

Novità e modifiche in Symantec™ Data Loss Prevention 15.1

Ultimo aggiornamento: 06 agosto 2018

Novità e modifiche in Symantec Data Loss Prevention 15.1

Versione della documentazione: 15.1

Note legali

Copyright © 2018 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

<http://www.symantec.com>

Sommario

Capitolo 1	Introduzione a Symantec Data Loss Prevention	
	15.1	7
	Informazioni su questa guida	7
	Riepilogo delle funzionalità nuove e modificate in Symantec Data Loss Prevention 15.1	7
	Integrazione con altri prodotti di protezione delle informazioni	
	Symantec	8
	Funzionalità di installazione e upgrade	9
	Funzionalità di Enforce Server e della piattaforma	9
	Funzionalità di rilevamento	11
	Funzionalità di Endpoint	13
	Funzionalità Discover	13
	Funzionalità di rete	14
	Funzionalità cloud	14
	Funzionalità rimosse e obsolete	15
Capitolo 2	Funzionalità nuove e modificate in Symantec Data Loss Prevention 15.1	16
	Funzionalità di installazione e upgrade	16
	Miglioramenti di installazione di Enforce Server e server di rilevamento	17
	Miglioramenti relativi all'aggiornamento di Enforce Server e dei server di rilevamento	17
	Funzionalità di Enforce Server e della piattaforma	18
	Supporto di Oracle 12c Standard Edition 2 Release 2	18
	Comunicazione protetta tra Enforce Server e il database Oracle	18
	Contrassegna automaticamente gli incidenti da eliminare	19
	Limite ampliato per il campo Aggiungi nota	19
	Le pagine della console di amministrazione di Enforce Server sono state rinnovate e rese più facile da usare.	19
	Nomi dei servizi aggiornati	19
	Istruzioni per il dimensionamento e le prestazioni di Enforce Server e del database	20
	Funzionalità di rilevamento	20

Rilevamento del contenuto contrassegnato utilizzando una nuova opzione di corrispondenza di classificazione	20
EDM a un unico passaggio	20
IDM a un unico passaggio	21
Indicizzazione IDM incrementale	21
Miglioramenti nella corrispondenza tra tipi di file	21
Supporto migliorato per l'Affordable Care Act	22
Identificatori di dati nuovi e aggiornati	22
Modelli di politica Regolamento generale per la protezione dei dati (GDPR) aggiornati	24
Inclusione di alias di posta elettronica in gruppi di utenti	27
Funzionalità di Endpoint	27
Unico programma di installazione per gli agenti di endpoint DLP, ICT e ICE	27
Miglioramenti di utilizzabilità per le funzionalità ICE degli endpoint	27
Aggiornamento al monitoraggio del browser	28
Possibilità di visualizzare i destinatari di e-mail bloccate nelle finestre di notifica pop-up	29
Supporto di Symantec Information Centric Encryption (ICE) per le applicazioni di archiviazione cloud	29
Funzionalità Discover	29
Scansione della griglia per i target SharePoint	30
Linee guida per le prestazioni e la scalabilità della scansione della griglia SharePoint	30
Configurare Network Protect in modo da mettere in quarantena i file riservati nei repository di Microsoft SharePoint	30
Funzionalità di rete	31
ICAP protetta per Network Prevent for Web con Blue Coat ProxySG	31
Aumento dei limiti di caratteri del filtro IP di rete e filtro mittente per Network Monitor	32
Funzionalità cloud	32
Aggiornamento di più facili domini di posta elettronica per Cloud Service for Email	32
Crittografare la posta utilizzando Symantec ICE con Cloud Service for Email	32
Funzionalità e piattaforme rimosse e obsolete	33
Informazioni sulle piattaforme obsolete	33
Supporto per il servizio stunnel	33
Supporto dei sistemi operativi per i server	33
Integrazioni prodotto Symantec	33
Supporto dei sistemi operativi per sistemi endpoint	33

Sistemi operativi obsoleti per sistemi endpoint	34
Supporto di target Exchange Server	34
Target Exchange Server obsoleti	34
Target di Documentum Content Server obsoleti	34
Supporto di target di rilevatore OpenText (Livelink)	34
Supporto dei desktop virtuali con Endpoint Prevent	34
Applicazione Endpoint Prevent	35
Applicazione Endpoint Prevent obsoleta	35
Target di IBM (Lotus) Notes	35
Target di database SQL	35
Target di database SQL obsoleti	35
Target del server SharePoint	35
Impostazioni di Advanced Server	35

Introduzione a Symantec Data Loss Prevention 15.1

Il capitolo contiene i seguenti argomenti:

- [Informazioni su questa guida](#)
- [Riepilogo delle funzionalità nuove e modificate in Symantec Data Loss Prevention 15.1](#)

Informazioni su questa guida

La *guida Novità e modifiche* in Symantec Data Loss Prevention 15.1 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 15.1, 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.

Riepilogo delle funzionalità nuove e modificate in Symantec Data Loss Prevention 15.1

Le funzionalità nuove e modificate in Symantec Data Loss Prevention 15.1 sono riassunte in questo capitolo. È possibile trovare ulteriori dettagli sulla distribuzione e una spiegazione di tali funzionalità nel capitolo 2.

Integrazione con altri prodotti di protezione delle informazioni Symantec

Tabella 1-1 Funzionalità nuove e modificate per le integrazioni di protezione delle informazioni per Symantec Data Loss Prevention 15.1

Funzionalità	Descrizione
Programma di installazione unico per DLP Agent, Information Centric Tagging (ICT) e utilità di Crittografia incentrata sulle informazioni (ICE)	<p>È possibile scegliere di installare tutti gli agenti nello stesso momento, oppure di installare ciascuno separatamente.</p> <p>Vedere "Unico programma di installazione per gli agenti di endpoint DLP, ICT e ICE" a pagina 27.</p>
Supporto di Symantec Information Centric Encryption (ICE) per le applicazioni di archiviazione cloud	<p>Utilizzare le funzionalità integrate di Symantec Information Centric Encryption (ICE) per crittografare file riservati che vengono caricati o scaricati utilizzando applicazioni di archiviazione cloud monitorate come Box e Microsoft OneDrive.</p> <p>Vedere "Supporto di Symantec Information Centric Encryption (ICE) per le applicazioni di archiviazione cloud" a pagina 29.</p>
Supporto di Symantec Information Centric Encryption per Cloud Service for Email	<p>Utilizzare le funzionalità di Symantec Information Centric Encryption per crittografare e-mail riservate inviate tramite applicazioni e-mail monitorate, come Microsoft Exchange on-site, Microsoft Office 365 e Gmail.</p> <p>Vedere "Crittografare la posta utilizzando Symantec ICE con Cloud Service for Email" a pagina 32.</p>
Integrazione avanzata con Symantec Information Centric Tagging (ICT)	<p>Consente di configurare facilmente le politiche di Data Loss Prevention in modo da rilevare il contenuto classificato in base alla tassonomia dalla distribuzione di Symantec Information Centric Tagging in uso.</p> <p>Vedere "Rilevamento del contenuto contrassegnato utilizzando una nuova opzione di corrispondenza di classificazione" a pagina 20.</p>
Utilizzabilità di Symantec ICE migliorata	<p>Le istantanee di incidenti indicano se un file è stato crittografato o crittografato e bloccato; altri miglioramenti semplificano la configurazione e l'interazione con l'utente finale.</p> <p>Vedere "Miglioramenti di utilizzabilità per le funzionalità ICE degli endpoint" a pagina 27.</p>

