clearswift
by HelpSystems

DATENBLATT *(Cybersicherheit)*

Clearswift Endpoint DLP

Angesichts von mehr als 4 Milliarden Datensätzen, die in der ersten Jahreshälfte 2019 durch Datenschutzverletzungen verloren gegangen sind, und neuer Datenschutzgesetze auf der ganzen Welt ist es für Unternehmen wichtiger denn je, zu wissen, wo sich ihre kritischen Informationen befinden, und sicherzustellen, dass sie nicht über Wechseldatenträger durchsickern können.

Geschäftliches Problem

Wir leben in einer datenzentrierten Welt. Unternehmen stellen ihren Mitarbeitern Zugang zu Daten zur Verfügung, damit sie ihre Arbeit erledigen können; um mit internen Mitarbeitern und externen Organisationen zusammenzuarbeiten. Es muss auch sichergestellt werden, dass die kritischen Daten, die sich auf Laptops, Servern und in Cloud-Diensten befinden, nur von den Personen genutzt werden, die sie benötigen und dass sie für die richtigen Zwecke verwendet werden.

Wir haben jedoch zu viele Fälle von versehentlichem Datenverlust gesehen, darunter:

- Laptops, die mit kritischen Informationen in unverschlüsseltem Zustand gestohlen werden
- USB-Sticks, die in Taxis zurückgelassen werden
- DVDs mit personenbezogenen Daten (PII), die auf dem Postweg verloren gehen
- Tragbare Festplatten, die nicht angemessen gesichert sind.

Neben dem versehentlichen Verlust können Mitarbeiter versucht sein, Unternehmensdaten mitzunehmen, wenn sie ihren Arbeitsplatz verlassen, oder sie können Daten absichtlich gegen Geld weitergeben oder entscheiden, dass die ethischen Vorstellungen ihres Arbeitgebers zweifelhaft sind und zum Whistleblower werden.

Die Herausforderung für Unternehmen besteht heute darin, die effektivste Sicherheitstechnologie für Laptops, Desktops und Geräte zu finden, die es den Anwendern ermöglicht, effizient zu arbeiten, aber mit dem heute erforderlichen Schutzniveau.

Architektur

Der Schutz der Endpunkte erfordert zwei Komponenten, um effektiv zu sein:

- Eine skalierbare Serverarchitektur, die eine granulare Richtlinienkontrolle von Benutzern und Gruppen über
- Die Produktkonsole. Diese Architektur darf keine Single Points of Failure haben und muss auf Tausenden von Endpunkten skalierbar sein
- Einfache, funktionsreiche Endpunkte, die die Richtlinien für Device Control, Data at Rest und Data in Use durchsetzen und bei Verstößen an die Server zurückmelden, aber auch dem Endbenutzer ein Feedback geben, um ihn zu informieren, wenn ein Fehler gemacht wurde.

Gerätekontrolle

Die Möglichkeit, Benutzer zu kontrollieren, die persönliche USB-Geräte oder Smart Devices mit dem Unternehmensnetzwerk verbinden, ist zu einer kritischen Sicherheitsanforderung geworden. Durch die unkontrollierte Nutzung von Wechselmedien können sensible Daten verloren gehen und bösartige Anwendungen in Netzwerke eingeschleust werden. Die Clearswift Endpoint DLP-Lösung bietet eine granulare Verwaltung von Wechseldatenträgern und ermöglicht so die legitime, produktivitätssteigernde Nutzung dieser Geräte bei gleichzeitiger Reduzierung von Netzwerkrisiken und Supportkosten - was zu einer erhöhten Datensicherheit führt.

Kontextabhängige Data In Use (DIU)-Richtlinien

Flexible Richtlinien und eine kontextbezogene Inhaltskontrolle bedeuten, dass Sie nicht mehr zwischen der produktiven Nutzung von Wechselmedien, Netzwerkfreigaben und Cloud-Speicher und einem inakzeptablen Risiko wählen müssen. Eine zu restriktive Richtlinie bedeutet, dass Mitarbeiter entweder nicht effektiv arbeiten können oder Wege finden, die Sicherheitsrichtlinie zu umgehen. Es können

Regeln erstellt werden, die verhindern, dass alle textbasierten Office-Dateien, die bestimmte Schlüsselbegriffe enthalten, auf externe Geräte, Netzwerkfreigaben und Cloud-Speicher kopiert werden. Alternativ können Dateien bei der Übertragung verschlüsselt werden - was sicherstellt, dass der Inhalt eines USB-Sticks nicht gelesen werden kann, wenn er in einem Taxi oder an einem anderen öffentlichen Ort zurückgelassen wird.

