box

So schützen Sie Ihr Unternehmen mit der Content Cloud

Inhalts-verzeichnis

03 Unternehmen von heute brauchen reibungslose Sicherheit

06 Die vier Grundprinzipien der Sicherheit von Box

08 Box-Sicherheit auf einen Blick

09 Verhindern Sie Datenschutzverletzungen mit Box Shield

11 Sicherung der Zusammenarbeit

13 Information Governance, Compliance und Datenschutz

14 Infrastruktursicherheit und Threat Management

15 Zertifizierungen für Industrien und Behörden

18 Schützen Sie Ihre wertvollen Daten mit der Content Cloud

Unternehmen von heute brauchen reibungslose Sicherheit

Wir alle wissen, dass Sicherheit in der heutigen Welt unverzichtbar ist. Unsere Arbeit ist viel komplexer geworden. Unternehmen stehen vor noch nie dagewesenen Herausforderungen, um ihre Inhalte zu schützen und Compliance zu gewährleisten. Im Zuge der technologischen Entwicklung haben sich IT-Services von einem zentralen hin zu einem höchst dezentralen Computernutzungsmodell entwickelt. Mobilität, Cloud-Services, Verbraucher-Apps und die weit verbreitete Akzeptanz von elektronischen Unterschriften haben den Bedarf der Mitarbeitenden erhöht, jederzeit, überall und von jedem Gerät aus arbeiten zu können.

Dabei muss die IT-Abteilung nicht nur für Teams vor Ort, sondern auch für externe Mitarbeitende, Lieferanten, Partner und Kunden ein nahtloses und sicheres Erlebnis schaffen. Während steigende Mobilität und Zusammenarbeit einen enormen Mehrwert für Unternehmen geschaffen haben, stellen sie IT- und C-Suite-Führungskräfte allerdings auch vor die Herausforderung, Inhalte in einem dezentralen Ökosystem zu schützen.

Angesichts der erheblichen Auswirkungen, die Datenschutzverletzungen auf die Finanzen und den Ruf Ihres Unternehmens haben können, ist die Aufrechterhaltung der Datensicherheit unerlässlich. Ohne strenge IT-Kontrollen ist das Risiko von menschlichen Fehlern, die zu Datenverlust führen, unglaublich hoch. Drei von vier Mitarbeitenden finden es in Ordnung, vertrauliche Arbeitsdokumente auf private Geräte zu übertragen. Wenn Dateien zwischen privaten Geräten, Verbraucheranwendungen und freigegebenen Laufwerken hin- und herbewegt werden, erhöht dies das Risiko von Datenverlusten. Außerdem ist die Sicherheit für mobile Teams nicht hoch genug, wenn Mitarbeitende außerhalb einer verwalteten Cloud-Architektur arbeiten: 87 % der Mitarbeitenden informieren niemanden, wenn ein USB-Stick nicht mehr auffindbar ist und 52 % benachrichtigen die Sicherheitsteams nicht schnell genug, wenn ein Computer (und damit die darauf enthaltenen Dateien) verloren geht.

Ein Verstoß kann sich massiv auf das Geschäftsergebnis Ihres Unternehmens auswirken. Schließlich belaufen sich die durchschnittlichen globalen Kosten pro Datenschutzverletzung auf 4,35 Millionen US-Dollar.[1]

Da heutzutage viele Unternehmen Millionen (oder sogar Dutzende Millionen) vertraulicher Datensätze speichern, ist das finanzielle Risiko einer Datenschutzverletzung höher denn je. Betrachtet man Ihre Beziehungen mit Ihren Kunden, dann ist die Beschädigung Ihres Markenimages nach einer Verletzung noch lange spürbar und nicht einfach wiederherzustellen.

[1] *IBM, Cost of a Data Breach report, 2022*

Fragmentierte Content-Strategien, Schatten-IT und ein zu umfassender Einsatz von E-Mails können zu gefährlichen Sicherheitslücken führen. Unternehmen, die 2022 im Verizon Data Breach Investigations Report untersucht wurden, gaben beispielsweise an, dass über 75 % der Malware-Vorfälle mit E-Mails begonnen haben. Und da die Bedrohungen zunehmen, wird es für Sicherheitsfachleute noch schwieriger, die große Anzahl von Sicherheitswarnungen zu verarbeiten, die bei ihnen eingehen.

Compliance im Unternehmen ist essentiell

Die Entwicklung weltweiter Gesetze und Verordnungen erhöht die Risiken nur noch mehr: IT-Führungskräfte müssen eine aktive Rolle bei der Verwaltung von Inhalten und dem Festlegen von Sicherheitsstrategien einnehmen.

Wodurch wird ein Verstoß verursacht?

83 % externe Angriffe

45 % gestohlene Anmeldeinformationen

IBM[2]

