MEHR POWER FÜR ENDGERÄTE:
Kombination von Datenschutz und Collaboration

Dieses Whitepaper zeigt die Herausforderungen an die IT auf, die durch mehr Mobilität und Collaboration von Mitarbeitern entstehen, und erläutert, wie Druva diese meistern kann.

Inhalt

Einführung

Es gibt immer mehr Laptops, Smartphones und Tablet-PCs – die sogenannten Endgeräte – und das verändert die Arbeitsweise moderner Unternehmen und stellt IT-Abteilungen vor völlig neue Herausforderungen. Die folgenden drei Herausforderungen haben bei vielen IT-Managern oberste Priorität:

- Auf Endgeräten befindliche kritische Unternehmensdaten müssen per Backup gesichert werden
- Auf Endgeräten befindliche sensible Unternehmensdaten müssen vor Sicherheitsverletzungen geschützt werden
- Mitarbeiter, die bei der Zusammenarbeit mit internen und externen Beteiligten Dateien gemeinsam nutzen, müssen dies auf sichere Weise tun

Darüber hinaus wird IT-Abteilungen zunehmend bewusst, dass sie diese Herausforderungen effizient mit minimaler Bandbreite und Speicherbelegung sowie mit geringem Verwaltungsaufwand bewältigen müssen.

Dieses Whitepaper erörtert die oben genannten Herausforderungen im Detail und beschreibt, weshalb bestehende Lösungen nicht ausreichen, um den entsprechenden IT-Bedarf zu decken. Außerdem wird erläutert, inwiefern Druva die beste Lösung bietet, indem es ein kombiniertes Produkt für Backup, gemeinsamen Dateizugriff und Collaboration auf Endgeräten bereitstellt, Datenschutzverletzungen vorbeugt und gleichzeitig den IT-Aufwand sowie Speicher- und Bandbreitenkosten minimiert.

Aktuelle Trends bedeuten neue Herausforderungen an die IT

Derzeit sind in Unternehmen zwei wichtige Trends erkennbar:

- Zunahme der Nutzung von Laptops/Mobilgeräten
- Zunahme von gemeinsamem Dateizugriff/Collaboration

Diese Trends setzen IT-Abteilungen extrem unter Druck und erschweren es ihnen erheblich, eine ihrer wichtigsten Aufgaben zu erfüllen – den Schutz der Unternehmensdaten.

Zunehmende Nutzung von Laptops/Mobilgeräten

Mitarbeiter werden immer mobiler. Eine IDC-Studie kommt zu dem Schluss, dass bis 2015 weltweit 1,3 Milliarden Beschäftigte mobil tätig sein werden, was 37 % aller Arbeitnehmer entspricht. Diese mobilen Mitarbeiter greifen heute an den unterschiedlichsten Orten auf sensible Unternehmensdaten zu, von Cafés über Flughäfen bis hin zum Rücksitz im Taxi, und nutzen dafür eine Vielzahl von Geräten, wie Laptops, Smartphones, Tablet-PCs usw. Häufig verwenden die

Mitarbeiter dabei auch private Mobiltelefone und Tablet-PCs, da viele Unternehmen mittlerweile die Nutzung eigener Geräte erlauben.

Daraus resultieren die folgenden Herausforderungen an die IT:

• Für kritische Daten auf Endgeräten fehlt ein Backup

Mitarbeiter speichern wichtige Unternehmensdaten oft auf Laptops und Mobilgeräten, kümmern sich jedoch selten um deren Backup. Eine kürzlich durchgeführte Studie ergab, dass 38 % aller Unternehmensdaten auf Laptops[2] gespeichert werden, während eine andere Umfrage belegt, dass allein auf US-amerikanischen Flughäfen bereits mehr als 600.000 Laptops verloren gegangen sind[3]. Darüber hinaus ergab eine von Druva selbst durchgeführte Befragung von IT-Managern, dass fast 50 % aller Unternehmen weniger als 10 % ihrer Laptops per Backup sichern (siehe Grafik unten). Wenn Sie sich in Ihrem Team umhören, werden Sie wahrscheinlich gleich mehrere Schilderungen zu hören bekommen, in denen ein Laptop verloren ging, zu Boden fiel oder mit Kaffee übergossen wurde. Was würde passieren, wenn kein Backup für die Daten auf diesen Laptops vorhanden wäre? Man kann sich nur schwer vorstellen, wie viel Aufwand die Wiederherstellung der Dateien erfordern würde.

Die IT muss daher sicherstellen, dass die verwendeten Endgeräte per Backup gesichert werden. Außerdem muss die IT Backup-Lösungen bereitstellen, die einfach zu benutzen sind und im Hintergrund laufen, sodass das Benutzererlebnis nicht beeinträchtigt wird. Zudem muss das Backup so durchgeführt werden, dass die Kosten für Bandbreite und Speicher auf ein Minimum beschränkt bleiben.

- Fast 38 % aller Unternehmensdaten sind ausschließlich auf Laptops gespeichert[1]
- 17 % dieser Laptops enthalten Daten, die nicht wiederherstellbar sind
- Über 600.000 Notebooks gingen allein an US-amerikanischen Flughäfen verloren[2]
- Nur 35 % aller Unternehmen verfügen über eine Backup-Lösung für Laptops
- Mehr als 70 % aller mobilen Mitarbeiter planen nie einen Backup ein, auch nicht vor oder während Reisen

• Die Sicherheit sensibler Daten auf Endgeräten ist gefährdet

Der Verlust oder Diebstahl von Geräten mit sensiblen Unternehmensdaten kann einem Unternehmen natürlich erhebliche Probleme bereiten. Stellen Sie sich vor, auf einem der 600.000 an Flughäfen verlorenen Laptops wären die aktuellen Verkaufszahlen Ihres Unternehmens, die Pläne für neue Produkte oder sogar der Quellcode für ein wichtiges Produkt gespeichert gewesen. Intel hat in einer kürzlich durchgeführten Forschungsstudie errechnet, dass die Durchschnittskosten für einen verlorenen Laptop 49.000 US-Dollar betragen, wobei über 80 % dieser Kosten aufgrund von Verletzungen der Datensicherheit entstehen[6]. Diese Kosten sind allerdings noch viel höher, wenn ein Unternehmen an regulatorische Vorgaben wie den Health Insurance Portability and Accountability Act (HIPAA) zum Schutz von Patientendaten gebunden ist. Dem britischen Verteidigungsministerium wurde die Bedeutung des Schutzes vor Datenverlusten (Data Loss Prevention**,** DLP) schmerzlich bewusst, als einem jungen Marineoffizier ein Laptop entwendet wurde. Auf dem Laptop waren die persönlichen Daten von 35.000 Rekruten gespeichert, einschließlich Reisepassdaten, Sozialversicherungsnummern, Familienangaben und Anschriften von Ärzten[4]. Doch trotz solch aufsehenerregender Datenverluste setzen viele Unternehmen keine DLP-Tools für Endgeräte ein. In den Studien von Druva gaben mehr als 50 % aller Unternehmen an, dass weniger als 10 % ihrer Laptops über DLP-Funktionen verfügen.