Adaptive Redaction mit DIU
Adaptive Redaction ist eine einzigartige und preisgekrönte Technologie für einen proaktiven Ansatz zum Schutz kritischer Informationen. Sie verhindert, dass sensible Daten versehentlich außerhalb oder innerhalb eines Unternehmens weitergegeben werden und entschärft eingehende gezielte Angriffe. Adaptive Redaction bietet einen Mechanismus, mit dem das traditionelle "Stoppen und Blockieren" herkömmlicher Data-Loss-Prevention-Lösungen überwunden werden kann, indem nur genau die Inhalte automatisch entfernt werden, die gegen die Richtlinien verstoßen - der Rest der Kommunikation kann ungehindert fortgesetzt werden.

Erkennung von Data At Rest (DAR)
Im Zusammenspiel mit der Clearswift Deep Content Inspection Engine können kritische Daten überall dort entdeckt werden, wo sie auf Desktops, Notebooks, Servern und gemeinsam genutzten Netzwerken gespeichert sind. Dies ermöglicht es Unternehmen, die Bereinigung kritischer Informationen in Data at Rest zu prüfen und zu verwalten. Wie bei den Data-in-Use-Richtlinien sind integrierte und anpassbare lexikalische Ausdrücke enthalten, die die Erkennung kritischer Informationen wie PII, PCI und anderer sensibler Daten ermöglichen. Clearswift Endpoint DLP läuft im Hintergrund und erkennt kritische Informationen, ohne die Aktivitäten der Endbenutzer zu unterbrechen. Dies bietet einen beispiellosen Einblick in potenzielle Datenschutzschwachstellen, die in Ihren Netzwerken und Systemen vorhanden sind.

Bereitstellung

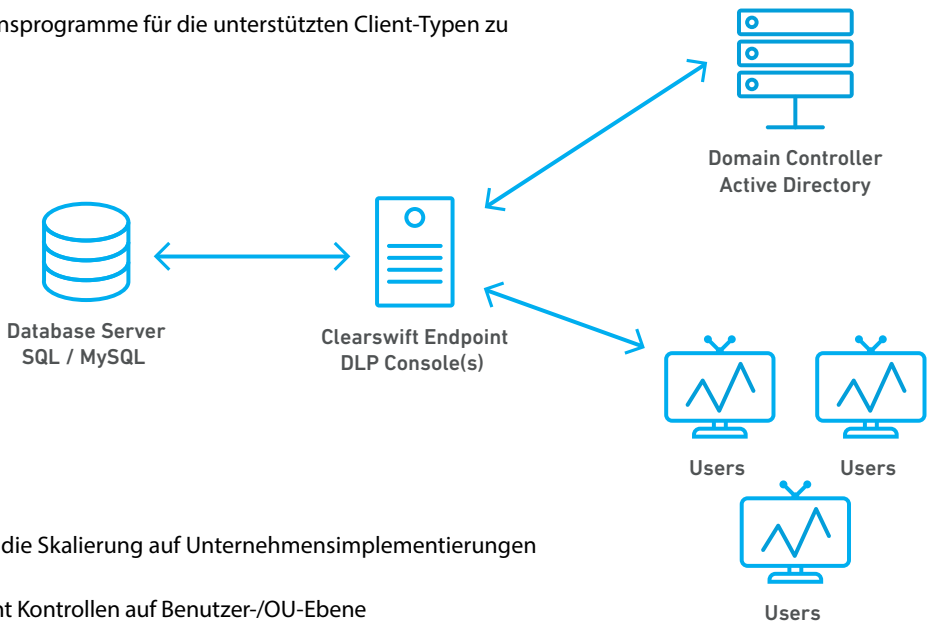
Die Clearswift Endpoint DLP-Konsolenkomponente wird auf einem Windows-Server installiert und erfordert Zugriff auf einen SQL-Server oder eine MySQL-Datenbank. Sie wird mit dem Active Directory des Unternehmens synchronisiert, um die Liste der Computer und Benutzer zu sammeln, so dass Richtlinien auf Domänenebene, auf Ebene der Organisationseinheit oder bis hinunter zu einer Ebene pro Benutzer erstellt werden können. Für eine hohe Verfügbarkeit können mehrere Konsolenserver mit den Endpunkt-Agenten verbunden sein.

Die Konsole wird verwendet, um die Installationsprogramme für die unterstützten Client-Typen zu erstellen und per Fernzugriff bereitzustellen:

- Windows 7 und 10
- Windows Server 2012 R2 und 2016
- Citrix-Umgebungen

Umfassende Berichte über die gesamte Bereitstellung sind über die Konsole verfügbar.

Für Unternehmensbereitstellungen können mehrere Administratoren definiert werden, um eine regionalisierte Verwaltung zu ermöglichen.