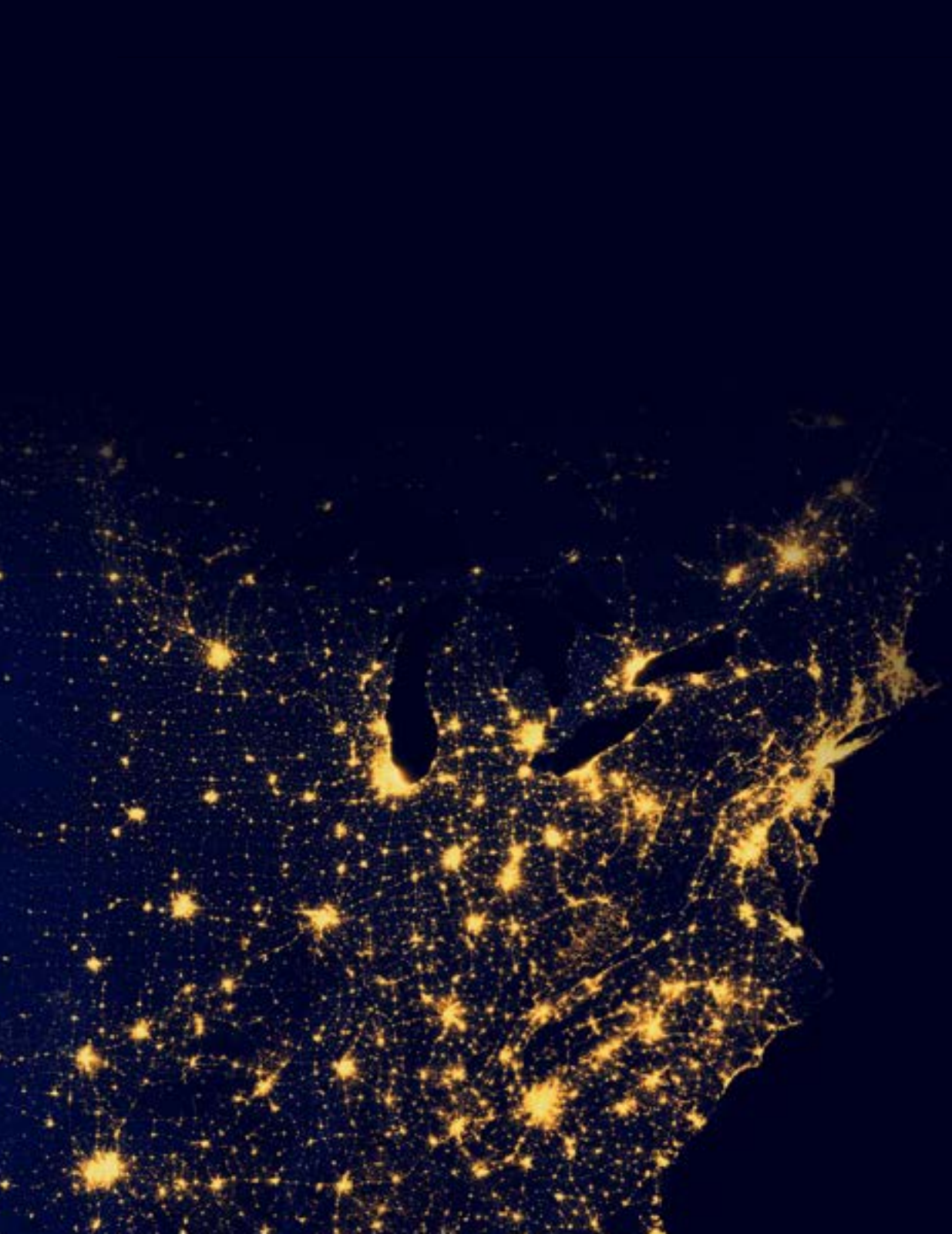
Compliance Management erfordert die Einhaltung komplexer branchen-, geschäftsbereichs- und regionsspezifischer Standards. Die Datenschutz-Grundverordnung (DSGVO) der Europäischen Union trat 2018 in Kraft und verschärft die Vorschriften für alle Unternehmen, die mit den Daten europäischer Bürger:Innen und Einwohner:Innen arbeiten – unabhängig davon, ob das Unternehmen seinen Sitz in der EU hat oder nicht. Eine ähnliche Verordnung trat 2020 in Kalifornien mit dem California Consumer Privacy Act (CCPA) in Kraft, gefolgt von der Einführung des California Privacy Rights Act (CPRA) im Jahr 2023. Dies ist nur die Spitze des Eisbergs; in anderen US-Bundesstaaten und Ländern werden zahlreiche unabhängige Datenschutzbestimmungen eingeführt.

Da Unternehmen Kund:Innen auf der ganzen Welt haben und mit globalen Partnern zusammenarbeiten, müssen sie bereit sein, die regionalen Anforderungen an Data Governance und Datenaufbewahrung zu erfüllen – oder es drohen erhebliche Strafen. DSGVO-Verstöße können Unternehmen beispielsweise bis zu 20 Mio. € oder 4 % ihres gesamten weltweiten Jahresumsatzes kosten, je nachdem, welcher Betrag höher ist.[3]

Bei Box ist die Sicherheit Teil unserer Philosophie. Und sie ist ein integraler Bestandteil der Content Cloud – einer zentralen, sicheren Plattform für den gesamten Lebenszyklus von Inhalten, von der Dateierstellung über die Freigabe und die elektronische Unterschriften bis hin zur Aufbewahrung. Durch die Integration von Sicherheit und Compliance in Ihre Content-Strategie erhalten Sie einen sicheren Ort, an dem Sie alle Ihre Inhalte verwalten und so Sicherheitslücken vermeiden und schnell und präzise auf Bedrohungen reagieren können. Es bietet eine wesentlich einfachere und weitaus sicherere Art der Zusammenarbeit.

Im weiteren Verlauf dieses E-Books erfahren Sie, wie die Content Cloud reibungslose Sicherheit und Compliance bietet und Ihnen hilft, Risiken zu reduzieren, ohne die Produktivität zu beeinträchtigen oder das Unternehmen zu verlangsamen.

[2]IBM, Cost of a Data Breach report, 2022
[3]Amtsblatt der Europäischen Union, Verordnung (EU) 2016/679, 2016



S&P Global

„Sicherheit ist entscheidend für jedes Unternehmen. Wir haben die Möglichkeit, souveräne Staaten zurückzustufen, deshalb ist Sicherheit für uns ein absolutes Muss. Wir müssen die richtigen Kontrollmechanismen wirklich sorgfältig einsetzen und sicherstellen, dass die Informationen nicht dort zugänglich sind, wo sie es nicht sein sollten.“

Seth Fox, Global Head of Workplace Services, S&P Global

Die vier Grund-prinzipien der Sicherheit von Box

Jedes Unternehmen muss sich auf die neue Art des Arbeitens ausrichten: Es bedarf schnellerer Prozesse über stärker dezentralisierte Teams hinweg, unterstützt durch moderne Cloud-Lösungen. Und das bedeutet, dass Unternehmen wie Ihres überdenken müssen, wie sie Daten schützen, kontrollieren und verwalten können. Risikominimierung bedeutet, Wege zu finden, um die Datenflüsse zu steuern, die heute schneller und umfangreicher als je zuvor fließen. Aber bei dem Versuch, Unternehmensdaten zu schützen, Datenschutz durchzusetzen und Compliance zu gewährleisten, brauchen Sie auch Lösungen, die Innovationen ermöglichen. Die Herausforderung besteht darin, ein Gleichgewicht zwischen Innovation und Sicherheit zu schaffen und den Datenfluss transparent und analysierbar zu machen, anstatt auf Datenkontrolle zu setzen.

1 Zero-Trust-Infrastruktur

Herkömmliche Sicherheitsmodelle gehen davon aus, dass alle Benutzer:Innen im Netzwerk vertrauenswürdig sind. Dies schützt jedoch nicht vor Bedrohungen durch Insider. Bei Box arbeiten wir auf der Grundlage eines Zero-Trust-Modells und gehen davon aus, dass ein:e Anwender:In oder ein Netzwerk niemals sicher ist. Das bedeutet, dass wir beispielsweise einen Laptop oder ein Smartphone nicht nur auf der Geräteebene schützen. Unser Schutz greift auch auf der detaillierteren, „granulareren“ Datenebene. Auf diese Weise werden die Daten nicht gefährdet, wenn das Gerät kompromittiert wird. Außerdem ergreifen wir die erforderlichen Maßnahmen zum Schutz aller Inhalte mit Sicherheitsbots, erweiterten Authentifizierungsverfahren wie Einmalkennwörtern und Out-of-Band-Genehmigung für sensible Aufgaben.