Funzionalità di installazione e upgrade

Tabella 1-2 Funzionalità nuove e modificate per l'installazione e l'aggiornamento per 15.1 Symantec Data Loss Prevention

Funzionalità	Descrizione
Installazione migliorata del server di rilevamento e di Enforce Server	<p>Il nuovo programma di installazione per i server di rilevamento ed Enforce Server consente di selezionare i componenti necessari per la propria implementazione. Se si selezionano solo i componenti necessari, il payload di installazione si riduce, così come l'utilizzo della larghezza di banda della rete.</p> <p>Vedere "Miglioramenti di installazione di Enforce Server e server di rilevamento" a pagina 17.</p>
Miglioramenti relativi all'aggiornamento di Enforce Server e dei server di rilevamento	<p>Il nuovo processo per l'upgrade dell'Enforce Server e dei server di rilevamento migliora le prestazioni rispetto agli upgrade nelle versioni precedenti. Inoltre, il nuovo processo di upgrade fornisce le funzionalità seguenti:</p> <ul style="list-style-type: none"> ■ Consente di aggiornare le istanze Windows e Linux a due e tre livelli direttamente dalla versione 14.x di Symantec Data Loss Prevention a Symantec Data Loss Prevention 15.1. ■ Consente di eseguire l'upgrade con la versione esistente di Symantec Data Loss Prevention in esecuzione. <p>Vedere "Miglioramenti relativi all'aggiornamento di Enforce Server e dei server di rilevamento" a pagina 17.</p>

Funzionalità di Enforce Server e della piattaforma

Tabella 1-3 Funzionalità di Enforce Server nuove e modificate per Symantec Data Loss Prevention 15.1

Funzionalità	Descrizione
Supporto di Oracle 12c Standard Edition 2 Release 2	<p>È possibile utilizzare Oracle 12c Standard Edition 2 Release 2 (versione 12.2.0.1) con Symantec Data Loss Prevention 15.1 per nuove installazioni e aggiornamenti.</p> <p>È possibile ottenere Oracle 12C Standard Edition 2 Release 2 direttamente da Symantec.</p> <p>Vedere "Supporto di Oracle 12c Standard Edition 2 Release 2" a pagina 18.</p>

Funzionalità	Descrizione
Comunicazione protetta tra Enforce Server e il database Oracle	<p>È possibile creare una connessione protetta tra Enforce Server e il database Oracle mediante TLS.</p> <p>Vedere "Comunicazione protetta tra Enforce Server e il database Oracle" a pagina 18.</p>
Contrassegna automaticamente gli incidenti da eliminare	<p>Contrassegna automaticamente gli incidenti per l'eliminazione in base a criteri quali l'età degli incidenti.</p> <p>Vedere "Contrassegna automaticamente gli incidenti da eliminare" a pagina 19.</p>
Limite ampliato per il campo Aggiungi nota	<p>Il limite per il campo Aggiungi nota per l'azione regola di risposta e l'azione incidente è stato aumentato da 1024 caratteri a 4000 byte.</p> <p>Vedere "Limite ampliato per il campo Aggiungi nota" a pagina 19.</p>
Le pagine della console di amministrazione di Enforce Server sono state rinnovate e rese più facile da usare.	<p>Layout aggiornati per i dashboard del quadro generale e le pagine Gruppi di politiche e Server di rilevamento cloud nella console di amministrazione di Enforce Server.</p> <p>Vedere "Le pagine della console di amministrazione di Enforce Server sono state rinnovate e rese più facile da usare." a pagina 19.</p>
Nomi dei servizi aggiornati	<p>Symantec Data Loss Prevention 15.1 include una modifica a tutti i nomi dei servizi; se il nome comincia con "Vontu," ora inizierà con "SymantecDLP." Tutti i nomi dei servizi che includevano "Monitor" ora includono "DetectionServer".</p> <p>Vedere "Nomi dei servizi aggiornati" a pagina 19.</p>
Istruzioni per la scalabilità e le prestazioni di Enforce Server	<p>La documentazione per Symantec Data Loss Prevention 15.1 include raccomandazioni su scalabilità e prestazioni di Enforce Server.</p> <p>Vedere "Istruzioni per il dimensionamento e le prestazioni di Enforce Server e del database" a pagina 20.</p>

Funzionalità di rilevamento

Tabella 1-4 Funzionalità di rilevamento nuove e modificate per Symantec Data Loss Prevention 15.1

Funzionalità	Descrizione
EDM in un unico passaggio e altri miglioramenti relativi all'EDM	<p>Le prestazioni di rilevamento dell'EDM in un unico passaggio sono state migliorate fino a 14 volte quando viene utilizzato un numero elevato di indici EDM. Altre modifiche all'EDM comprendono miglioramenti al comportamento delle clausole WHERE, delle parole non significative, dell'elaborazione in cinese, giapponese e coreano e della corrispondenza multitoken.</p> <p>La reindicizzazione dell'EDM è obbligatoria dopo l'esecuzione dell'upgrade a Symantec Data Loss Prevention 15.1.</p> <p>L'EDM presenta nuovi requisiti di memoria; sono inoltre state introdotte modifiche nella modalità di dimensionamento dei server di rilevazione. Il <i>Foglio elettronico dei requisiti di memoria EDM</i> è stato aggiornato.</p> <p>Vedere "EDM a un unico passaggio" a pagina 20.</p>
IDM a un unico passaggio	<p>Miglioramento delle prestazioni di rilevamento fino a 30% quando vengono utilizzati più indici.</p> <p>Vedere "IDM a un unico passaggio" a pagina 21.</p>
Indicizzazione IDM incrementale	<p>È possibile allegare file a un indice creato in precedenza senza sostituire l'intero indice distribuito.</p> <p>Vedere "Indicizzazione IDM incrementale" a pagina 21.</p>

