

Novità e modifiche in Symantec™ Data Loss Prevention 15.5

Ultimo aggiornamento: 03 marzo 2019

Novità e modifiche in Symantec™ Data Loss Prevention 15.5

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	Introduzione a Symantec Data Loss Prevention
15.5	8
Informazioni su questa guida	8
Cronologia delle modifiche	8
Riepilogo delle funzionalità nuove e modificate	9
Funzionalità di rilevamento	9
Funzionalità di Enforce Server e della piattaforma	11
Funzionalità di endpoint	11
Funzionalità Discover	14
Funzionalità cloud	16
Funzionalità di installazione e upgrade	16
Integrazione con altri prodotti Symantec	17
Funzionalità rimosse e obsolete	17
Capitolo 2	Funzionalità nuove e modificate in Symantec Data Loss Prevention 15.5
Funzionalità di rilevamento	18
Supporto per il rilevamento Identificatore dati corrispondenti esatti (EMDI)	19
Diagnostica per dimensionare le distribuzioni di server OCR	20
Possibilità di estrarre immagini da documenti di Office per OCR e Riconoscimento moduli	20
Dimensioni maggiori del file di ispezione e limiti più estesi per l'estrazione del contenuto	20
Supporto dell'estrazione del contenuto ad alte prestazioni per i file Office Open XML	21
Funzionalità di Enforce Server e della piattaforma	21
Identificatori di dati e modelli di politica nuovi e aggiornati	21
Nomi dei servizi aggiornati	24
Il parametro <code>SERVICE_NAME</code> ora è utilizzato per la connessione al database Oracle	25
Funzionalità di endpoint	25

Le politiche di Data Loss Prevention classificano in modo dinamico i documenti sull'endpoint	25
Possibilità di sottoporre a scansione e marcare i dati esistenti sugli endpoint	26
Endpoint Prevent per applicazioni di sincronizzazione cloud su Mac	26
L'agente registra con precisione l'ora dell'ultimo aggiornamento	26
Supporto del controllo applicazioni per gruppi di agenti specifici	27
Supporto di compatibilità del contenuto URL per Firefox 57 e versioni successive su endpoint Mac	27
Miglioramento del monitoraggio dei prompt dei comandi e della registrazione degli incidenti	27
Possibilità di visualizzare i domini di e-mail e i file allegati bloccati nelle finestre di notifica pop-up	28
Applicazione automatica della crittografia ICE a file e cartelle caricati dal browser	28
Supporto dell'autenticazione condivisa per Symantec Information Centric Encryption (ICE) e DLP Agent	28
Supporto dell'utilità ICE per l'utilizzo di proxy di rete per la connessione al cloud Symantec ICE	29
Installazione dell'utilità ICE necessaria per applicare automaticamente la crittografia ICE ai file che vengono copiati su dispositivi di archiviazione rimovibili	29
Nuovo evento di sistema per gli aggiornamenti di politiche di DLP Agent	29
Funzionalità Discover	30
Supporto per SMB2 in Network Discover e Network Protect	30
Supporto di Network Protect della quarantena dei file SharePoint riservati per le condivisioni file	30
Rilascio di Network Protect semplificato dei file SharePoint in quarantena	30
Nuovi avvisi e-mail per eventi di scansione di Network Discover	31
Supporto del server di rilevamento per l'utilizzo di proxy di rete per le comunicazioni tra Network Discover e il cloud Symantec ICE	31
Funzionalità cloud	32
Supporto aggiornato per i securlet CloudSOC	32
Regole di risposta smart nuove e aggiornate per i securlet CloudSOC	32
Funzionalità di installazione e upgrade	33

Nomi dei percorsi di installazione aggiornati	33
Integrazioni con altri prodotti di Symantec	33
Integrazione con Symantec Endpoint Protection (SEP) per Protezione intensiva Symantec e Information Centric Defense	34
Funzionalità e piattaforme rimosse e obsolete	35

Introduzione a Symantec Data Loss Prevention 15.5

Il capitolo contiene i seguenti argomenti:

- [Informazioni su questa guida](#)
- [Riepilogo delle funzionalità nuove e modificate](#)

Informazioni su questa guida

La guida *Novità e modifiche in Symantec Data Loss Prevention 15.5* descrive le nuove funzionalità e caratteristiche relative a questa versione. Inoltre illustra le modifiche rispetto alle versioni precedenti, compresa la rimozione di funzionalità o piattaforme supportate.

Questa guida non contiene dettagli di implementazione o configurazione per queste nuove funzionalità. Fornisce una panoramica di ogni nuova funzionalità in Symantec Data Loss Prevention 15.5, compresi, ove necessario, dettagli sufficienti a comprendere meglio il possibile utilizzo delle funzionalità. Inoltre comprende informazioni per pianificare meglio la distribuzione di queste nuove funzionalità nell'organizzazione.

Ove possibile, la guida fornisce rimandi a ulteriori informazioni sulle funzionalità nuove e modificate.

Per la libreria della documentazione completa di Symantec Data Loss Prevention 15.5, vedere <https://www.symantec.com/docs/DOC11228>.

Vedere anche la Guida in linea in https://help.symantec.com/home/dlp15.5?locale=EN_US.

Cronologia delle modifiche

L'elemento seguente è stato modificato dopo la pubblicazione di questa guida.

Tabella 1-1 Cronologia delle modifiche

Data	Descrizione
1 febbraio 2019	Aggiunto supporto dell'estrazione del contenuto ad alte prestazioni per i file Office Open XML."

Riepilogo delle funzionalità nuove e modificate

Le funzionalità nuove e modificate in Symantec Data Loss Prevention 15.5 sono riassunte in questo capitolo. È possibile trovare ulteriori dettagli sulla distribuzione e una spiegazione di tali funzionalità nel capitolo 2.

Funzionalità di rilevamento

Tabella 1-2 Funzionalità di rilevamento nuove e modificate per Symantec Data Loss Prevention 15.5

Funzionalità	Breve descrizione
Supporto per il rilevamento Identificatore dati corrispondenti esatti (EMDI)	<p>Il rilevamento Identificatore dati corrispondenti esatti (EMDI) è una potente tecnologia di rilevamento che consente di rilevare dati strutturati, soprattutto informazioni personali identificabili (PII), con un elevato livello di precisione. È possibile utilizzare EMDI, che aggiunge un'ulteriore convalida per gli identificatori di dati predefiniti e personalizzati, per rilevare la corrispondenza esatta con record indicizzati in tutti i canali di Data Loss Prevention, tra cui Endpoint. EMDI è una soluzione a esecuzione veloce e sicura che contribuisce alla riduzione e alla potenziale eliminazione dei falsi positivi nel proprio ambiente Data Loss Prevention.</p> <p>Vedere "Supporto per il rilevamento Identificatore dati corrispondenti esatti (EMDI)" a pagina 19.</p>