2 Ein reibungsloses Benutzererlebnis

Die Sicherheit sollte die Anwendererfahrung nicht beeinträchtigen. Bei IT-gestützten Lösungen mit schlechter Anwendererfahrung ist es wahrscheinlich, dass die Anwender:Innen auf Verbrauchertools mit Sicherheitsmängeln zurückgreifen. Bei Box ist es uns sehr wichtig, eine nahtlose und angenehme Nutzererfahrung zu schaffen. Deshalb laufen Sicherheitsfunktionen im Hintergrund, wo Anwender:Innen sie gar nicht bemerken. Das bedeutet, dass Sie in der Lage sind, Maßnahmen direkt dort zu ergreifen, wo Ihre Inhalte gespeichert sind. Sie müssen sich nicht bei einem separaten Tool anmelden, nur um Geschäftsprozesse mit einer elektronischen Unterschrift abzuschließen. Oder es bedeutet, dass man einfache Möglichkeiten zum Senden von Dateien über gemeinsame Links schafft, wobei Sie zwischen Link-Typen wie „Personen mit diesem Link“, „Personen in Ihrem Unternehmen“ oder „Nur eingeladene Personen“ wählen können. Für die IT bedeutet dies, dass die richtigen Leitplanken vorhanden sind und die Mitarbeitenden gleichzeitig in der Lage sind, ihre Arbeit effizient zu erledigen.

3 Ein zentrales Content-Repository in der Cloud

Die Zusammenführung Ihrer Inhalte in der Cloud erleichtert die Sicherung, Verwaltung und Steuerung Ihrer Dateien. Viele IT-Unternehmen sind auf ein dezentralisiertes System angewiesen, was zu fragmentierten Inhalten und einer größeren Angriffsfläche führt. Aber selbst wenn Sie auf einem modernen Cloud Stack arbeiten, könnten Sie am Ende ein massives Fragmentierungsproblem haben, wenn Sie die Cloud nicht als zentrale Ebene für Ihre Inhalte nutzen. Box ermöglicht Ihnen die zentrale Speicherung Ihrer Inhalte in der Cloud und verbessert dadurch die Sicherheit und vereinfacht die Verwaltung.

4 Sicherheit, die Ihre Dateien begleitet

Sicherheit als nachträglich aufgesetzte Lösung funktioniert nur selten – was Sie benötigen, sind Kontrollmechanismen, die in den Content-Lebenszyklus integriert sind. Auf diese Weise sind nicht nur Ihre Daten geschützt, denn das gleiche Maß an Sicherheit bleibt auch dann für Ihre Inhalte erhalten, wenn Sie in anderen Anwendungen arbeiten und Box als Ihre Content-Ebene nutzen. Wenn Sie also in Slack arbeiten oder eine elektronische Unterschrift mit Box Sign für einen Kundenvertrag in Salesforce anfordern (oder eine unserer anderen mehr als 1.500 Integrationen verwenden), erhalten Sie gleichzeitig Sicherheit auf Box-Ebene.

“Wir alle befinden uns auf dem Weg zu reibungsloser Sicherheit und Compliance. Im Vorteil sind diejenigen, die ihre Inhalte konsolidieren, sie mit integrierten Kontrollmechanismen sichern und die Risiken für ihre wertvollen Informationen mit einem Blick erfassen können.“

Julien Soriano, Chief Information Security Officer, Box

Box-Sicherheit auf einen Blick

Benutzer:Innen

- Starke Nutzerauthentifizierung über SSO und MFA
- Zweistufige Authentifizierung für externe Mitarbeitende
- Passwortkontrollen legen Anforderungen für interne/externe Anwender:Innen fest
- Erweiterte Anwenderverwaltung für Deaktivierung, Anmeldeaktivität und erzwungene Abmeldung
- Authentifizierung durch Unterzeichnende:n (per E-Mail, SMS oder Zugangscode)

Geräte

- Die Überprüfung der Geräteposition legt die Anforderungen an die Sicherheit und den Besitz des Geräts fest
- Geräte-Pinning beschränkt die Anzahl der Geräte mit Box-Zugriff
- MDM und MAM sichern den Zugriff mit Box für EMM-Integrationen
- Blockieren und Zulassen von Domänen beschränkt die Verwendung von Box auf genehmigte IPs

Anwendungen

- Mehr als 1.500 Integrationen sorgen über sichere APIs für eine zentrale Informationsquelle
- Berechtigungssynchronisierung verwaltet Berechtigungen für Slack, Teams, Salesforce und NetSuite
- Granulare Anwendungsbereiche setzen bewährte Verfahren mit den geringsten Berechtigungen durch
- Klassifizierungsbasierte App-Kontrollen* basierend auf der Vertraulichkeit der Datei

Inhalt

- Granulare Berechtigungen mit 7 Zugriffsebenen
- Der Ablauf des Freigabe-Links legt den automatischen Ablauf für öffentliche und nicht öffentliche Links fest
- Dynamisches Wasserzeichen für mehr als 120 Dateitypen
- Malware-Erkennung
- Speicherung, Löschung und gesetzliche Aufbewahrungsfristen*
- Klassifizierungsbasierte Zugriffskontrollen*

Sichtbarkeit

- Berichterstellung und zentralisierte Auditprotokolle für 7 Jahre
- Eine Ansicht aller intern und extern freigegebenen Inhalte, einschließlich der zur elektronischen Unterschrift gesendeten Inhalte
- ML-basierte Erkennung von Sicherheitsmängeln*
- CASB- und SIEM-Partner bieten eine einheitliche Ansicht über Apps und Netzwerke hinweg

Infrastruktur

- Regionale Speicherung* erfüllt die Anforderungen an die Speicherung von Daten
- Verschlüsselungscodeverwaltung* ermöglicht Ihnen die Verwaltung Ihrer eigenen Verschlüsselungscodes

