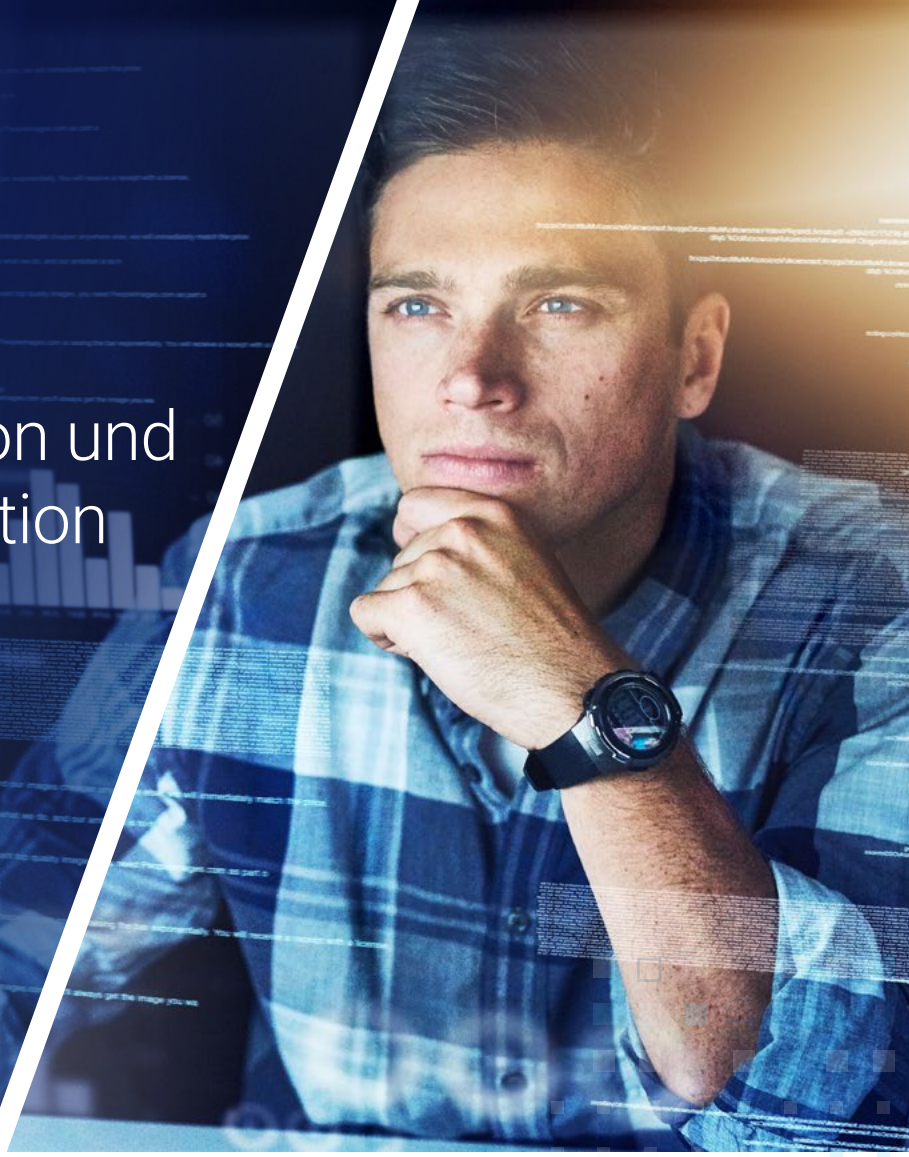
Data Loss Prevention und digitale Transformation



EINFÜHRUNG

Das heutige digitale Zeitalter hat eine beispiellose Menge an Daten hervorgebracht. Ein Großteil dieser Daten gilt als sensibel, wie beispielsweise personenbezogene Informationen über Kunden und Mitarbeiter, Finanzdaten und geistiges Eigentum, das Unternehmen schützen müssen. Früher wurden diese Informationen auf Papier gedruckt und in einem abgeschlossenen Aktenschrank aufbewahrt. Heutzutage wandern diese Nullen und Einsen von einem Ort zum anderen und sind anfälliger als je zuvor.