Funzionalità	Breve descrizione
<p>Diagnostica per dimensionare le distribuzioni di server OCR</p>	<p>È possibile acquisire dati sul traffico di immagini per aiutare a comprendere meglio le esigenze di dimensionamento dell'ambiente OCR. L'attivazione di un'impostazione avanzata del server consente di misurare il carico OCR e utilizzare tali valori nel foglio di calcolo per la stima del dimensionamento del server OCR.</p> <p>Vedere "Diagnostica per dimensionare le distribuzioni di server OCR" a pagina 20.</p>
<p>Possibilità di estrarre le immagini da documenti di Office per OCR e Riconoscimento moduli.</p>	<p>È possibile estrarre le immagini da documenti di Microsoft Office per la scansione di rilevamento OCR e Riconoscimento moduli.</p> <p>Vedere "Possibilità di estrarre immagini da documenti di Office per OCR e Riconoscimento moduli" a pagina 20.</p>
<p>Dimensioni maggiori del file di ispezione e limiti più estesi per l'estrazione del contenuto</p>	<p>Data Loss Prevention ora supporta dimensioni di file e limiti di estrazione del contenuto più grandi, oltre la dimensione massima predefinita di ispezione del contenuto di 30 MB..</p> <p>Le dimensioni massime di ispezione possono essere regolate facilmente su valori superiori sia a livello dei singoli server di rilevamento sia a livello di configurazione dell'agente. Linee guida per regolare le impostazioni del server e la memoria fisica sono fornite automaticamente nella console di amministrazione di Enforce Server.</p> <p>Vedere "Dimensioni maggiori del file di ispezione e limiti più estesi per l'estrazione del contenuto" a pagina 20.</p>
<p>Supporto dell'estrazione del contenuto ad alte prestazioni per i file Office Open XML</p>	<p>Symantec Data Loss Prevention supporta l'estrazione del contenuto di vari formati di file Office Open XML.</p> <p>Vedere "Supporto dell'estrazione del contenuto ad alte prestazioni per i file Office Open XML" a pagina 21.</p>

Funzionalità di Enforce Server e della piattaforma

Tabella 1-3 Funzionalità nuove e modificate per Enforce Server e la piattaforma Symantec Data Loss Prevention 15.5

Funzionalità	Breve descrizione
Identificatori di dati e modelli di politica nuovi e aggiornati	Symantec Data Loss Prevention include 64 identificatori di dati nuovi. Inoltre sono stati aggiornati otto identificatori e uno è stato rimosso. Sono stati aggiornati sei modelli di politica. Vedere " Identificatori di dati e modelli di politica nuovi e aggiornati " a pagina 21.
Nomi dei servizi aggiornati	Symantec Data Loss Prevention 15.5 include una modifica a tutti i nomi di servizio. A tutti i nomi dei servizi viene accodato "Servizio". Vedere " Nomi dei servizi aggiornati " a pagina 24.
Parametro <code>SERVICE_NAME</code> per la connessione al database Oracle	Symantec Data Loss Prevention utilizza il parametro <code>SERVICE_NAME</code> per la connessione al database Oracle. Vedere " Il parametro <code>SERVICE_NAME</code> ora è utilizzato per la connessione al database Oracle " a pagina 25.

Funzionalità di endpoint

Tabella 1-4 Funzionalità di endpoint nuove e modificate per Symantec Data Loss Prevention 15.5

Funzionalità	Breve descrizione
Le politiche di Data Loss Prevention classificano in modo dinamico i documenti sull'endpoint	È possibile utilizzare le politiche di Data Loss Prevention anziché le regole di Information Centric Tagging (ICT) per gestire la classificazione di documenti di Microsoft Office e Microsoft Outlook sull'endpoint. Gli utenti finali ricevono automaticamente le classificazioni suggerite in base alle politiche di Data Loss Prevention. Questa automazione aggiunge una protezione delle informazioni più efficace. Vedere " Le politiche di Data Loss Prevention classificano in modo dinamico i documenti sull'endpoint " a pagina 25.

Funzionalità	Breve descrizione
Possibilità di sottoporre a scansione e marcare i dati esistenti sugli endpoint	<p>Utilizzare le scansioni di classificazione per classificare i dati degli endpoint esistenti. Dopo avere configurato le destinazioni di endpoint per una scansione, Data Loss Prevention può applicare un tag appropriato in risposta a una violazione della politica.</p> <p>Vedere "Possibilità di sottoporre a scansione e marcare i dati esistenti sugli endpoint" a pagina 26.</p>
Endpoint Prevent per applicazioni di sincronizzazione cloud su Mac	<p>DLP Agent fornisce assistenza per il monitoraggio e la prevenzione per le applicazioni cloud di sincronizzazione e condivisione file sugli endpoint Mac.</p> <p>Vedere "Endpoint Prevent per applicazioni di sincronizzazione cloud su Mac" a pagina 26.</p>
L'agente registra con precisione l'ora dell'ultimo aggiornamento	<p>DLP Agent visualizza l'ora dell'ultimo aggiornamento nella colonna Ultimo aggiornamento ricevuto della schermata Elenco agenti.</p> <p>Vedere "L'agente registra con precisione l'ora dell'ultimo aggiornamento" a pagina 26.</p>
Supporto del controllo applicazioni per gruppi di agenti specifici	<p>È possibile controllare quali applicazioni e quali canali specifici monitorare per gruppi di agenti differenti.</p> <p>Vedere "Supporto del controllo applicazioni per gruppi di agenti specifici" a pagina 27.</p>
Supporto di compatibilità del contenuto URL per Firefox 57 e versioni successive su endpoint Mac	<p>Gli amministratori di Data Loss Prevention possono applicare filtri URL per il monitoraggio di Mozilla Firefox. I pop-up di blocco e notifica visualizzano URL quando vengono caricati file riservati.</p> <p>Vedere "Supporto di compatibilità del contenuto URL per Firefox 57 e versioni successive su endpoint Mac" a pagina 27.</p>
Miglioramento del monitoraggio dei prompt dei comandi e della registrazione degli incidenti	<p>I file spostati in condivisioni di rete utilizzando un prompt dei comandi vengono monitorati. Quando gli incidenti vengono registrati, la posizione del file è inclusa nei dettagli dell'incidente.</p> <p>Vedere "Miglioramento del monitoraggio dei prompt dei comandi e della registrazione degli incidenti" a pagina 27.</p>

Funzionalità	Breve descrizione
Possibilità di visualizzare i domini e gli allegati di e-mail bloccati nelle finestre di notifica pop-up	<p>È possibile configurare politiche per visualizzare i domini e-mail e i file allegati bloccati che contengono dati riservati nei pop-up di notifica endpoint.</p> <p>Vedere "Possibilità di visualizzare i domini di e-mail e i file allegati bloccati nelle finestre di notifica pop-up" a pagina 28.</p>
Applicazione automatica della crittografia ICE a file e cartelle di upload del browser	<p>Utilizzare le funzionalità integrate di Symantec Information Centric Encryption (ICE) per crittografare file riservati che vengono caricati con browser che utilizzano HTTPS negli endpoint Windows.</p> <p>Vedere "Applicazione automatica della crittografia ICE a file e cartelle caricati dal browser" a pagina 28.</p>
Supporto dell'autenticazione condivisa per Symantec Information Centric Encryption (ICE) e DLP Agent	<p>L'autenticazione viene richiesta una sola volta agli utenti quando eseguono la crittografia con DLP Agent o la decrittografia di file con l'utilità ICE. Gli utenti possono inoltre decrittografare i file crittografati quando non è disponibile una connessione a Internet.</p> <p>Vedere "Supporto dell'autenticazione condivisa per Symantec Information Centric Encryption (ICE) e DLP Agent" a pagina 28.</p>
Supporto dell'utilità ICE per l'utilizzo di proxy di rete per la connessione al cloud Symantec ICE	<p>L'utilità ICE ora supporta l'uso di proxy di rete per la connessione al cloud Symantec ICE.</p> <p>Inoltre, negli ambienti gestiti, l'utilità ICE utilizza lo stesso proxy di rete autorizzato di DLP Agent.</p> <p>Vedere "Supporto dell'utilità ICE per l'utilizzo di proxy di rete per la connessione al cloud Symantec ICE" a pagina 29.</p>

