

McAfee Network DLP Platform and Technical Specifications

Detailed platform and technical specifications for McAfee Network DLP (Data Loss Prevention) appliances are listed below.

McAfee Network DLP Appliance platform specifications

The following table lists platform specifications that apply to all McAfee Network DLP (Data Loss Prevention) Appliances.



Item	McAfee Network DLP Appliance 1650	McAfee Network DLP Appliance 3650
Form Factor	1RU	3RU
Dimensions (H x W x D) / Weight	1.7 x 17.2 x 27.75 in 43 x 437 x 705 mm. 39 lbs / 17.7 kg	5.2 x 17.2 x 25.5 in 132 x 437 x 648 mm 72 lbs / 32.7 kg
Optional Expansion Cards	External storage interconnection card	External storage interconnection card
Datastore Capacity	500GB	6TB
Drive Bays	4	16
Disk Capacity	500GB	500GB
Disk Technology	SATA2	SATA2
RAID	RAID-1	RAID-1 and RAID-5
System Memory	16GB	16GB
System Fans	6 cooling fans	5 cooling fans, redundant rear exhaust fans
Operating Temperature	10-35 degrees (C), 50-95 degrees (F)	
Humidity Range	8-90% non-condensing	
Power Supply	<ul style="list-style-type: none"> 1650 appliance: Redundant hot-swappable 650W AC-DC power supply, 100-240V AC, 50-60 Hertz 3650 appliance: Redundant hot-swappable 800W AC-DC power supply, 100-240V AC, 50-60 Hertz 	
Power Supply Safety/EMC	USA-UL, Canada-CUL, Germany-TUV, EN 60950 Compliant, IEC 60950 Compliant, CB Report, CCC Certification	
Network Interfaces	Two 10/100/1000 copper network interfaces	

McAfee Network DLP Discover technical specifications

The following table lists technical specifications that apply to McAfee Network DLP (Data Loss Prevention) Discover.

Technical specification	Description
Index Capacity	Supports indexing of up to 5TB of information and up to 2 million documents on the McAfee Network DLP Discover 1650 Appliance (1U), and up to 50TB of information and up to 25 million documents on the McAfee Network DLP Discover 3650 Appliance (3U). For environments in which the amount of information or number of files exceeds the limits of a single system, additional appliances can be deployed in parallel.
System Throughput	Supports up to 500Mbps content fetching throughput and up to 150Mbps content indexing throughput. Assumes target nodes are capable of sustaining throughput equivalent to or greater than that provided by McAfee. Scan operations can be throttled to control network burden if needed and can integrate cleanly with campus and WAN QoS architectures.
Content Types	Supports file classification of over 300 content types, including: <ul style="list-style-type: none"> • Office Documents • Design Files • Built-in Policies • Multimedia Files • Archives • Intellectual Property • Source Code • Encrypted Files
Policy Definition	Powerful policy definition and rule configuration, including keywords, regular expressions, and concepts. Document registration to rules including network path scanning on a configurable schedule. Thresholds based on percentage match. Document expiration and version tracking. Exclusion to discriminate between non-sensitive and sensitive information. Context definition to restrict rule and policy enforcement to specific scan operations.
Repositories	Common Internet File System/Server Message Block (CIFS/SMB support includes Microsoft Windows/Linux/UNIX/Apple with Samba, Novell with NFAP), Network File System (NFS support includes Linux/UNIX/Apple), HTTP (wiki, blog, portals), HTTPS, FTP, Microsoft Sharepoint, EMC Documentum, and more.
Document Registration	Documents can be registered from any repository as mentioned above. Signatures from registered documents can be used locally for detecting proliferation of sensitive material, or to other McAfee DLP Appliances.
Learning Applications	Learning applications allow you to perform a granular investigation and historical inspection of information to detect risk events and data exposure that may not have been considered previously. Key features and benefits include: <ul style="list-style-type: none"> • Quickly identify sensitive information through an intuitive search interface. Determine who is sending it, where it is going, and how—even if a rule wasn't previously configured. • Seamless transfer of search language to rule construction, allowing you to start with a search for identifying sensitive data and unapproved behavior and turn it directly into a rule. • Minimize time spent tuning rules by testing rule changes immediately against historical data. • Investigate user network activity, including web transactions, instant messenger conversations, email traffic, and more. • Conduct forensic analysis to correlate current and past risk events, detect risk trends, and identify threats.
Reporting	Powerful analytics engine for incident and search result views allow you to customize summary views based on any two contextual pivot points. List and detail views, as well as summary views with trending are available. All reports are customizable and can be saved for later use—or scheduled for periodic delivery. Over 20 pre-built reports are provided with the system.
Remediation	McAfee Network DLP Discover provides integrated case management. Supports notification to content owners or system administrators using configurable notification messages.