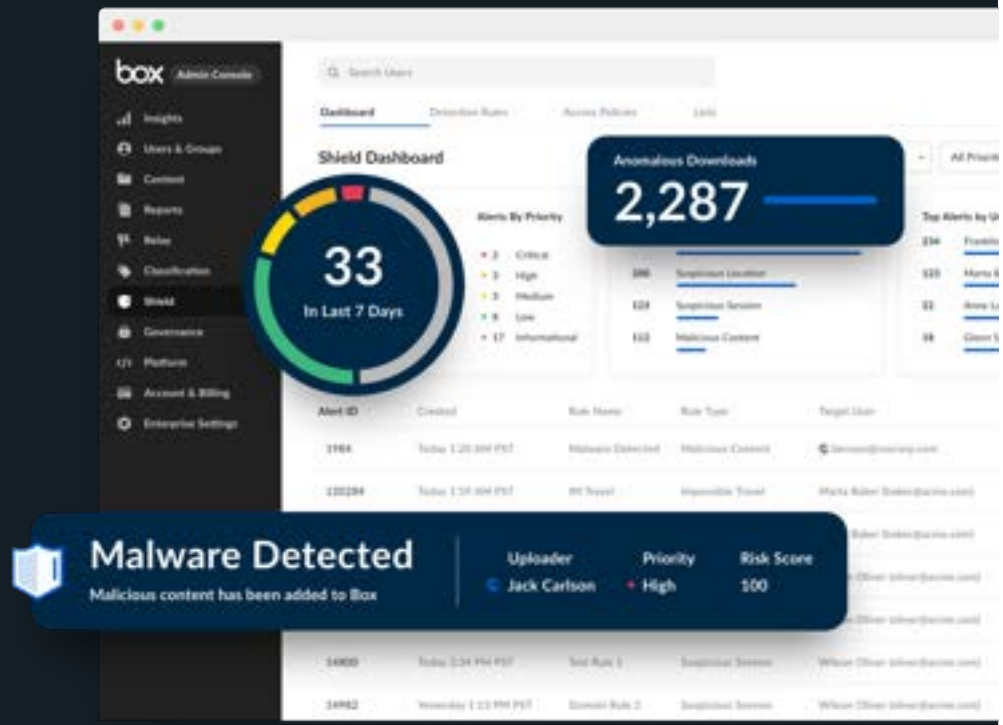
Box-Betriebskontrollen

- Verschlüsselung im Ruhezustand
- 99,9 % SLA
- Sicherer Softwareentwicklungszyklus
- Weltweit konforme Zertifizierungen, z. B. FINRA, HIPAA, FedRAMP, GxP, ISO 27001/27018
- Globale Sicherheitsvorgänge
- SSAE 16, Typ 2 Rechenzentren

*Erhältlich im Box Enterprise Plus-Tarif

„Mit Box Shield können wir eine gut durchdachte Strategie für Datenklassifizierung und Richtlinien entwickeln. Shield wird uns eine bessere Telemetrie zum Anwenderverhalten in Box bieten, unsere Daten besser schützen und gleichzeitig eine hervorragende Nutzererfahrung ermöglichen.“

JT Jacoby, CISO, International Rescue Committee



Verhindern Sie Datenschutz-verletzungen mit Box Shield

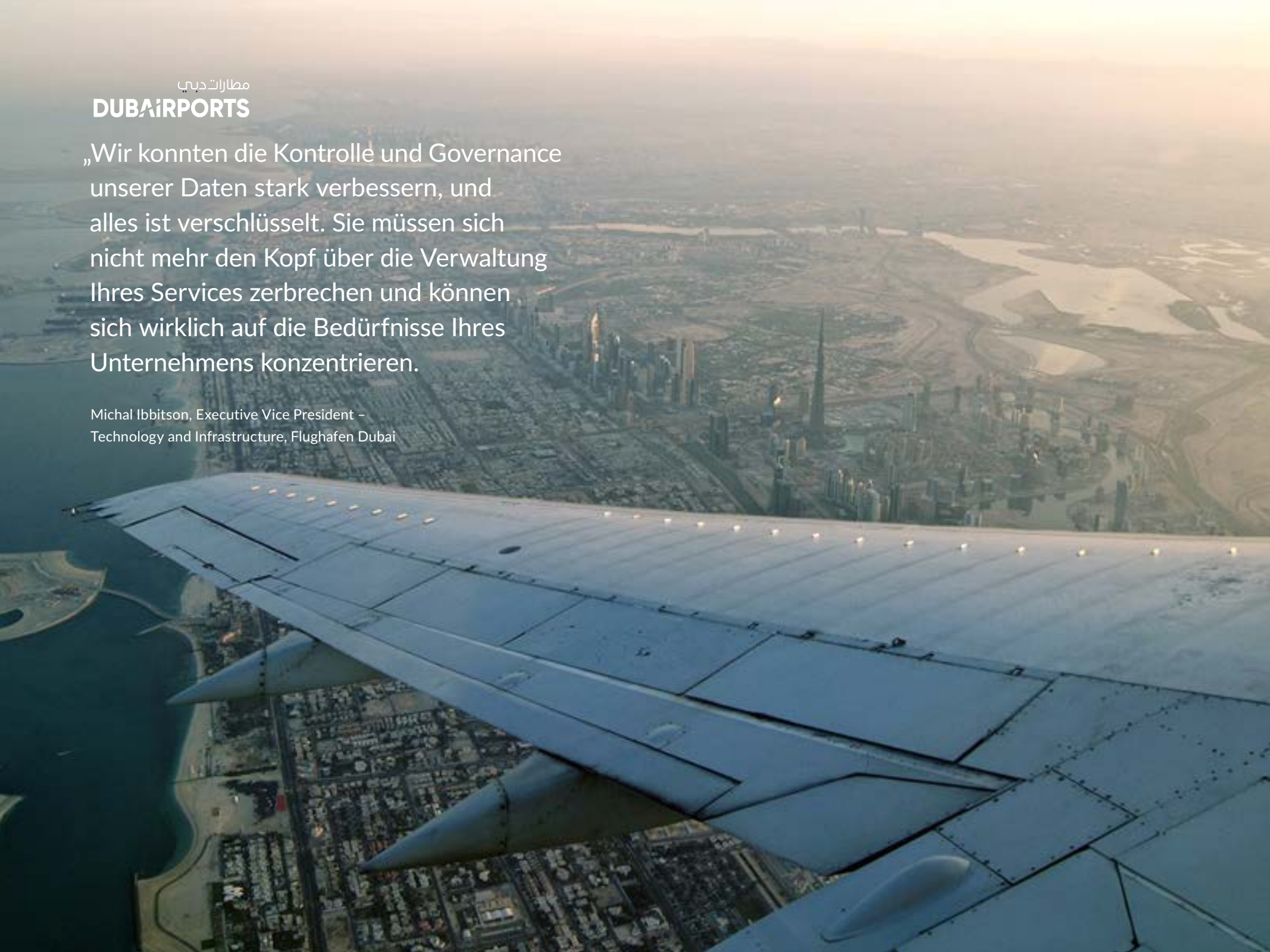
Da Ihre wertvollen Informationen in Ihrem Unternehmen ein- und ausgehen, reicht ein herkömmlicher Ansatz für die Informationssicherheit nicht mehr aus. Mithilfe von Box Shield können Sie Risiken mindern und die wertvollsten Informationen schützen, ohne Ihr Unternehmen auszubremsen.