Funzionalità	Descrizione
Miglioramenti tipo di file	<p>È possibile selezionare quattro regole di corrispondenza tipo file diverse per Outlook. Il supporto per il tipo di file Outlook è esteso a:</p> <ul style="list-style-type: none"> ■ File di messaggio Outlook: formato <code>.msg</code> ■ File di dati di Outlook per Mac: formato <code>.olm</code> ■ File Personal Storage Table di Outlook: formato <code>.pst</code> ■ File di dati di Outlook: formato <code>.ost</code>, da poco supportato anche in Symantec Data Loss Prevention 15.1. <p>In Symantec Data Loss Prevention 15.0 è disponibile solo il formato <code>.msg</code>.</p> <p>Vedere "Miglioramenti nella corrispondenza tra tipi di file" a pagina 21.</p>
Supporto migliorato per l'Affordable Care Act	<p>Symantec Data Loss Prevention 15.1 offre un supporto migliore per l'Affordable Care Act (ACA), grazie a un nuovo modello di politica e a tre i nuovi identificatori di dati per rilevare le informazioni sanitarie protette associate con i programmi Medicare e Medicaid degli Stati Uniti.</p> <p>Vedere "Supporto migliorato per l'Affordable Care Act" a pagina 22.</p>
Identificatori di dati nuovi e aggiornati	<p>Più di 40 identificatori di dati nuovi e aggiornati.</p> <p>Vedere "Identificatori di dati nuovi e aggiornati" a pagina 22.</p>
Modelli aggiornati per il Regolamento generale per la protezione dei dati (GDPR)	<p>Alcuni modelli della politica GDPR sono stati aggiornati in modo da riflettere i nuovi identificatori di dati dell'Identità personale Europa.</p> <p>Il GDPR sostituisce le Direttive UE sulla protezione dei dati a partire dal 25 maggio 2018.</p> <p>Vedere "Modelli di politica Regolamento generale per la protezione dei dati (GDPR) aggiornati" a pagina 24.</p>
Inclusione di alias di posta elettronica in gruppi di utenti	<p>È possibile includere gli alias di posta elettronica nelle configurazioni dei gruppi di utenti.</p> <p>Vedere "Inclusione di alias di posta elettronica in gruppi di utenti" a pagina 27.</p>

Funzionalità di Endpoint

Tabella 1-5 Funzionalità di Endpoint nuove e modificate per Symantec Data Loss Prevention 15.1

Funzionalità	Descrizione
Aggiornamenti del browser	<p>Il DLP Agent utilizza processi nativi del browser per monitorare i browser di Windows. Ciò consente di migliorare le prestazioni e impedire interruzioni nella copertura del monitoraggio.</p> <p>Il DLP Agent utilizza un'estensione per monitorare Safari in modo che risulti conforme ai protocolli di sicurezza di Safari.</p> <p>Vedere "Aggiornamento al monitoraggio del browser" a pagina 28.</p>
Possibilità di visualizzare i destinatari di e-mail bloccate nelle finestre di notifica pop-up	<p>È possibile configurare le politiche in modo da visualizzare le e-mail bloccate in pop-up di notifica per gli endpoint.</p> <p>Vedere "Possibilità di visualizzare i destinatari di e-mail bloccate nelle finestre di notifica pop-up" a pagina 29.</p>

Funzionalità Discover

Tabella 1-6 Funzionalità di Discover nuove e modificate per Symantec Data Loss Prevention 15.1

Funzionalità	Descrizione
Scansione della griglia per i target SharePoint	<p>La funzionalità di scansione della griglia di Network Discover ora supporta i target di scansione di Microsoft SharePoint. Le scansioni della griglia migliorano la velocità di scansione distribuendo il carico di lavoro tra più server di rilevamento.</p> <p>Vedere "Scansione della griglia per i target SharePoint" a pagina 30.</p>
Linee guida per le prestazioni e la scalabilità della scansione della griglia SharePoint	<p>La documentazione di Symantec Data Loss Prevention 15.1 include raccomandazioni relative a scalabilità e prestazioni per l'esecuzione di scansioni della griglia in target di scansione SharePoint.</p> <p>Vedere "Linee guida per le prestazioni e la scalabilità della scansione della griglia SharePoint" a pagina 30.</p>

Funzionalità	Descrizione
Quarantena Network Protect di file riservati nei repository di SharePoint	<p>Configurare Network Protect in modo da mettere automaticamente in quarantena file riservati nel repository di Microsoft SharePoint utilizzando l'azione di risposta Network Protect: metti file in quarantena.</p> <p>In alternativa, configurare l'azione di risposta smart Quarantena SharePoint in modo da risolvere gli incidenti manualmente.</p> <p>Vedere "Configurare Network Protect in modo da mettere in quarantena i file riservati nei repository di Microsoft SharePoint" a pagina 30.</p>

Funzionalità di rete

Tabella 1-7 Funzionalità di rete nuove e modificate per Symantec Data Loss Prevention 15.1

Funzionalità	Descrizione
ICAP protetta per Network Prevent for Web con Blue Coat ProxySG	<p>Utilizzare ICAP protetta per Network Prevent for Web con Blue Coat ProxySG. L'utilizzo del servizio stunnel non è più supportato.</p> <p>Vedere "ICAP protetta per Network Prevent for Web con Blue Coat ProxySG" a pagina 31.</p>
Aumento dei limiti di caratteri per il filtro IP di rete e il filtro mittente per Network Monitor	<p>I limiti di caratteri per il filtro IP di rete e il filtro mittente per la configurazione di Network Monitor sono stati aumentati.</p> <p>Vedere "Aumento dei limiti di caratteri del filtro IP di rete e filtro mittente per Network Monitor" a pagina 32.</p>

Funzionalità cloud

Tabella 1-8 Funzionalità cloud nuove e modificate per Symantec Data Loss Prevention 15.1

Funzionalità	Descrizione
Aggiornamento di più facile domini di posta elettronica per Cloud Service for Email	<p>Aggiungere e aggiornare i domini di e-mail per Cloud Service for Email per Microsoft Office 365 in modalità di riflessione nella console di amministrazione di Enforce Server.</p> <p>Vedere "Aggiornamento di più facile domini di posta elettronica per Cloud Service for Email" a pagina 32.</p>

Funzionalità rimosse e obsolete

Parecchie funzionalità sono state rimosse o indicate come obsolete in Data Loss Prevention versione 15.1. Vedere ["Funzionalità e piattaforme rimosse e obsolete"](#) a pagina 33.

Funzionalità nuove e modificate in Symantec Data Loss Prevention 15.1

Il capitolo contiene i seguenti argomenti:

- [Funzionalità di installazione e upgrade](#)
- [Funzionalità di Enforce Server e della piattaforma](#)
- [Funzionalità di rilevamento](#)
- [Funzionalità di Endpoint](#)
- [Funzionalità Discover](#)
- [Funzionalità di rete](#)
- [Funzionalità cloud](#)
- [Funzionalità e piattaforme rimosse e obsolete](#)

Funzionalità di installazione e upgrade

Le seguenti funzionalità di installazione e upgrade sono nuove o migliorate in Symantec Data Loss Prevention 15.1.

Miglioramenti di installazione di Enforce Server e server di rilevamento

Il nuovo processo di installazione per i server di rilevamento ed Enforce Server consente di selezionare i componenti necessari per una specifica implementazione. Selezionando componenti di installazione specifici viene ridotto il payload di installazione e l'utilizzo della larghezza di banda della rete rispetto al processo di installazione precedente.

Il nuovo processo di installazione richiede l'installazione di Java Runtime Environment (JRE), inclusi i file del programma di installazione Symantec Data Loss Prevention, prima di poter avviare l'installazione della piattaforma principale (Enforce Server). Poiché Java Runtime Environment è separato dall'installazione della piattaforma, è possibile eseguire l'aggiornamento man mano che Symantec certifica nuove versioni di JRE.

Nota: La parte dell'interfaccia utente grafica dell'installazione di Linux non è più necessaria.

