

Guida alla compatibilità e requisiti di sistema per Symantec™ Data Loss Prevention

Versione 15.5

Ultimo aggiornamento: 03 marzo 2019



Guida alla compatibilità e requisiti di sistema Symantec Data Loss Prevention

Versione della documentazione: 15.5

Informativa legale

Copyright © 2019 Symantec Corporation. Tutti i diritti riservati.

Symantec, CloudSOC, Blue Coat, il logo Symantec, il logo del segno di spunta, il logo Blue Coat e il logo a scudo sono marchi o marchi registrati di Symantec Corporation o di società affiliate negli Stati Uniti e altri Paesi. Gli altri nomi potrebbero essere marchi dei rispettivi proprietari.

Il presente prodotto Symantec può contenere programmi software di terze parti per i quali Symantec deve fornire attribuzione alle terze parti stesse ("Programmi di terze parti"). Alcuni dei programmi di terze parti sono disponibili con licenze Open Source o di software gratuito. Il contratto di licenza che accompagna il software non altera in alcun modo i diritti o gli obblighi eventuali derivanti da queste licenze Open Source o di software gratuito. Vedere l'appendice sull'informativa legale relativa a terzi di questa documentazione o il file Leggimi di TPIP che accompagna questo prodotto Symantec per maggiori informazioni sui programmi di terze parti.

Il prodotto descritto nel presente documento è distribuito in base alle condizioni di una licenza che ne limita l'utilizzo, la copia, la distribuzione e la decompilazione/decodificazione. Non è consentita la riproduzione anche parziale del documento in qualsiasi forma e con qualsiasi mezzo senza l'autorizzazione scritta di Symantec Corporation e degli eventuali licenzianti.

LA PRESENTE DOCUMENTAZIONE VIENE FORNITA COSÌ COM'È E VIENE NEGATA QUALSIASI GARANZIA, ESPLICITA O IMPLICITA, COMPRESE ANCHE E NON SOLO LE GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ, IDONEITÀ PER UNO SCOPO SPECIFICO O NON VIOLAZIONE DI DIRITTI ALTRUI NELLA MISURA MASSIMA CONSENTITA DALLA LEGGE. SYMANTEC CORPORATION NON SARÀ RESPONSABILE DI ALCUN TIPO DI DANNO INCIDENTALE O CONSEGUENZIALE COLLEGATO ALLA CONSEGNA, ALLE PRESTAZIONI O ALL'UTILIZZO DI QUESTA DOCUMENTAZIONE. LE INFORMAZIONI CONTENUTE NELLA PRESENTE DOCUMENTAZIONE SONO SOGGETTE A MODIFICA SENZA PREAVVISO.

Il Software e la Documentazione concessi in licenza sono ritenuti software commerciale per computer secondo le definizioni riportate nel FAR 12.212 e sono soggetti alle limitazioni di legge definite nel FAR Sezione 52.227-19 "Commercial Computer Software - Restricted Rights" e DFARS 227.7202 e successivi "Commercial Computer Software and Commercial Computer Software Documentation", per quanto applicabili, e nei regolamenti successivi, a prescindere dal fatto che siano forniti da Symantec come servizi in sede o host. Qualsiasi tipo di utilizzo, modifica, distribuzione, esecuzione, visualizzazione o divulgazione del software in licenza e della relativa documentazione da parte del Governo degli Stati Uniti potrà avvenire solo in conformità ai termini del presente contratto.

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

<https://www.symantec.com>

Supporto Symantec

Tutti i servizi di supporto verranno forniti conformemente al contratto di supporto e alla politica di supporto tecnico Enterprise corrente.

Articoli della Knowledge Base e Symantec Connect

Prima di contattare il supporto tecnico, consultare il contenuto gratuito disponibile nella nostra Knowledge Base online, che comprende istruzioni, articoli per la risoluzione dei problemi, avvisi e manuali dei prodotti. Nella casella di ricerca del seguente URL, digitare il nome del prodotto:

<https://support.symantec.com>

Accedere ai nostri blog e forum online per interagire con altri clienti, partner e dipendenti di Symantec su una vasta gamma di argomenti al seguente URL:

<https://www.symantec.com/connect>

Supporto tecnico e supporto clienti Enterprise

Il supporto Symantec gestisce i centri di supporto a livello globale 24 ore al giorno, 7 giorni alla settimana. Il ruolo primario del supporto tecnico è rispondere a query specifiche sulle funzioni e sulla funzionalità del prodotto. Il supporto clienti Enterprise assiste gli utenti che hanno richieste non tecniche, come l'attivazione della licenza, gli upgrade della versione software, l'accesso ai prodotti e i rinnovi.

Per i termini e condizioni, le politiche e altre informazioni relative al supporto Symantec, vedere:

<https://entced.symantec.com/default/ent/supportref>

Per contattare il supporto Symantec, vedere:

https://support.symantec.com/en_US/contact-support.html

Sommario

Supporto Symantec	4	
Capitolo 1	Informazioni su questa guida	7
	Informazioni sugli aggiornamenti ai requisiti di sistema di Symantec	
	Data Loss Prevention	7
	Informazioni sulle piattaforme obsolete	8
Capitolo 2	Raccomandazioni e requisiti di sistema	9
	Considerazioni sulla pianificazione della distribuzione	9
	L'effetto della scala sui requisiti di sistema	10
	Requisiti di sistema minimi per i server di Symantec Data Loss	
	Prevention	12
	Requisiti hardware minimi per installazioni a un livello	13
	Requisiti minimi dell'hardware per installazioni molto piccole	13
	Requisiti hardware minimi per installazioni piccole	15
	Requisiti hardware minimi per installazioni medie	16
	Requisiti hardware minimi per aziende grandi	18
	Requisiti di sistema operativo per server	20
	Requisiti di sistema operativo per server OCR	24
	Requisiti del computer endpoint per Symantec DLP Agent	24
	Requisiti di sistema operativo per sistemi endpoint	25
	Requisiti di memoria e spazio su disco per Symantec DLP	
	Agent	30
	Lingue supportate per il rilevamento	31
	Supporti lingue disponibili	33
	Requisiti del database Oracle	34
	Requisiti del browser per l'accesso alla console di amministrazione	
	dell'Enforce Server	36
	Distribuzione di Data Loss Prevention in infrastrutture cloud	
	pubbliche	36
	Distribuzione di Symantec Data Loss Prevention nell'infrastruttura	
	Amazon Web Services	36
	Distribuzione di Symantec Data Loss Prevention in Microsoft	
	Azure	37

Distribuzione di Symantec Data Loss Prevention in Oracle	
Cloud	37
Supporto di server virtuali	38
Supporto desktop virtuale e applicazione virtuale con Endpoint Prevent	39
Sistemi operativi supportati per gli indicatori EMDI, EDM e IDM remoti	41
Requisiti del software di terze parti e raccomandazioni	42

Capitolo 3	Compatibilità del prodotto	47
	Requisiti e compatibilità ambientale per Network Prevent for Email	47
	Compatibilità di server proxy con Network Prevent for Web	48
	Monitoraggio SSL con Network Monitor	49
	Supporto ICAP protetto per Network Prevent for Web tramite il servizio stunnel	50
	Schede di acquisizione di pacchetti ad alta velocità	50
	Compatibilità di Veritas Data Insight con Symantec Data Loss Prevention	51
	Integrazioni con altri prodotti di Symantec	52
	Compatibilità Network Discover/Cloud Storage Discover	55
	Target di archiviazione cloud Box supportati	55
	Target del file system supportati	55
	Target di IBM (Lotus) Notes supportati	56
	Target di database SQL supportati	56
	Target del server SharePoint supportati	57
	Destinazioni Exchange Server supportate	57
	Target supportati del rilevatore file system	57
	Target Documentum (rilevatore) supportati	58
	Target del rilevatore OpenText (Livelihood) supportati	58
	Target supportati del Web Server (rilevatore)	58
	Applicazioni supportate da Endpoint Prevent	59

Informazioni su questa guida

Il capitolo contiene i seguenti argomenti:

- [Informazioni sugli aggiornamenti ai requisiti di sistema di Symantec Data Loss Prevention](#)
- [Informazioni sulle piattaforme obsolete](#)

Informazioni sugli aggiornamenti ai requisiti di sistema di Symantec Data Loss Prevention

I requisiti di sistema descritti in questa guida vengono aggiornati occasionalmente man mano che le nuove informazioni diventano disponibili. È possibile trovare l'ultima versione della *Guida alla compatibilità e ai requisiti di sistema di Symantec Data Loss Prevention* al seguente collegamento del centro di supporto di Symantec.

<http://www.symantec.com/docs/DOC10602>

Iscriversi all'articolo del Centro di supporto per ricevere notifiche quando sono disponibili aggiornamenti.

La seguente tabella fornisce la cronologia degli aggiornamenti a questa versione della *Guida alla compatibilità e ai requisiti di sistema di Symantec Data Loss Prevention*.

Tabella 1-1 Cronologia delle modifiche alla *Guida alla compatibilità e ai requisiti di sistema Symantec Data Loss Prevention*

Data	Descrizione
5 febbraio 2019	Aggiunto nota e collegamento all'avviso del Centro di supporto relativo al monitoraggio di Chrome 72 sugli endpoint Windows. Aggiunto il supporto per il proxy di F5 BIG-IP 14.1.0 e McAfee Web Gateway 7.8.2.

Data	Descrizione
7 gennaio 2019	Aggiunto il supporto per il monitoraggio HTTPS di Firefox 64 sugli endpoint Windows e macOS. Aggiunto il supporto di DLP Agent per macOS 10.14.2.

Informazioni sulle piattaforme obsolete

Determinate piattaforme sono riportate come “obsolete”. Ciò indica che, sebbene la piattaforma obsoleta sia supportata nella versione corrente, Symantec non intende più fornire il supporto per tale piattaforma nelle versioni future. Se l'ambiente Symantec Data Loss Prevention include una piattaforma obsoleta, è necessario aggiornare la piattaforma a una versione più recente supportata o passare a una piattaforma diversa supportata appena possibile.

Raccomandazioni e requisiti di sistema

Il capitolo contiene i seguenti argomenti:

- [Considerazioni sulla pianificazione della distribuzione](#)
- [Requisiti di sistema minimi per i server di Symantec Data Loss Prevention](#)
- [Requisiti di sistema operativo per server OCR](#)
- [Requisiti del computer endpoint per Symantec DLP Agent](#)
- [Lingue supportate per il rilevamento](#)
- [Supporti lingue disponibili](#)
- [Requisiti del database Oracle](#)
- [Requisiti del browser per l'accesso alla console di amministrazione dell'Enforce Server](#)
- [Distribuzione di Data Loss Prevention in infrastrutture cloud pubbliche](#)
- [Supporto di server virtuali](#)
- [Supporto desktop virtuale e applicazione virtuale con Endpoint Prevent](#)
- [Sistemi operativi supportati per gli indicatori EMDI, EDM e IDM remoti](#)
- [Requisiti del software di terze parti e raccomandazioni](#)

Considerazioni sulla pianificazione della distribuzione

La pianificazione dell'installazione e i requisiti di sistema per Symantec Data Loss Prevention dipendono dai seguenti elementi:

- Il tipo e la quantità di informazioni che si desidera proteggere
- La quantità di traffico di rete che si desidera monitorare
- La dimensione dell'organizzazione
- Il tipo di server di rilevamento di Symantec Data Loss Prevention che si decide di installare

Questi fattori sono entrambi da considerare:

- Il tipo di livello di installazione che si sceglie di distribuire (a tre livelli, a due livelli o a livello singolo)
- I requisiti di sistema per l'installazione di Symantec Data Loss Prevention

Vedere ["L'effetto della scala sui requisiti di sistema"](#) a pagina 10.

L'effetto della scala sui requisiti di sistema

Alcuni requisiti di sistema variano a seconda delle dimensioni della distribuzione del software Symantec Data Loss Prevention. Determinare le dimensioni dell'organizzazione e la distribuzione Symantec Data Loss Prevention corrispondente tramite le informazioni in questa sezione.

Le considerazioni chiave per la determinazione delle dimensioni di distribuzione sono le seguenti:

- Numero di utenti di Enforce Server
- Numero di server di rilevamento
- Volume incidenti giornaliero
- Quantità di traffico di rete da monitorare
- Dimensione del profilo Corrispondenza dati esatti (EDM), del profilo Identificatore dati corrispondenti esatti (EMDI) o del profilo Corrispondenza dati indicizzati (IDM)
- Dimensioni del profilo Riconoscimento moduli

La seguente tabella delinea cinque distribuzioni campione in base alle dimensioni enterprise. Esaminare queste distribuzioni campione per comprendere la migliore corrispondenza per l'ambiente aziendale.

Tabella 2-1 Tipi di distribuzioni aziendali

Variabile	A un livello	Molto piccola (sistema minimo supportato)	Piccola	Media	Grande
Numero di utenti di Enforce Server	N/D	5	10	20	30
Numero di server di rilevamento	N/D	5	10	50	100+
Volume incidenti giornaliero	N/D	5000	10.000	50.000	100.000
Volume di traffico di rete da monitorare	30-40 Mbps	30-40 Mbps	30-40 Mbps	30-40 Mbps	> 40 Mbps
Dimensione indice EMDI/EDM/IDM	EDM da 4 milioni di celle o IDM da 250 MB (1400 file). Per informazioni sull'impatto di EDM, IDM ed EMDI sul dimensionamento per le distribuzioni aziendali, vedere il <i>Manuale dell'amministratore di Symantec Data Loss Prevention</i> .	Per informazioni sull'impatto di EDM, IDM ed EMDI sul dimensionamento per le distribuzioni aziendali, vedere il <i>Manuale dell'amministratore di Symantec Data Loss Prevention</i> .	Per informazioni sull'impatto di EDM, IDM ed EMDI sul dimensionamento per le distribuzioni aziendali, vedere il <i>Manuale dell'amministratore di Symantec Data Loss Prevention</i> .	Per informazioni sull'impatto di EDM, IDM ed EMDI sul dimensionamento per le distribuzioni aziendali, vedere il <i>Manuale dell'amministratore di Symantec Data Loss Prevention</i> .	Per informazioni sull'impatto di EDM, IDM ed EMDI sul dimensionamento per le distribuzioni aziendali, vedere il <i>Manuale dell'amministratore di Symantec Data Loss Prevention</i> .
Dimensioni del profilo Riconoscimento moduli	Consultare l'articolo TECH235074 nel centro di supporto Symantec per informazioni sul dimensionamento Riconoscimento moduli.	Consultare l'articolo TECH235074 nel centro di supporto Symantec per informazioni sul dimensionamento Riconoscimento moduli.	Consultare l'articolo TECH235074 nel centro di supporto Symantec per informazioni sul dimensionamento Riconoscimento moduli.	Consultare l'articolo TECH235074 nel centro di supporto Symantec per informazioni sul dimensionamento Riconoscimento moduli.	Consultare l'articolo TECH235074 nel centro di supporto Symantec per informazioni sul dimensionamento Riconoscimento moduli.