Datenlecks mit Präzision vermeiden

Mit Box Shield können Sie Dateien und Ordner so klassifizieren, wie Sie es wünschen – entweder manuell oder automatisch. Shield kann nun personenbezogene Daten und anwenderdefinierte Begriffe in Dateien identifizieren und diese automatisch basierend auf Ihren Richtlinien klassifizieren. Und durch die integrierte Zugriffssteuerung auf der Grundlage der Klassifizierung können Sie Leckagen in Echtzeit verhindern.

Sicherheitsteams mit intelligenter Erkennung unterstützen

Box Shield nutzt maschinelles Lernen und ein tiefes Verständnis dafür, wie Mitarbeitende über Box zusammenarbeiten, um Ihnen zeitnahe und detaillierte Warnungen zu Bedrohungen durch Insider, Kontenkompromittierung und Malware zu liefern. Bewerten Sie schnell Warnungen in Shield, oder senden Sie sie zur weiteren Analyse an Ihr bestehendes SIEM oder CASB.



„Wir konnten die Kontrolle und Governance unserer Daten stark verbessern, und alles ist verschlüsselt. Sie müssen sich nicht mehr den Kopf über die Verwaltung Ihres Services zerbrechen und können sich wirklich auf die Bedürfnisse Ihres Unternehmens konzentrieren.

Michal Ibbitson, Executive Vice President – Technology and Infrastructure, Flughafen Dubai

Sicherung der Zusammenarbeit

Durch die Bereitstellung einer sicheren Plattform für die Verwaltung all Ihrer Inhalte in der Cloud schützt Box Ihre wertvollen Inhalte und kollaborativen Prozesse, ohne die Produktivität der Endanwender:Innen zu beeinträchtigen. Die Sicherheitskontrollen von Box sind auf die Endanwender:Innen ausgerichtet, arbeiten im Einklang mit dem Informationsfluss und erstrecken sich auf Anwendungen von Drittanbietern. Dank einer zentralen Content-Ebene, die in über 1.500 branchenführende Anwendungen integriert ist, können Mitarbeitende Inhalte in einer zentralen Informationsquelle schützen – ohne auf Workarounds oder Verbraucherlösungen zurückgreifen zu müssen.

So schützt Box Ihre Inhalte:

- **Steuerung von Berechtigungen** umfasst die Kontrollen, mit denen Sie detaillierte Zugriffsberechtigungen (auch „Zugriffsrechte“ oder „Berechtigungen“) erteilen, beschließen, durchsetzen, entziehen und verwalten. Mit den Verfahren zur Steuerung der Berechtigungen kann die IT-Abteilung Zugriffsrichtlinien für Unternehmensinhalte im gesamten Unternehmen durchsetzen, die Cloud-Sicherheit somit erhöhen und das Risiko von Datensicherheitsverletzungen verringern.

  Das Angebot von Box:

  - Kontrollen für granulare Berechtigungen: Wählen Sie aus einer breiten Palette von Datei- und Ordnerberechtigungen für Mitarbeitende
  - IP-/Domänenblock- und Zulässigkeitsliste: Administrator:Innen ermöglichen, die Zusammenarbeit auf bestimmte Domains zu beschränken
  - Überprüfung des Gerätezustands: Einrichtung von Mindestanforderungen für Software oder Hardware für Geräte, die auf Box zugreifen
  - Ablauf von Zugriffsberechtigungen: Erlöschen der Zugriffsrechte auf Inhalte nach bestimmten Zeiträumen (z. B. Ablauf des gemeinsamen Links für öffentliche und nicht öffentliche Links)

- **Identitäts- und Zugriffsverwaltung** ist auf geschäftskritische Anforderungen ausgerichtet und stellt den Zugriff auf Unternehmensressourcen über zunehmend vielfältige und komplizierte Technologien und Personalumgebungen hinweg sicher, während gleichzeitig strenge Compliance-Standards eingehalten werden.

  Das Angebot von Box:

  - Starke Authentifizierung über Single Sign-On (SSO), TTOP, Multifaktor-Authentifizierung und Integration mit Identitätspartnern (z. B. Okta, Microsoft Azure AD, OneLogin, Ping Identity)
  - Zwei-Faktor-Authentifizierung (2FA) für externe Mitarbeitende
  - Erweiterte Anwenderverwaltung: Deaktivierung, Anmeldeaktivität, erzwungene Abmeldung
  - Authentifizierung der Unterzeichnenden mit E-Mail, SMS und Zugangscode mit Box Sign

- **Technologien zur Verhinderung von Datenverlust** prüfen die Inhalte und analysieren Data-at-Rest in Cloud-Anwendungen. Dadurch können Unternehmen sensible Daten im gesamten Unternehmen erkennen und das Risiko eines Verlusts dieser Daten verringern.

  Das Angebot von Box:

  - Box Shield: Umfasst eine native Funktion zur Klassifizierung von Dateien und Ordnern mit vertraulichen Inhalten und zur Definition von Zugriffsrichtlinien mit mehreren Sicherheitskontrollen, um Datenlecks durch unsachgemäße Freigabe, Zusammenarbeit und Downloads zu verhindern
  - Box Trust: Ein Ökosystem von Security- und Governance-Partnern, einschließlich Anbietern von Data Loss Prevention (DLP) und Cloud Access Security Brokern (CASB), die die native Cloud-Sicherheit von Box durch moderne, branchen- und regionsspezifische Datenverlustrichtlinien erweitern

Morgan Stanley

„Box ermöglicht es unseren Kund:Innen, nahtlos mit ihren Finanzberatern zusammenzuarbeiten und dabei die höchsten Standards in Bezug auf Datenschutz, -sicherheit und -kontrolle einzuhalten.“

Sal Cucchiara, Chief Information Officer for Wealth Management, Morgan Stanley

Information Governance, Compliance und Datenschutz

- **Governance**-Funktionen sind entscheidend für Unternehmen, die sensible Inhalte verwalten müssen.

Das Angebot von Box:

Box Governance bietet erweiterten Schutz für sensible Inhalte, stellt eine sichere eDiscovery für Rechtsstreitigkeiten zur Verfügung und ermöglicht die automatische Einrichtung von Zeitplänen zur Aufbewahrung und Löschung von Dateien in Box.