Il nuovo processo di installazione comprende miglioramenti che aumentano la facilità di utilizzo. È possibile utilizzare gli strumenti di distribuzione per eseguire l'installazione utilizzando MSI sui server Windows e RPM su server Linux. Ecco alcuni strumenti di distribuzione che è possibile utilizzare:

- Per RPM, è possibile utilizzare i repository YUM e strumenti SMS di terze parti quali System Center Configuration Manager.
- Per MSI, è possibile utilizzare la distribuzione GPO e strumenti SMS di terze parti quali System Center Configuration Manager.

Miglioramenti relativi all'aggiornamento di Enforce Server e dei server di rilevamento

Il nuovo processo di upgrade per Enforce Server e i server di rilevamento offre i seguenti miglioramenti:

- Consente di aggiornare le istanze a uno, due e tre livelli direttamente da Symantec Data Loss Prevention versione 14.0 e versioni successive alla versione 15.1. Non è più necessario eseguire l'upgrade in modo incrementale da una distribuzione principale o secondaria alla successiva.

Nota: Eseguire l'upgrade di DLP Agent almeno alla versione 14.0 prima di eseguire l'upgrade di Enforce Server a 15.1. Le versioni di DLP Agent precedenti alla 14.0 non possono comunicare con la versione 15.1 di Enforce Server e dei server di rilevamento.

- Consente di eseguire l'upgrade mentre la versione esistente di Symantec Data Loss Prevention continua a monitorare i dati.
- Consente di tornare facilmente a una versione precedente.

Nota: Il processo di aggiornamento esegue la migrazione di dati dall'istanza precedente a una nuova istanza che utilizza una nuova struttura di directory, compresi i plug-in che si trovano in `C:\SymantecDLP\Protect\plugins\ContentExtraction`. Il processo di migrazione non eseguire la migrazione di plug-in di fuori di questa posizione. Fare riferimento alla versione 15.1 del *Manuale di upgrade di Symantec Data Loss Prevention* nel seguente articolo del centro di supporto Symantec:

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

Se necessario, è possibile eseguire un ripristino dopo la migrazione. Per dettagli, fare riferimento alla versione 15.1 del *Manuale di manutenzione del sistema Symantec Data Loss Prevention* nel seguente articolo del centro di supporto Symantec:

<http://www.symantec.com/docs/DOC9267>.

Funzionalità di Enforce Server e della piattaforma

Le seguenti funzionalità di Enforce Server sono nuove o migliorate in Symantec Data Loss Prevention 15.1.

Supporto di Oracle 12c Standard Edition 2 Release 2

È possibile utilizzare Oracle 12c Standard Edition 2 Release 2 (versione 12.2.0.1) con Symantec Data Loss Prevention 15.1 per nuove installazioni e aggiornamenti. È possibile ottenere Oracle 12C Standard Edition 2 Release 2 direttamente da Symantec.

Symantec termina il supporto per Oracle 11g il 25 settembre 2018. Symantec consiglia di eseguire l'upgrade al database di Oracle 12C Standard Edition 2 Release 2 per continuare a ricevere le patch di sicurezza e le correzioni dei bug.

Per ulteriori informazioni, fare riferimento al *Manuale di installazione e upgrade di Symantec Data Loss Prevention Oracle 12c Standard Edition 2 Release 2* nel seguente articolo del centro di supporto Symantec: <http://www.symantec.com/docs/DOC10713>.

Comunicazione protetta tra Enforce Server e il database Oracle

È possibile stabilire una connessione protetta tra l'Enforce Server e il database Oracle mediante TLS 1.2. È possibile fare in modo che i certificati creino la connessione o utilizzino un certificato del server firmato da un'autorità di certificazione pubblica.

Contrassegna automaticamente gli incidenti da eliminare

È possibile contrassegnare automaticamente gli incidenti per l'eliminazione nella pagina **Sistema > Utilità di eliminazione degli incidenti > Contrassegna incidenti da eliminare** pagina. Ad esempio, è consigliabile contrassegnare automaticamente gli incidenti per l'eliminazione in base alla data. Contrassegnare automaticamente gli incidenti per l'eliminazione consente di risparmiare una notevole quantità di tempo e risorse, in particolare in caso di numero elevato di incidenti nel sistema.

Per contrassegnare automaticamente incidenti per l'eliminazione, creare report di incidenti con i criteri desiderati, ad esempio la data. È possibile creare un report per ogni categoria di incidente: **Rete**, **Endpoint**, **Discover**, e **Applicazioni**. È possibile personalizzare la pianificazione in base al contrassegno degli incidenti, oppure contrassegnare gli incidenti manualmente.

Dopo aver contrassegnato gli incidenti per l'eliminazione, è possibile pianificarli per l'eliminazione o eliminarli manualmente nella pagina **Sistema > Utilità di eliminazione degli incidenti > Elimina incidenti**.

Per ulteriori informazioni, vedere l'argomento della Guida [Informazioni su come contrassegnare automaticamente gli incidenti da eliminare](#).

Limite ampliato per il campo Aggiungi nota

Il limite per il campo **Aggiungi nota** per l'azione regola di risposta e l'azione incidente è stato aumentato da 1024 caratteri a 4000 byte.

Le pagine della console di amministrazione di Enforce Server sono state rinnovate e rese più facile da usare.

Symantec Data Loss Prevention 15.1 include layout aggiornati per i dashboard di quadro generale e la pagina **Gruppi di politiche** nella console di amministrazione di Enforce Server.

Per ulteriori informazioni sui dashboard di quadro generale, vedere l'argomento della Guida [Informazioni sui report dashboard e i riepiloghi executive](#).

Nomi dei servizi aggiornati

Symantec Data Loss Prevention 15.1 include una modifica a tutti i nomi di servizio. Nelle versioni precedenti, i nomi dei servizi erano preceduti da `Vontu`. Ora questi nomi di servizi sono preceduti da `SymantecDLP`. Oltre a questa modifica, il termine `Monitor` viene sostituito da `DetectionServer`. I nuovi nomi servizio sono i seguenti:

- `SymantecDLPDetectionServer`
- `SymantecDLPDetectionServerController`

- SymantecDLPIncidentPersister
- SymantecDLFManager
- SymantecDLFNotifier
- SymantecDLFUpdate

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

Istruzioni per il dimensionamento e le prestazioni di Enforce Server e del database

La documentazione per Symantec Data Loss Prevention 15.1 include raccomandazioni su dimensionamento e prestazioni di Enforce Server e del database.

Per ulteriori informazioni su queste raccomandazioni, vedere la *Symantec Data Loss Prevention Guida alla compatibilità e ai requisiti di sistema*.

Funzionalità di rilevamento

Le seguenti funzionalità di rilevamento sono nuove o migliorate in Symantec Data Loss Prevention 15.1.

Rilevamento del contenuto contrassegnato utilizzando una nuova opzione di corrispondenza di classificazione

È possibile creare regole di rilevamento scegliendo tag ICT dalla tassonomia di classificazione di Information Centric Tagging, che vengono importati e visualizzati nella console di amministrazione di Enforce Server. Utilizzare la nuova opzione *Classificazione corrispondenze contenuto* per rilevare il contenuto classificato in tutti i canali di Data Loss Prevention (rete, archiviazione, Endpoint, Cloud). I tag ICT vengono rilevati nelle e-mail e nei file. I tipi di file supportati includono i file di Microsoft Office (formati di versioni precedenti, Office 2007 e versioni successive), file PNG, file GIF e file PDF.