Variabile	A un livello	Molto piccola (sistema minimo supportato)	Piccola	Media	Grande
Requisiti hardware	Vedere "Requisiti hardware minimi per installazioni a un livello" a pagina 13.	Vedere "Requisiti minimi dell'hardware per installazioni molto piccole" a pagina 13.	Vedere "Requisiti hardware minimi per installazioni piccole" a pagina 15.	Vedere "Requisiti hardware minimi per installazioni medie" a pagina 16.	Vedere "Requisiti hardware minimi per aziende grandi" a pagina 18.

Per informazioni relative aggiuntive consultare inoltre le *linee guida su dimensionamento delle prestazioni Network Monitor e Prevent di Symantec Data Loss Prevention*, disponibile nel centro di supporto Symantec all'indirizzo <http://www.symantec.it/docs/DOC8253>.

Requisiti di sistema minimi per i server di Symantec Data Loss Prevention

Tutti i server Symantec Data Loss Prevention devono rispettare o superare i requisiti minimi di sistema per l'hardware e utilizzare uno dei sistemi operativi supportati.

- Vedere "Requisiti hardware minimi per installazioni a un livello" a pagina 13.
- Vedere "Requisiti minimi dell'hardware per installazioni molto piccole" a pagina 13.
- Vedere "Requisiti hardware minimi per installazioni piccole" a pagina 15.
- Vedere "Requisiti hardware minimi per installazioni medie" a pagina 16.
- Vedere "Requisiti hardware minimi per aziende grandi" a pagina 18.
- Vedere "Requisiti di sistema operativo per server" a pagina 20.

Nota: I requisiti per le appliance virtuali di Symantec Data Loss Prevention sono gli stessi delle controparti del server software, fatta eccezione per il supporto dell'ambiente virtuale. Vedere "Supporto di server virtuali" a pagina 38.

Se il database Oracle per Symantec Data Loss Prevention viene installato su un computer dedicato (distribuzione a tre livelli), quel sistema deve rispettare una serie di requisiti di sistema specifici.

Vedere "Requisiti del database Oracle" a pagina 34.

Requisiti hardware minimi per installazioni a un livello

La seguente tabella fornisce i requisiti di sistema per la distribuzione di a un livello in piccole aziende o filiali.

Poiché le distribuzioni a un livello includono Enforce Server, il database Oracle e il server di rilevamento sullo stesso computer, i requisiti di elaborazione e memoria sono superiori rispetto a quelli su server dedicati in una distribuzione a due o tre livelli.

Nota: La dimensione predefinita del contenuto per il rilevamento è 30 MB. Se si prevede di eseguire la scansione di file più grandi di 30 MB, vedere l'articolo <https://www.symantec.com/docs/TECH252393.html> nel Centro di supporto Symantec per informazioni sull'ottimizzazione del sistema per l'ispezione di file di grandi dimensioni.

Tabella 2-2 Requisiti hardware minimi per installazioni a un livello

Richiesto per	Installazione server singolo
Processore	CPU a otto core
Memoria	64 GB DI RAM
Disco	Configurazione RAID 5 da 3 TB (con un minimo di cinque assi)
NIC	1 NIC Ethernet in rame o fibra da 1 Gb (se si utilizza Network Monitor saranno necessari un minimo di due NIC)

Requisiti minimi dell'hardware per installazioni molto piccole

La seguente tabella fornisce i requisiti di sistema per l'installazione più piccola supportata da Symantec Data Loss Prevention. Questa è un'installazione a due livelli, in cui il database di Oracle e Enforce Server sono entrambi ospitati nello stesso computer.

Nota: La dimensione predefinita del contenuto per il rilevamento è 30 MB. Se si prevede di eseguire la scansione file più grandi di 30 MB, vedere l'articolo <https://www.symantec.com/docs/TECH252393.html> nel Centro di supporto Symantec per informazioni sull'ottimizzazione del sistema per l'ispezione file di grandi dimensioni.

Tabella 2-3 Requisiti minimi dell'hardware per installazioni molto piccole

Richiesto per	Enforce Server	Network Monitor	Network Discover/Cloud Storage Discover, Network Prevent, Cloud Prevent for Email o Endpoint Prevent
Processore	CPU a due core	CPU a quattro core	CPU a quattro core
Memoria	8 GB DI RAM	Da 6 a 8 GB di RAM (vedere il <i>Manuale dell'amministratore di Symantec Data Loss Prevention</i> per informazioni sull'impatto di EDM, IDM ed EMDI sul dimensionamento. Consultare l'articolo TECH235074 nel centro di supporto Symantec per informazioni sul dimensionamento di Riconoscimento moduli.)	Da 6 a 8 GB di RAM (vedere il <i>Manuale dell'amministratore di Symantec Data Loss Prevention</i> per informazioni sull'impatto di EDM, IDM ed EMDI sul dimensionamento. Consultare l'articolo TECH235074 nel centro di supporto Symantec per informazioni sul dimensionamento di Riconoscimento moduli.)
Disco	unità disco rigido con 500 GB di archiviazione. Per le distribuzioni di Network Discover/Cloud Storage Discover sono necessari circa 150 MB di spazio su disco per mantenere gli indici di scansione incrementali. Ciò si basa su un sovraccarico di 5 MB per target di scansione incrementale e 50 byte per elemento nel target.	140 GB	140 GB Per le distribuzioni di Network Discover/Cloud Storage Discover sono necessari circa 150 MB di spazio su disco per mantenere gli indici di scansione incrementali. Ciò si basa su un sovraccarico di 5 MB per target di scansione incrementale e 50 byte per elemento nel target.
NIC	Un NIC Ethernet 1 Gb/100 Mb in rame o fibra per comunicare con server di rilevamento.	1 NIC Ethernet 1 Gb/100 Mb in rame o fibra per comunicare con l'Enforce Server.	1 NIC Ethernet 1 Gb/100 Mb in rame o fibra per comunicare con l'Enforce Server.

Requisiti hardware minimi per installazioni piccole

La seguente tabella fornisce i requisiti di sistema per un'installazione piccola di Symantec Data Loss Prevention. Questa è un'installazione a tre livelli, in cui i database di Oracle e Enforce Server sono ospitati su computer diversi.

Nota: La dimensione predefinita del contenuto per il rilevamento è 30 MB. Se si prevede di eseguire la scansione file più grandi di 30 MB, vedere l'articolo <https://www.symantec.com/docs/TECH252393.html> nel Centro di supporto Symantec per informazioni sull'ottimizzazione del sistema per l'ispezione file di grandi dimensioni.

Tabella 2-4 Requisiti hardware minimi per installazioni piccole

Richiesto per	Enforce Server	Database Oracle	Network Monitor	Network Discover/Cloud Storage Discover, Network Prevent, Cloud Prevent for Email o Endpoint Prevent
Processore	CPU a due core	CPU a due core	CPU a quattro core	CPU a quattro core
Memoria	8 GB DI RAM	8 GB DI RAM	Da 6 a 8 GB di RAM (vedere il <i>Manuale dell'amministratore di Symantec Data Loss Prevention</i> per informazioni sull'impatto di EDM, IDM ed EMDI sul dimensionamento. Consultare l'articolo TECH235074 nel centro di supporto Symantec per informazioni sul dimensionamento di Riconoscimento moduli.)	Da 6 a 8 GB di RAM (vedere il <i>Manuale dell'amministratore di Symantec Data Loss Prevention</i> per informazioni sull'impatto di EDM, IDM ed EMDI sul dimensionamento. Consultare l'articolo TECH235074 nel centro di supporto Symantec per informazioni sul dimensionamento di Riconoscimento moduli.)

Richiesto per	Enforce Server	Database Oracle	Network Monitor	Network Discover/Cloud Storage Discover, Network Prevent, Cloud Prevent for Email o Endpoint Prevent
Disco	<p>unità disco rigido con 500 GB di archiviazione.</p> <p>Per le distribuzioni di Network Discover/Cloud Storage Discover sono necessari circa 150 MB di spazio su disco per mantenere gli indici di scansione incrementali. Ciò si basa su un sovraccarico di 5 MB per target di scansione incrementale e 50 byte per elemento nel target.</p>	<p>500 GB - 1 TB</p> <p>Vedere "Requisiti del database Oracle" a pagina 34.</p>	140 GB	<p>140 GB</p> <p>Per le distribuzioni di Network Discover/Cloud Storage Discover sono necessari circa 150 MB di spazio su disco per mantenere gli indici di scansione incrementali. Ciò si basa su un sovraccarico di 5 MB per target di scansione incrementale e 50 byte per elemento nel target.</p>
NIC	Un NIC Ethernet 1 Gb/100 Mb in rame o fibra per comunicare con server di rilevamento.	N/D	1 NIC Ethernet 1 Gb/100 Mb in rame o fibra per comunicare con l'Enforce Server.	1 NIC Ethernet 1 Gb/100 Mb in rame o fibra per comunicare con l'Enforce Server.

Requisiti hardware minimi per installazioni medie

La seguente tabella fornisce i requisiti di sistema per le installazioni medie di Symantec Data Loss Prevention. Questa è un'installazione a tre livelli, in cui i database di Oracle e Enforce Server sono ospitati su computer diversi.

Nota: La dimensione predefinita del contenuto per il rilevamento è 30 MB. Se si prevede di eseguire la scansione file più grandi di 30 MB, vedere l'articolo <https://www.symantec.com/docs/TECH252393.html> nel Centro di supporto Symantec per informazioni sull'ottimizzazione del sistema per l'ispezione file di grandi dimensioni.

Tabella 2-5 Requisiti hardware minimi per installazioni medie

Richiesto per	Enforce Server	Database Oracle	Network Monitor	Network Discover/Cloud Storage Discover, Network Prevent, Cloud Prevent for Email o Endpoint Prevent
Processore	CPU a due core	CPU a quattro core	CPU a quattro core	CPU a quattro core
Memoria	12 GB DI RAM (la dimensione di EDM/IDM e del profilo Riconoscimento moduli può aumentare i requisiti di memoria. Consultare l'articolo TECH235074 nel centro di supporto Symantec per informazioni sul dimensionamento di Riconoscimento moduli.)	16 GB DI RAM	Da 6 a 8 GB di RAM (vedere il <i>Manuale dell'amministratore di Symantec Data Loss Prevention</i> per informazioni sull'impatto di EDM, IDM ed EMDI sul dimensionamento. Consultare l'articolo TECH235074 nel centro di supporto Symantec per informazioni sul dimensionamento di Riconoscimento moduli.)	Da 6 a 8 GB di RAM (vedere il <i>Manuale dell'amministratore di Symantec Data Loss Prevention</i> per informazioni sull'impatto di EDM, IDM ed EMDI sul dimensionamento. Consultare l'articolo TECH235074 nel centro di supporto Symantec per informazioni sul dimensionamento di Riconoscimento moduli.)
Disco	500 GB di archiviazione ibrida. Per le distribuzioni di Network Discover/Cloud Storage Discover sono necessari circa 150 MB di spazio su disco per mantenere gli indici di scansione incrementali. Ciò si basa su un sovraccarico di 5 MB per target di scansione incrementale e 50 byte per elemento nel target.	500 GB - 1 TB Vedere "Requisiti del database Oracle" a pagina 34.	140 GB	140 GB Per le distribuzioni di Network Discover/Cloud Storage Discover sono necessari circa 150 MB di spazio su disco per mantenere gli indici di scansione incrementali. Ciò si basa su un sovraccarico di 5 MB per target di scansione incrementale e 50 byte per elemento nel target.

Richiesto per	Enforce Server	Database Oracle	Network Monitor	Network Discover/Cloud Storage Discover, Network Prevent, Cloud Prevent for Email o Endpoint Prevent
NIC	1 NIC Ethernet 1 Gb/100 Mb in rame o fibra per comunicare con server di rilevamento.	N/D	1 NIC Ethernet 1 Gb/100 Mb in rame o fibra per comunicare con l'Enforce Server.	1 NIC Ethernet 1 Gb/100 Mb in rame o fibra per comunicare con l'Enforce Server.

Vedere "Requisiti del database Oracle" a pagina 34.

Vedere "L'effetto della scala sui requisiti di sistema" a pagina 10.

Requisiti hardware minimi per aziende grandi

La seguente tabella fornisce i requisiti di sistema per le installazioni grandi di Symantec Data Loss Prevention. Questa è un'installazione a tre livelli, in cui i database di Oracle e Enforce Server sono ospitati su computer diversi.

Nota: La dimensione predefinita del contenuto per il rilevamento è 30 MB. Se si prevede di eseguire la scansione file più grandi di 30 MB, vedere l'articolo <https://www.symantec.com/docs/TECH252393.html> nel Centro di supporto Symantec per informazioni sull'ottimizzazione del sistema per l'ispezione file di grandi dimensioni.

