McAfee Application Data Monitor

Detect hidden threats with application-layer inspection.

The McAfee® Application Data Monitor appliance advances security and compliance beyond the limits of log management by monitoring all the way to the application layer. You can fully inspect application contents to achieve the deepest visibility into how your network is being used.

Key Advantages

- Decodes the entire application session, all the way to Layer 7, for hundreds of applications
- Includes pre-built detection rules for regulated and sensitive data
- Supports user-definable dictionaries and rules for customization
- Generates a complete audit trail of application events for compliance
- Operates passively to avoid application interference
- Integrates with McAfee Enterprise Security Manager to permit correlation of application contents with events and other data feeds
- Flexible, hybrid delivery options include physical and virtual appliances

The McAfee Application Data Monitor appliance decodes an entire application session to Layer 7, providing a full analysis of everything from the underlying protocols and session integrity to the contents of the application itself (such as the text of an email or its attachments). This level of detail allows accurate analysis of real application usage, while also enabling you to enforce application use policies and detect malicious, covert traffic.

This deep inspection supports compliance by tracking all use of sensitive data on the network. When the McAfee Application Data Monitor appliance detects a violation, it preserves all details of that application session for use in incident response and forensics or for compliance audit requirements.

At the same time, the McAfee Application Data Monitor appliance provides visibility into threats that may masquerade as legitimate applications:

- Advanced application-layer threats
- Unauthorized use or theft of confidential data
- Attacks on or from security "blind spots"
- Usage of dangerous legacy code
- Theft or misuse of user credentials
- Transmission of sensitive data via any application
- Broken business processes

Data Loss and Compliance Violations

The McAfee Application Data Monitor appliance can detect when sensitive information is being transmitted inside email attachments, instant messages, file transfers, HTTP posts, or any other application, notifying you immediately so that the loss can be mitigated.

You can detect sensitive data such as credit card information and Social Security numbers out of the box or customize the McAfee Application Data Monitor appliance's detection capabilities by defining your own dictionaries of sensitive and confidential information. The McAfee Application Data Monitor appliance will detect these sensitive data types, alert appropriate personnel, and log the transgression to maintain an audit trail.

Document Discovery

The McAfee Application Data Monitor appliance discovers more than 500 document types as they are being exchanged over the network by email, chat, P2P, file shares, and other means. The McAfee Application Data Monitor appliance discovers documents irrespective of the extension—documents masquerading as another type trying to bypass mail gateways and IDS/IPS devices. Even documents embedded inside other documents, as well as archived, compressed, and encoded documents are discovered with actionable metrics such as filename and operation being performed.

intel Security

More than 500 Supported Applications and Protocols

- **Low level network protocols**—TCP/IP, UDP, RTP, RPC, SOCKS, DNS, and others
- **Email**—MAPI, NNTP, POP3, SMTP, Microsoft Exchange
- **Webmail**—AOL Webmail, Hotmail, Yahoo! Mail, Gmail, Facebook, and MySpace email
- **Instant messaging**—AOL, ICQ, Jabber, MSN, SIP, and Yahoo
- **File transfer protocols**—FTP, HTTP, SMB, and SSL
- **Compression and extraction protocols**—BASE64, GZIP, MIME, TAR, ZIP, and others
- **Archive files**—RAR Archives, ZIP, BZIP, GZIP, Bin-hex, and UU-encoded archives
- **Installation packages**—Linux packages, InstallShield cabinets, Microsoft cabinets
- **Image files**—GIFs, JPEGs, PNGs, TIFFs, AutoCAD, Photoshop, Bitmaps, Visio, Digital RAW, and Windows icons
- **Audio files**—WAV, MIDI, RealAudio, Dolby Digital AC-3, MP3, MP4, MOD, RealAudio, SHOUTCast, and more
- **Video files**—AVI, Flash, QuickTime, Real Media, MPEG-4, Vivo, Digital Video (DV), Motion JPEG, and more
- **Other applications and files**—Databases, spreadsheets, faxes, web applications, fonts, executable files, Microsoft Office applications, games, and even software development tools
- **Other protocols**—Network printer, shell access, VoIP, and peer-to-peer

Application-Layer Threats

New, sophisticated threats exploit the vulnerabilities in common business applications to penetrate your network and export sensitive data. While these application-layer threats are difficult to detect using traditional firewalls and intrusion detection systems (IDS) and intrusion prevention systems (IPS), the McAfee Application Data Monitor appliance is able to look into the entire contents of an application—including the underlying protocols—to detect hidden payloads, malware, and even covert communication channels—for example an executable embedded inside a PDF document.

Protocol Anomalies

Anomaly detection can proactively identify imminent threats, reducing risk and minimizing loss. While some traditional security solutions are limited to the analysis of network flows, the McAfee Application Data Monitor appliance takes this approach to the next level. We look past network behavior to detect anomalies within applications and protocols, delivering a stronger, more proactive risk detection methodology.

No Interference with Applications

Since the McAfee Application Data Monitor appliance operates on a SPAN port, it will not interfere with application performance or reliability or introduce latency.

Integrated with Your Infrastructure

While most network monitoring solutions operate in isolation, the McAfee Application Data Monitor appliance works in concert with other information security systems. Through McAfee Enterprise Security Manager, it connects to the rest of your security infrastructure to simplify security operations, improve overall efficiency, and lower costs. You can integrate loss and fraud detection with powerful analytics, network inspection, database event monitoring, and more.

Example Use Cases

The McAfee Application Data Monitor appliance can detect a variety of unauthorized activity, policy violations, theft, and fraud. Here are some examples.

Theft of confidential information

An employee logged in as jdoe@company.com sent an email to accomplice@gmail.com. The email contained a file called shoo.doc that included the words “secret formula.” The email was sent at 12:20 pm from the host desktop0232 (192.168.0.36) using the SMTP server (10.0.2.13) with this subject: got it.

Use of unauthorized applications

An employee violated policy by transferring music using a peer-to-peer file sharing application that he installed. He sent large files during work hours, consuming valuable bandwidth. More investigation revealed the employee as a regular offender. He uses Jabber and IRC and runs an unauthorized web server on his desktop.

Cyberslacking in the work place

An employee is also a secret day trader. During the workday, she connects to financial trading sites for an average of one hour each morning and afternoon. She also uses the company’s VoIP (SIP) system to make an average of six calls daily and spends hours on Yahoo! Messenger as “traderjoe” talking to “traderbob” and “tradergill.”

User of weak passwords

Your company’s security policy requires the use of strong passwords for all user system and application accounts. Microsoft Active Directory accounts are strictly managed. However, dozens of weak passwords are being used on external-facing FTP servers, mail servers, and critical web applications that don’t use Active Directory.

For more information, visit **mcafee.com/siem**.

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com