Vedere [Sincronizzazione con Information Centric Tagging](#) e [Condizioni per la corrispondenza del contenuto](#) nella Guida in linea.

EDM a un unico passaggio

Le prestazioni dell'EDM a un unico passaggio sono state migliorate fino a 14 volte rispetto alle versioni precedenti quando più indici EDM vengono distribuiti in un set di criteri. Altre modifiche all'EDM comprendono miglioramenti al comportamento delle clausole WHERE, delle parole

non significative, dell'elaborazione in cinese, giapponese e coreano e della corrispondenza multitoken.

Le nuove linee guida sul dimensionamento dei nuovi server di rilevamento risultano rispecchiate nel foglio di lavoro aggiornato relativo ai requisiti di memoria EDM. Il foglio di calcolo si trova nel centro di supporto Symantec: <http://www.symantec.com/docs/DOC8255.html>.

È necessario reindicizzare gli indici EDM quando si esegue l'upgrade a Symantec Data Loss Prevention 15.1.

Vedere [Informazioni sull'upgrade delle distribuzioni EDM](#) nella Guida in linea.

IDM a un unico passaggio

Con l'IDM a un unico passaggio, le prestazioni di rilevamento vengono migliorate fino al 30% quando sono configurate due o più regole IDM e si utilizzano più indici.

L'IDM a un unico passaggio è disponibile sul server; tuttavia, non è disponibile nell'endpoint.

Quando si esegue l'upgrade a Symantec Data Loss Prevention 15.1, è necessario reindicizzare gli indici IDM.

Vedere [Reindicizzazione dei profili IDM dopo un upgrade importante](#) nella Guida in linea.

Indicizzazione IDM incrementale

Conserva sempre i file è una nuova opzione di Indicizzatore IDM remoto. Quando si sceglie questa opzione, i file che si trovano nell'indice precedente, ma non nell'origine dati attuale, non vengono eliminati. I file possono ora essere aggiunti a un indice creato in precedenza; non è necessario sostituire l'intero indice quando si aggiungono file.

L'opzione **Conserva sempre i file** è disponibile nell'interfaccia della riga di comando dell'Indicizzatore IDM remoto su Windows e Linux e la versione dell'interfaccia utente dell'Indicizzatore IDM remoto su Windows.

Vedere [Indicizzazione incrementale](#) nella Guida in linea.

Miglioramenti nella corrispondenza tra tipi di file

Quando si usa la condizione Tipo file corrispondente per il rilevamento, è ora possibile selezionare una delle quattro diverse regole di tipo file corrispondente a ogni tipo di Outlook supportato, incluso il nuovo tipo di file `.ost` supportato:

- File messaggio di Outlook: identificazione del tipo di file `.msg`, estrazione di metadati ed estrazione dei file secondari per i file messaggio di Outlook.
- File di dati di Outlook per Mac: identificazione del tipo di file `.olm` ed estrazione dei metadati per i file di macOS.

- File Personal Storage Table di Outlook: supporto per l'identificazione del tipo di file `.pst` per iCard.
- File di dati di Outlook: identificazione del tipo di file `.ost`, estrazione di metadati ed estrazione di file secondari per i file di dati di Outlook.

Se il formato dei file di messaggio Outlook (`.msg`) è stato selezionato in Symantec Data Loss Prevention 15.0, quando si passa alla versione Symantec Data Loss Prevention 15.1, tutti e quattro i tipi di file sono selezionati. Se nessun formato di file di Outlook è stato selezionato nella versione 15.0, nessuno dei quattro tipi di file risultano selezionati quando si esegue l'upgrade alla versione 15.1.

Vedere [Formati supportati per l'identificazione dei tipi di file](#) nella Guida in linea.

Supporto migliorato per l'Affordable Care Act

Symantec Data Loss Prevention 15.1 offre un supporto migliore per l'Affordable Care Act (ACA), grazie a un nuovo modello di politica: **Medicare e Medicaid (incluso PHI)**. Questa politica rileva le informazioni sanitarie protette (PHI) associate ai programmi Medicare e Medicaid degli Stati Uniti, compresi i numeri dei beneficiari di Medicare, i numeri delle richieste di rimborso dell'assicurazione sanitaria e i codici CPT (Current Procedural Terminology) correnti utilizzati dal sistema di codifica delle procedure di assistenza sanitaria più comuni (Healthcare Common Procedure Coding System).

Ci sono tre nuovi dati identificatori associati con il modello di politica **Medicare e Medicaid (incluso PHI)** :

- **Healthcare Common Procedure Coding System (codice CPT HCPCS)** : il sistema di codifica delle procedure comuni per l'assistenza sanitaria (HCPCS) è un insieme di codici di procedure mediche basati sulla Current Procedural Terminology (CPT) dell'American Medical Association.
- **Numero di assicurazione sanitaria** : il numero di assicurazione sanitaria (HICN) viene assegnato dall'amministrazione della previdenza sociale a un individuo allo scopo di identificarlo come beneficiario di assistenza sanitaria.
- **Identificatore beneficiario di assistenza sanitaria** : l'Identificatore beneficiario di assistenza sanitaria (MBI) è assegnato a un individuo allo scopo di identificarlo come beneficiario di assistenza sanitaria. Entro aprile 2019 l'MBI sostituirà il numero di assicurazione sanitaria (HICN) su tutte le tessere Medicare.

Per ulteriori informazioni sul nuovo modello di politica **Medicare e Medicaid (incluso PHI)**, vedere l'argomento della Guida [Medicare e Medicaid \(incluso PHI\)](#).

Identificatori di dati nuovi e aggiornati

Symantec Data Loss Prevention 15.1 include diversi identificatori di dati nuovi e aggiornati.

Identificatori di dati nuovi:

- Numero di partita IVA austriaco
- Numero di identificazione fiscale danese
- Numero di partita IVA danese
- Numero di patente finlandese
- Numero di previdenza sociale europea della Finlandia
- Numero di passaporto finlandese
- Numero di identificazione fiscale finlandese
- Numero di partita IVA finlandese
- Numero di identificazione fiscale tedesco
- Codice fiscale della Grecia (AMKA)
- Numero di passaporto irlandese
- Numero di identificazione fiscale irlandese
- Numero di partita IVA irlandese
- Numero di patente di guida giapponese
- Numero di identificazione personale lettone
- Numero di passaporto lussemburghese
- Numero di identificazione fiscale lussemburghese
- Numero di partita IVA lussemburghese
- Numero di patente di guida portoghese
- Numero di identificazione nazionale portoghese
- Numero di passaporto portoghese
- Numero di identificazione fiscale portoghese
- Numero di partita IVA portoghese
- Numero di identificazione nazionale rumeno
- Numero di identificazione nazionale slovacco
- Numero identificativo cittadini della Slovenia
- Numero di partita IVA spagnolo
- Numero di patente di guida svedese
- Numero di identificazione personale svedese

- Numero di identificazione fiscale svedese
- Numero di partita IVA svedese
- Coordinate bancarie di un numero di conto britannico
- Numero di partita IVA britannico (VAT)

Identificatori di dati aggiornati:

- Numero di previdenza sociale austriaco
- Numero di cittadinanza univoco bulgaro (EGN)
- Social Insurance Number (numero di previdenza sociale) canadese
- ID Hong Kong
- Numero di patente di guida italiana
- Numero di identificazione personale giapponese - Aziendale
- Numero di identificazione fiscale lettone
- Codice statistico polacco (REGON)
- Numero di identificazione personale rumeno
- Numero di identificazione personale svedese

Per ulteriori informazioni su questi identificatori di dati nuovi e aggiornati, consultare l'argomento della Guida [Identificatori di dati definiti dal sistema](#).