Die IT muss sicherstellen, dass alle verfügbaren Maßnahmen angewandt werden, um eine Verletzung der Sicherheit von Unternehmensdaten auf Endgeräten zu verhindern, sodass diese nicht in falsche Hände gelangen können.

Intel hat in einer kürzlich durchgeführten Forschungsstudie errechnet, dass die Durchschnittskosten für einen verlorenen Laptop 49.000 US-Dollar betragen, wobei über 80 % dieser Kosten aufgrund von Verletzungen der Datensicherheit entstehen[6].

Erhöhter Bedarf für gemeinsamen Dateizugriff und Collaboration

Die Unternehmen verändern sich, da immer mehr Mitarbeiter nach einfach zu bedienenden Tools für die Zusammenarbeit mit Kollegen und externen Partnern verlangen. Eine vor kurzem durchgeführte Untersuchung von Harris Interactive ergab, dass in 46 % aller Unternehmen der Bedarf besteht, kritische Geschäftsinformationen mit Partnern auszutauschen[5]. Dieser Trend bedingt zwei weitere Herausforderungen für IT-Abteilungen:

• Mitarbeiter erwarten von Unternehmenstools die gleiche einfache Bedienung wie bei Consumergeräten

Mitarbeiter erwarten heutzutage, dass geschäftlich genutzte Produkte die gleichen einfach bedienbaren und intuitiven Schnittstellen bieten wie Consumerprodukte. Daher bringen die Mitarbeiter häufig ihre privaten Lösungen für gemeinsamen Datenzugriff und Collaboration in das Unternehmen mit. Allein Dropbox umfasst mehr als 25 Millionen Benutzer und verzeichnet 200 Millionen Datei-Uploads pro Tag. Viele dieser 25 Millionen Benutzer nutzen Dropbox sowohl am Arbeitsplatz als auch zu Hause. Die Untersuchungen von Druva bestätigen die breit angelegte Nutzung solcher Tools. So gab fast ein Viertel aller befragten Unternehmen an, dass der Einsatz dieser Tools entweder „in vielen Teams üblich“ oder „im Unternehmen weit verbreitet“ ist.

• Consumerlösungen für gemeinsamen Dateizugriff und Collaboration sind nicht sicher

Obwohl Dropbox und ähnliche Tools bei vielen Endanwendern sehr beliebt sind, stellen Sie doch ein enormes Risiko für sensible Unternehmensdaten und somit ein großes Problem für die IT-Abteilung dar. Mitarbeiter machen sich bei der Collaboration nur selten Gedanken um die Sicherheit der Daten. Die Bedrohung für die Datensicherheit ist jedoch durchaus reell, da Collaboration-Tools aus dem Consumersegment nur sehr begrenzte Sicherheitsfunktionen aufweisen und z.B. über keine ausreichend starke Verschlüsselung verfügen. Außerdem machen diese Consumertools es den

Mitarbeitern sehr leicht, Daten auf Geräten zu speichern, die nicht von der IT-Abteilung ausgegeben wurden. Wenn beispielsweise ein Benutzer Dropbox sowohl auf seinem Arbeitsplatzrechner als auch auf einem privaten Gerät installiert, lädt Dropbox automatisch alle freigegebenen Arbeitsdateien auch auf das Privatgerät. Solche Geräte sind aber nur selten mit Sicherheitsfunktionen der Unternehmensklasse ausgestattet, sodass sich Eindringlinge viel leichter Zugang zu diesen Geräten und somit zu sensiblen Unternehmensdaten verschaffen können.

Kurz gesagt: Die IT benötigt ein sicheres System, das auf allen Endgeräten Daten per Backup sichert, Datenverluste auf gestohlenen/verlorenen Geräten verhindert und gemeinsamen Dateizugriff sowie Collaboration problemlos ermöglicht. Dieses System muss zugleich auch die Kosten für Speicher und Bandbreite auf ein Minimum reduzieren.

Einschränkungen bestehender Lösungen

Bestehende Lösungen für Backup, gemeinsamen Dateizugriff und Collaboration lassen sich in drei Kategorien einteilen:

- **Reines Backup**
- **Gemeinsamer Dateizugriff und Collaboration auf Consumerniveau**
- **Gemeinsamer Dateizugriff und Collaboration in der Cloud auf Unternehmensniveau**

Leider bietet keine dieser Kategorien eine umfassende Lösung für die oben geschilderten IT-Herausforderungen.

Reines Backup

Reine Backup-Software-Systeme wurden ursprünglich für die Unternehmens-IT konzipiert. Solche Systeme schneiden in Hinblick auf einige der zentralen IT-Kriterien gut ab:

- **Sicherheit** – die Systeme bieten im Allgemeinen ein sicheres und zuverlässiges Backup für im Unternehmen befindliche PCs (nicht für mobile PCs)
- **Transparenz und Audit-Pfad** – die Systeme bieten der IT den benötigten transparenten Einblick in den Backup-Prozess; die IT wird auf Probleme hingewiesen und verfügt über die Tools, um diese zu beheben
- **Skalierbarkeit** – für gewöhnlich lassen sich diese Systeme problemlos auf große Benutzerzahlen im Unternehmen skalieren (nicht für mobile Benutzer)

Diese Systeme wurden jedoch nicht für die Nutzung auf Endgeräten konzipiert. Sie waren vor allem für Umgebungen ausgelegt, in denen die Endanwender auf Desktoprechnern innerhalb des Unternehmensnetzwerks arbeiten. Daher weisen die Systeme auch verschiedene entscheidende Schwachstellen auf:

- **Mangelhaftes Backup auf dem Endgerät** – auf Laptops und Mobilgeräten nutzen die Anwender oft unzuverlässige WAN-Verbindungen mit geringerer Bandbreite und häufigen Unterbrechungen. Reine Backup-Systeme benötigen dagegen erhebliche Bandbreiten und funktionieren daher unter