Dass diese Daten geschützt werden müssen, ist unbestritten. Sie sind das Lebenselixier der Organisation und enthalten Informationen, die der Organisation zum Schutz anvertraut wurden. Bestimmte Arten von Daten sind daher reguliert, und Unternehmen müssen bei missbräuchlicher Verwendung mit hohen Strafen rechnen. Natürlich sind diese Daten auch im Darknet wertvoll, wo eine einzelne Kreditkartennummer mit Adresse bis zu fünf Dollar einbringt – die Art von Informationen, die in vielen Datenbanken in großem Umfang gespeichert werden. Aus all diesen Gründen ist es für Organisationen obligatorisch geworden, umfassende DLP-Lösungen (Data Loss Prevention) zu implementieren.

DIE NOTWENDIGKEIT VON DLP

Eine DLP-Lösung besteht aus einer Reihe von Technologien und Verfahren, mit denen Daten im Unternehmensnetzwerk überwacht und untersucht werden, damit sensible Daten nicht verloren gehen oder gestohlen werden. Eine DLP-Lösung sollte immer Bestandteil einer unternehmensweiten Datenschutzinitiative sein, bei der Geschäftsleitung und IT-Verantwortliche gemeinsam Kriterien für „sensible Daten“ festlegen und entscheiden, wie diese Daten behandelt werden sollten und wie ein Verstoß aussehen könnte. Diese Leitlinien können anschließend in einem DLP-Tool als Regeln festgelegt werden. DLP-Lösungen gehen drei wesentliche Herausforderungen von Organisationen an: Erfüllung gesetzlicher Auflagen, Schutz vor Datenverlust und Transparenz.

1

Erfüllung gesetzlicher Auflagen:

Laut Gartner[1] ist die Erfüllung gesetzlicher Auflagen der bei weitem häufigste DLP-Anwendungsfall, auf den in 75 Prozent aller DLP-Deployments verwiesen wird. Seit Inkrafttreten der europäischen Datenschutz-Grundverordnung (DSGVO) im Mai 2018 wurden DLP-Lösungen auch von Organisationen außerhalb der regulierten Branchen übernommen, die schon immer bestimmte Maßnahmen zum Schutz personenbezogener Daten und vertraulicher Gesundheitsinformationen ergreifen mussten. Die Verwendung einer DLP-Lösung ist zwar per Gesetz nicht zwingend vorgeschrieben, das Konzept von DLP erleichtert jedoch häufig die Erfüllung von Datenschutzauflagen.

Klingt für mich nach DLP...

Das New York State Department of Financial Services (NYDFS) – 23 NYCRR 500 – spielt zwar auf die Verwendung von DLP für Datenübertragungsprozesse (Data-in-Motion) an, nennt DLP aber nicht explizit:

Abschnitt 500.15 (a)

„(...) Jede betroffene Entität muss Kontrollen, einschließlich Verschlüsselung, durchführen, um nicht öffentliche Informationen, die sich im Besitz der Entität befinden oder von dieser übertragen werden, sowohl während der Übertragung über externe Netzwerke als auch im Ruhezustand zu schützen.“

[1] Market Guide for Enterprise Data Loss Prevention:
https://www.gartner.com/en/documents/3890116/market-guide-for-enterprise-data-loss-prevention

DIE NOTWENDIGKEIT VON DLP

2 Schutz vor Datenverlust

Die Gründe, weshalb man sensible Informationen vor dem Zugriff durch Unbefugte schützen sollte, gehen weit über Compliance hinaus. Sensible Daten sind ein häufiges Diebstahlsziel. Wie wertvoll nicht regulierte Daten sind, zeigt sich an der Bereitschaft von Betrügern, im Darknet einen höheren Preis für die Nummern von Prämienkarten oder Treueprogrammen als für US-Sozialversicherungsnummern zu zahlen[2].

Organisationen bemühen sich zwar um Einhaltung der Vorschriften, da sie die Bußgelder und auferlegten Einschränkungen des Geschäftsbetriebs vermeiden wollen, die ihnen bei Missachtung drohen. Datenverluste bergen jedoch viel weiter reichende finanzielle und rufschädigende Risiken, beispielsweise den Verlust von Kunden, die Erstattung oder Rückzahlung verlorener Mitgliedspunkte, die Schädigung der Marke oder sogar rechtliche Konsequenzen.