Funktionen

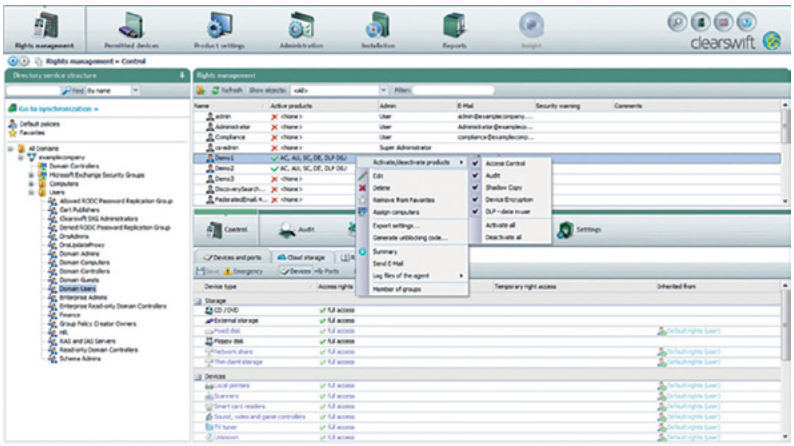
Die Clearswift Endpoint DLP-Lösung wurde für die Skalierung auf Unternehmensimplementierungen entwickelt und bietet:

- Granulare Richtlinienkontrolle - ermöglicht Kontrollen auf Benutzer-/OU-Ebene
- Gerätemanagement - Kontrolle nach Bus und Gerätetyp
- Cloud-Zugriffskontrolle - kontrolliert den Zugriff auf Standard-Cloud-Sharing-Dienste wie OneDrive, Dropbox, Box, etc.
- Data in Use - stellt sicher, dass Daten, die auf externe Geräte, Netzwerkfreigaben und Cloud-Speicher geschrieben werden, einer Inhaltsprüfung unterzogen wurden und nur geeignete Dateitypen verwendet werden können
- Data at Rest scanning - periodisches Scannen der lokalen Festplatte und Freigaben kann auf Dateitypen und -inhalte überprüft werden
- Syslog-Unterstützung - zentralisierte Protokollierung von Ereignisdaten kann an SIEM-Systeme exportiert werden.

Einfach zu bedienende GUI

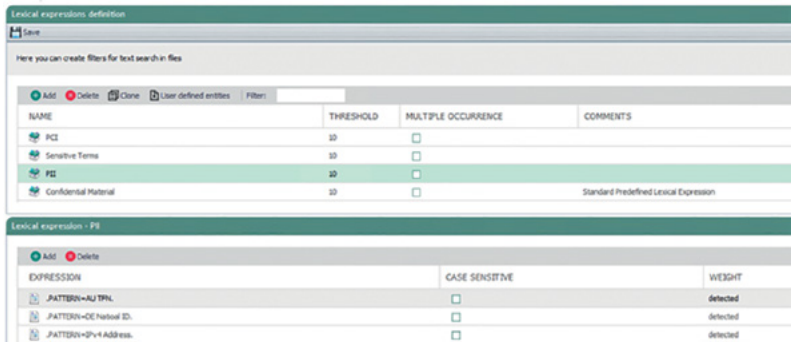
Die Clearswift Endpoint DLP-Verwaltungsoberfläche ist in logische Abschnitte unterteilt, in denen Richtlinien auf Organisationseinheiten angewendet werden können, die aus Active Directory entnommen wurden. Diese Ansicht macht es auch einfach zu sehen, welche Zugriffskontrollregeln sowie Inhaltsrichtlinien angewendet werden.

Funktionen können je nach Bedarf für die Organisation lizenziert werden oder ein Benutzer wird automatisch angemeldet.
Features can be licensed as needed for the organization, or a user automatically enrolled.

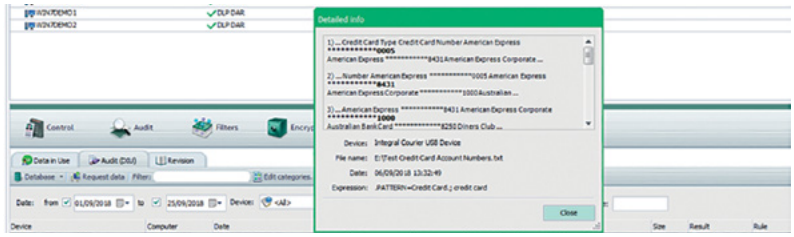


Listen mit lexikalischen Ausdrücken werden mit Wörtern, Phrasen, Token (wie Kreditkarte, IP-Adresse usw.) und regulären Ausdrücken erstellt. Diese Phrasen werden gewichtet und können zusammen verwendet werden, um sinnvolle Suchkriterien zu bilden.