- **Technologien zur Verwaltung von Verschlüsselungscodes** ermöglichen es Ihnen, Ihre eigenen Verschlüsselungscodes zu steuern, ohne dass der Cloud-Anbieter diese ebenfalls verwaltet. So erhalten Sie zusätzlichen Schutz Ihrer Daten und Inhalte.

Das Angebot von Box:

Box KeySafe bietet Ihnen die unabhängige Kontrolle über Ihre Verschlüsselungscodes ohne Einbußen bei Benutzerfreundlichkeit, Mobilität und Integrationen mit Box. Jegliche Verwendung der Schlüssel wird in einem nicht veränderbaren und detaillierten Protokoll erfasst, sodass Sie genau überwachen können, warum und wie die Schlüssel Ihres Unternehmens abgerufen werden. Und sollten Sie einmal verdächtige Aktivitäten feststellen, kann Ihr Sicherheitsteam jederzeit den Zugriff auf den Inhalt unterbrechen.

- **Datenhoheit** ist ein Thema für jedes Unternehmen, das global agiert. Bestimmte Länder und Regionen erfordern, dass Daten mit Sitz in diesem Land bzw. dieser Region auch dort aufbewahrt werden. Box nimmt sich des Themas Datenhoheit an und beseitigt regulatorische und Compliance-Hürden bei der Einführung der Cloud, sodass Unternehmen weltweit ihre Inhalte besser verwalten und schützen können.

Das Angebot von Box:

Box Zones bietet Datenspeicherung in der Region, um Kunden bei Fragen und Bedenken in puncto Datenhoheit und Datenschutz zu unterstützen. Mit Box Zones werden die Daten in der Region gespeichert, indem alle Funktionen von der Speicherebene getrennt werden. Tatsächlich ist der Speicherort der Inhalte für die Endanwender:Innen nicht sichtbar. Auf diese Weise können Endanwender:Innen mit ihrer Arbeit beginnen, ohne jemals darüber nachzudenken, wo ihre Daten gespeichert werden müssen. Wir bieten regionale Speicherung in einer oder mehreren der folgenden Regionen, alle auf derselben Box-Instanz.

Um mehr über Box Zones zu erfahren, besuchen Sie **box.com/zones**.

Infrastruktursicherheit und Threat Management

Wenn Sie Ihre Inhalte mit Box verwalten, können Sie in einer sicheren, stabilen Umgebung arbeiten, in der Sie Bedrohungen verhindern und steuern können. Wenn Ihre Endanwender:Innen Box geöffnet haben, arbeiten sie innerhalb einer einzigen redundanten, integrierten und zentralen Architektur mit integrierter Sicherheit in der gesamten Infrastruktur und in allen Prozessen. Dies bedeutet, dass Mitarbeitende Inhalte direkt und sicher über die Cloud abrufen und freigeben können. Dadurch entfällt der Anreiz zur Nutzung nicht autorisierter Methoden und Services und der Zugriff über eine hochverfügbare Softwarelösung wird ermöglicht.

- **Infrastruktursicherheit und -schutz** ist das Fundament, auf dem Box betrieben wird. Box verarbeitet jeden Tag über eine Milliarde Dateien und verfügt über mehrere Rechenzentren mit zuverlässiger Stromzufuhr und Backup-Systemen.

Das Angebot von Box:

- 99,9 % SLAs
- Verschlüsselung von Data-in-Transit und Data-at-Rest (256-Bit-AES)
- Kundengetriebene Penetrationstests
- Dedizierte Reaktion auf Zwischenfälle rund um die Uhr
- Recht auf Audit
- Hardwaresicherheitsmodule (HSMs)
- Automatisierung von Intrusion Prevention-Systemen (IPS) und Intrusion Detection-Systemen (IDS) in Firewalls
- Nur US-Bürger:Innen haben Zugang zu kritischen Produktionsbereichen (eine FedRAMP-Anforderung)

Zertifizierungen für Industrien und Behörden

Die Content Cloud ermöglicht die Einhaltung erweiterter Datenschutz- und Compliance-Anforderungen in der globalen, digitalen Welt von heute. Unser Anliegen ist es, eine sichere Content-Plattform bereitzustellen, die Ihnen hilft, Ihre gesetzlichen und Compliance-Anforderungen und -Verpflichtungen zu erfüllen und zu übertreffen. Box hat mehrere Zertifizierungen erhalten, die unser Engagement für Sicherheit belegen, unter anderem:

- **SOC 1, SOC 2 und SOC 3**
  Box verfügt über SOC 1-, SOC 2- und SOC 3-Berichte, die von unabhängigen externen Bewertern herausgegeben wurden. Mit dem SOC 1 können Unternehmen, die Box verwenden, ihre Anforderungen an die Finanzberichterstattung (z. B. Sarbanes-Oxley) erfüllen und gewährleisten, dass Box über angemessene interne Kontrollen verfügt. Die SOC 2- und SOC 3-Berichte validieren die Kontrollen und Prozesse, die Box implementiert hat, um Box sicher und hochverfügbar zu machen und gleichzeitig die Vertraulichkeit der Kundendaten zu schützen.

- **ISO 27001, 27017, 27018 und 27701**
  ISO 27001 ist ein weltweit anerkannter Sicherheitsstandard. Er bietet eine Richtlinie für Methoden und Kontrollmechanismen, die Unternehmen zur Sicherung von Daten nutzen sollten. Der Standard legt die international vereinbarten Anforderungen und Best Practices für den systematischen Ansatz zur Entwicklung, Bereitstellung und Verwaltung eines risiko- bzw. gefahrenbasierten Sicherheits-Managementsystems fest. Box ist für unsere Informationssicherheits-Managementsysteme (ISMS) gemäß ISO 27001 zertifiziert, wodurch das Box-Produkt und die gesamte Infrastruktur abgedeckt sind. ISO 27017 demonstriert den Anwender:Innen die Sicherheit von Cloud-Diensten, während ISO 27018 die sichere Verarbeitung personenbezogener Daten gewährleistet und ISO 27701 eine Erweiterung der ISO 27001 um den Datenschutz darstellt.

Weitere Informationen erhalten Sie im **Box Trust Center.**

- **Cross Border Privacy Rules (CBPR) und Privacy Recognition for Processors (PRP) der APEC (Asia-Pacific Economic Cooperation)**
  Die CBPR und PRP der APEC stärken das Vertrauen von Verbraucher:Innen, Unternehmen und Aufsichtsbehörden in den grenzüberschreitenden Austausch von personenbezogenen Daten (PII) und die damit einhergehende Verarbeitung. Diese Zertifizierungen bestätigen, dass Box die internationalen Best Practices in Bezug auf den Datenschutz erfüllt.