Modelli di politica Regolamento generale per la protezione dei dati (GDPR) aggiornati

Regolamento generale per la protezione dei dati (GDPR) è un regolamento con cui la Commissione europea vuole rafforzare e unificare la protezione dei dati delle persone all'interno dell'UE. Tratta inoltre dell'esportazione dei dati personali all'esterno dell'UE. Gli obiettivi principali del GDPR sono di restituire ai cittadini il controllo sui propri dati personali e di semplificare le norme per le aziende internazionali unificando i regolamenti all'interno dell'UE. Il GDPR sostituisce le Direttive UE sulla protezione dei dati a partire dal 25 maggio 2018.

Symantec Data Loss Prevention 15.1 include aggiornamenti ad alcuni modelli della politica GDPR che riflettono i nuovi identificatori di dati dell'Identità personale Europa.

Il modello di politica **Regolamento generale per la protezione dei dati (attività bancarie e finanza)** include questi nuovi identificatori di dati:

- Numero di partita IVA austriaco
- Numero di identificazione fiscale danese
- Numero di partita IVA danese

- Numero di patente finlandese
- Numero di passaporto finlandese
- Numero di identificazione fiscale finlandese
- Numero di partita IVA finlandese
- Numero di identificazione fiscale tedesco
- Numero di passaporto irlandese
- Numero di identificazione fiscale irlandese
- Numero di partita IVA irlandese
- Numero di identificazione personale lettone
- Numero di passaporto lussemburghese
- Numero di identificazione fiscale lussemburghese
- Numero di partita IVA lussemburghese
- Numero di patente di guida portoghese
- Numero di passaporto portoghese
- Numero di identificazione fiscale portoghese
- Numero di partita IVA portoghese
- Numero di identificazione nazionale rumeno
- Numero di partita IVA spagnolo
- Numero di patente di guida svedese
- Numero di identificazione fiscale svedese
- Numero di partita IVA svedese

Il modello di politica **Regolamento generale per la protezione dei dati (identificazione governativa)** include questi nuovi identificatori di dati:

- Numero di partita IVA austriaco
- Numero di identificazione fiscale danese
- Numero di partita IVA danese
- Numero di patente finlandese
- Numero di passaporto finlandese
- Numero di identificazione fiscale finlandese
- Numero di partita IVA finlandese

- Numero di identificazione fiscale tedesco
- Numero di passaporto irlandese
- Numero di identificazione fiscale irlandese
- Numero di partita IVA irlandese
- Numero di passaporto lussemburghese
- Numero di identificazione fiscale lussemburghese
- Numero di partita IVA lussemburghese
- Numero di patente di guida portoghese
- Numero di passaporto portoghese
- Numero di identificazione nazionale portoghese
- Numero di identificazione fiscale portoghese
- Numero di partita IVA portoghese
- Numero di patente di guida svedese
- Numero di identificazione fiscale svedese
- Numero di partita IVA svedese

Il modello di politica **Regolamento generale per la protezione dei dati (sanità e assicurazioni)** include questi nuovi identificatori di dati:

- Numero di patente finlandese
- Numero di patente di guida portoghese
- Numero di identificazione nazionale portoghese

Il modello di politica **Regolamento generale per la protezione dei dati (viaggi)** include questi nuovi identificatori di dati:

- Numero di patente finlandese
- Numero di passaporto finlandese
- Numero di passaporto irlandese
- Numero di passaporto lussemburghese
- Numero di patente di guida portoghese
- Numero di identificazione nazionale portoghese

Per ulteriori informazioni sui modelli delle politiche GDPR, vedere l'argomento della Guida [Modelli di politiche relative al Regolamento generale per la protezione dei dati \(GDPR\)](#).

Inclusione di alias di posta elettronica in gruppi di utenti

È possibile configurare gruppi di utenti per includere gli alias di posta elettronica. Ad esempio, se un utente ha l'indirizzo e-mail primario "giovanni_rossi@azienda.com" e un alias di posta elettronica "gianni_rossi@azienda.com", in Microsoft Active Directory selezionando **Includi alias di posta** si aggiungono all'indice DGM entrambi gli indirizzi e-mail per tale utente. Si tenga presente che l'indicizzazione di alias di posta elettronica aumenta la dimensione dell'indice.

Per ulteriori informazioni sull'inclusione di alias di posta elettronica in gruppi di utenti, vedere l'argomento della Guida online [Configurazione di gruppi di utenti](#).

Funzionalità di Endpoint

Symantec Data Loss Prevention consente di monitorare gli endpoint Windows e macOS. Salvo indicazione contraria, le funzionalità descritte qui si applicano agli endpoint sia macOS sia Windows.

Le seguenti funzionalità di rete sono nuove o migliorate in Symantec Data Loss Prevention 15.1.

Unico programma di installazione per gli agenti di endpoint DLP, ICT e ICE

Oltre a DLP Agent, il processo di creazione dei pacchetti del programma di installazione degli endpoint Windows può includere gli agenti ICT e ICE, e il processo di creazione dei pacchetti del programma di installazione degli endpoint macOS può includere gli agenti DLP e ICE.

È possibile scegliere di installare tutti gli agenti nello stesso momento, oppure di installare ciascuno separatamente.

Includere questi agenti endpoint in un unico pacchetto facilita la distribuzione di soluzioni integrate, tra cui Symantec Data Loss Prevention, Symantec Information Centric Tagging e Symantec Information Centric Encryption.

Per ulteriori informazioni sul processo di installazione di ciascun prodotto, vedere il *Manuale di installazione di Symantec Data Loss Prevention*, versione 15.1 nel seguente articolo del centro di supporto Symantec:

<http://www.symantec.com/docs/DOC9257>

Miglioramenti di utilizzabilità per le funzionalità ICE degli endpoint

I seguenti miglioramenti semplificano e migliorano il modo in cui gli amministratori e gli utenti degli endpoint di Enforce Server interagiscono con Symantec ICE:

- La regola di risposta Prevent: Crittografia funziona sugli endpoint di Microsoft Windows in esecuzione in modalità provvisoria.
- Le istantanee degli incidenti visualizzano due nuove risposte agente:
 - **Azione crittografata** - Indica che un utente gestito ha cercato di copiare o spostare un file riservato tramite un canale supportato e il file è stato crittografato automaticamente.
 - **Crittografia azione bloccata** - Indica che l'azione di un utente è stata bloccata e un file è stato crittografato in quanto un utente non gestito ha cercato di copiarlo o spostarlo utilizzando un canale supportato, oppure perché un utente gestito ha cercato di copiare o spostare il file utilizzando un canale non supportato.