Funzionalità	Breve descrizione
Installazione dell'utilità ICE necessaria per applicare automaticamente la crittografia ICE ai file che vengono copiati su dispositivi di archiviazione rimovibili	<p>Le funzionalità di Symantec Information Centric Encryption per Endpoint Prevent sono state modificate. Endpoint Prevent ora applica la crittografia ICE ai file riservati che vengono copiati su dispositivi di archiviazione rimovibili solo tramite Esplora risorse di Windows, riga di comando o PowerShell. I file che vengono copiati tramite altri supporti su dispositivi di archiviazione rimovibili vengono bloccati.</p> <p>Vedere "Installazione dell'utilità ICE necessaria per applicare automaticamente la crittografia ICE ai file che vengono copiati su dispositivi di archiviazione rimovibili" a pagina 29.</p>
Nuovo evento di sistema per gli aggiornamenti di politiche di DLP Agent	<p>Quando le politiche di DLP Agent vengono aggiornate, Symantec Data Loss Prevention visualizza un evento di livello INFO nella pagina Sistema > Agenti > Eventi.</p> <p>Vedere "Nuovo evento di sistema per gli aggiornamenti di politiche di DLP Agent" a pagina 29.</p>

Funzionalità Discover

Tabella 1-5 Funzionalità di Discover nuove e modificate per Symantec Data Loss Prevention 15.5

Funzionalità	Breve descrizione
Supporto del protocollo Server Message Block (SMB) 2 per Network Discover e Network Protect	<p>Symantec Data Loss Prevention ora supporta SMB2 per il rilevamento Network Discover e la risposta Network Protect agli incidenti.</p> <p>Vedere "Supporto per SMB2 in Network Discover e Network Protect" a pagina 30.</p>

Funzionalità	Breve descrizione
<p>Quarantena Network Protect dei file SharePoint riservati sulle condivisioni file</p>	<p>Configurare Network Protect per mettere automaticamente in quarantena i file riservati dagli archivi Microsoft SharePoint a una condivisione di file utilizzando l'azione di risposta Network Protect: metti file in quarantena.</p> <p>In alternativa, configurare l'azione di risposta smart Quarantena SharePoint per mettere in quarantena manualmente i file SharePoint su una condivisione di file.</p> <p>Vedere "Supporto di Network Protect della quarantena dei file SharePoint riservati per le condivisioni file" a pagina 30.</p>
<p>Rilascio di Network Protect semplificato dei file SharePoint in quarantena</p>	<p>Per rilasciare file di Microsoft SharePoint in quarantena, configurare l'azione di risposta smart Network Protect: rilascio di SharePoint da quarantena. Non è necessario configurare il plug-in di FlexResponse Rilascio di SharePoint da quarantena. È possibile rilasciare i file in quarantena nella posizione originale da un percorso di quarantena di SharePoint o da un percorso di quarantena di condivisione file.</p> <p>Vedere "Rilascio di Network Protect semplificato dei file SharePoint in quarantena" a pagina 30.</p>
<p>Nuovi avvisi e-mail per eventi di scansione di Network Discover</p>	<p>Quando si avvia una scansione utilizzando Network Discover, ora è possibile configurare fino a cinque nuovi avvisi e-mail in base allo stato della scansione, utilizzando i codici evento corrispondenti.</p> <p>Vedere "Nuovi avvisi e-mail per eventi di scansione di Network Discover" a pagina 31.</p>
<p>Supporto del server di rilevamento per l'utilizzo di proxy di rete per le comunicazioni tra Network Discover e il cloud Symantec ICE</p>	<p>Utilizzare la console di amministrazione di Enforce Server per specificare un server proxy nell'ambiente e, opzionalmente, fornire le credenziali per la connessione a tale server. Durante le scansioni SharePoint e File System (condivisioni file), Network Discover utilizza il proxy di rete autorizzato per comunicare con il cloud Symantec ICE.</p> <p>Vedere "Supporto del server di rilevamento per l'utilizzo di proxy di rete per le comunicazioni tra Network Discover e il cloud Symantec ICE" a pagina 31.</p>

Funzionalità cloud

Tabella 1-6 Funzionalità cloud nuove e modificate per Symantec Data Loss Prevention 15.5

Funzionalità	Breve descrizione
Supporto aggiornato per i securlet CloudSOC	<p>Symantec Data Loss Prevention include il supporto per i securlet Symantec CloudSOC seguenti:</p> <ul style="list-style-type: none"> ■ Amazon S3 ■ Cisco Spark ■ Slack <p>Vedere "Supporto aggiornato per i securlet CloudSOC" a pagina 32.</p>
Regole di risposta smart nuove e aggiornate per i securlet CloudSOC	<p>Symantec Data Loss Prevention include le seguenti nuove regole di risposta smart per i securlet Symantec CloudSOC:</p> <ul style="list-style-type: none"> ■ Crittografia ■ Remove collaborators (Rimuovi collaboratori) ■ Rimuovi collegamenti condivisi <p>La regola di risposta Metti in quarantena dati a riposo è stata aggiornata e ora include un file marker personalizzabile.</p> <p>Vedere "Regole di risposta smart nuove e aggiornate per i securlet CloudSOC" a pagina 32.</p>

Funzionalità di installazione e upgrade

Tabella 1-7 Funzionalità nuove e modificate per l'installazione e l'upgrade di Symantec Data Loss Prevention 15.5

Funzionalità	Breve descrizione
Nomi dei percorsi di installazione aggiornati	<p>I percorsi di installazione per Symantec Data Loss Prevention 15.5 non contengono più spazi.</p> <p>Vedere "Nomi dei percorsi di installazione aggiornati" a pagina 33.</p>

Integrazione con altri prodotti Symantec

Tabella 1-8 Funzionalità nuove e modificate di Integrazioni con altri prodotti Symantec per Symantec Data Loss Prevention 15.5

Funzionalità	Breve descrizione
Integrazione con Symantec Endpoint Protection (SEP), servizio di valutazione dell'attendibilità file di Protezione intensiva Symantec e Information Centric Defense	<p>Symantec Data Loss Prevention può sfruttare le informazioni di Symantec Endpoint Protection (SEP) sulla reputazione delle applicazioni e creare incidenti quando per aprire i file vengono utilizzate applicazioni sospette. Questa capacità viene fornita anche se non si dispone di una distribuzione SEP. Se SEP è distribuito, Symantec Data Loss Prevention può notificare a SEP la presenza di file riservati tramite una nuova regola di risposta. L'integrazione di SEP e Symantec Data Loss Prevention aggiunge funzionalità di sicurezza Information Centric Defense dell'organizzazione.</p> <p>Vedere "Integrazione con Symantec Endpoint Protection (SEP) per Protezione intensiva Symantec e Information Centric Defense" a pagina 34.</p>

Funzionalità rimosse e obsolete

Parecchie funzionalità sono state rimosse o indicate come obsolete in Data Loss Prevention versione 15.5.

Vedere ["Funzionalità e piattaforme rimosse e obsolete"](#) a pagina 35.

Funzionalità nuove e modificate in Symantec Data Loss Prevention 15.5

Il capitolo contiene i seguenti argomenti:

- [Funzionalità di rilevamento](#)
- [Funzionalità di Enforce Server e della piattaforma](#)
- [Funzionalità di endpoint](#)
- [Funzionalità Discover](#)
- [Funzionalità cloud](#)
- [Funzionalità di installazione e upgrade](#)
- [Integrazioni con altri prodotti di Symantec](#)
- [Funzionalità e piattaforme rimosse e obsolete](#)

Funzionalità di rilevamento

Le seguenti funzionalità di rilevamento sono nuove o migliorate in Symantec Data Loss Prevention 15.5.