- **DSGVO, CCPA und C5**
  Die Datenschutz-Grundverordnung (DSGVO) harmonisiert die Datenschutzgesetze und -bestimmungen in der EU, schützt EU-Bürger:Innen im Bereich Datenschutz und gestaltet die Art und Weise neu, wie Unternehmen in der gesamten Region (und darüber hinaus) Datenschutz betreiben. Box verfügt über die folgenden Zertifizierungen, um die Einhaltung der DSGVO zu ermöglichen: Processor Binding Corporate Rules, Controller Binding Corporate Rules (BCRs), die E.U.-U.S. Privacy Shield und Swiss-U.S. Privacy Shield Frameworks bieten rechtlich anerkannte Möglichkeiten, Daten über europäische Grenzen hinweg zu übertragen.

  Der California Consumer Privacy Act (CCPA) zielte darauf ab, den Einwohner:Innen Kaliforniens mehr Kontrolle über ihre persönlichen Daten (PI) zu geben. Er verlangt außerdem von den Unternehmen mehr Transparenz darüber, wie sie solche Daten sammeln, weitergeben oder verarbeiten. Im Jahr 2020 stimmten die kalifornischen Wähler:Innen mit überwältigender Mehrheit für Proposition 24, besser bekannt als California Privacy Rights Act (CPRA), der wesentliche Änderungen am CCPA vorsieht. Box schließt die Lücke in der CPRA-Bereitschaft, indem die Kontrolle darüber vereinfacht wird, wo Ihre Daten gespeichert sind und wie auf sie zugegriffen wird. Darüber hinaus erhalten Sie Funktionen für die Datenminimierung, die verbesserte Sicherheit und die zeitnahe Beantwortung von Anfragen zu kalifornischen Verbraucherschutzrechten.

  Wir haben außerdem den Cloud Computing a Compliance Controls Catalogue (C5) erhalten, der zeigt, dass wir von unabhängigen deutschen Unternehmen auf ihre hohen Sicherheits- und Datenschutz-Standards geprüft wurden.

- **GxP** Validierung mit Box GxP ermöglicht es Unternehmen aus dem Bereich Life Science, Box zu validieren, um damit ihre regulierten klinischen Daten sowie Labor- und Produktionsinhalte zu bearbeiten, zu verwalten und weiterzugeben.

- **HIPAA (Health Insurance Portability and Accountability Act)**
  HIPAA ist ein US-Bundesmandat, das Schutz von geschützten Gesundheitsdaten (PHI) erfordert. Box unterstützt die Einhaltung der HIPAA, einschließlich der endgültigen Omnibus rule and Health Information Technology for Economic and Clinical Health (HITECH) Act.

- **Export-Control International Trafficking and Arms Regulations (ITAR) und Export Administration Regulation (EAR)**
  ITAR ist eine Exportkontrollverordnung des zum US-Außenministerium gehörenden Directorate of Defense Trade Controls (DDTC). EAR ist eine Exportkontrollverordnung des Bureau of Industry and Security (BIS) des US-Handelsministeriums. Kunden können Box so konfigurieren, dass die Anforderungen von ITAR und EAR erfüllt werden.

- **FINRA**
  Box kann Daten in Übereinstimmung mit der Financial Industry Regulatory Authority (FINRA) speichern und aufbewahren, wie in Abschnitt 17a-4 des SEC Act festgelegt. Darin ist geregelt, wie bestimmte elektronische Datensätze in nicht wiederbeschreibbaren, nicht löschbaren Formaten für bestimmte Zeiträume beibehalten werden sollen.

- **Internal Revenue Service Publication 1075 (IRS 1075)**
  IRS 1075 bietet Hinweise zur Minimierung des Risikos von Verlust, Verletzung oder Missbrauch von Steuerinformationen (Federal Tax Information; FTI). Die IRS hat eine Box-Implementierung für die Verwendung von IRS-1075 akzeptiert, und die Kunden können die Box Platform so konfigurieren, dass sie FTI auf eine konforme Weise speichern.

- **PCI DSS**
  Der Payment Card Industry Data Security Standard (PCI DSS) ist ein globaler Datensicherheitsstandard, der von Bezahlkarten-Marken als Richtlinie für alle Einheiten entwickelt wurde, die Daten von Karteninhaber:Innen verarbeiten, speichern oder übertragen. Dieser Standard bestätigt, dass Box grundlegende Sicherheitsmaßnahmen zum Schutz der Daten von Bezahlkarten aufrechterhält.

- **Department of Defense Cloud Computing SRG Impact Level 4**
  Die DoD Cloud SRG legt die Sicherheitsanforderungen für das Department of Defense for Cloud Computing fest. Box wurde für die Vertraulichkeitsstufe 4 (Impact Level 4) akkreditiert. Diese gilt für kontrollierte, nicht klassifizierte Informationen (Controlled Unclassified Information; CUI), die Exportkontrolle, Datenschutzinformationen und geschützte Gesundheitsinformationen umfassen.

- **FedRAMP/FISMA**
  FedRAMP ist ein alle Bereiche der US-Bundesregierung umfassendes Programm, das einen standardisierten Ansatz für die Sicherheitsbewertung, Autorisierung und kontinuierliche Überwachung von Cloud-Produkten und -Services bietet. Box ist auf der FedRAMP-Stufe „Moderate Impact“ (mittlere Vertraulichkeit) autorisiert und ist auf FedRAMP.gov als FedRAMP-konformes System aufgeführt. Box ist außerdem FISMA-konform. Sowohl FedRAMP als auch FISMA basieren auf dem Kontrollstandard NIST 800-53.

AstraZeneca

„Box hat sich zum Industriestandard auf diesem Gebiet entwickelt. Wir haben uns für Box entschieden, um unsere fortlaufenden Ziele im Hinblick auf Effizienz, Sicherheit und Anwenderfreundlichkeit für alle unsere Mitarbeitenden zu erreichen.“

David Smoley, CIO, AstraZeneca

Schützen Sie Ihre wertvollen Daten mit der Content Cloud

Über uns

Box (NYSE:BOX) ist die Content Cloud, eine zentrale Plattform, die es Unternehmen ermöglicht, den gesamten Lebenszyklus von Inhalten zu verwalten, von überall aus sicher zu arbeiten und führende Anwendungen zu vernetzen. Box wurde 2005 gegründet und genießt das Vertrauen von 67 % der Fortune 500-Unternehmen, darunter AstraZeneca, General Electric, JLL und Nationwide. Box hat seinen Hauptsitz in Redwood City, Kalifornien und weitere Niederlassungen weltweit, inklusive Deutschland. Besuchen Sie **box.com**, um mehr zu erfahren.