- solchen Bedingungen nicht gut. Außerdem erhalten mobile Benutzer häufig nicht-statische IP-Adressen, die nicht im Unternehmen veröffentlicht werden. Die oben beschriebenen Systeme können solche IP-Adressen nur schlecht handhaben. Hinzu kommt, dass reine Backup-Systeme den Endanwendern oft keine Erstellung von Backup-Richtlinien ermöglichen. Da viele Benutzer ein Gerät sowohl privat als auch geschäftlich einsetzen, empfiehlt es sich, den Benutzern die Kontrolle über die Backup-Richtlinien für ihr Gerät zu ermöglichen.
- **Unzureichende Unterstützung für Mobilgeräte** – diese Systeme bieten oft keinen Datenzugriff oder -schutz für Smartphones und Tablet-PCs, was angesichts der starken Zunahme dieser Geräte in Unternehmen einen enormen Nachteil darstellt
- **Keine Funktionen für gemeinsamen Dateizugriff und Collaboration** – die reinen Backup-Systeme sind, wie ihr Name schon sagt, nicht mehr als ein Backup. Das bedeutet, dass die IT ein anderes System für gemeinsamen Dateizugriff und Collaboration verwenden und somit eine weitere Struktur aus Berechtigungen, Benutzern, Richtlinien usw. verwalten muss.
- **Kein Schutz vor Datenverlusten** – diese Systeme bieten keinerlei Funktion, um sicherzustellen, dass auf verlorenen oder gestohlenen Geräten kein böswilliger Zugriff auf Daten möglich ist.
- **Umständliches Endanwendererlebnis** – diese Systeme sind ressourcenintensiv und belegen einen hohen Anteil der Prozessor- und Bandbreiten-Ressourcen, was wiederum das Benutzererlebnis beeinträchtigt. Die Benutzer müssen häufig ihre Arbeit unterbrechen, um auf die Fertigstellung des Backups zu warten, weshalb sie schließlich die Backup-Vorgänge zu umgehen versuchen.
- **Teure Bereitstellung und Konfiguration** – diese herkömmlichen Unternehmenssysteme erfordern viel Zeit und Aufwand für ihren unternehmensweiten Rollout und die laufende Wartung. Der Installationsvorgang dauert oft Wochen und muss von spezialisierten Fachkräften vor Ort betreut werden. Für die vertraglich festgelegte Wartung am Standort durch einen professionellen Dienstanbieter fallen normalerweise hohe Kosten an.
- **Eingeschränkte Bereitstellungsoptionen** – diese Lösungen können nur direkt am Standort bereitgestellt werden, was für manche Unternehmen auch durchaus sinnvoll ist. Andere Unternehmen würden dagegen vielleicht eine Bereitstellung über die Cloud bevorzugen, die einen einfacheren Rollout sowie eine bedarfsgesteuerte Skalierung und Preisgestaltung ermöglicht.

NACHTEILE VON REINEN BACKUP-SYSTEMEN:
- Mangelhaftes Backup auf dem Endgerät
- Unzureichende Unterstützung für Mobilgeräte
- Keine Funktionen für gemeinsamen Dateizugriff und Collaboration
- Kein Schutz vor Datenverlusten
- Umständliches Endanwendererlebnis
- Teure Bereitstellung und Konfiguration

Gemeinsamer Dateizugriff und Collaboration auf Consumerniveau

Diese Software-Tools wurden für den Endanwender konzipiert, und zwar ausschließlich für gemeinsamen Dateizugriff und Collaboration. Die Tools bieten eine einfache Bedienung, umfangreiche Funktionen für gemeinsamen Zugriff und Collaboration sowie eine umfassende Unterstützung für iOS- und Android-Mobilgeräte.

In puncto Sicherheit sind diese Lösungen jedoch mangelhaft und verursachen häufig große Probleme für die IT-Abteilungen. Die Tools weisen folgende Schwachstellen auf:

- **Keine Sicherheit der Unternehmensklasse** – diese Tools verursachen große Sicherheitsrisiken für ein Unternehmen. Dropbox, eines der beliebtesten Tools in diesem Segment, verzeichnete vor kurzem eine Sicherheitsverletzung, aufgrund derer die Benutzerdateien mehr als 4 Stunden lang ungeschützt (also ohne Passwort zugänglich) waren. Obwohl einige dieser Tools die Daten verschlüsseln, verwenden sie doch den gleichen kryptografischen Schlüssel für alle Kunden, was ein schwerwiegendes Sicherheitsrisiko darstellt. Darüber hinaus unterstützen diese Tools keinen Single-Sign-on für beliebte Verzeichnisdienste wie Microsoft Active Directory.
- **Keine zentralisierten Richtlinien und Berechtigungen** – diese Tools bieten keinerlei Kontrolle für die IT und lassen die Benutzer nach Belieben agieren. Die IT kann keine spezifischen Berechtigungen für Benutzer bzw. Benutzergruppen festlegen, keine zusätzlichen Sicherheitsvorkehrungen für Schlüsseldateien treffen, keine Passwort-Richtlinien erstellen, keine Zeitlimits für Verknüpfungen zu gemeinsam genutzten Dateien definieren und keine längere Aufbewahrungszeit für sensible Dateien vorsehen.
- **Fehlende IT-Transparenz und Compliance** – die IT muss aus Gründen der Sicherheit sowie der Compliance einen transparenten Einblick in den gemeinsamen Zugriff auf sensible Unternehmensdateien haben. Diese Consumertools bieten keine entsprechende Funktionalität, sodass die IT hier völlig im Dunkeln tappt.
- **Kein Backup auf dem Endgerät und kein durchgehender Schutz** – diese Tools bieten zwar einen gewissen Schutz für die auf dem Endgerät gespeicherten Dateien, sind aber von einem umfassenden System zum Schutz von Endgeräten weit entfernt. Sie überlassen die Verantwortung für den Schutz der Dateien weitgehend dem Endanwender, der nur selten weiß, welche wichtigen Systemdateien per Backup gesichert werden sollten. Außerdem führen diese Tools keine regelmäßigen Backups durch und können keine verschiedenen Backup-Versionen speichern. Somit kann der Benutzer die Dateien nicht auf ein früheres Datum zurücksetzen und wiederherstellen.