Tabella 2-6 Requisiti di sistema minimi per aziende grandi

Richiesto per	Enforce Server	Database Oracle	Network Monitor	Network Discover/Cloud Storage Discover, Network Prevent, Cloud Prevent for Email o Endpoint Prevent
Processore	CPU a quattro core	CPU a sei core	CPU a otto core	CPU a otto core

Richiesto per	Enforce Server	Database Oracle	Network Monitor	Network Discover/Cloud Storage Discover, Network Prevent, Cloud Prevent for Email o Endpoint Prevent
Memoria	<p>16 GB DI RAM</p> <p>(la dimensione di EDM/IDM e del profilo Riconoscimento moduli può aumentare i requisiti di memoria. Consultare il <i>Manuale dell'amministratore di Symantec Data Loss Prevention</i> per informazioni sul dimensionamento di EDM e IDM.</p> <p>Consultare l'articolo TECH235074 nel centro di supporto Symantec per informazioni sul dimensionamento Riconoscimento moduli.</p>	<p>32 GB DI RAM</p>	<p>8–16 GB di RAM (consultare il <i>Manuale dell'amministratore di Symantec Data Loss Prevention</i> per informazioni relative all'impatto sul dimensionamento di EDM, IDM ed EMDI.</p> <p>Consultare l'articolo TECH235074 nel centro di supporto Symantec per informazioni sul dimensionamento Riconoscimento moduli.</p>	<p>8–16 GB di RAM (consultare il <i>Manuale dell'amministratore di Symantec Data Loss Prevention</i> per informazioni relative all'impatto sul dimensionamento di EDM, IDM ed EMDI.</p> <p>Consultare l'articolo TECH235074 nel centro di supporto Symantec per informazioni sul dimensionamento Riconoscimento moduli.</p>
Requisiti del disco	<p>1 TB di archiviazione SSD.</p> <p>Per le distribuzioni di Network Discover/Cloud Storage Discover è necessario circa 1 GB di spazio su disco per mantenere gli indici di scansione incrementali. Ciò si basa su un sovraccarico di 5 MB per target di scansione incrementale e 50 byte per elemento nel target.</p>	<p>500 GB - 1 TB</p> <p>Vedere "Requisiti del database Oracle" a pagina 34.</p>	<p>140 GB</p>	<p>140 GB</p> <p>Per le distribuzioni di Network Discover/Cloud Storage Discover è necessario circa 1 GB di spazio su disco per mantenere gli indici di scansione incrementali. Ciò si basa su un sovraccarico di 5 MB per target di scansione incrementale e 50 byte per elemento nel target.</p>
NIC	<p>Per comunicare con i server di rilevamento:</p> <p>1 NIC Ethernet 1 Gb/100 Mb in rame o fibra</p>	<p>N/D</p>	<p>Per comunicare con l'Enforce Server:</p> <p>1 Ethernet 1 Gb/100 Mb in rame o fibra</p> <p>Per monitoraggio del traffico di rete (selezionare uno):</p> <p>1 NIC Ethernet 1 Gb/100 Mb in rame o fibra.</p>	<p>Per comunicare con l'Enforce Server:</p> <p>1 NIC Ethernet 1 Gb/100 Mb in rame o fibra</p>

Richiesto per	Enforce Server	Database Oracle	Network Monitor	Network Discover/Cloud Storage Discover, Network Prevent, Cloud Prevent for Email o Endpoint Prevent
Schede di acquisizione di pacchetti ad alta velocità	N/D	N/D	Vedere "Schede di acquisizione di pacchetti ad alta velocità" a pagina 50.	N/D

Vedere ["Requisiti del database Oracle"](#) a pagina 34.

Vedere ["L'effetto della scala sui requisiti di sistema"](#) a pagina 10.

Requisiti di sistema operativo per server

I server Symantec Data Loss Prevention possono essere installati su un sistema operativo Linux o Windows supportato. I diversi sistemi operativi possono essere utilizzati per diversi server in un ambiente eterogeneo.

Nota: Se si utilizza Windows Server 2012 R2, è necessario installare due patch. Vedere ["Installazione di patch per Windows Server 2012 R2"](#) a pagina 22.

Symantec Data Loss Prevention supporta i seguenti sistemi operativi a 64 bit per computer server di rilevazione ed Enforce Server:

- Microsoft Windows Server 2008 R2 SP1, Enterprise Edition con patch
- Microsoft Windows Server 2008 R2 SP1, Standard Edition con patch
- Microsoft Windows Server 2012 R2, Datacenter Edition con patch
Vedere ["Installazione di patch per Windows Server 2012 R2"](#) a pagina 22.
- Microsoft Windows Server 2012 R2, Standard Edition con patch
Vedere ["Installazione di patch per Windows Server 2012 R2"](#) a pagina 22.
- Microsoft Windows Server 2016, Standard Edition
- Microsoft Windows Server 2016, Datacenter Edition
- Red Hat Enterprise Linux 6.8, 6.9 e 6.10
Vedere ["Installazione di tipi di carattere su server Linux"](#) a pagina 24.
- Red Hat Enterprise Linux da 7.3 a 7.5
Vedere ["Installazione di tipi di carattere su server Linux"](#) a pagina 24.
- Oracle Linux 7.3 e 7.4

Vedere ["Installazione di tipi di carattere su server Linux"](#) a pagina 24.

Symantec Data Loss Prevention supporta i sistemi operativi a 64 bit per i computer server di rilevamento su Microsoft Windows Server 2016, Core.

Requisiti del sistema operativo per distribuzioni di server singolo

Symantec Data Loss Prevention supporta i seguenti sistemi operativi a 64 bit per distribuzioni di server singolo:

- Microsoft Windows Server 2008 R2 SP1, Enterprise Edition con patch
- Microsoft Windows Server 2008 R2 SP1, Standard Edition con patch
- Microsoft Windows Server 2012 R2, Datacenter Edition con patch
Vedere ["Installazione di patch per Windows Server 2012 R2"](#) a pagina 22.
- Microsoft Windows Server 2012 R2, Standard Edition con patch
Vedere ["Installazione di patch per Windows Server 2012 R2"](#) a pagina 22.
- Microsoft Windows Server 2016, Standard Edition
- Microsoft Windows Server 2016, Datacenter Edition
- Red Hat Enterprise Linux 6.8, 6.9 e 6.10
Vedere ["Installazione di tipi di carattere su server Linux"](#) a pagina 24.
- Red Hat Enterprise Linux da 7.3 a 7.5
Vedere ["Installazione di tipi di carattere su server Linux"](#) a pagina 24.
- Oracle Linux 7.3 e 7.4
Vedere ["Installazione di tipi di carattere su server Linux"](#) a pagina 24.

Sono supportate la lingua inglese e le versioni localizzate dei sistemi operativi Linux e Windows.

Vedere ["Lingue supportate per il rilevamento"](#) a pagina 31.

Consultare inoltre il *Manuale dell'amministratore di Symantec Data Loss Prevention* per informazioni dettagliate sulle lingue e sui set di caratteri supportati. È possibile individuare il *Manuale dell'amministratore di Symantec Data Loss Prevention* nel centro di supporto Symantec qui: <http://www.symantec.com/docs/DOC9261>.

Requisiti di sistema operativo per l'agente del controller di dominio

L'agente del controller di dominio consente di risolvere i nomi utente dagli indirizzi IPv4 negli incidenti HTTP/S e FTP. Consultare il *Manuale di installazione di Symantec Data Loss Prevention* per i dettagli di installazione dell'agente del controller di dominio.

Symantec Data Loss Prevention supporta i seguenti sistemi operativi per l'agente del controller di dominio:

- Microsoft Windows Server 2008 R2, Enterprise Edition (a 64 bit)

- Microsoft Windows Server 2008 R2, Standard Edition (a 64 bit)
- Microsoft Windows Server 2008 R2 SP1, Enterprise Edition (a 64 bit) con patch
- Microsoft Windows Server 2008 R2 SP1, Standard Edition (a 64 bit) con patch
- Microsoft Windows Server 2012, Datacenter Edition (a 64 bit)
- Microsoft Windows Server 2012, Standard Edition (a 64 bit)
- Microsoft Windows Server 2012 R2, Datacenter Edition con patch
 Vedere ["Installazione di patch per Windows Server 2012 R2"](#) a pagina 22.
- Microsoft Windows Server 2012 R2, Standard Edition con patch
 Vedere ["Installazione di patch per Windows Server 2012 R2"](#) a pagina 22.

Installazione di patch per Windows Server 2012 R2

Se si utilizza Windows Server 2012 R2, è necessario installare tre patch Microsoft: KB2919355, KB2919442 e KB2999226.

Accedere all'indirizzo <https://support.microsoft.com/en-us/kb/2919355> e installare KB2919355.

Accedere all'indirizzo <https://support.microsoft.com/en-us/kb/2919442> e installare KB2919442.

Accedere all'indirizzo <https://support.microsoft.com/en-us/kb/2999226> e installare KB2999226.

Installazione di tipi di carattere su server Linux

Sui server Linux è necessario che sia installato almeno un tipo di carattere. Tuttavia, Symantec consiglia di installare tutti i tipi di carattere disponibili sul server Linux se si intende utilizzare il rilevamento Riconoscimento moduli. Per installare tutti i tipi di carattere disponibili, eseguire:
`yum groupinstall fonts` su ogni server Linux Enforce e di rilevamento.

Linee guida di partizione Linux

I requisiti di spazio libero minimo per partizioni Linux variano in base ai dettagli specifici dell'installazione Symantec Data Loss Prevention. La tabella seguente fornisce linee guida generali che dovrebbero essere adattate all'installazione in base alla garanzia delle circostanze. Symantec consiglia di utilizzare partizioni separate per i diversi file system, come indicato nella tabella. Se si combinano più file system in un numero minore di partizioni o in una singola partizione radice, assicurarsi che la partizione disponga di spazio libero sufficiente per conservare le dimensioni combinate dei file system elencati nella tabella.

Nota: Le linee guida delle dimensioni di partizione per server di rilevamento sono simili a quelle per Enforce Server senza un database Oracle.

Vedere [Tabella 2-8](#) a pagina 23.

Tabella 2-7 Le linee guida delle dimensioni minime di partizione Linux—Enforce Server con database Oracle

Partizione	Spazio libero minimo	Descrizione e commenti
/home	6 GB	Memorizzare gli strumenti di installazione Oracle, i file ZIP di installazione Oracle e i file di aggiornamento della patch critica Oracle (CPU) in /home.
/tmp	1.2 GB	Gli strumenti di installazione e il programma di installazione Oracle richiedono spazio in questa directory.
/opt	500 GB per installazioni piccole/medie 1 TB per installazioni grandi	Contiene programmi installati come Symantec Data Loss Prevention, server Oracle e database Oracle. Il database Oracle richiede spazio significativo in questa directory. Per prestazioni migliorate, è possibile desiderare di installare questa partizione in dischi/SAN/RAID diversi da quelli in cui la partizione radice è installata.
/var	15 GB per installazioni piccole/medie 46 GB per installazioni grandi	Contiene i registri, gli indici EDM/IDM, gli indici Riconoscimento moduli, gli indici di scansione incrementale e le directory di acquisizione dei pacchetti di rete. Nota: Le directory /var/spool/pcap e /var/SymantecDLP/drop_pcap devono trovarsi nella stessa partizione o nello stesso punto di installazione.
/boot	100 MB	Deve trovarsi nella stessa partizione ext2 o ext3, non parte di softRAID (hardware RAID supportato).
swap	Uguale a RAM	Se è necessario il dump della memoria in caso di arresto del sistema (per debug), è preferibile aumentare le quantità.

Tabella 2-8 Le linee guida delle dimensioni minime di partizione Linux—Enforce Server senza un database o server di rilevamento

Partizione	Linee guida delle dimensioni minime	Descrizione e commenti
/opt	10 GB	Contiene programmi installati come Symantec Data Loss Prevention e il client Oracle.

Partizione	Linee guida delle dimensioni minime	Descrizione e commenti
/var	15 GB per installazioni piccole/medie 46 GB per installazioni grandi	Contiene i registri, gli indici EDM/IDM, gli indici Riconoscimento moduli, gli indici di scansione incrementale e le directory di acquisizione dei pacchetti di rete. Nota: Le directory /var/spool/pcap e /var/Symantec/DataLossPrevention/drop_pcap devono trovarsi nella stessa partizione o nello stesso punto di installazione.
/boot	100 MB	Deve trovarsi nella stessa partizione ext2 o ext3, non parte di softRAID (hardware RAID supportato).
swap	Uguale a RAM	Se è necessario il dump della memoria in caso di arresto del sistema (per debug), è preferibile aumentare le quantità.

Installazione di tipi di carattere su server Linux

Sui server Linux è necessario che sia installato almeno un tipo di carattere. Tuttavia, Symantec consiglia di installare tutti i tipi di carattere disponibili sul server Linux se si intende utilizzare il rilevamento Riconoscimento moduli. Per installare tutti i tipi di carattere disponibili, eseguire: `yum groupinstall fonts` su ogni server Linux Enforce e di rilevamento.

Requisiti di sistema operativo per server OCR

Symantec supporta la distribuzione dei server OCR sul sistema operativo Windows. Gli stessi server Windows supportati per l'installazione di Enforce Server sono supportati per l'installazione dei server OCR.

Vedere "Requisiti di sistema operativo per server" a pagina 20.

Per ulteriori informazioni sui requisiti di sistema per i server OCR e le linee guida di dimensionamento, vedere "Symantec Data Loss Prevention Requisiti di sistema e stime del dimensionamento per i server OCR" all'indirizzo <http://www.symantec.com/docs/doc10612>.

Requisiti del computer endpoint per Symantec DLP Agent

Se si installa Endpoint Prevent, i computer endpoint su cui viene installato Symantec DLP Agent devono soddisfare i requisiti descritti nelle seguenti sezioni.

- Vedere ["Requisiti di sistema operativo per sistemi endpoint"](#) a pagina 25.
- Vedere ["Requisiti di memoria e spazio su disco per Symantec DLP Agent"](#) a pagina 30.