Supporto per il rilevamento Identificatore dati corrispondenti esatti (EMDI)

Il rilevamento Identificatore dati corrispondenti esatti (EMDI) è una potente tecnologia per il rilevamento di corrispondenze esatte che consente di rilevare dati strutturati, soprattutto informazioni personali identificabili (PII), con un elevato livello di precisione. È possibile utilizzare EMDI per confrontare esattamente record indicizzati su tutti i canali di Data Loss Prevention. Ottime prestazioni e sicurezza consentono a EMDI di aiutare a ridurre ed eliminare potenzialmente i falsi positivi nell'ambiente di Data Loss Prevention. EMDI fornisce migliori prestazioni di corrispondenza e maggiore efficienza della memoria rispetto a Exact Data Matching (EDM).

EMDI funziona come controllo di convalida aggiuntivo rispetto ai modelli di corrispondenza di Identificatore dati. Ad esempio, invece di lasciare che Data Loss Prevention faccia affidamento sull'identificatore di dati Numero carta di credito per confrontare qualsiasi modello che è simile a un numero di carta di credito, EMDI consente ai clienti di individuare esattamente solo i numeri di carta di credito che sono contenuti negli loro indice dei record specificando almeno una colonna aggiuntiva di dati di identificazione nell'origine dati utilizzata per il profilo EMDI. Sono supportati sia gli identificatori dati di sistema (impostazione predefinita) che quelli personalizzati.

EMDI ha una tecnologia di rilevamento base diversa da EDM e non è un'alternativa o una soluzione sostitutiva rispetto a EDM, ma fornisce all'endpoint una tecnologia per il rilevamento delle corrispondenze esatte. EDM non è disponibile nell'endpoint. Altri vantaggi e termini di confronto con EDM includono i seguenti:

- EMDI può supportare ogni scenario di rilevamento EDM che implica la corrispondenza con due o più colonne di un'origine dati di profilo laddove almeno una di queste colonne corrisponde a un identificatore di dati.
- EMDI esegue la corrispondenza all'interno di DLP Agent, pertanto non è necessario per implementare il rilevamento a due livelli.
- Supporta entrambi i DLP Agent a 64 bit per Windows e per macOS.
- Nella maggior parte dei casi, il rilevamento corrispondenze di EMDI risulta più rapido rispetto a EDM.
- La memoria impegnata da EMDI è 1/5 di quella di quella impegnata da EDM per la stessa origine dati indicizzata. Tuttavia EMDI ha un limite di dimensione massima inferiore per le origini dati indicizzate.
- EMDI dispone di un rigido modello di sicurezza che lo rende adatto per la distribuzione di profili sugli endpoint.

EMDI viene configurato nello stesso modo di EDM, in **Gestisci > Profili dati > Dati esatti > Aggiungi profilo Identificatore dati corrispondenti esatti**.

Diagnostica per dimensionare le distribuzioni di server OCR

È possibile misurare dati sul traffico di immagini per aiutare a comprendere meglio le esigenze di dimensionamento dell'ambiente OCR. Quando si attiva l'impostazione avanzata `OCR.RECORD_REQUEST_STATISTICS`, i risultati vengono visualizzati nel registro OCR. I valori risultanti possono essere utilizzati nel foglio di calcolo per la stima del dimensionamento server OCR, al fine di determinare il dimensionamento della distribuzione server OCR.

Il foglio di calcolo per la stima del dimensionamento server OCR è disponibile nel Centro supporto Symantec in <https://www.symantec.com/docs/DOC10612>.

Possibilità di estrarre immagini da documenti di Office per OCR e Riconoscimento moduli

È possibile estrarre le immagini da documenti di Microsoft Office per il rilevamento OCR e Riconoscimento moduli. Data Loss Prevention può estrarre i formati di file immagine BMP, PNG e JPG da Word (doc e docx), Excel (xls e xlsx) e PowerPoint (ppt e pptx).

Dimensioni maggiori del file di ispezione e limiti più estesi per l'estrazione del contenuto

Data Loss Prevention 15.5 supporta file di dimensioni più grandi e limiti di estrazione del contenuto maggiori. Fornisce inoltre agli amministratori un metodo più facile per configurare le impostazioni dei file di grandi dimensioni. Le dimensioni massime predefinite del file di ispezione sono invariate (30 MB), ma è possibile regolare facilmente le dimensioni massime a valori superiori. Le regolazioni sono eseguibili sia a livello dei singoli server di rilevamento sia a livello di configurazione dell'agente.

A seconda della dimensione di ispezione del contenuto scelta, determinate impostazioni avanzate vengono regolate automaticamente. Per la configurazione delle impostazioni nei file di proprietà, che vengono modificati manualmente, sono disponibili [Linee guida per l'ottimizzazione](#). Inoltre, la console di amministrazione di Enforce Server segnala automaticamente se è necessaria memoria di sistema aggiuntiva in base alla dimensione ispezione del contenuto desiderato.

Nota: Le dimensioni massime di ispezione per i servizi cloud Symantec Data Loss Prevention non sono state modificate. Gli amministratori non possono aumentare questi limiti per i servizi cloud. Questa funzionalità è disponibile solo per server di rilevamento, appliance e DLP Agent.

È possibile implementare questa funzionalità nella console di amministrazione di Enforce Server. Per i server di rilevamento, l'ottimizzazione può essere eseguita nella scheda **Server > Configurazione**. Per i DLP Agent, l'ottimizzazione può essere eseguita nella scheda **Configurazione agente > Impostazioni**.

Per ulteriori informazioni sulle dimensioni di file più grandi e sui limiti di estrazione del contenuto, vedere gli argomenti della Guida [Configurazione del server - base](#) e [Informazioni sulle configurazioni dell'agente](#).

Supporto dell'estrazione del contenuto ad alte prestazioni per i file Office Open XML

Symantec Data Loss Prevention supporta l'estrazione del contenuto di vari formati di file Office Open XML. Per impostazione predefinita, Microsoft Office 2007 e versioni successive utilizzano il formato Office Open XML per formati di file come DOCX, DOTX, PPTX e XLSX. Questa funzionalità è attiva con Microsoft Office Desktop 2007, 2010, 2013 e 2016, nonché con Microsoft Office 365. Questa funzionalità ora è disponibile sui server, mentre al momento non lo è su DLP Agent.

Funzionalità di Enforce Server e della piattaforma

Le seguenti funzionalità di Enforce Server e della piattaforma sono nuove o migliorate in Symantec Data Loss Prevention 15.5.