Laut Ponemon Cost of Data Breach Study von 2019[3] erleben 30 Prozent der Unternehmen alle zwei Jahre einen Verstoß mit durchschnittlichen finanziellen Folgen von:

an Kosten **3,9 Mio. USD** **25.000** **verlorene Datensätze**

Bei Branchen wie dem Gesundheitswesen oder Finanzdiensten, die regulatorischer Compliance unterliegen, sind die Kosten der Verstöße höher. Die durchschnittlichen Kosten pro gestohlenem Datensatz beliefen sich auf:

429 USD	210 USD	150 USD
Gesundheitswesen	**Finanzdienste**	**Alle Branchen**

DLP-Lösungen sind besonders wichtig, um versehentlichen Datenverlust aufgrund menschlicher Fehler zu verhindern, wie zum Beispiel die unbeabsichtigte Weitergabe sensibler Daten über gemeinsam genutzte Dateien und soziale Medien oder durch ein Versagen von IT- und Geschäftsprozessen[4]. Trotz strenger Auflagen für den Umgang mit Gesundheitsinformationen kommt versehentlicher Datenverlust im Gesundheitssektor besonders häufig vor, wo der Anteil von unbeabsichtigter Offenlegung laut Verizon Protected Health Information Data Breach Report von 2018 bei 57,5 Prozent liegt.[5] Verizon stellte fest, dass dies die einzige Branche ist, in der von Insidern eine größeres Datenverlustrisiko ausgeht als von externen Betrügern.

[2] https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/; https://www.comparitech.com/blog/information-security/how-much-are-stolen-frequent-flyer-miles-worth-on-the-dark-web/#gref

[3] [4] Ponemon 2019 Data Breach: https://databreachcalculator.mybluemix.net/

[5] Protected Health Information Data Breach Report: http://www.verizonenterprise.com/resources/protected_health_information_data_breach_report_en_xg.pdf

DIE NOTWENDIGKEIT VON DLP

3 Datentransparenz

Die digitale Transformation konfrontiert Organisationen und insbesondere CISOs mit Herausforderungen hinsichtlich der Sichtbarkeit von Datenaktivitäten, die in ihren Netzwerken vor sich gehen. Angesichts zunehmender Datenmengen, vieler verschiedener Datenbesitzer und noch mehr Orten, an denen sich diese Daten befinden, ist es schwierig, alle sensiblen Informationen zu identifizieren und Maßnahmen für ihren Schutz zu ergreifen. Schließlich können Sie nicht schützen, was Sie nicht sehen. Drei wichtige Trends führen bei Organisationen zu toten Winkeln: Wechsel in die Cloud, Mobilität von Benutzern und Verschlüsselung.

Der Wechsel in die Cloud zwingt Organisationen, alle Daten des Unternehmens zu kontrollieren, nicht nur die im Rechenzentrum gespeicherten. Bevor Sie Ihre Daten in die Cloud verlagern, müssen Sie wissen, welche Daten Sie besitzen.

Mitarbeiter sind nicht mehr auf ihre Schreibtische begrenzt, sondern greifen jederzeit von überall aus auf ihre Applikationen und Arbeitsdateien zu. Diese **mobilen Benutzer** können außerhalb des Rechenzentrums auf Daten zugreifen und Dateien speichern. Dabei wird das Unternehmen bezüglich dieser Daten oftmals im Dunkeln gelassen.

Organisationen verwenden zunehmend **Verschlüsselungstechniken**, um Daten zu schützen. Hardware-basierte Sicherheitssysteme können den Inhalt verschlüsselter Dateien jedoch nicht überprüfen, sodass Organisationen die darin enthaltenen Datentypen nicht erkennen.

DIE NOTWENDIGKEIT VON DLP

Daten wechseln von einem Kanal zum anderen

In unserer digitalisierten Welt bewegen sich Daten freier als je zuvor. Sie können sich jederzeit in einem von drei Kanälen befinden: auf einem Endgerät, im Speicher oder im Transit. Jeder Kanal, in dem Daten entweder gespeichert oder übertragen werden, benötigt andere Tools oder Techniken zur Verhinderung von Datenverlust. DLP-Lösungen sind entsprechend der drei Kanäle segmentiert, die sie schützen:

Daten auf dem Endgerät: DLP-Lösungen für Endgeräte basieren auf Agenten und überwachen die Datenverarbeitung auf dem Endgerät. Ihre Funktionen variieren, schränken in der Regel aber Druckvorgänge ein und verhindern das Kopieren/Einfügen zwischen Anwendungen sowie das Herunterladen auf portable Speicher wie USB.

Data-at-Rest: Alle Daten in Dateiservern, Datenbanken oder Cloud-Speichern gelten als ruhend. DLP für Data-at-Rest scannt sämtliche Repository-Inhalte, um sensible Informationen zu erkennen.