McAfee Network DLP Monitor technical specifications

The following table lists technical specifications that apply to McAfee Network DLP (Data Loss Prevention) Monitor.

Technical specification	Description
Storage/Capture Capacity	McAfee Network DLP Monitor supports to 500GB of usable storage capacity on the McAfee Network DLP 1650 Appliance (1U) and up to 6TB of usable storage capacity on the McAfee Network DLP 3650 Appliance (3U). For environments that require greater levels of retention, multiple devices can be deployed.
System Throughput	Supports up to 200Mbps of full content analysis, indexing, and storage throughput. For networks with higher throughput requirements, multiple devices can be used in a load-balanced configuration.
Network Integration	Integrates passively into the network using either a SPAN port or a physically inline network tap (optional).
Content Types	Supports file classification of over 300 content types, including: <ul style="list-style-type: none"> • Office Documents • Design Files • Built-in Policies • Multimedia Files • Archives • Intellectual Property • Source Code • Encrypted Files
Protocols	Supports all transmissions over any protocol or port utilizing TCP as a transport protocol. Classifies applications based on PDUs, byte signatures, and statistics, not by port number. Includes protocol handlers for HTTP, HTTPS, SMTP, IMAP, POP3, FTP, Telnet, Rlogin, SSH, webmail, Yahoo Chat, AOL Chat, MSN Chat, ICY, RTSP, SOCKS, PCAnywhere, RDP, VNC, SMB, Citrix, Skype, IRC, LDAP, DASL, NTLM, Kazaa, BitTorrent, eDonkey, Gnutella, DirectConnect, MP2P, WinMX, Sherlock, eMule, and more.
Built-In Policies	Provides a wide range of built-in policies and rules for common requirements, including regulatory compliance, intellectual property, and acceptable use. Enables complete customization of rules to meet business-specific needs by leveraging the McAfee capture database.

McAfee Network DLP Prevent technical specifications

The following table lists technical specifications that apply to McAfee Network DLP (Data Loss Prevention) Prevent.

Technical specification	Description
Storage/Capture Capacity	McAfee Network DLP Prevent supports up to 500GB of usable storage capacity on the McAfee Network DLP 1650 Appliance (1U) and up to 6TB of usable storage capacity on the McAfee Network DLP 3650 Appliance (3U)
System Throughput	Up to 200Mbps of full content analysis, indexing, and storage throughput. For networks with higher throughput requirements, multiple devices can be used in a load-balanced configuration.
Network Integration	Integrates into the network as an off-path appliance that is active within the data path using MTAs and ICAP-compliant web proxies.
Content Types	Supports file classification of over 300 content types, including: <ul style="list-style-type: none"> • Office Documents • Design Files • Built-in Policies • Multimedia Files • Archives • Intellectual Property • Source Code • Encrypted Files
Protocols	Supports HTTP, HTTPS, FTP, and Instant Messaging protocols via the ICAP protocol to an ICAP-compliant proxy. Please refer to your proxy vendor for protocols supported by your proxy. Supports SMTP via integration with MTAs.
Built-In Policies	Provides a wide range of built-in policies and rules for common requirements, including regulatory compliance, intellectual property, and acceptable use. Enables complete customization of rules to meet business-specific needs by leveraging the McAfee capture database.

