IBM 协议分析模块

IBM 安全入侵防御系统技术内的保护引擎

要点

- 在威胁影响到您的网络及网络资产，如服务器、桌面和网络基础架构之前将其阻止。
- 保护终端用户抵制日常应用如文档格式、数据表、报告、多媒体文件和 web 浏览器中隐藏的漏洞。
- 模块可扩展架构，允许随着威胁的变化添加新的安全技术和功能。

先于威胁 — 阻止网络威胁，防患于未然。

IBM 安全入侵防御系统（IPS）技术在网络威胁影响您的业务之前将其阻止，防患于未然。我们独有的安全形式是基于我们的引擎 —— IBM 协议分析模块（PAM）的，能够预防多种网络威胁。PAM 的建立基于 IBM X-Force® 研发团队多年收集的安全情报。X-Force 是一家世界知名的安全研究组织，致力于前摄性地检测威胁和威胁企图利用的潜在软件漏洞。

通过模块可扩展框架，PAM 不断发展以遏制最具挑战性的安全威胁，消除了购买额外单点解决方案的需求。依靠世界知名的 IBM X-Force 研发团队的支持，PAM 定期自动地注入新的安全情报，使您领先于最新的威胁。而对于其它解决方案，您只能寄希望于其个人保护签名与漏洞匹配，这个过程太缓慢，难以阻止不断发展的威胁，还会导致更高的误报和漏报率。

IBM 协议分析模块技术

IBM 协议分析模块技术	**作用：**
虚拟补丁	保护漏洞不受单独开发的软件补丁的影响，同时减少针对新威胁的补丁演习，保障您的安全。仍然对关键系统进行补丁修复，但现在可执行自己的补丁管理测试流程。如果您的补丁管理过程没有达到最佳实践，IBM 可帮助您将端点管理集成到整体方法中，从而保障包括网络、服务器和客户端在内的安全。
客户端应用程序保护	保护终端用户免受目标应用程序，如 Microsoft Office 文件、Adobe PDF 文件、多媒体文件和 Web 浏览器，日常遇到的攻击。
Web 应用程序保护	保护 web 服务器免受高级应用程序级攻击，如 SQL 注入、XSS（跨站编写脚本）、PHP 文件，含 CSRF（跨站请求伪造）。
威胁探测与防御	发现并防御全部类型的威胁，而不限于某项具体漏洞。
数据安全	监控并识别未加密个人身份识别信息（PII）和其它机密信息用于数据处理。同时也提供通过网络浏览数据流的能力，从而帮助确定是否存在潜在威胁。
应用程序控制	管理已定义的网络区域中未授权应用程序和风险的控制，如 ActiveX 指纹识别、点对点、即时消息和管道传输。

PAM 能够监控、探测或防御以下类别的网络威胁：

威胁类别	监控	探测	防御
应用程序攻击	✓	✓	✓
攻击混淆	✓	✓	✓
缓冲器溢出攻击	✓	✓	✓
跨站编写脚本攻击	✓	✓	✓
数据泄露	✓	✓	✓
数据库攻击	✓	✓	✓
DoS 和 DDoS 攻击	✓	✓	✓
下载隐患	✓	✓	✓
内部威胁	✓	✓	✓
即时消息传递	✓	✓	✓
恶意文档类型	✓	✓	✓
恶意媒体文件	✓	✓	✓
操作系统攻击	✓	✓	✓
点对点	✓	✓	✓
管道传输协议	✓	✓	✓
SQL 注入攻击	✓	✓	✓
Web 浏览器攻击	✓	✓	✓
Web 服务器攻击	✓	✓	✓

为应对这些攻击类别，PAM 采用了多种入侵防御技术串联运行，包括：

- *端口分配*
- *端口追踪*
- *协议分析*
- *管道传输协议*
- *模式匹配*
- *内容分析*
- *注入逻辑引擎*
- *恶意代码试探法*
- *RFC 遵从性验证*
- *TCP 重组*
- *流程组装*

IBM 协议分析模块阻止的主要网络威胁

尽管网络威胁层出不穷，但我们也不能忽视旧的攻击方法，许多攻击者根据已有的防御技术逃避探测。IBM 协议分析模块旨在阻止以下网络威胁：

网络攻击类型	危险的原因	阻止它的 PAM 模块
后门	提供系统入口，绕过传统登录验证。	威胁控制与防御
僵尸网络	由按照控制器的命令执行任务的感染计算机组成，通常带有传播垃圾邮件和/或恶意软件。	威胁控制与防御
客户端攻击	对操作系统或个人计算机上运行的应用程序造成影响的漏洞。这些漏洞针对的对象可能是电子邮件客户端、Web 浏览器、文件浏览器和多媒体应用程序。	客户端应用程序保护
跨站点编写脚本	该漏洞基于网络，用于将恶意代码嵌入可在用户计算机上执行的合法链接，通常意在盗取信息。	Web 应用程序保护
分布式拒绝服务（DdoS）	利用多种受到感染的系统，通过海量发送信息攻击单个目标，使目标系统关闭。	威胁控制与防御
内部威胁	内部用户可将病毒、蠕虫和木马引入网络，或企图盗取专有数据。	威胁控制与防御
即时消息	可将木马、病毒和其它恶意软件引入网络。	应用程序控制
恶意内容	黑客嵌入到文件中的恶意多媒体代码及恶意代码。	客户端应用程序保护
恶意电子邮件	间谍软件和钓鱼骗局的常用载体，诱使用户访问恶意网络，然后可能将恶意软件引入网络。	客户端应用程序保护
点对点（P2P）网络	协助传输被木马和病毒感染的文件，旨在引入拒绝服务攻击和破损数据。	应用控制
管道传输协议	通常在较高级协议中将恶意数据分层，使其能够遍历阻止较低级协议的网络分区。	应用程序控制
侦察	汇集了各种威胁，包括强算、枚举、猜测密码和端口扫描。	威胁控制与防御
黑客软件包	集合了为黑客提供管理员权限或使其从根部访问网络或系统的各种工具或程序。	威胁控制与防御
垃圾邮件	通过网络海量发送消息的未经请求的邮件。	客户端应用程序保护
鱼叉式网络钓鱼	经过精心设计，针对高价值目标，旨在盗取机密信息的攻击。	数据安全