- **Keine flexible Bereitstellung** – diese Tools arbeiten rein cloudbasiert. Obwohl eine Cloud-Bereitstellung für viele Unternehmen durchaus sinnvoll sein kann, bevorzugen andere vielleicht am Standort betriebene Lösungen mit Blick auf Kosten, Compliance-Vorgaben oder interne Richtlinien.

NACHTEILE VON SYSTEMEN FÜR GEMEINSAMEN DATEIZUGRIFF UND COLLABORATION AUF CONSUMERNIVEAU:
- Keine Sicherheit der Unternehmensklasse
- Keine zentralisierten Richtlinien und Berechtigungen
- Fehlende IT-Transparenz und Compliance
- Kein Backup auf dem Endgerät und kein durchgehender Geräteschutz
- Keine flexible Bereitstellung

Das Fehlen dieser Funktionen stellt für IT-Abteilungen ein großes Problem dar. So ergaben die Untersuchungen von Druva, dass 65 % der befragten IT-Manager die „Verwaltung von IT-Richtlinien“ als wichtiges Kriterium für eine Dateizugriffslösung betrachten. Das Kriterium „Datensicherheit“ wird sogar von 81 % der IT-Manager bei einer solchen Lösung vorausgesetzt.

Gemeinsamer Dateizugriff und Collaboration in der Cloud auf Unternehmensniveau

Diese Lösungen ähneln insofern den oben genannten Lösungen, als dass auch sie ausschließlich für gemeinsamen Dateizugriff und Collaboration sowie mit Blick auf den Endanwender konzipiert wurden. Daher verfügen diese Tools über umfangreiche Funktionen zur Collaboration sowie einfach zu bedienende Schnittstellen, ähnlich wie die des Consumersegments. Genau wie die oben genannten Lösungen bieten auch diese Tools eine breite Unterstützung für Mobilgeräte. Allerdings bieten sie zusätzlich auch einige Sicherheitsfunktionen für Unternehmen, wie zum Beispiel: starke

Datenverschlüsselung, Unterstützung für Single-Sign-on-Dienste (z. B. MS Active Directory), zentralisierte Verwaltung von Richtlinien und Berechtigungen.

Trotz dieser Unternehmensfunktionen sind diese Tools aber bei Weitem nicht in der Lage, die IT-Anforderungen für die Sicherung von Unternehmensdaten zu erfüllen. Die Tools weisen folgende Schwachstellen auf:

- **Kein Backup auf dem Endgerät und kein durchgehender Schutz** – ähnlich wie die oben geschilderten Lösungen bieten diese Tools zwar einen gewissen Schutz für die auf dem Endgerät gespeicherten Dateien, sind aber von einem umfassenden System zum Schutz von Endgeräten weit entfernt. Die Tools überlassen die Verantwortung für den Schutz der Dateien weitgehend dem Endanwender, der nur selten weiß, welche wichtigen Systemdateien per Backup gesichert werden sollten. Außerdem führen diese Tools keine regelmäßigen Backups durch und können keine verschiedenen Backup-Versionen speichern. Somit kann der Benutzer keine Backup-Wiederherstellung auf ein früheres Datum durchführen.
- **Eingeschränkte Analysefunktionen** – die Tools bieten zwar umfassende Berichte über erfolgte Dateizugriffe, liefern jedoch nicht die für die IT so wichtigen Berichte über erforderliche Investitionen in Speicher und Bandbreite.
- **Keine flexible Bereitstellung** – diese Tools ermöglichen nur selten eine Bereitstellung am Standort. Wie oben bereits erwähnt, kann eine Cloud-Bereitstellung zwar für bestimmte Unternehmen durchaus sinnvoll sein, andere bevorzugen dagegen vielleicht am Standort betriebene Lösungen mit Blick auf Kosten, Compliance-Vorgaben oder interne Richtlinien.

NACHTEILE VON SYSTEMEN FÜR GEMEINSAMEN DATEIZUGRIFF UND COLLABORATION IN DER CLOUD AUF UNTERNEHMENSNIVEAU:

- Kein Backup auf dem Endgerät und kein durchgehender Schutz
- Eingeschränkte Analysefunktionen
- Keine flexible Bereitstellung

Weitere Einschränkungen bestehender Lösungen

Zusätzlich zu den oben genannten Nachteilen fehlt allen drei vorgestellten Kategorien von Software-Tools eine wichtige Fähigkeit, die für die Unternehmenssicherheit entscheidend ist. Sie alle besitzen keine Funktionen für den Schutz vor Datenverlusten (Data Loss Prevention, DLP), die Unternehmensdaten im Falle eines Verlusts oder Diebstahls von Geräten schützen (siehe den oben aufgeführten Fall des britischen Marineoffiziers). Die IT muss in die Lage versetzt werden, Daten auf verlorenen/gestohlenen Geräten per Fernzugriff zu löschen und so viele Informationen wie möglich über den Standort des abhandengekommenen Geräts einzuholen. Unsere Untersuchungen ergaben, dass mehr als 50 % der befragten IT-Manager es für „sehr wichtig“ oder „extrem wichtig“ halten, die Smartphones und Tablet-PCs ihrer Mitarbeiter bei Verlust bzw. Dienstahl per Fernzugriff deaktivieren zu können.

Hinzu kommt, dass die oben beschriebenen Tools keine oder nur eingeschränkte Fähigkeiten zur Deduplizierung besitzen, mit denen die Speicher- und Bandbreitennutzung optimiert werden könnten. Druva hat festgestellt, dass 80 % aller Unternehmensdaten aufseiten der Benutzer dupliziert werden. So ist zum Beispiel die Verkaufspräsentation, die der Vertriebsleiter letzte Woche versandt hat, nun auf fünf verschiedenen PCs gespeichert. Ein System, das diese Duplizierung nicht berücksichtigt, wird das Zehnfache an Bandbreiten- und Speicher-Ressourcen benötigen.