Data-in-Motion: Die auch als Web-DLP oder Netzwerk-DLP bezeichneten Lösungen für Data-in-Motion überprüfen den gesamten Traffic, der über das Web (Internet) oder per E-Mail von Punkt A nach B übertragen wird, z. B. Daten, die vom Cloud-Speicher zum Endgerät unterwegs sind.

Die digitale Transformation hat Benutzerverhalten und Traffic-Muster verändert, was sich auch auf Endgeräte und Kanäle für ruhende Daten auswirkt. Angesichts der zunehmenden Verlagerung von Daten in die Cloud werden Lösungen für ruhende Daten irrelevant, da ihre Funktion von CASB-Lösungen (Cloud Access Security Provider) übernommen werden kann. Außerdem verbleiben weniger Daten und Anwendungen auf Endgeräten, wodurch sich der Schwerpunkt auf die Absicherung der Datenübertragung zwischen Endgeräten, Cloud-Anwendungen und Speicher einer **Lösung für** Data-in-Motion verlagert.

WARUM HAT DLP DIE ERWARTUNGEN NICHT ERFÜLLT?

Der DLP-Markt entwickelt sich weiter

DLP-Lösungen sind seit 15 Jahren verfügbar und der Markt ist ausgereift. Da es nur wenige Unterschiede zwischen konkurrierenden Enterprise DLP-Lösungen gibt, hat die führende Analystenfirma Gartner ihren Magic Quadrant für Enterprise DLP eingestellt. Stattdessen konzentriert sich Gartner auf einen Market Guide, der die Bedeutung ganzheitlicher Datenschutzstrategie hervorhebt und Anleitungen zum Einsatz von integrierten DLP-Lösungen gibt.

Im Gegensatz zu **Enterprise DLP-Lösungen**, die in der Regel eine Vielzahl von Produkten (Agenten, physische und virtuelle Appliances) über alle Kanäle hinweg enthalten, werden **integrierte DLP-Lösungen** nativ über Technologien wie Secure Web Gateway, Content-Management-Systeme, E-Mail-Verschlüsselung oder CASB bereitgestellt und haben dadurch einen engeren Fokus.

Enterprise DLP-Lösungen sind bekanntermaßen komplex und kostspielig. Organisationen, die Enterprise DLP erwerben, nutzen oft nur einen kleinen Teil der Funktionen und gehen nur elementare Anwendungsfälle an, die auch mit einer integrierten DLP-Lösung zu bewältigen sind, die der Organisation die kostspielige, zeitaufwendige Einrichtung und Integration erspart hätte.

Laut Schätzungen von Gartner

> „werden 90% aller Organisationen bis 2021 zumindest eine Form von integrierter DLP einführen, was einer Steigerung von 50% im Vergleich zu heute entspricht.“ [6]

Allerdings schließen sich Enterprise DLP und integrierte DLP nicht zwangsläufig aus. Organisationen, die bereits in solche Produkte investiert haben, sollten mit ihrer vorhandenen Infrastruktur arbeiten. Trotzdem sollte jede Organisation die Ergänzung von integrierter DLP in Betracht ziehen, um weitere Anwendungsfälle einzubeziehen und die Lücken in ihrer bestehenden Datenschutzstrategie zu schließen, die durch die digitale Transformation entstanden sind.

[6] How to Choose Between Enterprise DLP and Integrated DLP Approaches
https://www.gartner.com/doc/3757464?ref=mrktg-srch

WARUM HAT DLP DIE ERWARTUNGEN NICHT ERFÜLLT?

Data Loss Prevention ist eine unternehmensweite Initiative, kein IT-Tool

Obwohl es sich um eine ausgereifte Lösung handelt, berichten Organisationen weiterhin von Problemen beim DLP-Deployment. Viele dieser Probleme sind auf schlechte Planung und andere organisatorische Mängel zurückzuführen.

Viele Organisationen glauben fälschlicherweise, dass DLP nur von der IT-Sicherheit implementiert und langfristig verwaltet werden sollte. Sobald DLP-Regeln festgelegt sind, sollte die Verantwortung für die DLP-Lösung auf den Geschäftsbetrieb übertragen werden. Darüber hinaus müssen diejenigen, die DLP-Lösungen bereitstellen, das Buy-in der Firmenleitung sicherstellen, um einzelne Geschäftsbereiche oder die Arbeit des Risikomanagement-Teams wieder transparent zu machen.