Identificatori di dati e modelli di politica nuovi e aggiornati

Symantec Data Loss Prevention include i seguenti identificatori di dati nuovi:

- Numero di patente di guida australiana
- Numero di partita IVA bulgara
- Patente di guida canadese
- Numero di passaporto canadese
- Numero di residenza permanente (PR) Canada
- Numero di identificazione nazionale croato
- Codice di identificazione fiscale di Cipro
- Numero di partita IVA di Cipro
- Numero di patente di guida della Repubblica Ceca
- Numero di identificazione fiscale ceco
- Numero di partita IVA della Repubblica Ceca
- Numero di patente di guida estone
- Codice di identificazione personale estone
- Numero di passaporto estone

- Numero di partita IVA estone
- Numero della tessera sanitaria europea
- Numero di passaporto greco
- Numero di partita IVA greca
- Numero di patente di guida ungherese
- Numero di passaporto ungherese
- Numero di passaporto islandese
- Numero di identificazione nazionale islandese
- Numero di partita IVA islandese
- Numero di carta RuPay indiana
- Numero di passaporto kazako
- Numero di patente di guida lettone
- Numero di passaporto della Lettonia
- Numero di partita IVA lettone
- Numero di passaporto degli abitanti del Liechtenstein
- Codice di identificazione personale della Lituania
- Codice di identificazione fiscale lituano
- Numero di partita IVA lituana
- Numero di identificazione individuale di Macao
- Numero di passaporto malese
- Codice di identificazione nazionale maltese
- Codice di identificazione fiscale maltese
- Numero di partita IVA maltese
- Numero di conto bancario olandese
- Numero di patente di guida neozelandese
- Numero di passaporto neozelandese
- Numero di patente di guida norvegese
- Numero di identificazione nazionale norvegese
- Numero di partita IVA norvegese
- Numero di patente di guida polacca

- Numero di previdenza sociale europea della Polonia
- Numero di passaporto della Polonia
- Numero di partita IVA della Polonia
- Numero di patente di guida romena
- Numero di partita IVA della Romania
- Numero identificatore creditore SEPA North
- Numero identificatore creditore SEPA South
- Numero identificatore creditore SEPA West
- Numero identificativo cittadini della Serbia
- Numero di partita IVA serba
- Numero di patente di guida slovacca
- Numero di passaporto slovacco
- Numero di partita IVA slovacco
- Numero di passaporto della Slovenia
- Codice di identificazione fiscale sloveno
- Numero di partita IVA della Slovenia
- Numero di identificazione nazionale di Sri Lanka
- Numero della tessera sanitaria svizzera
- Numero di passaporto svizzero
- Numero di partita IVA svizzera
- Numero di passaporto thailandese

Symantec Data Loss Prevention include aggiornamenti per i seguenti identificatori di dati:

- Numero di passaporto francese
- ID Hong Kong
- Indirizzo IPv6
- Numero di identificazione fiscale messicano
- Documento di identità cinese
- Numero di previdenza sociale svizzero (AHV)
- US Individual Tax Identification Number (ITIN - codice di identificazione fiscale statunitense)

Il seguente identificatore dati è stato rimosso da Symantec Data Loss Prevention:

- Numero di conto bancario brasiliano

Nota: Se in una o più politiche è stato incluso l'identificatore dati Numero di conto bancario brasiliano, l'identificatore di dati rimarrà com'è nella distribuzione di Symantec Data Loss Prevention. Se questo identificatore dati non è stato incluso nelle politiche, verrà rimosso automaticamente dalla distribuzione dopo l'aggiornamento.

I seguenti modelli di politica sono stati aggiornati:

- **CAN-SPAM Act** : totale corrispondenze IDM modificato da 100% a 90%.
- **Linee guida sulla sicurezza del NERC per le società elettriche** : totale corrispondenze IDM modificato da 100% a 90%.
- **Regolamento generale per la protezione dei dati (attività bancarie e finanza)** : aggiunti nuovi identificatori di dati europei.
- **Regolamento generale per la protezione dei dati (identificazione governativa)** : aggiunti nuovi identificatori di dati europei.
- **Regolamento generale per la protezione dei dati (sanità e assicurazioni)** : aggiunti nuovi identificatori di dati europei.
- **Regolamento generale per la protezione dei dati (viaggi)** : aggiunti nuovi identificatori di dati europei.
- **Compatibilità Symantec DLP e Prevenzione** : rimossa la parola chiave "Vontu" dall'elenco parole chiave.

Nomi dei servizi aggiornati

Symantec Data Loss Prevention 15.5 include una modifica a tutti i nomi di servizio. A tutti i nomi dei servizi viene accodato "Servizio". Questa modifica si verifica automaticamente durante l'aggiornamento alla versione 15.5. I nuovi nomi servizio sono i seguenti:

- SymantecDLPManagerService
- SymantecDLPDetectionServerControllerService
- SymantecDLPNotifierService
- SymantecDLPIncidentPersisterService
- SymantecDLPDetectionServerService

Per ulteriori informazioni sull'utilizzo dei servizi di Symantec Data Loss Prevention, vedere l'argomento della Guida [Informazioni sui servizi di Symantec Data Loss Prevention](#).

Il parametro `SERVICE_NAME` ora è utilizzato per la connessione al database Oracle

Symantec Data Loss Prevention utilizza il parametro `SERVICE_NAME` per la connessione al database Oracle, che offre maggiore flessibilità nella distribuzione di Oracle per Data Loss Prevention.

Se si esegue l'aggiornamento da una versione precedente di Symantec Data Loss Prevention, si passa da `SID` al parametro `SERVICE_NAME` prima di iniziare il processo di migrazione.

Vedere il *Manuale di upgrade di Symantec Data Loss Prevention*. Questa guida è disponibile online nel centro di supporto Symantec:

<http://www.symantec.com/docs/DOC9258>

Nota: Se è stato scaricato Symantec Data Loss Prevention versione 15.1 a partire dal 21 settembre 2018, è già stato effettuato il passaggio da `SID` al parametro `SERVICE_NAME`. È possibile eseguire l'upgrade alla versione Symantec Data Loss Prevention 15.5 senza completare passaggi aggiuntivi.

Funzionalità di endpoint

Le seguenti funzionalità di rete sono nuove o migliorate in Symantec Data Loss Prevention 15.5.

Le politiche di Data Loss Prevention classificano in modo dinamico i documenti sull'endpoint

È possibile utilizzare le politiche di Data Loss Prevention anziché le regole di Information Centric Tagging (ICT) per gestire la classificazione di documenti di Microsoft Office e Microsoft Outlook sull'endpoint. Gli utenti finali ricevono automaticamente le classificazioni suggerite in base alle politiche di Data Loss Prevention. Questa automazione aggiunge una protezione delle informazioni più efficace.

Per attivare questa funzionalità:

- Utilizzare la console ICT per configurare l'integrazione della politica di Data Loss Prevention.
- Utilizzare la console di amministrazione di Enforce Server per creare regole di risposta (tipo di azione **Classificazione e tagging ICT**) che applicano tag ICT importati per classificare il contenuto.

Possibilità di sottoporre a scansione e marcare i dati esistenti sugli endpoint

Utilizzare le scansioni di classificazione per classificare i dati degli endpoint esistenti. Dopo avere configurato le destinazioni di endpoint per una scansione, Data Loss Prevention può applicare un tag appropriato in risposta a una violazione della politica. Tenere presente che se si configura una scansione di sola classificazione, non vengono generati incidenti.

Durante la creazione di politiche, si definiscono regole di risposta, utilizzando il tipo di azione **Classificazione e tagging ICT**, che utilizzano tag Information Centric Tagging (ICT) importati per classificare il contenuto.

Endpoint Prevent per applicazioni di sincronizzazione cloud su Mac

DLP Agent esegue il monitoraggio delle applicazioni cloud di sincronizzazione e condivisione file sugli endpoint Mac. Se viene aggiunto contenuto riservato a file che devono essere sincronizzati nell'applicazione cloud, Symantec Data Loss Prevention impedisce lo spostamento del file riservato nel cloud e crea un nuovo incidente di Archiviazione cloud. Il file sensibile viene messo in quarantena sull'endpoint. L'utente di endpoint può ripristinare la versione del file precedente che non includeva contenuto riservato dalla posizione di ripristino configurata.