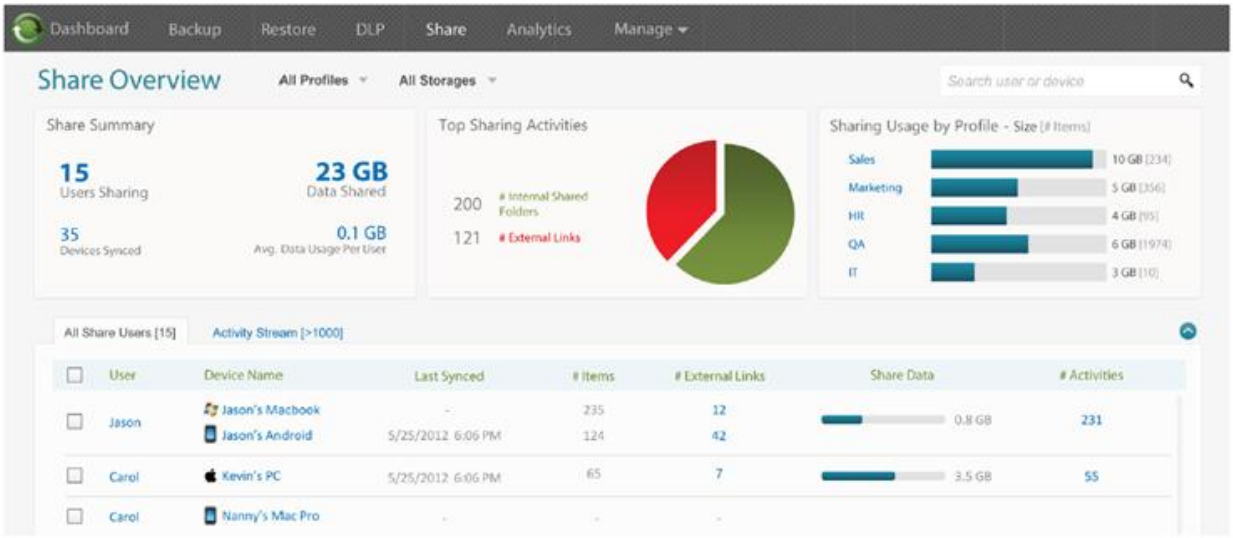
Darüber hinaus fehlt bei allen oben genannten Tools eine scheinbar nebensächliche Sicherheitsfunktion, die jedoch von entscheidender Bedeutung ist. Obwohl die meisten der oben genannten Produkte die Daten der Kundendateien verschlüsseln, stellen sie jedoch keine Verwaltung einmaliger Schlüssel für jeden einzelnen Kunden bereit, sondern verwenden den gleichen kryptografischen Schlüssel für alle Kunden. Die Bereitstellung eines einmaligen kryptografischen Schlüssels (ein als erweiterte Zwei-Faktor-Verschlüsselung bezeichnetes Verfahren) schafft eine zusätzliche Sicherheitsebene.

Druva kombiniert Sicherheit und Collaboration auf Endgeräten

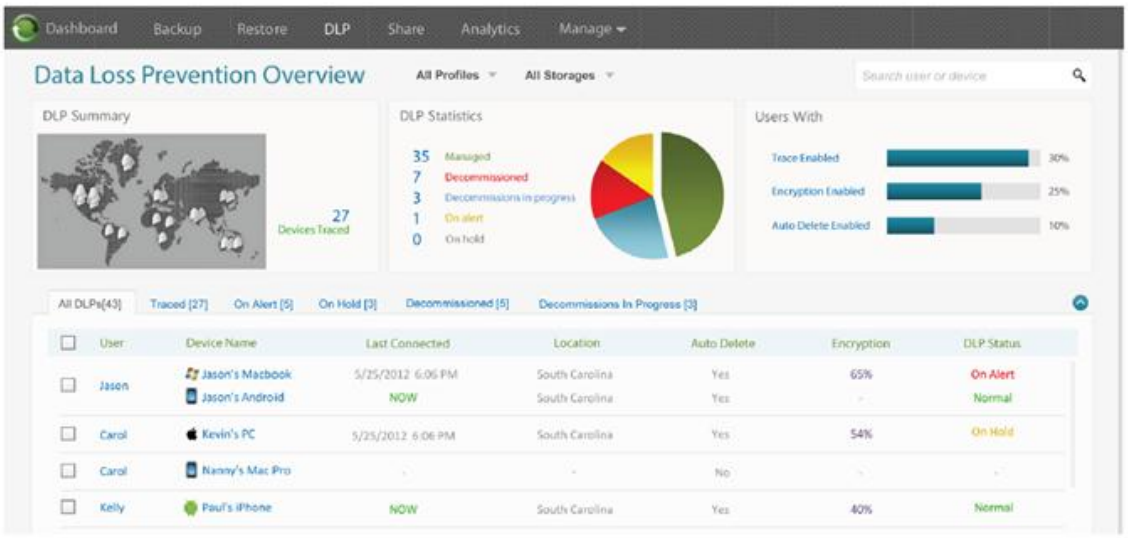
Druva inSync ist die einzige Unternehmenslösung, die eine umfassende Suite für die Sicherheit auf Endgeräten bietet, mit einer preisgekrönten Backup-Funktion, gemeinsamem Dateizugriff und Collaboration sowie Schutz vor Datenverlusten über alle Endgeräte hinweg, einschließlich Laptops, Smartphones und Tablet-PCs. inSync ist sowohl für die IT als auch für Endanwender konzipiert. Die IT-Abteilung kann damit sichergehen, dass Unternehmensdaten auf Endgeräten geschützt, gesichert und konform sind. Endanwender können jederzeit von einem beliebigen Gerät aus auf ihre Daten zugreifen und Dateien gemeinsam mit Kollegen nutzen – all das über ein Tool, das so einfach zu bedienen ist wie ein Consumerprodukt. Kein Wunder also, dass inSync als „unternehmensfähig und anwenderfreundlich“ bewertet wurde. Im Folgenden beschreiben wir die wichtigsten Stärken von inSync sowie seine einzigartigen Merkmale.

- **Backup auf dem Endgerät und durchgehender Schutz** – mit der preisgekrönten Backup-Lösung von inSync erhält die IT die volle Kontrolle und es ist gewährleistet, dass alle wichtigen Dateien entweder in der Cloud oder am Standort per Backup gesichert werden. Die erweiterten Alarmfunktionen und Berichtstools von inSync bieten der IT einen transparenten Einblick in den Backup-Prozess sowie einen dazugehörigen Audit-Pfad. Da inSync von Grund auf für Endgeräte konzipiert wurde, kommt die Lösung gut mit unzuverlässigen WAN-Verbindungen und begrenzten Bandbreiten zurecht.