Requisiti di sistema operativo per sistemi endpoint

Endpoint Data Loss Prevention può funzionare su sistemi Endpoint che utilizzano i seguenti sistemi:

Tabella 2-9 Sistemi operativi Windows supportati da Endpoint Data Loss Prevention

Sistema operativo	Versione	Versione DLP 14.0	Versione DLP 14.5	DLP versione 14.6	DLP versione 15.0	DLP versione 15.1	DLP versione 15.5
Windows Server	2003 SP2 R2	Sì	No	Sì	No	No	No
Windows Server Enterprise o Standard (a 64 bit)	2008 R2	Sì	Sì	Sì	Sì	Sì	Sì
	2012 R2	Sì	Sì	Sì	Sì	Sì	Sì
Microsoft Windows Server 2016 Standard o Datacenter Edition (a 64 bit)	Nessun service pack	No	No	Sì (su DLP Agent versione 14.6 MP1 e MP2)	Sì	Sì	Sì
Windows 7 Enterprise, Professional, Ultimate (32 bit)	Nessun service pack	Sì	Sì	Sì	No	No	No
	SP1	Sì	Sì	Sì	Sì	Sì	Sì
Windows 7 Enterprise, Professional, Ultimate (64 bit)	Nessun service pack	Sì	Sì	Sì	No	No	No
	SP1	Sì	Sì	Sì	Sì	Sì	Sì

Sistema operativo	Versione	Versione DLP 14.0	Versione DLP 14.5	DLP versione 14.6	DLP versione 15.0	DLP versione 15.1	DLP versione 15.5
Sistema operativo Windows 8 Enterprise PC (32 bit)	Senza patch	No	No	No	No	No	No
Sistema operativo Windows 8 Enterprise PC (64 bit)	Senza patch	Sì	Sì	Sì	No	No	No
Sistema operativo Windows 8.1 Enterprise, Pro PC (a 64 bit)	Senza patch	Sì	Sì	Sì	Sì	Sì	Sì
	Update 1	Sì	Sì	Sì	Sì	Sì	Sì
	Update 2	Sì	Sì	Sì	Sì	Sì	Sì
	Update 3	Sì	Sì	Sì	Sì	Sì	Sì

Sistema operativo	Versione	Versione DLP 14.0	Versione DLP 14.5	DLP versione 14.6	DLP versione 15.0	DLP versione 15.1	DLP versione 15.5
Sistema operativo Windows 10 Enterprise, Pro PC (a 64 bit)	Senza patch	Sì (14.0.1)	Sì	Sì	Sì	No	No
	Versione 1511 (November Update)	No	Sì	Sì	Sì	Obsoleta	Obsoleta
	Versione 1607 (Anniversary Update)	No	Sì	Sì	Sì	Obsoleta	Obsoleta
	Creators Update (versione 1703)	No	No	Sì (sulla versione 14.6 MP1 e MP2 di DLP Agent)	Sì	Sì	Sì
	Versione 1709 (Fall Creators Update)	No	No	Sì (sulla versione 14.6 MP1 e MP2 di DLP Agent)	Sì	Sì	Sì
	Versione 1803 (April 2018 Update) [build #17134.48]	No	No	No	Sì (sulla versione 15.0 MP1 di DLP Agent)	Sì	Sì
	Versione 1607 LTSC	No	No	No	No	Sì (nella versione 15.1 MP1 di DLP Agent)	Sì
	Creators Update (versione 1809)	No	No	No	No	Sì (nella versione 15.1 MP1 di DLP Agent)	Sì

Per dettagli aggiuntivi relativi al supporto di Windows 10 Creators Update, consultare l'articolo [TECH240808](#) nel centro di supporto Symantec.

Tabella 2-10 Sistemi operativi macOS supportati da Endpoint Data Loss Prevention

Sistema operativo	Versione DLP 14.0	Versione DLP 14.5	DLP versione 14.6	DLP versione 15.0	DLP versione 15.1	DLP versione 15.5
Apple macOS 10.8 (a 64 bit)	Sì	No	No	No	No	No
Apple macOS 10.9 (a 64 bit)	Sì	Sì	Sì	No	No	No
Apple macOS 10.10 (a 64 bit)	Sì	Sì	Sì	Obsoleta	No	No
Apple macOS 10.11 (a 64 bit)	No	Sì	<ul style="list-style-type: none"> Fino alla 10.11.5 10.11.6 su 14.6 MP2 con Hotfix 14.6.0205 	<ul style="list-style-type: none"> Fino alla 10.11.5 10.11.6 su 15.0 MP1 con Hotfix 15.0.0101 	Sì	Sì
Apple macOS 10.12 (a 64 bit)	No	Sì (nella versione 14.5 MP1 di DLP Agent)	<ul style="list-style-type: none"> Fino alla 10.12.5 sulla versione 14.6 MP1 di DLP Agent 10.12.6 su 14.6 MP2 con Hotfix 14.6.0205 	<ul style="list-style-type: none"> Fino alla 10.12.5 10.12.6 su 15.0 MP1 con Hotfix 15.0.0101 	Sì	Sì

Sistema operativo	Versione DLP 14.0	Versione DLP 14.5	DLP versione 14.6	DLP versione 15.0	DLP versione 15.1	DLP versione 15.5
Apple macOS 10.13 (a 64 bit)	No	No	<ul style="list-style-type: none"> ■ 10.13.1 sulla versione 14.6 MP2 di DLP Agent ■ 10.13.2 su 14.6 MP2 con Hotfix 14.6.0205 ■ 10.13.3 su 14.6 MP2 con Hotfix 14.6.0205 ■ 10.13.4 su 14.6 MP2 con Hotfix 14.6.0205 <p>Per visualizzare dettagli aggiuntivi, consultare questa tabella.</p>	<ul style="list-style-type: none"> ■ 10.13.1 sulla versione 15.0 di DLP Agent ■ 10.13.2 sulla versione 15.0 MP1 con Hotfix 15.0.0101 ■ 10.13.3 sulla versione 15.0 MP1 con Hotfix 15.0.0101 ■ 10.13.4 sulla versione 15.0 MP1 con Hotfix 15.0.0101 ■ 10.13.5 sulla versione 15.0 MP1 con Hotfix 15.0.0107.01001 ■ 10.13.6 sulla versione 15.0 MP1 con Hotfix 15.0.0107.01001 <p>Per visualizzare dettagli aggiuntivi, consultare questa tabella.</p>	Sì (fino a 10.13.6)	Sì (fino a 10.13.6)

Sistema operativo	Versione DLP 14.0	Versione DLP 14.5	DLP versione 14.6	DLP versione 15.0	DLP versione 15.1	DLP versione 15.5
Apple macOS 10.14 (a 64 bit)	No	No	No	No	10.14.1 e 10.14.2 nella versione 15.1 MP1 Per visualizzare dettagli aggiuntivi, consultare questa tabella.	Sì

Ulteriori informazioni sul supporto di macOS sono disponibili nei seguenti articoli del centro di supporto Symantec:

- [Problemi noti relativi all'utilizzo di macOS 10.13 sulle versioni 14.6 MP2 e 15.0 di DLP Agent](#)
- [DLP Agent distribuito con profili MDM su macOS 10.13.2 non si carica](#)
- [Monitoraggio delle applicazioni macOS in cui SIP è attivato](#)
- [Utilizzo di Accesso ai file di applicazione per monitorare Safari su macOS 10.12.4 e versioni successive](#)
- [Problemi noti relativi all'upgrade da macOS 10.13.6 a macOS 10.14 con le versioni 15.1 di DLP Agent](#)

I Symantec DLP Agent possono inoltre essere installati su versioni localizzate supportate di questi sistemi operativi Windows e macOS.

Vedere ["Lingue supportate per il rilevamento"](#) a pagina 31.

Consultare inoltre il *Manuale dell'amministratore di Symantec Data Loss Prevention* per informazioni dettagliate sulle lingue e sui set di caratteri supportati.

Requisiti di memoria e spazio su disco per Symantec DLP Agent

A seconda della versione, il software Symantec DLP Agent riserva un minimo di 25-30 MB della memoria sul computer endpoint. DLP Agent utilizza temporaneamente memoria aggiuntiva mentre rileva il contenuto o comunica con il server Endpoint Prevent. Al termine di queste attività, l'utilizzo della memoria torna al minimo precedente.

L'installazione iniziale di Symantec DLP Agent utilizza tra 70 e 80 MB circa di spazio su disco. L'importo minimo effettivo dipende dalla dimensione e dal numero di politiche che si distribuiscono al computer endpoint. È quindi necessario spazio su disco aggiuntivo per archiviare temporaneamente i dati degli incidenti sul computer endpoint fino a quando Symantec

DLP Agent non invia i dati al server Endpoint Prevent. Se il computer endpoint non è in grado di connettersi al server Endpoint Prevent per un periodo di tempo prolungato, Symantec DLP Agent continua a utilizzare spazio su disco aggiuntivo man mano che vengono creati nuovi incidenti. Lo spazio su disco viene liberato solo dopo che il software dell'agente si riconnette al server Endpoint Prevent e trasferisce gli incidenti archiviati.

Nota: La dimensione predefinita del contenuto per il rilevamento è 30 MB. Se si prevede di eseguire la scansione di file più grandi di 30 MB, vedere l'articolo <https://www.symantec.com/docs/TECH252393.html> nel Centro di supporto Symantec per informazioni sull'ottimizzazione del sistema per l'ispezione di file di grandi dimensioni.

Lingue supportate per il rilevamento

Symantec Data Loss Prevention supporta molte lingue per il rilevamento. È possibile definire politiche che rilevano e segnalano accuratamente le violazioni trovate nel contenuto in queste lingue:

- Arabo
- Portoghese (Brasile)
- Cinese (tradizionale)
- Cinese (semplificato)
- Ceco
- Danese
- Olandese
- Inglese
- Finlandese
- Francese
- Tedesco
- Greco
- Ebraico
- Ungherese
- Italiano
- Giapponese
- Coreano

- Norvegese
- Polacco
- Portoghese
- Romeno
- Russo
- Spagnolo
- Svedese
- Turco*

* Symantec Data Loss Prevention non può essere installato su un sistema operativo Windows in lingua turca e non è possibile scegliere il turco come impostazioni locali alternative.

Per informazioni supplementari su specifiche lingue, vedere le *Note sulla versione di Symantec Data Loss Prevention*.

Questo supporto non include quanto segue:

- Supporto tecnico fornito in una lingua diversa dall'inglese. Sebbene Symantec Data Loss Prevention supporti una particolare lingua, ciò non implica che il supporto tecnico sia fornito in quella lingua.
- Interfaccia utente amministrativa e documentazione localizzate. Il supporto per una lingua non implica che l'interfaccia utente o la documentazione del prodotto sia stata localizzata in quella lingua. Tuttavia, anche senza un'interfaccia utente localizzata, parti della stessa definite dall'utente, come i messaggi di notifica sull'endpoint, possono ancora essere localizzate in qualsiasi lingua digitando il testo appropriato nell'interfaccia.
- Contenuto localizzato. Le parole chiave sono utilizzate in varie aree del prodotto, tra cui i modelli di politica e gli identificatori di dati. Il supporto per una lingua non implica che queste parole chiave siano state tradotte in quella lingua. Gli utenti possono tuttavia aggiungere parole chiave in una nuova lingua mediante la console di amministrazione di Enforce Server.
- Nuovi tipi di file, protocolli, applicazioni o codifiche. Il supporto per una lingua non implica l'assistenza per qualsiasi nuovo tipo di file, protocollo, applicazione o codifica che possono risultare prevalenti in quella lingua o regione.
- Normalizzazione specifica di una lingua. Un esempio di normalizzazione è considerare come uguali le versioni accentate e non accentate di un carattere. Il prodotto realizza già una serie di normalizzazioni, tra cui la normalizzazione Unicode standard che dovrebbe coprire la stragrande maggioranza dei casi. Tuttavia, non significa che tutte le normalizzazioni potenziali sono incluse.
- Normalizzazione e convalida specifica di un'area geografica. Un esempio è la consapevolezza che il prodotto ha del formato dei numeri di telefono nordamericani, che

consente di considerare come uguali differenti versioni di un numero e di identificare i numeri non validi nei file di origine EDM. Il supporto per una lingua non implica questo tipo di funzionalità per quella lingua o area geografica.

Gli elementi in queste categorie sono gestiti come singoli potenziamenti del prodotto specifici di una lingua o di un'area geografica. Contattare il supporto tecnico Symantec per informazioni supplementari sui potenziamenti relativi alle lingue o sulle lingue non elencate.

Supporti lingue disponibili

È possibile installare uno qualsiasi dei supporti lingue disponibili per la distribuzione di Symantec Data Loss Prevention. I supporti lingue forniscono una serie limitata di lingue diverse dall'inglese per l'interfaccia utente e la guida in linea della console di amministrazione di Enforce Server. Tenere presente che questi supporti lingue servono unicamente per fornire la traduzione di interfaccia utente e guida in linea; non sono necessari per il rilevamento di dati. Inoltre, il supporto lingue contiene anche le versioni tradotte di parte della documentazione di Symantec Data Loss Prevention.

Man mano che diventano disponibili, i supporti lingue di Symantec Data Loss Prevention vengono distribuiti insieme ai prodotti software che supportano. È inoltre possibile scaricare e aggiungere un supporto lingue a un'installazione esistente. I supporti lingue non richiedono acquisti o licenze aggiuntivi. Per informazioni dettagliate su come aggiungere e abilitare un supporto lingue, consultare il *Manuale dell'amministratore di Symantec Data Loss Prevention*. I supporti lingue vengono distribuiti nel file `Symantec_DLP_15.5_Lang_Pack-ML.zip` sul sito Web di Symantec FileConnect. Quando si estrae il contenuto del file ZIP, i singoli file del supporto lingue hanno nomi nel seguente formato:

`Symantec_DLP_15.5_Lang_Pack_<lingua>.zip`

Tabella 2-11 elenca i supporti lingue disponibili.

Tabella 2-11 Supporti lingue e corrispondenti codici internazionali

Lingua	Codice internazionale
Portoghese brasiliano	PT_BR
Cinese (semplificato)	ZH_CN
Cinese (tradizionale)	ZH_TW
Francese	FR_FR
Tedesco	DE_DE
Italiano	IT_IT
Giapponese	JA_JP

Lingua	Codice internazionale
Coreano	KO_KR
Spagnolo messicano	ES_MX
Russo	RU_RU

Nota: Non tutti i supporti lingue sono disponibili al momento del rilascio di un prodotto.