Le seguenti applicazioni cloud sono state aggiunte come elementi predefiniti alla schermata **Controllo applicazioni globale** :

- Box
- Dropbox
- iCloud
- OneDrive

Attivare la funzionalità selezionando **Archiviazione cloud** nella scheda **Canali** della schermata Configurazione agente. È inoltre possibile aggiungere un filtro file di monitoraggio in cui è attivato il monitoraggio Archiviazione Cloud. Quando si crea una politica per l'archiviazione cloud, impostare Symantec Data Loss Prevention per monitorare i dati caricati dall'endpoint utilizzando un'applicazione di sincronizzazione di archiviazione cloud.

L'agente registra con precisione l'ora dell'ultimo aggiornamento

La colonna **Ultimo aggiornamento ricevuto** nella schermata **Elenco agenti** registra l'ora dell'ultimo aggiornamento dell'agente. Gli aggiornamenti registrati per l'agente includono quanto segue:

- Quando si verifica un evento dell'agente
- Quando vengono aggiunti nuovi attributi
- Quando vengono create nuove politiche o vengono aggiornate quelle esistenti

- Quando gli incidenti vengono generati

Supporto del controllo applicazioni per gruppi di agenti specifici

È possibile controllare quali applicazioni e canali monitorare per un gruppo di agenti specifico. In precedenza era possibile monitorare solo le stesse applicazioni, con le stesse impostazioni di monitoraggio, per tutti i gruppi di agenti. La pagina generale del controllo applicazioni è ora la pagina **Controllo applicazioni globale** (in **Sistema > Agenti > Controllo applicazioni globale**). Per sovrascrivere le impostazioni nella pagina globale e personalizzare le impostazioni per una configurazione agente specifica, è possibile aggiungere applicazioni (Windows o Mac) e selezionare i filtri di monitoraggio desiderati in **Sistema > Agenti > Configurazione agente**, nella scheda **Controllo applicazioni**.

Per informazioni sull'utilizzo della scheda **Controllo delle applicazioni**, vedere l'argomento della Guida [Impostazioni di controllo applicazioni](#).

Supporto di compatibilità del contenuto URL per Firefox 57 e versioni successive su endpoint Mac

Gli amministratori di Data Loss Prevention possono applicare filtri URL per il monitoraggio di Mozilla Firefox su endpoint Mac. I pop-up di blocco e notifica visualizzano URL quando vengono caricati file riservati mediante il browser.

Per garantire la compatibilità del contenuto URL, DLP Agent utilizza un'estensione. Gli utenti degli endpoint devono attivare l'estensione Symantec sull'endpoint per attivare la funzionalità. La schermata **Panoramica agente** identifica gli endpoint in cui l'estensione non è ancora attivata.

Nota: Per questo supporto gli utenti di endpoint che eseguono Firefox 50-56 devono attivare l'estensione Symantec sull'endpoint per continuare a garantire il supporto del monitoraggio.

Per ulteriori informazioni sull'attivazione dell'estensione Symantec, vedere l'argomento della Guida [Attivazione del monitoraggio nel browser Firefox](#).

Miglioramento del monitoraggio dei prompt dei comandi e della registrazione degli incidenti

Il monitoraggio del prompt dei comandi negli endpoint Windows include i seguenti miglioramenti:

- I file copiati in condivisioni di rete vengono monitorati. Il monitoraggio si verifica nella posizione del file sull'endpoint.
- I file copiati sul disco locale dalle condivisioni di rete.

- Quando gli incidenti vengono registrati, la posizione del file è inclusa nei dettagli dell'incidente.

Possibilità di visualizzare i domini di e-mail e i file allegati bloccati nelle finestre di notifica pop-up

È possibile configurare politiche per visualizzare domini e-mail e file allegati a e-mail nella notifica per l'utente quando il sistema blocca un tentativo di inviare dati riservati.

Questa funzionalità si attiva aggiungendo la variabile **Allegati corrispondenti** per la corrispondenza con file e allegati e la variabile **Domini destinatari corrispondenti** per la corrispondenza con i domini destinatari quando si crea una regola di risposta.

Applicazione automatica della crittografia ICE a file e cartelle caricati dal browser

Le funzionalità di Symantec Information Centric Encryption (ICE) per Endpoint Prevent sono state espansive in modo che sia più facile applicare la crittografia ICE a cartelle o file riservati che vengono caricati mediante HTTPS con browser quali Chrome, Edge, Firefox e Internet Explorer. Si utilizza l'azione **Prevent: crittografia** nella regola di risposta per applicare automaticamente ICE a cartelle o file riservati che vengono monitorati mediante il canale browser sugli endpoint Windows. È necessario distribuire l'utilità ICE per visualizzare e gestire l'accesso utente ai file protetti.

Ora è possibile caricare file o cartelle ICE crittografati da un disco locale, una condivisione di rete o un dispositivo di archiviazione rimovibile utilizzando un browser. Quando un utente carica un file o una cartella riservata utilizzando un browser, DLP Agent blocca l'azione dell'utente, crittografa automaticamente il file con estensione HTML e sostituisce il file originale nel percorso di origine. Quando si configura l'azione **Prevent: crittografia** nella console di amministrazione di Enforce Server, è possibile creare un avviso che richiede all'utente di caricare il file o la cartella crittografata.

Per ulteriori informazioni, vedere l'argomento della Guida [Configurazione dell'azione Endpoint Prevent: crittografia](#).

Supporto dell'autenticazione condivisa per Symantec Information Centric Encryption (ICE) e DLP Agent

L'utilità ICE e DLP Agent ora condividono la stessa autenticazione. Di conseguenza, l'autenticazione viene richiesta solo una volta agli utenti degli endpoint quando eseguono la crittografia di un file utilizzando DLP Agent o la decrittografia del file con l'utilità ICE. In precedenza, gli utenti dovevano effettuare l'autenticazione separatamente utilizzando il DLP Agent e l'utilità ICE per crittografare o decrittografare un file.

La funzionalità consente inoltre al proprietario del file di decrittografare i file crittografati da ICE quando gli endpoint non sono connessi a Internet. In precedenza, per decrittografare i file anche i proprietari dei file dovevano effettuare l'autenticazione e accedere ai file crittografati prima della disconnessione da Internet.

Supporto dell'utilità ICE per l'utilizzo di proxy di rete per la connessione al cloud Symantec ICE

L'utilità Symantec ICE rileva automaticamente un proxy di rete che è configurato su un endpoint e lo utilizza per la connessione al cloud Symantec ICE.

Inoltre, negli ambienti gestiti, l'utilità ICE utilizza le stesse impostazioni di proxy di rete nella configurazione dell'agente per il DLP Agent che viene installato nello stesso endpoint.

Per ulteriori informazioni, vedere l'argomento della Guida [Impostazioni proxy dell'agente](#).

Installazione dell'utilità ICE necessaria per applicare automaticamente la crittografia ICE ai file che vengono copiati su dispositivi di archiviazione rimovibili

Le funzionalità di Symantec Information Centric Encryption per Endpoint Prevent sono state modificate. Endpoint Prevent ora applica la crittografia ICE ai file riservati che vengono copiati su dispositivi di archiviazione rimovibili solo tramite Esplora risorse di Windows, riga di comando o PowerShell. I file che vengono copiati tramite altri supporti su dispositivi di archiviazione rimovibili vengono bloccati.

Symantec Information Centric Encryption ora richiede l'installazione dell'utilità ICE per crittografare o decrittografare i file crittografati. L'utilità ICE decrittografa i file crittografati e li apre nelle applicazioni native sui dispositivi di archiviazione rimovibili.