- **Gemeinsamer Dateizugriff und Collaboration** – inSync bieten Endanwendern umfangreiche Funktionen zur Collaboration. Mit inSync können die Benutzer einen Ordner auf ihrem Desktop für den gemeinsamen Zugriff nutzen, dessen Inhalt automatisch auf den PCs von Kollegen sowie über die inSync-Webschnittstelle verfügbar gemacht wird. Die Benutzer können ihre Dateien zudem über verschiedene Endgeräte hinweg synchronisieren (z. B. Laptop, Smartphone, Tablet-PC). Sie können außerdem mit einem einzigen Klick eine URL-Verknüpfung zu einer Datei erstellen und diese über eine URL mit anderen Benutzern teilen, die inSync nicht installiert haben.



- **Schutz vor Datenverlusten auf dem Endgerät (Data Loss Prevention, DLP)** – inSync minimiert das Risiko, dass Ihre Unternehmensdaten in falsche Hände geraten. Mit inSync werden die Daten auf dem Endgerät verschlüsselt, sodass außer ihrem Inhaber oder dem IT-Administrator niemand auf sie zugreifen kann. inSync ermöglicht außerdem das Löschen von Gerätedaten per Fernzugriff. Auch hier ermöglicht inSync der IT eine umfassende Kontrolle, da diese Richtlinien dafür erstellen kann, welche Dateien auf dem Gerät verschlüsselt werden und wann Dateien per Fernzugriff gelöscht werden (z. B. wenn das Gerät X Tage lang nicht am Netz war). Natürlich kann die IT Geräte auch manuell deaktivieren, wenn sie befürchtet, dass eine Verletzung der Sicherheit vorliegt. Darüber hinaus verwendet inSync einen modernen Algorithmus zur Positionsbestimmung basierend auf WLAN-Zugriffsdaten sowie Informationen von GPS-Satelliten und Mobilfunkmasten, um so den Standort von Endgeräten bis auf 10 bis 20 Meter genau zu bestimmen.



- **Mobilzugang und Datenschutz** – wie oben ausgeführt, stellen Mobilgeräte eine große Herausforderung für die IT dar, da die Mitarbeiter immer mehr private Geräte in das Unternehmen einbringen, die nicht von der IT ausgegeben wurden (Stichwort „Bring Your Own Device/BYOD“). Die inSync-Technologie für Backup, Schutz vor Datenverlusten und Collaboration funktioniert auch auf Mobilgeräten in vollem Umfang und gewährleistet so, dass auf diesen Geräten befindliche Unternehmensdaten per Backup gesichert und geschützt werden. inSync gibt zudem den Endanwendern die Möglichkeit, von jedem beliebigen iOS- oder Android-Mobilgerät auf alle ihre gemeinsam genutzten und per Backup gesicherten Dateien zuzugreifen.
    - **Umfassende Datenanalysen** – der Ausspruch „Wissen ist Macht“ trifft auf das IT-Management in besonderem Maße zu. inSync liefert aussagekräftige Berichte, sodass die IT jederzeit im Detail über die auf den Endgeräten gespeicherten Daten auf dem Laufenden ist. Die IT kann die so gewonnenen Erkenntnisse zur Planung zukünftiger Speicher- und Bandbreitenanforderungen nutzen. inSync bietet außerdem eine Funktion für die vereinigte Suche in Echtzeit, mit der die IT jederzeit vertrauliche Dateien unternehmensweit auf jeglichen Endgeräten finden und verfolgen kann.
    - **Unternehmenssicherheit** – inSync wurde von Grund auf unter Berücksichtigung höchster Sicherheitsstandards entwickelt. inSync wendet die folgenden Sicherheitstechnologien und -verfahren an:
        - » **Datenverschlüsselung** – inSync verfügt über eine 256-Bit-SSL-Verschlüsselung für übertragene sowie eine 256-bit-AES-Verschlüsselung für gespeicherte Daten.
        - » **Zertifizierungen** – inSync läuft auf der Amazon-Cloud-Infrastruktur, die SAS-70-zertifiziert ist. Die Druva-Cloud-Strukturen und -Prozesse sind ebenfalls ISAE-3000-zertifiziert.
        - » **Verwaltung kryptografischer Schlüssel** – manche Cloud-Anbieter verwenden den gleichen kryptografischen Schlüssel für alle ihre Benutzer und teilen die Daten nicht für ihre einzelnen Kunden auf. inSync ist die branchenweit erste Anwendung mit einer erweiterten Zwei-Faktor-Verschlüsselung. inSync bietet die Verwaltung einmaliger Schlüssel für jeden Kunden, ebenso wie eine einmalige Authentifizierung

und Zugriffskontrolle für jeden Kunden. Dies stellt sicher, dass niemand außer dem Kunden, der über die Zugangsdaten verfügt, auf die verschlüsselten Daten eines Kunden zugreifen kann, auch nicht die Mitarbeiter von Druva.

» **Single-Sign-on** – für die Bereitstellung von Single-Sign-on-Funktionen verwendet inSync die Security Assertion Markup Language (SAML), einen XML-basierten offenen Standard. Benutzer können über das Internet eine sichere Anmeldung bei inSync tätigen, indem sie ihre Zugangsdaten bei externen Identitätsdiensten wie Microsoft Active Directory verwenden.

- **Einsparungen bei Speicher und Bandbreite** – die meisten Unternehmen verzeichnen ein exponentielles Wachstum bei ihren Unternehmensdaten, was die Kosten für Bandbreite und Speicher enorm in die Höhe treiben kann. Die gute Nachricht ist jedoch, dass geschätzte 80 % der Daten in einem Unternehmen dupliziert sind. inSync setzt eine fortschrittliche Deduplizierungstechnologie ein, um die Speicherung und Übertragung von Dateien auf ein Minimum zu reduzieren und so diese Kosten erheblich zu senken. Mit unseren Deduplizierungsfunktionen lassen sich viel höhere Einsparungen erzielen als mit anderen Branchenlösungen, da wir eine globale, clientseitige und anwendungssensible Deduplizierung einsetzen.

  Globale Deduplizierung bedeutet hierbei, dass inSync nur einen einzelnen Datenblock über alle Dateien auf einem Gerät hinweg sowie nur einen einzelnen Datenblock über alle Geräte hinweg speichert. Clientseitige Deduplizierung bedeutet, dass die Daten dedupliziert werden, bevor sie das Endgerät verlassen, wodurch Bandbreite eingespart wird.