Um nicht nach zusätzlichen Sponsoren und Anwendungsfällen zur Rechtfertigung des Projekts suchen zu müssen, was zwangsläufig zu mehr Ansprüchen und Komplexität beim Deployment führt, müssen Teams das interne Buy-in sicherstellen und DLP-Projekte an bestimmte Initiativen oder Ziele binden.

VORAUSSETZUNGEN VON CLOUD DLP

Wenn Unternehmen in die Cloud wechseln, sollte auch ihre Sicherheit dorthin verlagert werden. Herkömmliche Hardware-Stacks einfach neu zu konfigurieren ist ineffizient und bietet nicht den Schutz oder die Services einer in der Cloud bereitgestellten Lösung. Dies trifft auch auf DLP zu. Um die mit digitaler Transformation verbundenen Datenschutzherausforderungen zu meistern und die Mängel herkömmlicher DLP zu überwinden, bedarf es einer Cloud-basierten DLP-Lösung mit folgenden drei Elementen:

1. **Identischer Schutz für alle Benutzer innerhalb und außerhalb des Netzwerks**
   Bei herkömmlichen, im Rechenzentrum verankerten DLP-Lösungen hängt das Maß an Transparenz und Schutz davon ab, wo sich die Daten befinden. Remote-Benutzer, die sich außerhalb des Netzwerks befinden, können die Überprüfung umgehen und sich ohne VPN oder jegliche Schutzmaßnahmen direkt mit Cloud-Anwendungen verbinden. Um umfassenden Datenschutz zu gewährleisten, sollte eine DLP-Lösung allen Benutzern unabhängig von ihrem Standort – ob dies im Büro, am Flughafen oder im Homeoffice ist – identischen Schutz bieten.

2. **Überprüfung des verschlüsselten Traffic**
   Da 70 Prozent des Traffic heutzutage verschlüsselt werden, sollten Organisationen diesen Traffic unbedingt überprüfen. Weil Verschlüsselung jedoch ursprünglich als Sicherheitsmaßnahme konzipiert wurde, können herkömmliche Sicherheitslösungen diesen Traffic nicht nativ überprüfen. Infolgedessen neigen Organisationen dazu, nur einen Bruchteil ihres verschlüsselten Traffic zu untersuchen – aber was ist eine DLP-Lösung wert, wenn sie vielleicht nur 30% des gesamten Traffic sieht? Eine Erhöhung der Sicherheit mittels Hinzufügens von SSL-Appliances ist wahrscheinlich weder finanziell machbar, noch im Hinblick auf die IT-Komplexität akzeptabel. Um Einblick in verschlüsselten Traffic zu erhalten, muss man eine DLP-Lösung verwenden, die SSL nativ überprüft.

3. **Elastische Skalierbarkeit für Inline-Untersuchung**
   Das enorme Wachstum des Internet-Traffic erfordert ein ständiges Aktualisieren von herkömmlichen, auf Appliances basierten DLP-Lösungen, da deren Überprüfungskapazität schnell erschöpft ist. Um Kosten und Komplexität dieses Unterfangens zu vermeiden, verzichten viele Organisationen von vornherein auf den Inline-Einsatz einer DLP-Lösung. Das führt leider dazu, dass sie nur noch Schaden begrenzen können, wenn ihre Daten bereits kompromittiert wurden.
   Bei einer Cloud-Lösung ist die Überprüfungskapazität elastisch skalierbar, um den gesamten Traffic inline zu untersuchen und Datenverlust zu verhindern – bevor Daten kompromittiert werden können.