Requisiti del database Oracle

Symantec Data Loss Prevention supporta i seguenti database Oracle:

- Oracle 12c Enterprise Edition Release 2 (12.2.0.1)
Oracle 12.1.0.2 e 12.2.0.1 vengono testate con lo schema Symantec Data Loss Prevention. È necessario ottenere il software e il supporto da Oracle. Per i dettagli di implementazione, vedere la *Guida all'implementazione di Symantec Data Loss Prevention Oracle 12C Enterprise*, disponibile qui:
<http://www.symantec.com/docs/DOC9260>
- Oracle 12c Standard Edition 2 Release 2 (12c SE2 R2) (12.2.0.1)
Symantec fornisce Oracle 12.2.0.1 con Symantec Data Loss Prevention. Vedere il *Symantec Data Loss Prevention Manuale di installazione e aggiornamento di Oracle 12C Standard Edition 2 Release 2* per installare Oracle, disponibile qui:
<http://www.symantec.com/docs/DOC10713>

Symantec supporta la versione Standard Edition 2 del Database Oracle, ma lo schema del database Symantec Data Loss Prevention è supportato su tutte le versioni di Oracle.

Symantec Data Loss Prevention richiede il database Oracle per utilizzare il set di caratteri AL32UTF8. Se il database è configurato per un diverso set di caratteri, il programma di installazione avvisa l'utente e annulla l'installazione.

È possibile installare Oracle su un server dedicato (distribuzione a tre livelli) o sullo stesso computer di Enforce Server (distribuzione a uno o due livelli):

- Distribuzione a tre livelli.
I requisiti di sistema per un server Oracle dedicato sono elencati di seguito. Tenere presente che le distribuzioni del server Oracle dedicato richiedono inoltre l'installazione di Oracle 12c Client su computer Enforce Server per comunicare con l'istanza Oracle 12c SE2 remota.
- Distribuzioni a uno e due livelli.
Quando l'installazione avviene su un computer Enforce Server, i requisiti di sistema Oracle sono gli stessi di quelli di Enforce Server.

Vedere ["Requisiti hardware minimi per installazioni a un livello"](#) a pagina 13.

Vedere ["Requisiti minimi dell'hardware per installazioni molto piccole"](#) a pagina 13.

Se si installa Oracle su un server dedicato, tale computer deve rispettare i seguenti requisiti minimi di sistema per Symantec Data Loss Prevention:

- Uno dei seguenti sistemi operativi:
 - Microsoft Windows Server 2008 R2 Standard o Enterprise (64 bit)
 - Microsoft Windows Server 2008 R2 SP1 Standard o Enterprise (64 bit)
 - Microsoft Windows Server 2012 R2 Standard, Enterprise o Datacenter (64 bit)
 - Microsoft Windows Server 2016 Standard o Datacenter (64 bit)
 - Red Hat Enterprise Linux 6.9 (64 bit)
 - Red Hat Enterprise Linux da 7.3 a 7.5 (a 64 bit)
 - Oracle Linux 7.3
- 8-32 GB di RAM
- 8-16 GB di spazio di scambio (pari a RAM fino a 16 GB)
- 500 GB – 1 TB di spazio su disco per database Enforce

Su un sistema Linux, se il database Oracle si trova sullo stesso computer di Enforce Server, il file system `/opt` deve disporre di almeno 500 GB di spazio libero per installazioni medie o piccole. 1 TB di spazio libero è obbligatorio per le installazioni di grandi dimensioni. Se Oracle è installato su un diverso computer da Enforce Server, il file system `/opt` deve disporre di almeno 10 GB di spazio libero e il file system `/boot` di almeno 100 MB di spazio libero.

La quantità esatta di spazio su disco necessaria per il database Enforce dipende da variabili quali:

- Il numero di politiche che si desidera inizialmente distribuire
- Il numero di politiche che si desidera aggiungere nel tempo
- Il numero e le dimensioni degli allegati da memorizzare (se si decide di memorizzare allegati con i relativi incidenti)
- La durata di memorizzazione degli incidenti

Consultare il *Manuale dell'amministratore di Symantec Data Loss Prevention* per ulteriori informazioni sullo sviluppo di politiche.

Per ulteriori informazioni sull'installazione di Oracle, consultare il *Manuale all'installazione e all'aggiornamento di Symantec Data Loss Prevention su Oracle*.

Requisiti del browser per l'accesso alla console di amministrazione dell'Enforce Server

È possibile accedere alla console di amministrazione dell'Enforce Server mediante uno dei seguenti browser:

- Microsoft Internet Explorer 10 o 11
- Mozilla Firefox da 58 a 62 e Firefox Enterprise (ESR) 60.

È necessario utilizzare Adobe Flash Player, versione minima 27, per visualizzare il Report rischi cartelle per Network Discover/Cloud Storage Discover (**Incidenti > Discover > Report rischi cartelle**).

Distribuzione di Data Loss Prevention in infrastrutture cloud pubbliche

Symantec supporta la distribuzione dei server di Data Loss Prevention nei cloud pubblici Amazon Web Services (AWS), Microsoft Azure e Oracle Cloud.

Distribuzione di Symantec Data Loss Prevention nell'infrastruttura Amazon Web Services

Tabella 2-12 elenca i server e i sistemi operativi supportati per la distribuzione di Data Loss Prevention in AWS.

Tabella 2-12 Distribuzione di Symantec Data Loss Prevention 12.5 - 15.5 in AWS

Server di Data Loss Prevention	Sistemi operativi
Enforce Server con il database Oracle nello stesso computer (distribuzioni a due livelli)	Microsoft Windows Server 2012 R2 con patch
Cloud Prevent for Email	Microsoft Windows Server 2016
Network Prevent for Web	Red Hat Enterprise Linux 6.8, 6.9 e 6.10
Network Prevent for Email	Red Hat Enterprise Linux da 7.3 a 7.5
Endpoint Prevent	Nota: Le distribuzioni di AWS AMI in RHEL 6.x e 7.x richiedono un pacchetto aggiuntivo. Vedere il riferimento di seguito.
Network Discover/Cloud Storage Discover	

Per ulteriori informazioni, vedere *Distribuzione di Symantec Data Loss Prevention nell'infrastruttura Amazon Web Services (AWS)* all'indirizzo <http://www.symantec.com/docs/DOC9520>.

Distribuzione di Symantec Data Loss Prevention in Microsoft Azure

[Tabella 2-13](#) elenca i server e i sistemi operativi supportati per la distribuzione di Data Loss Prevention in Microsoft Azure.

Tabella 2-13 Distribuzione di Symantec Data Loss Prevention in Microsoft Azure

Server di Data Loss Prevention	Sistemi operativi
Enforce Server con database Oracle	Windows Server 2012 R2 con patch
Cloud Prevent for Email	Windows Server 2016
Network Prevent for Web	Red Hat Enterprise Linux 6.8 e 6.9
Network Prevent for Email	Red Hat Enterprise Linux 7.3 e 7.4
Endpoint Prevent	
Network Discover/Cloud Storage Discover	

Symantec supporta l'utilizzo del bilanciamento del carico di Azure per bilanciare le connessioni dei client endpoint a Endpoint Server.

Distribuzione di Symantec Data Loss Prevention in Oracle Cloud

Symantec Data Loss Prevention è supportato nei seguenti ambienti:

- Oracle Cloud IaaS
- Oracle Bare Metal Cloud con istanze di computer virtuali (VM) gestiti

[Tabella 2-14](#) elenca i server e i sistemi operativi supportati per la distribuzione di Data Loss Prevention in Oracle Cloud Infrastructure as a Service.

Tabella 2-14 Distribuzione di Symantec Data Loss Prevention in Oracle Cloud Infrastructure as a Service

Server di Data Loss Prevention	Sistemi operativi e configurazione
Enforce Server con il database Oracle nello stesso computer (distribuzioni a due livelli)	Oracle Linux 7.3 con kernel RHCK
Network Prevent for Email	
Endpoint Prevent	
Network Discover	

Nota: Le distribuzioni a tre livelli di Symantec Data Loss Prevention non sono supportate in Oracle.

Supporto di server virtuali

Symantec supporta l'esecuzione di server Symantec Data Loss Prevention su VMware ESXi 6.x e prodotti di virtualizzazione Windows Hyper-V, ammesso che l'ambiente di virtualizzazione stia eseguendo un sistema operativo supportato.

Nota: Le appliance virtuali di Symantec Data Loss Prevention sono supportati in un ambiente di virtualizzazione su VMware ESXi 5.5.0 Update 2 e VMware ESXi 6.5.

Vedere ["Requisiti di sistema operativo per server"](#) a pagina 20.

Assicurarsi che ogni ambiente di server virtuale disponga dei requisiti di sistema per i server descritti in questo documento.

Vedere ["Requisiti di sistema minimi per i server di Symantec Data Loss Prevention"](#) a pagina 12.

Durante la configurazione di un ambiente di server virtuale considerare le seguenti informazioni di supporto:

- I server Endpoint Prevent sono supportati solo per configurazioni che non superano il numero consigliato di agenti connessi.
- Symantec non supporta l'esecuzione del server di database Oracle su hardware virtuale VMware ESXi 5.x, VMware ESXi 5.x e VMware ESX 6.x. Se si distribuisce Enforce Server su un computer virtuale, è necessario installare il database Oracle mediante un hardware di server fisico.
- Symantec supporta l'esecuzione di server di database Enforce Server e in un ambiente Windows Hyper-V.
- Symantec non supporta installazioni server singolo su computer virtuali.

Diversi fattori influenzano le prestazioni del computer virtuale, incluso il numero di CPU, la quantità di RAM dedicata e le prenotazioni di risorse per i cicli della CPU e la RAM. Il sovraccarico di virtualizzazione e del sistema operativo guest può portare a un degrado delle prestazioni nel throughput grandi set di dati confrontati a un sistema che funziona sull'hardware fisico. Utilizzare i propri risultati di test come base per ridimensionare le distribuzioni su computer virtuali.

Per informazioni aggiuntive sul funzionamento di server Network Prevent su computer virtuali consultare le *linee guida sul dimensionamento delle prestazioni di Network Monitor e Prevent di Symantec Data Loss Prevention*, disponibili nel centro di supporto Symantec all'indirizzo <http://www.symantec.it/docs/DOC8253>.

Supporto desktop virtuale e applicazione virtuale con Endpoint Prevent

È possibile distribuire DLP Agent nei computer virtuali Citrix e VMware per monitorare i desktop virtuali e impedire agli utenti remoti di copiare i dati sensibili che sono accessibili tramite un desktop virtuale.

Supporto per la virtualizzazione Citrix

L'esecuzione di DLP Agente è supportata nelle seguenti workstation virtuali Citrix XenDesktop e configurazioni server Citrix XenApp:

- Citrix XenApp
 - Citrix XenApp 6.5 in Windows Server 2008 Enterprise Edition R2 (64 bit)
 - Citrix XenApp 7.6 in Windows Server 2008 Enterprise Edition R2 (a 64 bit) e Windows Server 2012 R2 Standard Edition
 - Citrix XenApp 7.9 in Windows Server 2008 Enterprise Edition R2 (a 64 bit) e Windows Server 2012 R2 Standard Edition
 - Citrix XenApp 7.11 in Windows Server 2008 Enterprise Edition R2 (a 64 bit) e Windows Server 2012 R2 Standard Edition
 - Citrix XenApp 7.12 in Windows Server 2008 Enterprise Edition R2 (a 64 bit) e Windows Server 2012 R2 Standard Edition
 - Citrix XenApp 7.13 in Windows Server 2008 Enterprise Edition R2 (a 64 bit) e Windows Server 2012 R2 Standard Edition
 - Citrix XenApp 7.14 in Windows Server 2008 Enterprise Edition R2 (a 64 bit) e Windows Server 2012 R2 Standard Edition
 - Citrix XenApp 7.15 su Windows Server 2016 Standard Edition
 - Citrix XenApp 7.15 Long Term Service Release (LTSR), Update 2 su Windows Server 2016 Standard Edition
 - Citrix XenApp 7.16 su Windows Server 2016 Standard Edition
 - Citrix XenApp 7.17 su Windows Server 2016 Standard Edition
 - Citrix XenApp 7.18 su Windows Server 2016 Standard Edition

Nota: I file salvati da Microsoft Office (utilizzando Salva con nome) nelle unità client ospitate su Citrix XenApp (da 7.13 a 7.18) non sono monitorati. Tuttavia, se si esegue Citrix XenApp 7.13 o una versione successiva con Virtual Delivery Agent (VDA) versione 7.12, i file salvati nelle unità client (utilizzando Salva con nome) sono monitorati. È possibile trovare la procedura di attivazione del monitoraggio per queste operazioni di salvataggio per il seguente articolo del centro di supporto Symantec:

<http://www.symantec.com/docs/TECH249988>

- Citrix XenDesktop
 - Citrix XenDesktop 7.6 in Windows 7 SP1 (32 bit o 64 bit)
 - Citrix XenDesktop 7.9 in Windows 7 SP1 (a 32 o 64 bit), in Windows 8.0, 8.1 e Windows 10 (a 64 bit)
 - Citrix XenDesktop 7.12 in Windows 7 SP1 (a 32 o 64 bit) e in Windows 10 (a 64 bit)
 - Citrix XenDesktop 7.12 in Windows 7 SP1 (a 32 o 64 bit) e in Windows 10 (a 64 bit)
 - Citrix XenDesktop 7.14 in Windows 7 SP1 (a 32 o 64 bit) e in Windows 10 (a 64 bit)
 - Citrix XenDesktop 7.15 in Windows 7 SP1 (a 64 bit) e Windows 10 RS2 (a 64 bit)
 - Citrix XenDesktop 7.15 Long Term Service Release (LTSR), Update 2 su Windows 7 SP1 (a 64 bit) e Windows 10 RS4 (versione 1803) (a 64 bit)
 - Citrix XenDesktop 7.16 su Windows 10 RS2 (a 64 bit)
 - Citrix XenDesktop 7.17 su Windows 10 RS3 (versione 1703) (a 64 bit)
 - Citrix XenDesktop 7.18 su Windows 10 RS4 (versione 1803) (a 64 bit)

Nota: I file salvati da Microsoft Office (utilizzando Salva con nome) nelle unità client ospitate su Citrix XenDesktop (da 7.13 a 7.18) non sono monitorati. Tuttavia, se si esegue Citrix XenDesktop 7.13 o una versione successiva con Virtual Delivery Agent (VDA) versione 7.12, i file salvati nelle unità client (utilizzando **Salva con nome**) sono monitorati. È possibile trovare la procedura di attivazione del monitoraggio per queste operazioni di salvataggio per il seguente articolo del centro di supporto Symantec:

<http://www.symantec.com/docs/TECH249988>

Supporto per la virtualizzazione VMware

Symantec supporta l'esecuzione del software Symantec DLP Agent in workstation virtuali tramite uno dei seguenti elementi:

- VMware Workstation 6.5.x

Nota: VMware Workstation 6.5.x non è più disponibile in Symantec Data Loss Prevention 15.0.