DLP Agent blocca l'operazione Salva con nome per un file crittografato in un dispositivo di archiviazione rimovibile. L'utilità ICE consente l'operazione di salvataggio quando l'utente aggiorna un file crittografato su un dispositivo di archiviazione rimovibile.

L'opzione **Fornisci questo contenuto crittografato dall'applicazione durante la lettura di file ICE** è stata rimossa dalla schermata **Controllo applicazioni**.

Nuovo evento di sistema per gli aggiornamenti di politiche di DLP Agent

Quando le politiche di DLP Agent vengono aggiornate, Symantec Data Loss Prevention visualizza un evento di livello INFO nella pagina **Sistema > Agenti > Eventi**. È inoltre possibile visualizzare questo evento nella pagina **Sistema > Agenti > Eventi > Dettagli evento**. Symantec Data Loss Prevention non visualizza questo evento se si aggiorna solo la regola di risposta di una politica di DLP Agent.

Funzionalità Discover

Le seguenti funzionalità Discover sono nuove o migliorate in Symantec Data Loss Prevention 15.5.

Supporto per SMB2 in Network Discover e Network Protect

Network Discover e Network Protect ora supportano il protocollo Server Message Block (SMB) 2 su Linux e Windows, fornendo protezione avanzata per i target di file system Network Discover. Questa modifica del supporto di SMB è trasparente e non richiede alcun intervento da parte dell'amministratore di Symantec Data Loss Prevention.

Supporto di Network Protect della quarantena dei file SharePoint riservati per le condivisioni file

È possibile configurare Network Protect per mettere automaticamente in quarantena i file riservati degli archivi di Microsoft SharePoint in una condivisione di rete, utilizzando l'azione di risposta **Network Protect: metti file in quarantena**. La posizione di quarantena viene configurata nella scheda **Proteggi** delle destinazioni di scansione SharePoint. È possibile selezionare SharePoint o File system (condivisioni file) come posizione di quarantena.

Per mettere in quarantena manualmente file SharePoint in una condivisione file, configurare l'azione di risposta smart **Network Protect: quarantena SharePoint**. È possibile selezionare SharePoint o File system (condivisioni file) come posizione di quarantena.

Per ulteriori informazioni, vedere gli argomenti della Guida [Configurazione Network Protect per i server SharePoint](#) e [Configurazione dell'azione di risposta smart quarantena SharePoint Network Protect](#).

Rilascio di Network Protect semplificato dei file SharePoint in quarantena

Ora è possibile configurare facilmente Network Protect per il rilascio dei file precedentemente messi in quarantena da archivi di Microsoft SharePoint. È possibile rilasciare i file in quarantena nella posizione originale in SharePoint da un percorso di SharePoint o da un percorso di condivisione file.

Per rilasciare i file di SharePoint in quarantena utilizzando una regola di risposta smart, utilizzare l'azione di risposta **Network Protect: rilascio di SharePoint da quarantena**.

Non è necessario configurare il plug-in di FlexResponse Rilascio di SharePoint da quarantena. Inoltre, è anche possibile rilasciare i file che erano stati messi precedentemente in quarantena utilizzando il plug-in SharePoint Quarantine FlexResponse. Se è stata installata la soluzione SharePoint e un file di SharePoint è stato messo in quarantena mediante Symantec Data Loss Prevention 15.1, al rilascio dalla quarantena i metadati del file vengono ripristinati. Se il file è

stato messo in quarantena utilizzando una versione precedente alla 15.1, il file viene rilasciato senza il ripristino dei metadati.

A partire da questa distribuzione il plug-in SharePoint Quarantine FlexResponse di Symantec Data Loss Prevention non è più supportato. A partire dalla versione 15.5, è necessario utilizzare l'azione di risposta **Network Protect: rilascio di SharePoint da quarantena** per rilasciare manualmente file di SharePoint dalla quarantena, invece del plug-in di FlexResponse Rilascio di SharePoint da quarantena.

Per ulteriori informazioni, vedere l'argomento della Guida [Configurazione dell'azione di risposta smart di Network Protect: rilascio di SharePoint da quarantena](#).

Nuovi avvisi e-mail per eventi di scansione di Network Discover

Network Discover ora registra fino a cinque nuovi eventi di scansione, a seconda dell'avanzamento della scansione o delle azioni dell'amministratore:

- Scansione avviata (1720)
- Scansione sospesa (1721)
- Scansione interrotta (1722)
- Scansione in coda (1723)
- Scansione non riuscita (1724)

Nota: L'evento esistente Scansione completata (1702) resta invariato.

È possibile configurare avvisi e-mail per i nuovi eventi di scansione, in modo da fornire aggiornamenti remoti in tempo reale sullo stato delle scansioni in corso.

Supporto del server di rilevamento per l'utilizzo di proxy di rete per le comunicazioni tra Network Discover e il cloud Symantec ICE

È possibile identificare un proxy di rete nell'installazione e, opzionalmente, specificare le credenziali di autenticazione per la connessione a tale proxy. Network Discover utilizza il server proxy per comunicare con il Cloud ICE ogni volta che le scansioni File system (condivisione file) e SharePoint attivano un'azione di risposta di crittografia.

Per le scansioni File System, è possibile attivare un proxy direttamente nella configurazione del server di rilevamento. Per le scansioni SharePoint, è possibile attivare un proxy di rete utilizzando la schermata **Applica a impostazioni proxy del cloud** nella schermata **Sistema > Generale > Impostazioni**.

Per i proxy di rete che richiedono l'autenticazione, è necessario salvare le credenziali di autenticazione nella console di amministrazione di Enforce Server prima di configurare le

impostazioni proxy. Per impostazione predefinita, i server di rilevamento sono configurati in modo da non utilizzare un proxy di rete o da presupporre l'esistenza di un proxy trasparente.

Per ulteriori informazioni, vedere gli argomenti della Guida [Configurazione di Network Discover per utilizzare un proxy per connettersi al Cloud Symantec ICE per le scansioni di condivisione file](#) e [Configurazione di Enforce Server per utilizzare un proxy per connettersi ai servizi cloud](#).

Funzionalità cloud

Le seguenti funzionalità cloud sono nuove o migliorate in Symantec Data Loss Prevention 15.5.

Supporto aggiornato per i securlet CloudSOC

Symantec Data Loss Prevention include il supporto per i securlet Symantec CloudSOC seguenti:

- Amazon S3
- Cisco Spark
- Slack

Per ulteriori informazioni sull'utilizzo di Symantec CloudSOC per rilevare le violazioni delle politiche nelle applicazioni cloud, vedere l'argomento della Guida [Informazioni su Rilevamento applicazioni](#).

Regole di risposta smart nuove e aggiornate per i securlet CloudSOC

Symantec Data Loss Prevention include le seguenti nuove regole di risposta smart per i securlet Symantec CloudSOC:

- **Crittografa** : consente di crittografare i file riservati nei repository di archiviazione cloud.
- **Rimuovi accesso collaboratore** : rimuove l'accesso dei collaboratori ai file riservati nei repository di archiviazione cloud.
- **Rimuovi collegamenti condivisi** : rimuove i collegamenti condivisi ai file riservati nei repository di archiviazione cloud.

La regola di risposta Metti in quarantena dati a riposo è stata aggiornata e ora include un file marker personalizzabile.

Per ulteriori informazioni sulle regole di risposta smart per i securlet CloudSOC, vedere l'argomento della Guida [Azioni di regole di risposta per rilevatori Applicazioni cloud e appliance API](#).