Einen höheren ROI erzielen und die Arbeitsweise verbessern

Unabhängig von Ihrer Branche kann Box Ihr Unternehmenswachstum beschleunigen und Einsparungen erzielen. Durch Steigerung der Effizienz, die Reduzierung der Kosten für die IT-Infrastruktur und die deutlich geringere Wahrscheinlichkeit einer kostspieligen Datenschutzverletzung sorgt Box dafür, dass Einsparungen nichts im Wege steht.

Basierend auf Umfragen und Interviews mit Box-Kunden ergab eine Studie von Forrester Research[4], dass Kunden in den ersten drei Jahren mit Box einen ROI von bis zu 332 % und Produktivitätssteigerungen in Höhe von 8,8 Mio. USD erzielen können.

[4]Forrester Research, „Total Economic Impact™ of the Box Content Cloud“, 2021

Erfahren Sie mehr darüber, wie Box Ihnen helfen kann

In den letzten 18 Jahren haben wir uns darauf konzentriert, unsere Produkte kontinuierlich weiterzuentwickeln und zu verbessern, um unseren Kunden einen besseren Service zu bieten.

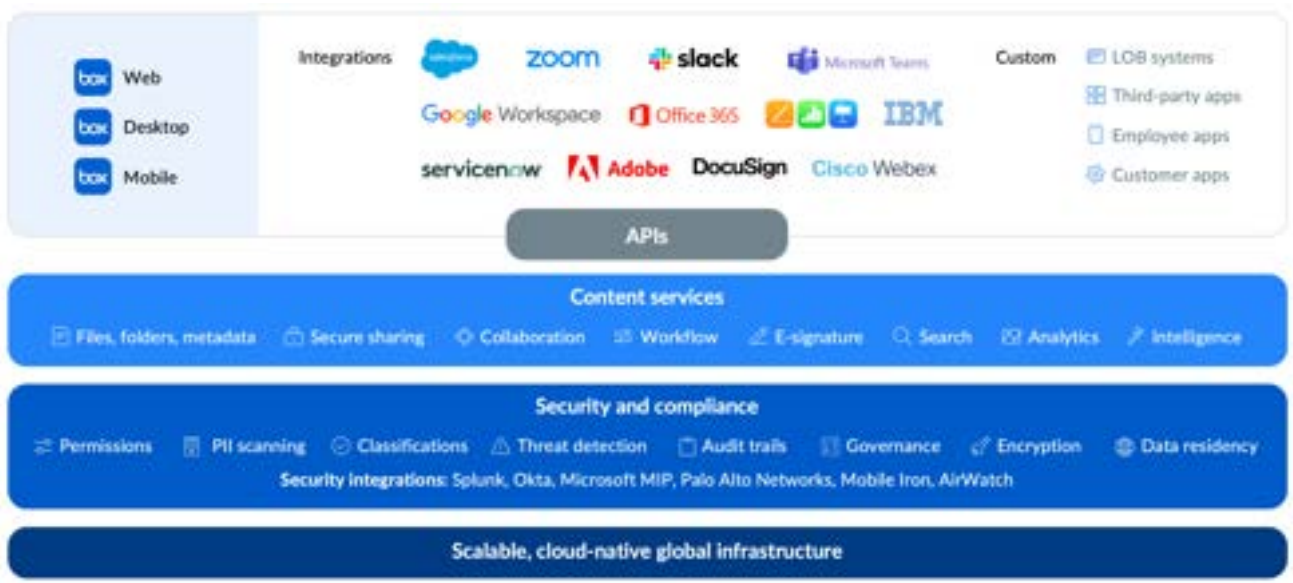
Mit der Content Cloud können Sie den gesamte Content-Prozess auf einer zentralen, offenen Plattform verwalten. Sie ist auf die Bedürfnisse von Endanwender:Innen, IT und Developer:Innen abgestimmt.

Der erste Schritt besteht darin, alle Ihre Inhalte in die Cloud zu übertragen. Durch das brandneue Box Shuttle ist die Migration von Inhalten einfach, schnell und kostengünstig. Sobald sich Ihre Inhalte in Box befinden, können Sie von allen Sicherheitsvorteilen profitieren.

Mit unserem Workflow-Tool Box Relay können Sie Metadaten, Zusammenarbeit und Workflows für Ihre Inhalte verwalten. Box Sign bietet nativ integrierte Funktionen für elektronische Signaturen direkt an den Ort, an dem Ihre Inhalte in Box gespeichert sind.

Wir haben unsere Sicherheits- und Hosting-Services verbessert und eine Reihe von Funktionen für erweiterte Sicherheit mit Box Shield, die Verwaltung des Lebenszyklus von Inhalten mit Box Governance, Verwaltung von Verschlüsselungscodes mit Box KeySafe und regionale Datenspeicherung mit Box Zones hinzugefügt. Darüber hinaus deckt die Content Cloud alle Ihre Anforderungen an Ihre Daten-Compliance und die Einhaltung von Vorschriften ab – mit einer breiten Palette von Zertifizierungen von ISO bis DSGVO.

Außerdem haben wir APIs definiert und veröffentlicht, mit denen Developer:Innen die Leistungsfähigkeit von Box, einschließlich elektronische Unterschriften, auf Anwendungen von Drittanbietern ausweiten können. Box entwickelt sich ständig weiter und durch die Nutzung hochmoderner Technologien, wie maschinelles Lernen, bieten wir unseren Kunden die neuesten und besten Services mit der Content Cloud.



Wir glauben, dass jedes Unternehmen wie ein digitales Unternehmen arbeiten kann und sollte. Die Content Cloud hilft Ihnen dabei, dieses Ziel zu erreichen.

Mit der Content Cloud werden manuelle Prozesse digitalisiert und automatisiert. Die Teams müssen nicht mehr jeden Tag stundenlang nach Informationen suchen, und die Produktivität steigt. Die Zusammenarbeit innerhalb und außerhalb des Unternehmens verläuft nahtlos, und die neuesten Technologien für maschinelles Lernen helfen Ihnen, potenzielle Bedrohungen zu überwachen und zu erkennen. Schluss mit abgeschotteten Inhalten. Schluss mit der aufwändigen Suche nach Informationen. Sie erhalten die Freiheit, echte, sinnvolle Arbeit zu erledigen.

Schützen Sie das, was am wichtigsten ist – mit Box.

box

Weitere Informationen finden Sie unter **box.com/security-compliance**