- VMware View 4.6
- VMware Horizon View 6.0.1 e 6.2.1
- VMware Horizon View 7.1, 7.3.1, 7.4 e 7.6.
- VMware Fusion 7 (macOS)
- Hyper-V e Hyper-V (WS 2012 R2)

Sistemi operativi supportati per gli indicatori EMDI, EDM e IDM remoti

È possibile installare l'indicizzatore EMDI remoto, l'indicizzatore EDM remoto e l'indicizzatore IDM remoto sui seguenti sistemi operativi Windows:

- Windows 7 (a 32 bit) Enterprise, Professional, Ultimate Edition
- Windows 7 (a 32 bit) (SP1) Enterprise, Professional, Ultimate Edition
- Windows 7 (a 64 bit) Enterprise, Professional, Ultimate Edition
- Windows 7 (a 64 bit) (SP1) Enterprise, Professional, Ultimate Edition
- Windows 8.1 (a 64 bit) Enterprise, Professional
- Windows 8.1 Update 1 (a 64 bit) Enterprise, Professional
- Windows 8.1 Update 2 (a 64 bit) Enterprise, Professional
- Windows 8.1 Update 3 (a 64 bit) Enterprise, Professional
- Windows 10 Update [1511] (a 64 bit) Enterprise, Professional
- Windows 10 Update pietra Red [1607 - RS1] (a 64 bit) Enterprise, Professional
- Microsoft Windows 10 Creators Update (RS2 v1703)
- Microsoft Windows 10 Creators Update (RS3 v1709)
- Microsoft Windows 10 Creators Update (RS4 v1803))

Requisiti del software di terze parti e raccomandazioni

Symantec Data Loss Prevention richiede determinato software di terze parti. È consigliato altro software di terze parti. Vedere:

- [Tabella 2-15](#) per il software richiesto
- [Tabella 2-16](#) per i Linux RPM richiesti
- [Tabella 2-17](#) per il software consigliato

Tabella 2-15 Software di terze parti richiesto

Software	Richiesto per	Descrizione
Adobe Reader	Tutti i sistemi	Adobe Reader è richiesto per leggere la documentazione di Symantec Data Loss Prevention. Scaricarlo dal sito di Adobe .
Apache Tomcat versione 9	Enforce Server	Richiesto per supportare il sistema di reporting. La versione corretta di Tomcat viene installata automaticamente su Enforce Server dalla Procedura guidata di installazione di Symantec DLP e non deve essere ottenuta o installata separatamente.
Java Runtime Environment (JRE) 1.8.0_181	Tutti i server	La Procedura guidata di installazione di Symantec DLP installa automaticamente la versione JRE corretta.
Flex SDK 4.6	Server Network Discover/Cloud Storage Discover	SDK richiesto per il reporting dei rischi delle cartelle.

Software	Richiesto per	Descrizione
Pacchetto driver Napatech 8.0.3 (versione driver 3.5.1) (Windows Server 2012 R2 e Windows Server 2016) e pacchetto driver 8.1.0 (versione driver 3.5.0), (RHEL 6x/7x)	Scheda di acquisizione pacchetti ad alta velocità Napatech NT20E2, NT4E, NT40A01 e NT40E3	<p>Consente il monitoraggio ad alta velocità.</p> <p>Symantec supporta</p> <ul style="list-style-type: none"> ■ Più porte di acquisizione per scheda di acquisizione di rete Napatech ■ Acceleratore di rete Napatech NT40A01 ■ Interfacce 10 gigabit NT40E3 e NT20E2 ■ Acquisizione di pacchetti multi-thread ■ Filtraggio hardware Napatech ■ Driver della scheda di terza generazione Napatech per le piattaforme Windows e RHEL ■ Data Loss Prevention Network Monitor virtualizzato con schede di acquisizione come dispositivi PCI pass-through nella piattaforma VMware ESXi <p>Le schede Napatech non sono supportate sulle installazioni server singolo.</p>
WinPcap 4.1.3	<p>Richiesto per il server Network Monitor basato su Windows. WinPcap 4.1.3 è richiesto per Microsoft Windows Server 2012.</p> <p>Consigliato per tutti i server di rilevamento basati su Windows.</p>	<p>Libreria di acquisizione di pacchetti Windows.</p> <p>Scaricarlo da winpcap.org.</p>
Driver di scheda Endace 5.3.1	Server di rilevamento dotati di una scheda di misurazione di rete Endace.	<p>Le schede Endace non sono supportate su installazioni server singolo.</p> <p>Scaricarlo dal sito di Endace.</p> <p>Vedere "Requisiti hardware minimi per installazioni medie" a pagina 16.</p>
VMware	<p>Richiesto per eseguire i componenti supportati in un ambiente virtualizzato.</p> <p>Vedere "Supporto di server virtuali" a pagina 38.</p>	<p>Software di virtualizzazione.</p> <p>Scaricarlo dal sito di VMware.</p>

Software	Richiesto per	Descrizione
Microsoft Active Directory 2003, 2008 R2, 2012, 2012 R2 o 2016	Versioni richieste per la connessione ad Active Directory.	Fornisce i servizi di directory per le reti di dominio Windows.

Oltre all'installazione minima di Linux, i server Symantec Data Loss Prevention basati su Linux richiedono i Red Hat Package Manager (RPM) elencati in [Tabella 2-16](#).

Tabella 2-16 Linux RPM richiesti

Server basati su Linux	RPM richiesti
Enforce Server Server Oracle	apr apr-util binutils expat libicu Xorg-x11* * Richiesto solo per l'installazione grafica. L'installazione nella modalità console non richiede un server X.
Server Network Monitor	apr apr-util expat libicu Xorg-X11* * Richiesto solo per l'installazione grafica. L'installazione nella modalità console non richiede un server X.

Red Hat Enterprise Linux 6 ha queste dipendenze aggiuntive:

- Pacchetto del gruppo Desktop Platform Development (`yum groupinstall "Desktop Platform Development"`)
- `compat-openldap`
- `compat-expat1`
- `compat-db43`
- `openssl098e`

Red Hat Enterprise Linux 7 ha queste dipendenze aggiuntive solo per i pacchetti a 64 bit:

- Pacchetto del gruppo server con GUI (`yum groupinstall "Server with GUI"`)
- Pacchetto del gruppo Dev Tools (`yum groupinstall "Development Tools"`)

- compat-openldap
- compat-db
- libpng
- compat-libtiff3
- gtk+-devel
- gtk2-devel
- gstreamer
- libX11
- libXext
- libXi
- libXrender
- libXtst
- wget
- unzip

Nota: SeLinux deve essere disattivato su tutti i server basati su Linux.

Symantec consiglia il software di terzi elencato in [Tabella 2-17](#) per la configurazione e la risoluzione dei problemi della distribuzione di Symantec Data Loss Prevention.

Tabella 2-17 Software di terzi consigliato

Software	Posizione	Descrizione
Wireshark	Qualsiasi computer server	Utilizzare Wireshark (precedentemente Ethereal) per verificare che la scheda NIC del server di rilevamento riceva il traffico corretto dalla porta o dal tap SPAN. È inoltre possibile usare Wireshark per diagnosticare i problemi di rete tra altri server. Scaricare la versione più recente dal sito di Wireshark .
dagsnap	Computer server Network Monitor che utilizzano schede Endace	Utilizzarlo in combinazione con Wireshark per verificare che la scheda NIC Endace del server di rilevamento riceva il traffico corretto dalla porta o dal tap SPAN. Dagsnap è incluso con le schede Endace e non è richiesto con le schede non Endace.

Software	Posizione	Descrizione
Sysinternals Suite	Qualsiasi computer server Windows	Utilità di risoluzione dei problemi. Consigliato per la diagnostica dei problemi su computer server Windows. Scaricare la versione più recente dal sito di Microsoft .
Browser LDAP	Enforce Server	Un browser LDAP è consigliato per la configurazione o la risoluzione dei problemi di Active Directory o LDAP.

Compatibilità del prodotto

Il capitolo contiene i seguenti argomenti:

- [Requisiti e compatibilità ambientale per Network Prevent for Email](#)
- [Compatibilità di server proxy con Network Prevent for Web](#)
- [Monitoraggio SSL con Network Monitor](#)
- [Supporto ICAP protetto per Network Prevent for Web tramite il servizio stunnel](#)
- [Schede di acquisizione di pacchetti ad alta velocità](#)
- [Compatibilità di Veritas Data Insight con Symantec Data Loss Prevention](#)
- [Integrazioni con altri prodotti di Symantec](#)
- [Compatibilità Network Discover/Cloud Storage Discover](#)
- [Applicazioni supportate da Endpoint Prevent](#)

Requisiti e compatibilità ambientale per Network Prevent for Email

Il server Network Prevent for Email è compatibile con un'ampia gamma di servizi e-mail ospitati e con MTA con conformità SMTP di terze parti di livello aziendale. Consultare il fornitore MTA o il servizio e-mail ospitato per domande di supporto specifiche.

Il server Network Prevent for Email può integrarsi con un MTA o un servizio e-mail ospitato che soddisfi i seguenti requisiti:

- Il MTA o il servizio e-mail ospitato deve essere conforme a SMTP. Deve essere in grado di inviare e ricevere e-mail unicamente tramite i seguenti verbi del comando: HELO (o EHLO), RCPT TO, MAIL FROM, QUIT, NOOP e DATA.

- Durante l'esecuzione del server Network Prevent for Email in modalità di riflessione, l'MTA a monte deve essere in grado di indirizzare i messaggi al server Network Prevent for Email una sola volta per ogni messaggio.

È possibile utilizzare un MTA conforme a SMTP che indirizza i messaggi in uscita dall'infrastruttura di posta interna al server Network Prevent for Email. Per la compatibilità della modalità di riflessione, l'MTA deve inoltre essere in grado di indirizzare i messaggi restituiti dal server Network Prevent for Email ai destinatari previsti.

Il server Network Prevent for Email tenta di avviare una connessione TLS con un MTA downstream solo quando l'MTA di upstream emette il comando STARTTLS. La connessione TLS riesce solo se l'MTA a valle o il servizio e-mail ospitato supporta TLS. Deve anche autenticarsi al server Network Prevent for Email. Una corretta autenticazione richiede che le chiavi e i certificati X509 appropriati siano disponibili per ciascun server di posta nella catena di messaggi con proxy.

Consultare la *guida all'integrazione MTA Symantec Data Loss Prevention per Network Prevent for Email* per informazioni sulla configurazione del supporto TLS per i server Network Prevent for Email funzionanti in modalità di inoltro o riflessione.

Compatibilità di server proxy con Network Prevent for Web

I server Network Prevent for Web utilizzano un'interfaccia Internet Content Adaptation Protocol (ICAP) standard e supportano molti server proxy. [Tabella 3-1](#) indica i server e i protocolli.

Symantec Data Loss Prevention supporta inoltre ICAP protetta (SICAP). È possibile configurare ICAP protetta con Blue Coat ProxySG tramite la console di amministrazione di Enforce Server. È possibile configurare altri proxy con ICAP protetta tramite il servizio stunnel. L'utilizzo di stunnel per ICAP protetta è obsoleto in Symantec Data Loss Prevention versione 15.1 e sarà rimosso in una versione successiva. Vedere "[Supporto ICAP protetto per Network Prevent for Web tramite il servizio stunnel](#)" a pagina 50.

Tabella 3-1 Server proxy supportati da Network Prevent for Web

Proxy	Protocolli supportati	Informazioni di configurazione
Blue Coat ProxySG versioni 6.6. e 6.7.x per Network Prevent for Web	Proxy ICAP, SICAP, HTTP, HTTPS o FTP	Documentazione del prodotto Blue Coat
Cisco IronPort S-Series versioni 9.1.x, 10.1.x e 10.5.x	ICAP, HTTP, HTTPS	Documentazione del prodotto Cisco IronPort 9.1.x e 10.5.x supportano Secure ICAP 10.1.x non supporta SICAP

Proxy	Protocolli supportati	Informazioni di configurazione
F5 BIG-IP System versione 12.0.x, 13.1.0.8, 14.1.0	SICAP, HTTP, HTTPS	Vedere "Utilizzo di F5 Proxy con Symantec Data Loss Prevention Network Prevent for Web" nel centro di supporto Symantec all'indirizzo http://www.symantec.com/docs/TECH235856 per informazioni sull'integrazione di F5 BIG-IP System con Network Prevent for Web come soluzione client-server ICAP.
Fortinet FortiGate-VM 5.6.x4206150	ICAP, HTTP, HTTPS	Documentazione del prodotto FortiGate-VM
McAfee Web Gateway (denominato in precedenza Secure Computing Secure Web Webwasher) versione 7.7.x, 7.8.2	Proxy ICAP, SICAP, HTTP, HTTPS o FTP	Documentazione di Secure Web (in particolare il capitolo che descrive la configurazione di Secure Web con una soluzione DLP)
Squid Web Proxy versioni 3.5.x	ICAP, HTTP, HTTPS	Consultare la <i>Guida all'integrazione di Symantec Data Loss Prevention per Squid Web Proxy</i> .
Websense Appliance V5000 e V10000, con Websense Web Security versione 8.4	ICAP, HTTP, HTTPS, FTP	Non supporta la redazione. Supporta solo "Blocca HTTP/HTTPS". RESPMOD non è supportato. Websense blocca il traffico solo quando la dimensione del messaggio di rifiuto di Symantec Data Loss Prevention (nella regola di risposta) è superiore a 512 byte. Se la dimensione del messaggio di rifiuto è inferiore a 512 byte, viene generato un incidente ma il traffico di rete non è bloccato.

Monitoraggio SSL con Network Monitor

Symantec ha certificato Network Monitor per il monitoraggio di Blue Coat SSL Visibility Appliance.

Per i dettagli, consultare l'articolo [TECH231642](#) nel centro di supporto Symantec.