Außerdem ist die Technologie von inSync anwendungssensibel, d.h. sie erkennt das On-Disk-Format gängiger Anwendungen (z. B. MS Office) und kann so eine effizientere, exaktere und schnellere Deduplizierung bieten. Stellen Sie sich zum Beispiel vor, ein Benutzer speichert ein JPG-Bild, fügt dieses auch in ein MS Word-Dokument ein und verschickt dieses wiederum als Anhang zu einer E-Mail. Andere Backup-Tools arbeiten mit einer „blockbasierten“ Deduplizierung und speichern somit drei Kopien des Bildes. inSync mit seiner anwendungssensiblen Technologie speichert dagegen nur eine einzige Kopie des Bildes. Druva-Tests haben gezeigt, dass eine anwendungssensible Deduplizierung eine um bis zu 300 % effizientere Deduplizierung ermöglichen kann.

- **Einfache Bereitstellung und Verwaltung** – mit dem Aufkommen von Mobilgeräten ist der Arbeitsaufwand für IT-Manager erheblich gestiegen. Wir bei Druva wollen diesen Arbeitsaufwand verringern und haben daher für eine einfache Bereitstellung und Verwaltung von inSync gesorgt. inSync bietet vorkonfigurierte Benutzerprofile, mit denen sich nahezu alle in einem Unternehmen vorhandenen Benutzertypen abdecken lassen. Diese Benutzerprofile sind so eingerichtet, dass weit verbreitete Datenquellen wie E-Mail und Dokumentenordner per Backup gesichert werden. IT-Administratoren können die Profile unverändert verwenden oder sie als Ausgangsbasis nutzen, um innerhalb weniger Minuten neue Profile zu erstellen.

Die Bereitstellung einer Client-Anwendung auf Hunderten oder gar Tausenden von Endanwendergeräten kann einen enormen Aufwand darstellen. Aus diesem Grund ermöglicht inSync die Massenbereitstellung der Client-Anwendung über bestehende Unternehmenstools wie Microsoft Active Directory, Microsoft SCCM und Casper (JAMF-Software).
Darüber hinaus ermöglicht inSync der IT eine automatische Aktualisierung aller Client-Geräte mit der jeweils neuesten Version der inSync-Client-Anwendung. Dies reduziert den Aufwand für die IT sowie für die Endanwender erheblich.

- **Bereitstellungsoptionen** – die Entscheidung, ob Daten in der Cloud oder vor Ort gespeichert werden sollen, ist nicht einfach. Oft legen IT-Manager dieser Entscheidung die folgenden Faktoren zugrunde: Budgets, Zeit, IT-Personalausstattung, interne Unternehmensrichtlinien, externe Compliance-Vorgaben oder Investitionen in die IT-Infrastruktur. Wir bei Druva wollen diese Entscheidung erleichtern und haben inSync daher so konzipiert, dass sowohl Installationen in der Cloud als auch am Standort unterstützt werden. Zusätzlich bieten wir auch hybride Bereitstellungsmodelle an, sodass IT-Manager noch flexibler vorgehen können. Mit einer hybriden Bereitstellung erhalten IT-Manager sowohl die Vorteile der Bereitstellung am Standort als auch die der Bereitstellung in der Cloud. Beispielsweise könnte eine Installation am Standort die Cloud für Disaster-Recovery-Funktionen nutzen, und eine Cloud-Installation könnte eine Replizierung auf einen Standortserver durchführen, um eine höhere Geschwindigkeit zu erreichen usw.
- **Skalierbarkeit der Unternehmensklasse** – in den meisten Unternehmen wächst der Personalbestand schneller, als die für dessen Unterstützung erforderliche IT-Mitarbeiter eingestellt werden können. Daher benötigen diese Unternehmen Software-Lösungen, die wachsende Endanwenderzahlen mit minimalen IT-Personalressourcen handhaben können. inSync leistet genau das. Die kombinierte Administratorkonsole von inSync ermöglicht die einfache Verwaltung von Benutzern, Richtlinien und Daten über zahlreiche inSync-Server hinweg.
  inSync nutzt die AWS-Infrastruktur von Amazon zur Bereitstellung einer wirklich bedarfsgesteuerten Speichererweiterung. Unternehmen können den Cloud-Speicher nutzen und die Anzahl der Benutzer erhöhen, ohne jemals an Grenzen zu stoßen. Bei der Bereitstellung am Standort sind ebenfalls sehr hohe Volumen möglich. So kann inSync bis zu 10.000 Benutzer auf einem einzelnen Server handhaben.
  Außerdem verwendet inSync die HyperCache-Technologie, um eine Erhöhung der Benutzerzahl zu ermöglichen. HyperCache ist ein serverseitiger, selektiver und speicherinterner Cache, der den Disk I/O um bis zu 90 % reduziert und so eine Skalierung der einzigartigen Deduplizierungstechnologie von Druva bei gleichzeitiger Einsparung von Speicher und Bandbreite ermöglicht.
- **Endanwendererlebnis** – wie bereits ausgeführt erwarten Mitarbeiter heutzutage, dass Business-Produkte die gleichen einfach bedienbaren und intuitiven Schnittstellen besitzen wie Consumerprodukte. Die Entwickler von Druva sind sich dieses Umstands bewusst und haben inSync speziell für die Endanwender konzipiert. inSync bietet einfach zu bedienende Schnittstellen und läuft im Hintergrund, ohne die Aufgaben des Benutzers zu beeinträchtigen.
  Mit inSync müssen Ihre Mitarbeiter ihre Arbeit nicht mehr unterbrechen, um auf die Fertigstellung eines Backups zu warten.

- **Komplettlösung** – IT-Manager haben heute mehr zu tun als je zuvor und können sich nicht mit der Einrichtung der gleichen Benutzerprofile und Richtlinien über verschiedene Unternehmensprodukte hinweg beschäftigen. Aus diesem Grund hat Druva eine kombinierte Lösung entwickelt, die Backups auf dem Endgerät, Schutz vor Datenverlusten und Collaboration in einem bietet. Mit Druva inSync müssen IT-Manager nur einen Satz an Benutzern, Richtlinien und Berechtigungen einrichten.

Lösungsarten – Gegenüberstellung

Die folgende Tabelle liefert einen grundsätzlichen Vergleich zwischen den drei oben beschriebenen Lösungsarten und Druva inSync.

