencrypted data in your network using predefined and custom signatures. This technology provides the ability to create compound data-set search inspections and inspect compound documents including Microsoft® Office documents, PDFs, Zip files and over 10 different protocols.	Data Security
Flow Assembly	Analyzes the entire network connection—not just the individual packets—to block malicious traffic that may have been inserted into the communication stream to take advantage of an open connection. Flow assembly complements TCP reassembly by analyzing traffic at a higher level to prevent advanced threats.	Threat Detection and Prevention
Injection Logic Engine	Heuristically identifies malicious injection attempts such as SQL injection and shell command injection. Covers current and future vulnerabilities without signature updates.	Web application Protection
Port Assignment	IPS should not assume that a particular type of traffic will appear on a particular TCP/IP port. If they do and the traffic type matches the assumed port, and is allowed through, attackers could gain access. IBM Security IPS products inspect all traffic regardless of the port that traffic is destined to.	Virtual Patch
Port Following	Tracks communication sessions to ensure that the port initially used to establish a connection is the only one used. This prevents attackers who access an open port with authentic credentials from connecting to another open port to transfer data unnoticed.	Virtual Patch
Protocol Analysis	Examines network traffic for deviant behavior that does not match accepted norms and can decode protocols down to Layer 2 of the OSI model. Protocol analysis enables IBM Security IPS products to detect anomalous behavior without relying on signatures.	Virtual Patch

Attack Prevention Methods	What It Means	PAM Module That Supports It
Protocol tunneling	Sometimes used in conjunction with port assignment, IBM Security IPS products detect and prevent protocol tunneling to find malicious and/or proprietary data embedded in higher level protocols that could be allowed to traverse network segments where lower level protocols might be blocked. Protocol tunneling prevents attackers from bypassing firewalls to gain uncontested network access and prevents both insiders and attackers from establishing and using tunnels to extract data from within a corporation.	Application Control
RFC compliance checking	Compares traffic against RFC standards for network communications between hosts, applications and the network stack. If the traffic does not conform, IBM Security IPS products will block it.	Application Control
Shellcode Hueristics	Identifies and stops malicious code based on its behavior, rather than matching a particular attack signature or pattern. Heuristics can prevent evolving threats, which will change minor aspects of their signatures to bypass traditional IPS solutions.	Threat Detection and Prevention
Stateful pattern matching	Uses advanced algorithms to detect attack patterns—but only in particular portions of traffic where an attack could actually exist—greatly reducing false positives. IBM Security IPS products use stateful pattern matching in conjunction with heuristics to prevent evolving threats that change their patterns to evade detection.	Threat Detection and Prevention
TCP reassembly	Reassembles network packets, examining them for potential threats.	Virtual Patch

The IBM Protocol Analysis Module advantage

The IBM Protocol Analysis Module within the IBM Security IPS technologies is the result of continuous research into the nature of vulnerabilities and attack methods. As threats continue to evolve, but older exploits never truly become extinct, IBM constantly strengthens the PAM engine with technologies designed to block entire classes of threats—both new and old.

For more information

To learn more about IBM Security Solutions and preemptive protection, please contact your IBM Sales representative or IBM Business Partner, or visit the following Web site: **ibm.com**/tivoli/solutions/threat-mitigation.

About Tivoli software from IBM

Tivoli® software from IBM helps organizations efficiently and effectively manage IT resources, tasks and processes to meet ever-shifting business requirements and deliver flexible and responsive IT service management, while helping to reduce costs. The Tivoli portfolio spans software for security, compliance, storage, performance, availability, configuration, operations and IT life-cycle management, and is backed by world-class IBM services, support and research.

Additionally, financing solutions from IBM Global Financing can enable effective cash management, protection from technology obsolescence, improved total cost of ownership and return on investment. Also, our Global Asset Recovery Services help address environmental concerns with new, more energy-efficient solutions. For more information on IBM Global Financing, visit: **ibm.com**/financing

IBM Corporation
Software Group
Route 100
Somers, NY 10589 U.S.A.

Produced in the United States of America
May 2010

Tivoli software

WGD03001-USEN-00