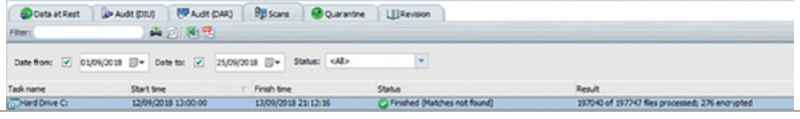
Diese Ausdruckslisten werden verwendet, um DIU- und DAR-Richtlinien zu bilden.



DIU-Scans zeigen, wann Versuche unternommen wurden, sensible Daten zu exfiltrieren und welche Sicherheitsrichtlinien genau verletzt wurden.



DAR-Scans können in Echtzeit angezeigt werden, um den Fortschritt zu zeigen und ob Objekte gefunden wurden.



Feature	Vorteil
Verzeichnis-Integration	Integriert in Verzeichnisservern mit geplanten Synchronisierungsereignissen, um sicherzustellen, dass Änderungen wie neue Mitarbeiter und Computer in den Richtlinien berücksichtigt werden können. Richtlinien für Benutzer und Computer können auf Basis ihrer Struktur innerhalb des Verzeichnisses konfiguriert werden, z. B. Festlegung von Regeln für die Organisationseinheit "Vertrieb". Vorhandene Richtlinien-Standardrichtlinien können für alle Benutzer und Computer einfach erstellt werden, spezifische Änderungen an Benutzern/Computern können nach Bedarf vorgenommen werden.
Data in Use Policies	Die Inhaltskontrolle von Dateien, die auf Wechseldatenträger geschrieben werden, ermöglicht eine konsistente Definition von Wörtern, Phrasen und Richtlinien, um potenzielle Datenverletzungen zu erkennen und zu verhindern.
Data at Rest Policies	Agents können so geplant werden, dass sie fest installierte und/oder Wechseldatenträger zu bestimmten Tageszeiten oder an bestimmten Wochentagen scannen und dabei dieselben Richtlinien zur Inhaltsinspektion verwenden, die für Data In Use Policies erstellt wurden.
Zugriffskontrolle	Physische Geräte wie Wechseldatenträger, Drucker, Modems usw. können nach Name, Typ, Seriennummer oder ID gesperrt werden.
Cloud-Zugriffskontrolle	Um die Änderungen der Schatten-IT zu reduzieren, werden Kontrollen bereitgestellt, um den Zugriff auf gängige Cloud-Filesharing-Anwendungen wie Box, Dropbox, OneDrive und GoogleDrive basierend auf Richtlinien einzuschränken, unabhängig davon, ob sie sich innerhalb oder außerhalb des Unternehmensnetzwerks befinden.
Dateifilter	Dateien können nach bestimmten Datentypen blockiert werden. Es werden die Kopfzeilen und nicht nur die Erweiterungen überprüft, um sicherzustellen, dass Dateien nicht gefälscht werden. Vordefinierte Typen wurden bereitgestellt, um Kunden eine schnelle und einfache Implementierung zu ermöglichen.
Verschlüsselung von Wechseldatenträgern	Bietet umfassende Sicherheit für alle Geräte, die in Wechseldatenträgern abgelegt werden, unabhängig davon, ob sie als geheim oder vertraulich gekennzeichnet wurden oder PCI- und PII-Daten enthalten. Verschlüsselte USB-Geräte können intern mit nahtloser Interaktion mit den entsprechenden Benutzern freigegeben werden.
SQL-Datenbank-Unterstützung	Ermöglicht Kunden die Nutzung von Ressourcen auf bestehenden SQL-Systemen oder die Bereitstellung auf Microsoft SQL Server, MySQL oder SQL Express für kleine Unternehmen/Evaluierungen.
Low Footprint Agent	Agents wurden entwickelt, um die Ressourcennutzung zu minimieren und eine maximale Benutzerfreundlichkeit zu gewährleisten.
Remote-Bereitstellung	Agents können über die Konsole oder mit den Standard-Windows-Massenbereitstellungsoptionen Remote bereitgestellt werden.
Online-/Offlinemodus	Agents, die offline sind, arbeiten weiterhin mit der zuletzt synchronisierten Richtlinie und behalten Protokolle und Alarme bei, bis das Gerät wieder mit dem Unternehmensnetzwerk verbunden ist.

clearswift
by HelpSystems

www.clearswift.de

Über HelpSystems

HelpSystems ist ein Softwareunternehmen, in dem die Menschen an erster Stelle stehen. Getreu unserem Motto Build a Better IT TM unterstützen wir außergewöhnliche Unternehmen bei ihrer Arbeit. Unsere ganzheitliche Produktsuite aus Sicherheits- und Automatisierungslösungen schafft eine einfachere, intelligentere und leistungsstarke IT. Kunden in über 100 Ländern und in den unterschiedlichsten Branchen vertrauen auf HelpSystems. Erfahren Sie mehr unter www.helpsystems.com/de.