	REINES BACKUP	COLLABORATION AUF CONSUMER-NIVEAU	COLLABORATION AUF UNTERNEHMENS-NIVEAU	DRUVA INSYNC
BACKUP AUF DEM ENDGERÄT	Eingeschränkte Fähigkeiten			Preisgekröntes Backup
DATEIZUGRIFF UND COLLABORATION				
SCHUTZ VOR DATENVERLUSTEN (DLP) AUF DEM ENDGERÄT				
UMFASSENDE DATENANALYSEN				
BENUTZERMOBILITÄT				
ENDANWENDER-ERLEBNIS				
SKALIERBARKEIT				
UNTERNEHMENS-SICHERHEIT				2-Faktor-Verschlüsselung
EINFACHE BEREITSTELLUNG UND KONFIGURATION				
BEREITSTELLUNGS-OPTIONEN	Nur am Standort	Nur in der Cloud	Nur in der Cloud	Cloud, Standort, hybrid
SPEICHER- UND BANDBREITEN-EINSPARUNGEN				

Fazit

Die Zunahme der Endgeräte in Unternehmen sowie der wachsenden Collaboration-Bedarf stellen die IT heute vor neue Herausforderungen. Es wird für die IT immer schwieriger zu gewährleisten, dass auf Endgeräten gespeicherte Unternehmensdaten sicher sind und den Mitarbeitern zugleich einfach bedienbare und sichere Tools zur Collaboration zur Verfügung stehen. Die derzeit auf dem Markt erhältlichen Software-Produkte bieten nur teilweise eine Antwort auf diese Herausforderung, sodass die IT-Abteilung entweder eine unzureichende Lösung einsetzen oder eine komplexe Mischung aus verschiedenen Produkten zusammenstellen muss.

Druva inSync ist das einzige Produkt, das eine kombinierte Plattform für den Schutz von Endgeräten sowie für die Collaboration über alle Endgeräte hinweg bietet. inSync vereint drei zentrale Funktionen in einer Plattform: Backup auf Endgeräten, Verhinderung von Datenverlusten sowie gemeinsamer Dateizugriff und Collaboration.

inSync erfüllt sowohl den Bedarf der IT nach einer Sicherung der Daten auf Endgeräten als auch den Bedarf der Endanwender nach einer einfachen Collaboration. Darüber hinaus bietet Druva hocheffiziente Funktionen für Datendeduplizierung und WAN-Optimierung, die die Übertragung von Daten auf Endgeräten beschleunigen und die Kosten für Speicher und Bandbreite minimieren. Anders als herkömmliche IT-Produkte für Unternehmen ist inSync einfach zu installieren und zu verwalten und kann problemlos auf das Wachstum des Unternehmens skaliert werden. Daher überrascht es nicht, dass Druva bereits zahlreiche Preise errungen hat, darunter auch die von Gartner vergebene Auszeichnung als „Cool Vendor“ sowie den renommierten CODiE Award.

Datenquellen und Referenzen

1. IDC-Studie „Worldwide Mobile Worker Population 2011-2015 Forecast“, Dezember 2011, http://www.idc.com/getdoc.jsp?containerId=232073
2. Gartner-Studie Nr. 160375 „Options for PC Data Backup“
3. Ponemon-Institute-Studie, zitiert im PC-World-Artikel „Laptops lost like hot cakes at airports“, http://www.pcworld.com/businesscenter/article/147739/laptops_lost_like_hot_cakes_at_us_airports.html
4. PC-World-Artikel „British Navy loses laptop containing personnel data“, http://www.pcworld.com/article/141565/british_navy_loses_laptop_containing_personnel_data.html
5. Harris-Interactive-Umfrage unter IT-Entscheidungsträgern, zitiert im CIO-Magazine-Artikel „IT Must provide Enterprise Collaboration Tools Employees Will Use“, http://www.cio.com/article/702971/IT_Must_Provide_Enterprise_Collaboration_Tools_Employees_Will_Use
6. Intel-Bericht „The Billion Dollar Lost-Laptop Study“, http://newsroom.intel.com/docs/DOC-1544 Druva, Inc.

Sind Sie bereit ?

Der erste Schritt bei der Erstellung eines Notfallplans, Kombination von Datenschutz und Collaboration, besteht darin, sich die Zeit zu nehmen und sich die Vorkehrungen für Ihre Unternehmens-Complicance genau anzusehen und zu definieren.

Fortschrittliche Unternehmen suchen dann zunehmend die Zusammenarbeit mit strategischen Partnern, um Ihre Unternehmens-Complinance durch bessere Massnahmen, die durch mehr Mobilität und Collaboration Ihrer Mitarbeiter entstehen, zu optimieren.

Unsere spezialisierten Partner arbeiten eng mit Ihnen zusammen und berücksichtigen die vorhandenen Backup-Systeme und Prozesse ihres Unternehmens. Dadurch wird ein nahtloser Übergang sichergestellt und Ihr Unternehmen für den Ernstfall gerüstet.

Erfahren Sie mehr darüber, wie Druva Ihr Unternehmen für den Ernstfall rüsten kann. Kontaktieren Sie uns noch heute per E-Mail unter beate.lange@druva.com und unter der Rufnummer +49 (0) 160 5518 752.

Über Druva

Druva inSync ist die einzige Unternehmenslösung, die eine umfassende Suite für die Sicherheit auf Endgeräten bietet, mit einer preisgekrönten Backup-Funktion, gemeinsamem Dateizugriff und Collaboration sowie Schutz vor Datenverlusten über alle Endgeräte hinweg, einschließlich Laptops, PCs, Smartphones und Tablet-PCs. inSync ist die einzige Lösung, die sowohl für die IT als auch im Hinblick auf das Endanwendererlebnis konzipiert wurde. Die IT-Abteilung kann damit sichergehen, dass Unternehmensdaten auf Endgeräten geschützt, gesichert und konform sind. Endanwender können jederzeit von jedem beliebigen Gerät aus auf ihre Daten zugreifen und Dateien gemeinsam mit Kollegen nutzen. Druva hat mehr als 1.250 Kunden und schützt über 900.000 Endgeräte in 42 Ländern. Druva ist ein privat geführtes Unternehmen, finanziert von Nexus Venture Partners und Sequoia Capital. Es unterhält Niederlassungen in den USA sowie in Indien, Großbritannien und Deutschland. Weitere Informationen zu Druva finden Sie auf: www.Druva.com

Nord- und Südamerika: +1 888-248-4976
EMEA: +44.(0)20.3150.1722
Germany: +49 (0) 160 5518 752
Asien-Pazifik und Japan: +919886120215
sales@druva.com
www.druva.com