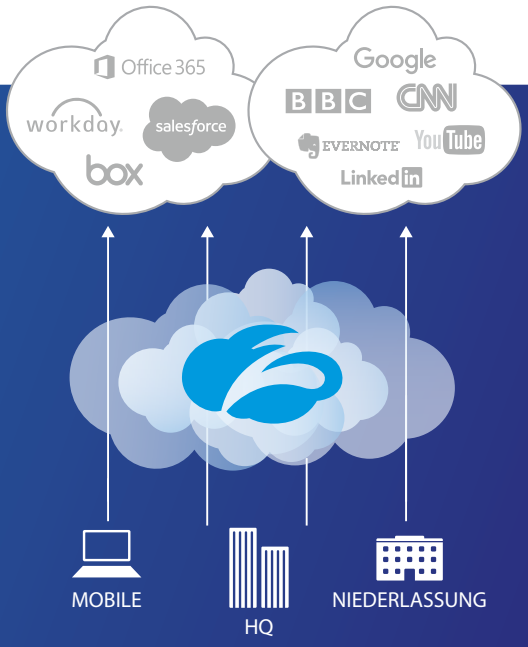
ZSCALER™ CLOUD DLP

Bestandteil von Zscaler Internet Access

Zscaler Internet Access™ (ZIA™) ist ein sicheres Internet- und Web-Gateway, das als Cloud-Service bereitgestellt wird. ZIA ist zwischen Benutzern und dem Internet platziert und überprüft mithilfe mehrerer Sicherheitstechniken jedes Byte des Traffic, selbst SSL, inline, um kompletten Schutz vor Internetbedrohungen zu bieten. Die speziell entwickelte Cloud-Plattform umfasst Cloud Sandbox, Next-Generation Firewall, Transparenz und Kontrolle von Cloud-Anwendungen sowie Cloud DLP.

Überblick über Cloud DLP

Zscaler Cloud DLP bietet umfassenden Datenschutz mit vollständiger Kontext- und Inhaltsuntersuchung sämtlicher Data-in-Motion sowie erweiterte Funktionen wie Exact Data Match, maschinelles Lernen und granulare Richtlinien für optimalen Schutz.



Zscaler Cloud DLP erfüllt die drei Voraussetzungen

Zscaler Cloud DLP bietet allen Benutzern dasselbe Sicherheitsniveau, indem Ihre Datensicherheit in die Cloud verlagert wird. Zscaler befindet sich zwischen den Benutzern und den Anwendungen, zu denen sie Verbindungen herstellen. Die Cloud-basierte DLP-Richtlinie folgt den Benutzern an jeden Arbeitsplatz – innerhalb und außerhalb des Netzwerks – und bietet allen Benutzern jederzeit dasselbe Maß an Schutz.

Cloud DLP untersucht auch den gesamten verschlüsselten Traffic. Rund 70 Prozent des ausgehenden Traffic sind verschlüsselt und werden deshalb von herkömmlichen DLP-Lösungen nicht überprüft. Mit Zscaler gibt es keine Kapazitätsbeschränkungen für die SSL-Untersuchung in großem Maßstab. Zscaler ist als Proxy konzipiert und führt SSL-Überprüfungen des gesamten Traffic ohne die Limitierungen von Appliances durch.

Darüber hinaus befindet sich Zscaler inline und kann dadurch sensible Daten blockieren, bevor sie das Netzwerk verlassen – statt auf Schadenskontrolle im Fall kompromittierter Daten beschränkt zu sein. Die Sicherheitsarchitektur von Zscaler wurde von Grund auf in der Cloud entwickelt. Der Service orientiert sich an Benutzern, nicht an Kapazitäten, sodass Cloud-basierte DLP-Untersuchung gemäß per SLAs garantierter Leistung flexibel skaliert werden kann.

FAZIT

DLP sollte als klar definierter Sicherheitsprozess betrachtet werden, der von einer gut gesteuerten Support-Technologie unterstützt wird. Dennoch haben Organisationen selbst in diesem reifen Stadium von DLP-Lösungen noch Probleme mit dem DLP-Deployment. Dies liegt hauptsächlich an einer internen Falschdarstellung der DLP-Lösungen im Rahmen eines Sicherheitsprogramms. Außerdem überbewerten viele auf dem Markt die Einfachheit des Deployment, den Grad von vorkonfigurierter Genauigkeit bei Inhaltsidentifizierung und Transparenz und die Kontrolle über alle Anwendungen.

Steigendes Risiko und vermehrte Datenschutzbestimmungen erfordern, dass Organisationen die durch Cloud und Mobilität verursachten Sicherheitslücken schließen. In der Vergangenheit bedeutete dies, einem bereits komplexen Security-Stack noch mehr Appliances hinzuzufügen. Zscaler bietet eine bessere Option. Mit Zscaler DLP können Sie Datenschutzlücken unabhängig davon, wo sich Benutzer verbinden oder Anwendungen gehostet werden, ohne kostspielige, komplexe Appliances schließen.

Über Zscaler

Zscaler ermöglicht Organisationen eine sichere Transformation ihrer Netzwerke und Anwendungen für eine mobile Cloud-First-Welt. Zscaler verbindet Benutzer unabhängig von ihrem Gerät, Standort oder Netzwerk mit Anwendungen und Cloud-Services und bietet gleichzeitig umfassende Sicherheit und eine schnelle Nutzererfahrung. All dies ohne kostspielige, komplexe Gateway-Appliances.

zscaler™