Funzionalità di installazione e upgrade

Le seguenti funzionalità di installazione e upgrade sono nuove o migliorate in Symantec Data Loss Prevention 15.5.

Nomi dei percorsi di installazione aggiornati

I percorsi di installazione per Symantec Data Loss Prevention 15.5 non contengono più spazi. La [Tabella 2-1](#) elenca le directory di installazione per i sistemi Windows e Linux.

Tabella 2-1 Nomi dei percorsi di installazione aggiornati

Componente	System	Nuovo percorso
Enforce Server	Windows	C:\Programmi\Symantec\DataLossPrevention\EnforceServer
	Linux	/opt/Symantec/DataLossPrevention/EnforceServer
Server di rilevamento	Windows	C:\Programmi\Symantec\DataLossPrevention\DetectionServer
	Linux	/opt/Symantec/DataLossPrevention/DetectionServer
A un livello	Windows	C:\Programmi\Symantec\DataLossPrevention\SingleTierServer
	Linux	/opt/Symantec/DataLossPrevention/SingleTierServer
Servizio di estrazione del contenuto	Windows	C:\Programmi\Symantec\DataLossPrevention\ContentExtractionService
	Linux	/opt/Symantec/DataLossPrevention/ContentExtractionService
Server Platform Common	Windows	C:\Programmi\Symantec\DataLossPrevention\ServerPlatformCommon
	Linux	/opt/Symantec/DataLossPrevention/ServerPlatformCommon
Server JRE	Windows	C:\Programmi\Symantec\DataLossPrevention\ServerJRE
	Linux	/opt/Symantec/DataLossPrevention/ServerJRE

Integrazioni con altri prodotti di Symantec

Le seguenti funzionalità di integrazione sono nuove o migliorate in Symantec Data Loss Prevention 15.5.

Integrazione con Symantec Endpoint Protection (SEP) per Protezione intensiva Symantec e Information Centric Defense

Symantec Data Loss Prevention 15.5 si integra con Symantec Endpoint Protection (a partire da SEP 14.0.1) per attivare un nuovo canale di monitoraggio endpoint denominato Protezione intensiva SEP. Sfruttando le informazioni di reputazione applicazioni fornite da SEP, DLP Agent può monitorare in modo dinamico le applicazioni e impedire ad applicazioni potenzialmente dannose l'accesso a file riservati sull'endpoint.

È possibile configurare DLP Agent utilizzando un controllo Livello di intensità SEP durante la configurazione dell'agente, per monitorare le applicazioni con una soglia di reputazione specificata stabilita da SEP; la reputazione dell'applicazione può essere Nociva, Sospetta o Sconosciuta. È possibile utilizzare queste reputazioni come condizioni nelle regole di risposta create, consentendo a Symantec Data Loss Prevention di intraprendere azioni diverse sulla base delle diverse reputazioni per più canali e politiche endpoint.

DLP Agent è in grado di ottenere le informazioni di reputazione dell'applicazione da SEP in due modi:

- Se l'agente SEP è installato sull'endpoint, invia direttamente le informazioni a DLP Agent. Se l'agente SEP non dispone di informazioni, DLP Agent ottiene informazioni dal servizio di valutazione dell'attendibilità di Protezione intensiva SEP nel cloud Symantec.
- Se l'agente SEP non è installato, DLP Agent ottiene le informazioni dal servizio di valutazione dell'attendibilità di Protezione intensiva SEP nel cloud Symantec.

I dettagli dell'incidente per il controllo applicazioni dinamico includono la reputazione delle applicazioni. È anche possibile filtrare gli incidenti per categorie di Livello di intensità SEP.

Il monitoraggio dinamico delle applicazioni in base alla reputazione richiede solo una licenza di Endpoint Prevent; non è necessaria alcuna licenza aggiuntiva.

Symantec Data Loss Prevention 15,5 include anche una nuova regola di risposta Endpoint, **Information Centric Defense**. In un ambiente in cui SEP è distribuito e integrato con Data Loss Prevention, la regola di risposta segnala a SEP l'esistenza di file riservati. In una prossima distribuzione di SEP, le informazioni fornite a SEP da Data Loss Prevention verranno utilizzate per fornire una robusta sicurezza Information Centric Defense (oltre a Protezione delle informazioni) per l'ambiente SEP-Data Loss Prevention.

Funzionalità e piattaforme rimosse e obsolete

Supporto rimosso

Tabella 2-2 Piattaforme rimosse e funzionalità in Symantec Data Loss Prevention 15.5

Area del prodotto	Funzionalità	Dettagli
Endpoint	Sistemi operativi endpoint Microsoft Windows 10 versione 1511 e versione 1607	Il supporto è stato rimosso per Endpoint Data Loss Prevention.
	Regola di risposta Limita conservazione dati incidenti	La regola di risposta Limita conservazione dati incidenti non è più supportata in Endpoint Discover. Se le politiche esistenti utilizzano questa regola di risposta, le violazioni della politica attivano un incidente, ma i dati dell'incidente attivato non vengono allegati.
	Applicazioni Endpoint Prevent	Le seguenti applicazioni non sono più supportate in Endpoint Prevent: <ul style="list-style-type: none"> ■ Microsoft Office 2007 ■ Edge RS1
Network Discover	Target di database SQL	I seguenti target di database SQL non sono più supportati con Network Discover: <ul style="list-style-type: none"> ■ Oracle 10g ■ SQL Server 2005
	Target server Microsoft Exchange Server 2007 SP3	Il supporto è stato rimosso.
	Supporto di target del rilevatore file system	I seguenti target del rilevatore file system non sono più supportati: <ul style="list-style-type: none"> ■ Red Hat Enterprise Linux 5.x ■ AIX 6.5 ■ Solaris 9 (piattaforma SPARC)
	Plug-in di FlexResponse per Quarantena SharePoint e Rilascio di SharePoint da quarantena	Quarantena SharePoint e Rilascio di SharePoint da quarantena ora sono supportati per le regole di risposta automatica e le azioni di risposta smart in Network Protect. Non è più necessario installare e configurare un plug-in di FlexResponse per attivare e utilizzare queste funzioni.

Area del prodotto	Funzionalità	Dettagli
Enforce Server e piattaforma	Database Oracle 11g (11.2.0.4)	Il supporto è stato rimosso. Nota: Il supporto Symantec è esteso fino a dicembre 2020 se è stato acquistato il piano di supporto esteso.
	Supporto per il servizio stunnel	Il supporto è stato rimosso.
	Red Hat Enterprise Linux 7.1 e 7.2 per server Symantec Data Loss Prevention on-site e il database Oracle.	Il supporto è stato rimosso.

Supporto obsoleto

Funzionalità segnalate come obsolete indica che, sebbene la funzionalità sia supportata nella distribuzione corrente, Symantec non intende più fornire il supporto per tale piattaforma nelle versioni future. Se l'ambiente Symantec Data Loss Prevention include una funzionalità obsoleta, è necessario pianificare un aggiornamento a una versione più recente supportata o a una differente funzionalità supportata appena possibile.

Tabella 2-3 Funzionalità obsolete in Symantec Data Loss Prevention 15.5

Area del prodotto	Funzionalità	Descrizione
Network Discover	Target Documentum (rilevatore)	Tutte le versioni sono obsolete.
	Target del rilevatore livelink	Tutte le versioni sono obsolete.

Per dettagli completi sulle piattaforme supportate per Symantec Data Loss Prevention 15.5, consultare il *Guida alla compatibilità e ai requisiti di sistema di Symantec Data Loss Prevention* all'indirizzo <https://www.symantec.com/docs/DOC10602>.