Supporto ICAP protetto per Network Prevent for Web tramite il servizio stunnel

Il supporto per il servizio stunnel non è disponibile nella versione 15.1 e sarà rimosso in una versione successiva.

A partire da Symantec Data Loss Prevention 15.1, è possibile riconfigurare il sistema in modo da utilizzare Secure ICAP integrato per Network Prevent for Web invece di stunnel. Per i dettagli della configurazione, vedere la *Guida dell'amministratore Symantec Data Loss Prevention* o la Guida in linea.

Schede di acquisizione di pacchetti ad alta velocità

Questo argomento descrive le schede di acquisizione di pacchetti ad alta velocità supportate per Network Monitor.

Tabella 3-2 Schede di acquisizione di pacchetti ad alta velocità

Scheda	Versione	Versione del driver
Endace	DAG 7.5 G2/G4 (PCI-E) DAG 10X2 Nota: Le schede Endace per l'utilizzo con Data Loss Prevention sono supportate solo su sistemi Linux a 64 bit. Le schede Endace non sono supportate su installazioni server singolo.	5.7.1

Scheda	Versione	Versione del driver
Napatech	NT20E2, NT20E3, NT4E, NT40A01 e NT40E3	<p>Pacchetto driver 8.0.3 (versione driver 3.5.1) per Windows</p> <p>Pacchetto driver 8.1.0 (versione driver 3.5.0) per Linux</p> <p>Symantec supporta i seguenti</p> <ul style="list-style-type: none"> ■ Più porte di acquisizione per scheda di acquisizione di rete Napatech ■ Acceleratore di rete Napatech NT40A01 ■ Acquisizione di pacchetti multi-thread ■ Filtraggio hardware Napatech ■ Driver della scheda di terza generazione Napatech per le piattaforme Windows e RHEL ■ Schede di rete 10 gigabit ■ Data Loss Prevention Network Monitor virtualizzato con schede di acquisizione come dispositivi PCI pass-through nella piattaforma VMware ESXi

Compatibilità di Veritas Data Insight con Symantec Data Loss Prevention

Veritas Data Insight è un'opzione concessa separatamente in licenza in Symantec Data Loss Prevention che consente alle organizzazioni di risolvere il problema dell'identificazione di proprietari di dati e parti responsabili delle informazioni a causa di metadati o informazioni di tracciatura incompleti o imprecisi. Data Insight fornisce una connessione da Enforce Server a un server di gestione di Data Insight.

Tabella 3-3 Versioni supportate di Veritas Data Insight e Symantec Data Loss Prevention

Versione di Data Insight	Versione DLP 14.0	Versione DLP 14.5	DLP versione 14.6	DLP versione 15.0	DLP versione 15.1	DLP versione 15.5
2.0 - 4.5.1	No	No	No	No	No	No
4.5.2, 4.5.3	Sì	No	No	No	No	No
5.0	Sì	Sì	No	No	No	No
5.1	Sì	Sì	No	No	No	No

Versione di Data Insight	Versione DLP 14.0	Versione DLP 14.5	DLP versione 14.6	DLP versione 15.0	DLP versione 15.1	DLP versione 15.5
5.1.1	No	No	Sì	Sì	Sì	Sì
5.2	No	No	Sì	Sì	Sì	Sì
6.0	No	No	Sì, nella versione 14.6 MP1	Sì	Sì	Sì
6.1	No	No	Sì, nella versione 14.6 MP2	Sì	Sì	Sì
6.1.1	No	No	No	Sì, nella versione 15.0 MP1	Sì	Sì
6.1.2	No	No	No	No	Sì	Sì
6.1.3	No	No	No	No	Sì, nella versione 15.1 MP1	Sì

Integrazioni con altri prodotti di Symantec

Questa sezione descrive la compatibilità di varie integrazioni di Symantec Data Loss Prevention con altri prodotti Symantec.

Tabella 3-4 Compatibilità del prodotto Symantec con Symantec Data Loss Prevention

Prodotto Symantec	Versione	Nota	Versione DLP 14.0	Versione DLP 14.5	DLP versione 14.6	DLP versione 15.0	DLP versione 15.1	DLP versione 15.5
PGP Universal Gateway Email Symantec	2.63		No	No	No	No	No	No
	3.3.x		Sì	Sì	No	Sì	Sì	Sì

Prodotto Symantec	Versione	Nota	Versione DLP 14.0	Versione DLP 14.5	DLP versione 14.6	DLP versione 15.0	DLP versione 15.1	DLP versione 15.5
Symantec Message Gateway (SMG)	7.5		No	No	No	No	No	No
	8.0		No	No	No	No	No	No
Serie 8200 e 8300	10.0.1.2		Sì	Sì	No	Sì	No	No
	10.0.2		Sì	Sì	No	Sì	No	No
	10.5.0-8		Sì	Sì	No	Sì	No	No
	10.5.3		Sì	Sì	No	No	No	No
	10.6.x				Sì	Sì	Sì	Sì
Symantec Web Gateway (SWG)	5.0, 5.0.2.8		Sì	Sì	No	No	No	No
	5.2.7		No	Sì	Sì	Sì	Sì	Sì

Prodotto Symantec	Versione	Nota	Versione DLP 14.0	Versione DLP 14.5	DLP versione 14.6	DLP versione 15.0	DLP versione 15.1	DLP versione 15.5
Symantec Endpoint Protection	12.1, 12.1 RU4	Per informazioni sulla configurazione di Symantec Endpoint Protection per l'utilizzo con Network Discover/Cloud Storage Discover e Network Monitor, consultare le note sulla versione di Symantec Data Loss Prevention 14.0.	Sì	No	No	No	No	No
	12.1.5 (12.1 RU5)		Sì	Sì	Sì	No	No	No
	12.1.6 (12.1 RU6 MP6)		No	No	Sì	Sì	Sì	Sì
	14.0		No	No	No	Sì	Sì	Sì
	14.0.1 e 14.0.1 MP1		No	No	No	Sì	Sì	Sì
Symantec Encryption Management Server (DLP Encryption Insight)	3.3		Sì	Sì	Sì	Sì	No	No
	3.4		No	No	Sì	Sì	Sì	Sì

Prodotto Symantec	Versione	Nota	Versione DLP 14.0	Versione DLP 14.5	DLP versione 14.6	DLP versione 15.0	DLP versione 15.1	DLP versione 15.5
Server OCR	1		No	No	No	Sì	Sì	Sì

Compatibilità Network Discover/Cloud Storage Discover

Network Discover/Cloud Storage Discover individua i dati confidenziali esposti sottoponendo a scansione un'ampia gamma di archivi di dati aziendali, ad esempio: file server, database, Microsoft SharePoint, Lotus Notes, Documentum, Livelink, Microsoft Exchange e server Web.

Vedere ["Target del file system supportati"](#) a pagina 55.

Vedere ["Target di IBM \(Lotus\) Notes supportati"](#) a pagina 56.

Vedere ["Target di database SQL supportati"](#) a pagina 56.

Vedere ["Target del server SharePoint supportati"](#) a pagina 57.

Vedere ["Destinazioni Exchange Server supportate"](#) a pagina 57.

Vedere ["Target supportati del rilevatore file system"](#) a pagina 57.

Vedere ["Target Documentum \(rilevatore\) supportati"](#) a pagina 58.

Vedere ["Target del rilevatore OpenText \(Livelink\) supportati"](#) a pagina 58.

Vedere ["Target supportati del Web Server \(rilevatore\)"](#) a pagina 58.

Target di archiviazione cloud Box supportati

Il target di Box supporta la scansione di file e cartelle in account di archiviazione cloud Box aziendali.

Target del file system supportati

Il target del file system supporta la scansione dei seguenti file system di rete.

File server supportati:

- Solo server CIFS

Condivisioni file supportate:

- CIFS:
 - Windows Server 2008 R2 (SMB 1.0 e 2.0 supportati su server Network Discover/Cloud Storage Discover Windows e Linux)

- Windows Server 2012 R2 (SMB 1.0 e 2.0 supportati su server Network Discover/Cloud Storage Discover Windows e Linux)
- Windows Server 2016 (SMB 1.0 e 2.0 supportati su server Network Discover/Cloud Storage Discover Windows e Linux)
- NFS su Red Hat Enterprise Linux 6.x, e 7.x
- Scansione DFS su Windows 2008 R2, 2012 R2 e 2016.

Nota: DFS non è supportato con Network Protect.

Inoltre, il target del file system supporta la scansione dei seguenti tipi di file:

- Cartelle personali di Microsoft Outlook (file `.pst`) create con Outlook , 2010, 2013 e 2016. Il server Network Discover/Cloud Storage Discover che esegue la scansione di questo target deve avere un sistema operativo Windows e Outlook 2007 o versione successiva deve essere installato nel sistema.
- File system sui sistemi Unix, anche se non sono mostrati come condivisioni NFS o CIFS. Utilizzare il protocollo SFTP per fornire un metodo simile alle scansioni delle condivisioni di file.
 È inoltre possibile eseguire la scansione del file system locale su un server Network Discover/Cloud Storage Discover Linux elencandone il nome del percorso nella radice del contenuto. Ad esempio, è possibile immettere `/home/myfiles`.

Target di IBM (Lotus) Notes supportati

Il target di IBM Notes (precedentemente denominato Lotus Notes) supporta la scansione delle versioni seguenti:

- Lotus Notes 8.5.x
- IBM Notes 9.0.x

I file `Notes.jar` e `NCSO.jar` si trovano nella directory di installazione del client di Lotus Notes. Il numero di versione manifesto di questi file dipende dalla versione del server Domino.

- La versione 8 ha una versione manifesto nel file JAR di 1.5.0
- La versione 9 ha una versione manifesto nel file JAR di 1.6.0

Target di database SQL supportati

I seguenti database SQL sono stati testati con scansioni di target di Network Discover/Cloud Storage Discover:

- Oracle 11g (11.2.x), 12c (12.1.x) e 18c (12.2.x) (il `vendor_name` è `oracle`)

- SQL Server 2014 e 2016 (*vendor_name* è `sqlserver`)
- DB2 10.5 (il *vendor_name* è `db2`)

Contattare il supporto di Symantec Data Loss Prevention per informazioni sulla scansione di altri database SQL.

Target del server SharePoint supportati

I seguenti target del server SharePoint sono supportati:

- Microsoft Office SharePoint Server 2010 SP2
- Microsoft Office SharePoint Server 2013 SP1
- Microsoft Office SharePoint Server 2016

Destinazioni Exchange Server supportate

Symantec Data Loss Prevention supporta le seguenti destinazioni Exchange Server:

- Microsoft Exchange Server 2010 SP3
- Microsoft Exchange Server 2013
- Microsoft Exchange Server 2013 SP1
- Microsoft Exchange Server 2016 (on-site)

Per utilizzare il connettore servizi Web di Exchange, è necessario che i servizi Web di Exchange e il servizio Autodiscover siano attivati sul server Exchange e siano accessibili al server Network Discover/Cloud Storage Discover.

È possibile eseguire la scansione degli oggetti dati archiviati nelle cartelle pubbliche, quali:

- Messaggi e-mail
- Allegati dei messaggi
- Documenti di Microsoft Word
- Fogli di calcolo Excel

La scansione Exchange opera anche sulla posta archiviata negli archivi personali di Exchange 2013 e 2016.

Target supportati del rilevatore file system

È possibile eseguire la scansione dei seguenti sistemi Windows remoti:

- Windows Server 2008 R2
- Windows Server 2012 R2

- Windows Server 2016

È possibile eseguire la scansione dei seguenti file system Linux:

- Red Hat Enterprise Linux 6.x
- Red Hat Enterprise Linux 7.4

È possibile eseguire la scansione dei seguenti file system AIX:

- AIX 7.1

AIX richiede le seguenti librerie di runtime C, come Java 1.8 e Java 8 JRE:

- `xlC.aix50.rte` (v8.0.0.0+)
- `xlC.rte` (v8.0.0.0+)

È possibile eseguire la scansione dei seguenti file system Solaris a 32 bit (i sistemi a 64 bit non sono supportati):

- Solaris 10 (piattaforma SPARC)

Solaris richiede i seguenti livelli di patch per il rilevatore:

- Solaris 9, 115697-01

I file system su sistemi UNIX possono inoltre essere sottoposti a scansione tramite il protocollo SFTP. Questo protocollo fornisce un metodo simile alla scansione di file basati sulla condivisione, invece che utilizzare il Rilevatore file system. Contattare i servizi professionali Symantec per dettagli.

Target Documentum (rilevatore) supportati

Il rilevatore Documentum supporta la scansione di un archivio Documentum Content Server 5.3.x o 6.6.x e 6.7. Tutte le versioni sono obsolete in Symantec Data Loss Prevention 15.5. I rilevatori Documentum saranno rimossi nella prossima distribuzione di Symantec Data Loss Prevention.

Target del rilevatore OpenText (Livelink) supportati

Il rilevatore Livelink supporta la scansione dei target di OpenText (Livelink) Server 9.x. Questa versione è obsoleta in Symantec Data Loss Prevention 15.5. I rilevatori Livelink saranno rimossi nella prossima distribuzione di Symantec Data Loss Prevention.

Target supportati del Web Server (rilevatore)

Il rilevatore Web Server supporta la scansione di un sito Web HTTP statico.

Applicazioni supportate da Endpoint Prevent

Tabella 3-5 descrive le singole applicazioni che possono essere monitorate utilizzando Endpoint Prevent con Windows; **Tabella 3-6** descrive i browser che possono essere monitorati utilizzando Endpoint Prevent con macOS.

Endpoint Prevent consente di aggiungere il supporto di monitoraggio per altre applicazioni di terzi non elencate nelle seguenti tabelle. Un esempio di applicazione di terzi è Thunderbird. Si aggiunge il supporto del monitoraggio per un'applicazione nella console di amministrazione di Enforce Server. Verificare sempre il supporto del monitoraggio per le applicazioni prima di abilitare il monitoraggio su un numero elevato di endpoint. Potrebbe essere necessario applicare ulteriori impostazioni di filtraggio alle singole applicazioni per mantenere prestazioni accettabili. Per ulteriori informazioni, consultare il *Manuale dell'amministratore di sistema di Symantec Data Loss Prevention* per ulteriori informazioni sulla configurazione e l'utilizzo del controllo applicazioni.