Nota: Gli utenti della console di amministrazione di Enforce Server possono anche selezionare queste risposte agente durante la configurazione dei filtri nella sezione **Filtri avanzati e riepilogo** dei report di incidenti endpoint.

- Durante la configurazione della regola di risposta Prevent: crittografia, vengono configurati solo due messaggi di avviso, invece di tre:
 - Avviso di blocco
 - Avviso di crittografia

Nota: Quando un utente non gestito tenta di copiare o spostare un file riservato tramite un canale supportato o non supportato, viene visualizzato un avviso di blocco.

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

- La regola di risposta Prevent: crittografia ora mostra le notifiche agli utenti di Endpoint e non richiede alcuna azione da parte dell'utente.
- I file crittografati da ICE non vengono decrittografati quando gli utenti li copiano con Esplora risorse da dispositivi di archiviazione USB su unità di rete condivise o sul disco locale.
- I file crittografati da ICE non vengono bloccati quando gli utenti tentano di copiarli da dispositivi di archiviazione USB su unità di rete condivise.
- La crittografia dei file è supportata sui dispositivi di archiviazione USB formattati con il file system FAT32.

Aggiornamento al monitoraggio del browser

Il DLP Agent utilizza processi nativi del browser per monitorare Microsoft Edge, Firefox (su Windows) e Internet Explorer. Gli aggiornamenti aiutano a migliorare le prestazioni e a impedire

interruzioni di copertura del monitoraggio dopo aggiornamenti dell'architettura del browser. Gli aggiornamenti al monitoraggio di Microsoft Edge sono conformi ai nuovi standard di sicurezza di Microsoft.

Per monitorare Safari, DLP Agent utilizza un'estensione. Questo metodo è conforme ai protocolli di sicurezza Safari introdotti con l'aggiornamento di sicurezza della patch Apple 2018-001. Gli utenti endpoint devono attivare l'estensione per consentire il monitoraggio dell'endpoint. La schermata **Panoramica agente** identifica gli endpoint in cui l'estensione non è ancora attivata.

Per ulteriori informazioni, vedere [Informazioni sul controllo applicazioni](#) nella Guida in linea.

Possibilità di visualizzare i destinatari di e-mail bloccate nelle finestre di notifica pop-up

È possibile configurare le politiche in modo da visualizzare le e-mail bloccate in pop-up di notifica per gli endpoint. La funzionalità è supportata per le seguenti piattaforme e applicazioni:

- Windows con Outlook 2013 e 2016 e IBM Notes 9.0.x
- macOS con Outlook 2011 e 2016

Questa funzionalità utilizza nelle politiche la nuova regola Destinatari corrispondenti, al fine di identificare e-mail singole o domini interi nelle finestre pop-up di notifica.

Supporto di Symantec Information Centric Encryption (ICE) per le applicazioni di archiviazione cloud

Le funzionalità di Symantec Information Centric Encryption (ICE) per Endpoint Prevent sono state ampliate in modo da poter applicare più facilmente la crittografia ICE ai file sensibili che vengono caricati utilizzando applicazioni di archiviazione cloud monitorate, come Box e Microsoft OneDrive. Si utilizza l'azione Prevent: crittografia nella regola di risposta per applicare automaticamente ICE ai file riservati che vengono monitorati mediante il canale Cloud sugli endpoint. È necessario distribuire la console del cloud ICE per visualizzare e gestire l'accesso ai file protetti.

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

Funzionalità Discover

Le seguenti funzionalità Discover sono nuove o migliorate in Symantec Data Loss Prevention 15.1.

Scansione della griglia per i target SharePoint

La funzionalità di scansione griglia di Network Discover ora supporta i target di scansione di Microsoft SharePoint. La scansione di griglia consente a Symantec Data Loss Prevention di eseguire scansioni in modo più efficiente, distribuendo il carico di lavoro tra più server di rilevamento.

Quando si configura una scansione di griglia, è necessario selezionare almeno due server di rilevamento affinché la funzionalità di scansione di griglia venga eseguita correttamente. Quando si avvia una scansione della griglia, un server di rilevamento viene designato come elemento principale della griglia; questo è il server che individua tutti gli elementi nell'archivio di SharePoint e invia i loro URL ad altri server di rilevamento nella griglia. Gli altri server di rilevamento quindi tentano di scaricare il contenuto dell'archivio e di rilevare informazioni riservate nel target della scansione. Quando viene rilevata una violazione, i server di rilevamento inviano un incidente a Enforce Server. L'elemento principale della griglia invia aggiornamenti sullo stato della scansione a Enforce Server, gestisce l'indice incrementale e aggiorna tutte le statistiche di scansione.

Per ulteriori informazioni vedere questi argomenti della Guida in linea:

- [Informazioni sulle scansioni di griglia](#)
- [Configurazione delle scansioni di griglia](#)
- [Configurazione ed esecuzione delle scansioni dei server SharePoint](#)

Linee guida per le prestazioni e la scalabilità della scansione della griglia SharePoint

La documentazione per Symantec Data Loss Prevention 15.1 include le linee guida su prestazioni e scalabilità per l'esecuzione di scansioni di griglia su target di scansione SharePoint.

Per ulteriori informazioni, visitare il seguente articolo nel centro di supporto Symantec:
<http://www.symantec.com/docs/TECH247591>.

Configurare Network Protect in modo da mettere in quarantena i file riservati nei repository di Microsoft SharePoint

È possibile configurare Network Protect in modo da mettere in quarantena file di Microsoft SharePoint direttamente nella console di amministrazione di Enforce Server. Nelle versioni precedenti di Symantec Data Loss Prevention era necessario installare e configurare un plug-in di FlexResponse per mettere in quarantena i file di SharePoint. Ora non è più necessario installare, configurare e utilizzare il plug-in di FlexResponse.

Per mettere in quarantena i file di SharePoint utilizzando una regola di risposta automatica, scegliere l'azione di risposta Network Protect: metti file in quarantena. Inoltre, quando si

configura un target di scansione SharePoint, si forniscono dettagli sulla posizione di quarantena nella scheda **Proteggi** del target di scansione.

Per mettere in quarantena i file di SharePoint utilizzando una regola di risposta Smart, selezionare l'azione Network Protect: quarantena SharePoint.

Il plug-in SharePoint Quarantine FlexResponse di Symantec Data Loss Prevention non è più supportato a partire da questa versione. A partire dalla versione 15.1, è necessario utilizzare l'azione di risposta Network Protect: metti file in quarantena in Network Protect per mettere automaticamente in quarantena file riservati invece del plug-in SharePoint Quarantine FlexResponse.

Per mettere in quarantena i file di SharePoint utilizzando Network Protect, gli utenti esistenti devono prima disinstallare il plug-in Symantec Data Loss Prevention SharePoint Quarantine FlexResponse.

Per rilasciare i file SharePoint riservati dalla quarantena, è necessario proseguire con l'installazione e l'uso della distribuzione SharePoint Symantec Data Loss Prevention dal plug-in FlexResponse della quarantena.