SQL 注入	通过 Web 应用程序的动态逻辑层在目标代码中搭载恶意 SQL 代码从而使应用程序提供数据库访问。	Web 应用程序保护
木马	将危险代码藏入表面无害的程序或数据中。	威胁控制与防御
蠕虫	通过将自身作为电子邮件附件或部分网络消息进行转发从而自我复制的病毒。	威胁控制与防御
零日攻击	试图在软件供应商提供补丁前利用未公开漏洞的威胁。	虚拟补丁

IBM 协议分析模块中的多层防御技术

PAM 集合了多种威胁防御技术的强大功能，共同阻止网络威胁。PAM 利用了以下攻击防御方法：

攻击防御方法	**含义**	**阻止它的 PAM 模块**
浏览器漏洞防御	使用 JavaScript™ 模糊处理阻止对 Web 浏览器的攻击。	客户端应用程序保护
内容分析	使用预先定义的签名和自定义签名检查和阻止网络中的未加密数据。该技术能够创建复合数据集搜索检查并检查复合文件，包括 Microsoft® Office 文件、PDF、Zip 文件和 10 多个不同协议。	数据安全
流程组装	分析整个网络连接（不仅是单个数据包）阻止可能插入到通信流中利用开放连接的恶意流量。流程组装通过从较高层面分析流量与 TCP 重组相辅相成，从而防御高级威胁。	威胁控制与防御
注入逻辑引擎	试探性地识别恶意注入，如 SQL 注入和外壳命令注入。无需签名更新即可处理当前和未来漏洞。	Web 应用程序保护
端口分配	IPS 不应假设特定类型的流量将会出现在特定的 TCP/IP 端口上。如果这样假设，且流量类型与假设的端口相匹配，且允许通过，那么黑客就能够进入。IBM 安全 IPS 产品对所有流量进行检查，不考虑流量目的端口。	虚拟补丁
端口追踪	追踪通信会话确保最初用于建立连接的端口是唯一在用端口。这样做阻止了利用可信凭证访问开放端口的黑客不被察觉地连接到另一个开放端口以传播数据。	虚拟补丁
协议分析	检查网络流量，针对不符合通用规则和能将协议解码到 OSI 模型第二层的异常行为。通过协议分析，IBM 安全IPS 产品能够不依赖签名探测异常行为。	虚拟补丁

攻击防御方法	含义	阻止它的 PAM 模块
管道传输协议	有时与端口分配联合使用，IBM 安全 IPS 产品通过探测并防止管道传输协议从而找到嵌入到较高级协议中的恶意和/或专有数据，这些数据能够遍历阻止较低级协议的网络分区。管道传输协议防止黑客绕过防火墙肆无忌惮地访问网络，同时还防止内部用户和黑客建立并使用管道从企业内部提取数据。	应用程序控制
RFC 遵从性验证	验证流量是否符合主机、应用程序和网络堆栈间网络通信的 RFC 标准。如不符，IBM 安全 IPS 产品则阻止该流量。	应用程序控制
恶意代码试探法	根据行为来识别和阻止恶意代码，而不是根据与特定攻击签名或模式相匹配。试探法可防御不断发展的威胁，这些威胁会通过小范围改变签名绕过传统的 IPS 解决方案。	威胁控制与防御
说明性模式匹配	使用高级算法探测攻击模式 — 仅针对真正存在攻击的流量 — 极大地降低了误报率。IBM 安全 IPS 产品结合使用说明性模式匹配和试探法来防御通过改变模式来逃避探测的威胁。	威胁控制与防御
TCP 重组	重组网络数据包，检查其是否存在潜在威胁。	虚拟补丁

IBM 协议分析模块的优势

IBM 协议分析模块使用 IBM 安全 IPS 技术，是对漏洞和攻击方法的本质不懈研究的结果。由于威胁不断发展，旧有漏洞从未真正消失，IBM 利用旨在阻止新旧所有威胁的技术不断强化 PAM 引擎。

更多内容

有关 IBM 安全解决方案和预先保护的更多内容，请联系您的IBM 销售代表或 IBM 业务合作伙伴，或访问以下网站：**ibm.com**/tivoli/solutions/threat-mitigation.

IBM Tivoli 软件简介

IBM 的 Tivoli® 软件帮助组织有效地管理 IT 资源、任务和流程，从而满足不断变化的业务需求，在降低成本的同时提供灵活且响应及时的 IT 服务管理。Tivoli 产品组合涉及安全、一致性、存储、性能、可用性、配置、运营和 IT 生命周期管理，并得到世界一流的 IBM 服务、支持和研究的支持。

此外，**IBM Global Financing** 提供的融资解决方案能够实现有效的现金管理、免受技术过时带来的损失、改善总持有成本和投资回报。不仅如此，我们的 **Global Asset Recovery Services** 还提供新的、更高能效的解决方案来帮助解决环境问题。有关**IBM Global Financing** 的更多内容，请访问：**ibm.com**/financing

IBM 公司
软件团队
Route 100
Somers, NY 10589 U.S.A.

制订于美利坚合众国
2010 年 5 月

Tivoli. software

WGD03001-USEN-00