Applicazioni supportate da Endpoint Prevent su Windows

Tabella 3-5 Applicazioni supportate da Endpoint Prevent su Windows

Funzionalità	Software	Versioni	DLP 14.0	DLP 14.5	DLP 14.6	DLP 15.0	DLP 15.1	DLP 15.5
HTTP	Tutti i browser	Tutti	Sì	Sì	Sì	Sì	Sì	Sì

Funzionalità	Software	Versioni	DLP 14.0	DLP 14.5	DLP 14.6	DLP 15.0	DLP 15.1	DLP 15.5
HTTP protetto (HTTPS)	Internet Explorer	6.0	No	No	No	No	No	No
		7.0	No	No	No	No	No	No
		8.0	No	No	No	No	No	No
		9.0	Sì	Sì	Sì	Sì (Windows Server 2008 R2)	No	No
		10.0	Sì	Sì	Sì	Sì (Windows Server 2008 R2)	Sì	Sì
		11.0	Sì (Windows 7, 8.1 Enterprise, 10 Enterprise e Windows Server 2012 R2, solo modalità Desktop ed EPM disattivato)	Sì (Windows 7, 8.1 Enterprise, 10 Enterprise e Windows Server 2012 R2, solo modalità Desktop ed EPM disattivato)	Sì	Sì	Sì	Sì
	Edge	RS1	No	No			Obsoleta	No

Funzionalità	Software	Versioni	DLP 14.0	DLP 14.5	DLP 14.6	DLP 15.0	DLP 15.1	DLP 15.5
					Sì No (su Windows 10 Creators Update [versioni 1703 e 1709]. La tabella seguente fornisce dettagli sull'attivazione del monitoraggio Edge per questo scenario.)	Sì No (su Windows 10 Creators Update [versioni 1703 e 1709]. La tabella seguente fornisce dettagli sull'attivazione del monitoraggio Edge per questo scenario.)		
		RS2	No	No	No	No	Sì	Sì
		RS3 e RS4	No	No	No	No	Sì	Sì
	Firefox	2.0 - 5.0	No	No	No	No	No	No
		Da 23 a 46.0.1	Sì (da 35 a 46.0.1 e fino a 47.0 in DLP Agent versione 14.0.2)	Sì	Sì (38-44), compreso Firefox a 64 bit, che è stato introdotto in Firefox 43.	Sì	Sì	Sì
		51-54	No	No	Sì	Sì	Sì	Sì
		56-61	No	No	Sì	Sì	Sì	Sì
		62	No	No	No	Sì	Sì	Sì
		Firefox, continua	63	No	No	No	No	Sì, nella versione 15.1 MP1
		64	No	No	No	No	No	Sì
					Sì	Sì	Sì	

Funzionalità	Software	Versioni	DLP 14.0	DLP 14.5	DLP 14.6	DLP 15.0	DLP 15.1	DLP 15.5
	Google Chrome	Da 38 a 59	Sì (51 e 52 supportato in Windows 10 con DLP Agent versione 14.0.2)	Sì (il supporto di Windows 10 inizia con la versione 51) 55 nella versione 14.5 MP1 di DLP Agent	38-44, 51-57 58 e 59 nella versione 14.6 MP1 di DLP Agent			
		Da 60 a 69	No	No	Sì	Sì	Sì	Sì
	Google Chrome, continua	70, 71	No	No	No	No	Sì, nella versione 15.1 MP1	Sì
		72						Vi sono attualmente problemi noti nell'utilizzo di Chrome 72 su Windows Symantec Data Loss Prevention. Vedere AVVISO 2641 per informazioni dettagliate.

Funzionalità	Software	Versioni	DLP 14.0	DLP 14.5	DLP 14.6	DLP 15.0	DLP 15.1	DLP 15.5
Messaggistica istantanea	AIM	N/D	Sì	Sì	Sì	Sì	Sì	Sì
	AIM Pro	N/D	Sì	Sì	Sì	Sì	Sì	Sì
	AIM6	N/D	Sì	Sì	Sì	Sì	Sì	Sì
	Microsoft Office Communicator	N/D	Sì	Sì	Sì	Sì	Sì	Sì
	Skype	N/D	Sì	Sì	Sì	Sì	Sì	Sì
E-mail	Outlook	2007	Sì	No	No	No	No	No
		2010	Sì	Sì	Sì	Sì	Sì	Sì
		2013	Sì	Sì	Sì	Sì	Sì	Sì
		2016	No	Sì	Sì	Sì	Sì	Sì
		2019	No	No	No	No	Sì, su 15.1 MP1	Sì
	Outlook Web Access (modalità RTF e light)	2007	Sì	No	No	No	No	No
		2010	Sì	Sì	Sì	Sì	Sì	Sì
		2013		Sì	Sì	Sì	Sì	Sì
		2016	No	Sì	Sì	Sì	Sì	Sì
	Outlook.com	N/D	Sì	Sì	Sì	Sì	Sì	Sì
	Lotus Notes	6.5 - 8.5	No	No	No	No	No	No
	Lotus Notes (IBM Domino)	8.5.x	Sì	Sì (8.5.3)	Sì (8.5.3)	Sì (8.5.3)	Sì (8.5.3)	Sì (8.5.3)
		9.x	Sì	Sì	Sì	Sì	Sì	Sì
FTP		N/D	Sì	Sì	Sì	Sì	Sì	Sì

Funzionalità	Software	Versioni	DLP 14.0	DLP 14.5	DLP 14.6	DLP 15.0	DLP 15.1	DLP 15.5
CD/DVD	BsClip	N/D	Sì	Sì	Sì	Sì	Sì	Sì
	Bs Recorder Gold	N/D	Sì	Sì	Sì	Sì	Sì	Sì
	BurnAware	N/D	Sì	Sì	Sì	Sì	Sì	Sì
	Cheetah Burner	N/D	Sì	Sì	Sì	Sì	Sì	Sì
	Command Burner	N/D	Sì	Sì	Sì	Sì	Sì	Sì
	CopyToDVD	N/D	Sì	Sì	Sì	Sì	Sì	Sì
	Creator10	N/D	Sì	Sì	Sì	Sì	Sì	Sì
	GEAR per Windows	N/D	Sì	Sì	Sì	Sì	Sì	Sì
	mkisofs	N/D	Sì	Sì	Sì	Sì	Sì	Sì
	Nero	N/D	Sì	Sì	Sì	Sì	Sì	Sì
	Nero Start Smart	N/D	Sì	Sì	Sì	Sì	Sì	Sì
	Roxio	N/D	Sì	Sì	Sì	Sì	Sì	Sì
	Roxio RecordNow	N/D	Sì	Sì	Sì	Sì	Sì	Sì
	Roxio5	N/D	Sì	Sì	Sì	Sì	Sì	Sì
	Roxio Mediahub	N/D	Sì	Sì	Sì	Sì	Sì	Sì
	Silent Night Micro Burner	N/D	Sì	Sì	Sì	Sì	Sì	Sì
	Star Burn	N/D	Sì	Sì	Sì	Sì	Sì	Sì

Funzionalità	Software	Versioni	DLP 14.0	DLP 14.5	DLP 14.6	DLP 15.0	DLP 15.1	DLP 15.5
Applicazioni di sincronizzazione cloud	Box	4.0.6169	Sì	Sì	Sì	Sì	Sì	Sì
		Versione più recente disponibile					Sì	Sì
	Dropbox	3.2.x, 6.4.x, 8.4.x 12.4.x, 13.4.x, 14.4.x, 15.4.x, 17.4.x, 19.4.x, 20.4.x - 38.4.x	3.2.9	Sì Versione 20.4.x-29.4.x supportata in DLP Agent, versione 14.5 MP1.	Sì Versione 20.4.x-29.4.x supportata in DLP Agent, versione 14.6 MP1.	Sì Versione 20.4.x-38.4.x	Sì Versione 31.4.x-38.4.x	Sì
		Versione più recente disponibile					Sì	Sì
	Microsoft OneDrive	15.0.4675.1003 per Win 8.1 (predefinito) 17.3.4726.0226 e 17.3.6517.0809 per Win 7 x86/x64 (client desktop)	Sì	Sì, e OneDrive Personal e OneDrive for Business 17.3.6390.0509, 17.3.6517.0809	Sì	Sì	Sì	Sì
	Hightail	2.4.7.1621	Sì	Sì	Sì	Sì	Sì	Sì
	Backup e sincronizzazione Google	3.35.x		Sì	Sì	Sì	Sì	Sì
		3.37.x				Sì	Sì	Sì
		3.41.x					Sì	Sì

Funzionalità	Software	Versioni	DLP 14.0	DLP 14.5	DLP 14.6	DLP 15.0	DLP 15.1	DLP 15.5
	Google Drive	1.20.x, 1.30.x, 1.32.x, 2.34.x - 3.37.x	Sì, 1.20.x	Sì Versione 2.34.x supportata in DLP Agent, versione 14.5 MP1.	Sì Versione 2.34.x supportata in DLP Agent, versione 14.6 MP1.	Sì	Sì	Sì
	Apple iCloud	4.0.3.56, 4.0.5.20	Sì	Sì	Sì	Sì	Sì	Sì
Varie	Adobe Reader		Sì	Sì	Sì	Sì	Sì	Sì
	Apple iTunes		Sì	Sì	Sì	Sì	Sì	Sì
	Click-to-Run	Microsoft Pro 2013	No	Sì	Sì	Sì	Sì	Sì
	Roxio_Central	N/D	Sì	Sì	Sì	Sì	Sì	Sì
	Modulo di comunicazione WebEx	N/D	Sì	Sì	Sì	Sì	Sì	Sì

Nota: Gli agenti delle versioni 14.6.x e 15.0 in esecuzione in Windows 10 Creators Update (versioni 1703 e 1709) non supportano il monitoraggio di Edge per impostazione predefinita. Per ulteriori informazioni sull'attivazione del monitoraggio di Edge per questo scenario, vedere il seguente articolo nel Centro di supporto Symantec.

<http://www.symantec.com/docs/TECH240808>

Deprecazione di Microsoft Office

Microsoft Office 2007 è obsoleto in Symantec Data Loss Prevention 15.0.

Applicazioni supportate da Endpoint Prevent in macOS

Tabella 3-6 Applicazioni supportate da Endpoint Prevent in macOS

Funzionalità	Software	Versione software	DLP 14.0	DLP 14.5	DLP 14.6	DLP 15.0	DLP 15.1	DLP 15.5
HTTP protetto (HTTPS)	Firefox	36.0.4, ESR 31.X	Sì	Sì	Sì	No	No	Sì
		38 ESR, 45 ESR, 45.1.1 ESR, 45.4.0, 46.0.1 ESR, 49.0.2 ESR	No	No	Sì	Sì	Sì	Sì
		49 e 50	No	Sì (nella versione 14.5 MP1 di DLP Agent)	Sì	Sì	Sì	Sì
		51-54	No	No	Sì	Sì	Sì	Sì
		56-61	No	No	Sì	Sì	Sì	Sì
		62	No	No	No	Sì	Sì	Sì
	Firefox, continua	63	No	No	No	No	Sì, nella versione 15.1 MP1	Sì
		64	No	No	No	No	No	Sì
	Safari	6.0.x, 7.0.x e 8.0.x	Sì	No	No	No	No	No
		9.1	No	Sì (su macOS 10.11)	Sì	Sì	No	No
		10.0.x	No		Sì	Sì	Sì	Sì

Funzionalità	Software	Versione software	DLP 14.0	DLP 14.5	DLP 14.6	DLP 15.0	DLP 15.1	DLP 15.5
				Sì (per DLP Agent, versione 14.5 MP1 in macOS 10.11.6)				
		10.1.x	No	No	Sì (per DLP Agent, versione 14.6 MP1 in macOS 10.11.6) No (su macOS 10.12.4)	Sì (su macOS 10.11.x, 10.12.1, 10.12.2 e 10.12.3) No (su macOS 10.12.4, 10.12.5 e 10.12.6)	Sì (macOS 10.11, 10.12.1, 10.12.2 e 10.12.3)	Sì
		11			No	No	Sì (su macOS 10.12.4 e versioni successive)	Sì
	Google Chrome	41.0.x	Sì	Sì	No	No	No	Sì
		50	No	Sì	Sì	Sì	Sì	Sì
		51	Sì (sulla versione 14.0.2 di DLP Agent)	Sì	Sì	Sì	Sì	Sì
		52	Sì (sulla versione 14.0.2 di DLP Agent)	Sì	Sì	Sì	Sì	Sì
		53	Sì	Sì	Sì	Sì	Sì	Sì
		55			Sì	Sì	Sì	Sì

Funzionalità	Software	Versione software	DLP 14.0	DLP 14.5	DLP 14.6	DLP 15.0	DLP 15.1	DLP 15.5
				Sì 14.5 MP1				
		56	No	No	Sì	Sì	Sì	Sì
		57	No	No	Sì	Sì	Sì	Sì
		58	No	No	Sì (a partire da DLP Agent versione 14.6 MP1)	Sì	Sì	Sì
		59	No	No	Sì (a partire da DLP Agent versione 14.6 MP1)	Sì	Sì	Sì
		Da 60 a 69	No	No	Sì	Sì	Sì	Sì
	Google Chrome, continua	70, 71	No	No	No	No	Sì, nella versione 15.1 MP1	Sì
E-mail	Outlook	2011	No	Sì	Sì	Sì	Sì	Sì
		2016	No	No	Sì	Sì	Sì	Sì
		2019	No	No	No	No	Sì, nella versione 15.1 MP1	Sì
Messaggistica istantanea	Cisco Jabber	N/D	No	Sì	Sì	Sì	Sì	Sì
	Skype	N/D	No	Sì	Sì	Sì	Sì	Sì

Supporto del monitoraggio delle applicazioni protette da System Integrity Protection (SIP)

DLP Agent monitora le applicazioni che sono protette da System Integrity Protection (SIP) in macOS 10.11, 10.12, 10.13 e 10.14. È possibile trovare il supporto delle versioni più recenti di macOS nel seguente articolo del Centro di supporto Symantec:

<http://www.symantec.com/docs/TECH235226>