Per informazioni sull'installazione e la disinstallazione dei plug-in FlexResponse, fare riferimento alla *Symantec Data Loss Prevention Guida all'implementazione del plug-in SharePoint Quarantine FlexResponse*.

Per ulteriori informazioni, vedere questi argomenti:

- [Configurazione ed esecuzione delle scansioni dei server SharePoint](#)
- [Configurazione di Network Protect per i server SharePoint](#)
- [Configurazione dell'azione di risposta smart Quarantena SharePoint](#)

Funzionalità di rete

Le seguenti funzionalità di rete sono nuove o migliorate in Symantec Data Loss Prevention 15.1.

ICAP protetta per Network Prevent for Web con Blue Coat ProxySG

ICAP protetta sostituisce stunnel ed è ora disponibile per Network Prevent for Web con Blue Coat ProxySG.

È possibile configurare ICAP protetta nella pagina **Configura Server** selezionando **ICAP protetta** quando si aggiunge un server Network Prevent for Web. È inoltre necessario disporre di un archivio chiavi configurato e fornire la relativa password. La configurazione del client viene impostata in Blue Coat ProxySG.

Vedere [Network Prevent for Web Server - Configurazione di base](#) nella guida in linea.

Aumento dei limiti di caratteri del filtro IP di rete e filtro mittente per Network Monitor

È possibile utilizzare un numero di caratteri maggiore per il filtro di origine IP di rete, il filtro di destinazione IP, il filtro mittente L7 e il filtro destinatario L7 per i protocolli utilizzati dalla configurazione Network Monitor. Il limite precedente era 2048 caratteri; il nuovo limite è 2800 caratteri.

Funzionalità cloud

Le seguenti funzionalità cloud sono nuove o migliorate in Symantec Data Loss Prevention 15.1.

Aggiornamento di più facile domini di posta elettronica per Cloud Service for Email

È possibile aggiornare rapidamente i domini di posta elettronica delle e-mail aziendali che si vuole sottoporre a scansione da parte di Cloud Service for Email senza dover contattare il supporto Symantec per apportare le modifiche. Questa nuova funzionalità si applica solo alle e-mail inviate da Microsoft Office 365 in modalità di riflessione.

Quando si aggiunge o si rimuove un dominio nella console di amministrazione di Enforce Server, il nuovo elenco viene inviato immediatamente a Symantec. Tutti i domini sono verificati e aggiornati ogni 15 minuti dal servizio Symantec Cloud.

Vedere [Aggiornamento dei domini e-mail](#) nella Guida in linea.

Crittografare la posta utilizzando Symantec ICE con Cloud Service for Email

Utilizzare le funzionalità di Symantec Information Centric Encryption (ICE) per crittografare e-mail riservate inviate tramite applicazioni e-mail monitorate, come Microsoft Exchange on-site, Microsoft Office 365 e Gmail. ICE offre la possibilità di crittografare solo l'allegato, oppure sia l'e-mail sia l'allegato.

Si configura ICE per e-mail nella console di amministrazione di Enforce Server e si utilizza l'azione di crittografia nella regola di risposta. Vengono visualizzati incidenti nella pagina **Dettagli incidente** con collegamenti alla console del cloud ICE. Si visualizza e gestisce l'accesso a file protetti nella console del cloud ICE.

Per ulteriori informazioni sulla distribuzione della console del cloud ICE e sull'impostazione di ICE, vedere *Guida alla distribuzione di Symantec Information Centric Encryption* in <http://www.symantec.com/docs/DOC9707.html>.

Vedere anche [Configurazione di Enforce Server per connettersi al cloud ICE di Symantec](#) nella Guida in linea.

Funzionalità e piattaforme rimosse e obsolete

Informazioni sulle piattaforme obsolete

Determinate piattaforme sono indicate 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.

Supporto per 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.

Supporto dei sistemi operativi per i server

I seguenti sistemi operativi server non sono più supportati:

- Red Hat Enterprise Linux 6.7.
- Windows Server 2012 Standard Edition, Datacenter Edition ed Enterprise (distribuzione iniziale)
Windows Server 2012 R2 è ancora supportato.

Integrazioni prodotto Symantec

Symantec Encryption Management Server (DLP Encryption Insight) versione 3.3 non è più supportato.

Supporto dei sistemi operativi per sistemi endpoint

I seguenti sistemi operativi endpoint non sono più supportati:

- Windows 7 Enterprise, Professional, Ultimate (32 bit) (distribuzione iniziale)
Windows 7 Service Pack 1 è ancora supportato.
- Windows 7 Enterprise, Professional, Ultimate (64 bit) (distribuzione iniziale)
Windows 7 Service Pack 1 è ancora supportato.

- Sistema operativo Windows 8 Enterprise PC (64 bit)
- macOS 10.10 (a 64 bit)

Sistemi operativi obsoleti per sistemi endpoint

I seguenti sistemi operativi endpoint sono obsoleti:

- Windows 10 Update Enterprise e Professional (a 64 bit) [1511]
- Windows 10 Red Stone Update Enterprise e Professional (a 64 bit) [1607 - RS1]

Supporto di target Exchange Server

I seguenti target di Exchange server non sono più supportati:

- Microsoft Exchange Server 2010
- Microsoft Exchange Server 2010 SP1
- Microsoft Exchange Server 2010 SP2

Target Exchange Server obsoleti

Microsoft Exchange Server 2007 SP3 è obsoleto.

Target di Documentum Content Server obsoleti

I seguenti target di Documentum Content Server sono obsoleti:

- 5.3.x
- 6.6.x
- 6.7

Supporto di target di rilevatore OpenText (Livelink)

Il supporto della scansione dei target di OpenText (Livelink) Server 9.x target è obsoleto nella versione 15.1.

Supporto dei desktop virtuali con Endpoint Prevent

I desktop virtuali seguenti non sono più supportati in Endpoint Prevent:

- Citrix XenDesktop 5.6
- VMware Workstation 6.5.x

Applicazione Endpoint Prevent

Le seguenti applicazioni non sono più supportate in Endpoint Prevent:

- Safari 9.1
- Internet Explorer 9
- Microsoft Office 2007

Applicazione Endpoint Prevent obsoleta

Il browser Edge RS1 è obsoleto.

Target di IBM (Lotus) Notes

Versioni 7.0 - 8.0 dei target di Lotus Notes non più supportate in Network Discover.

Target di database SQL

DB2 9.1, 9.2, e 9.5 non sono più supportati in Network Discover.

Target di database SQL obsoleti

Oracle 10g è obsoleto.

Target del server SharePoint

I seguenti target del server SharePoint non sono più supportati:

- Microsoft Office SharePoint Server 2007 (tutti i service pack)
- Microsoft Office SharePoint Server 2010
- Microsoft Office SharePoint Server 2010 SP1
- Microsoft Office SharePoint Server 2013
- Microsoft Office SharePoint Online 2010 (modalità dedicata)
- Microsoft Office SharePoint Online 2013 (modalità dedicata)
- Microsoft Office SharePoint Online 2016 (modalità dedicata)

Impostazioni di Advanced Server

Le seguenti impostazioni di Advanced Server per la configurazione delle politiche EDM non sono più supportate:

- Lexer.MaxTokensPerMultiToken
- Lexer.StopwordLanguages