box

How to secure your business with the Content Cloud

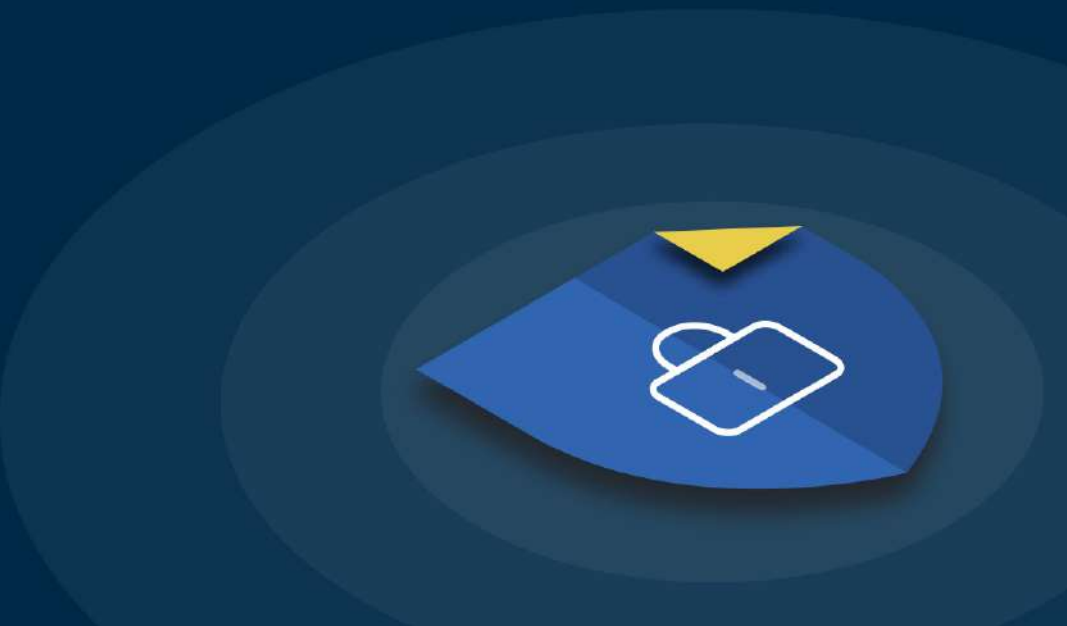


Table of contents

Today's companies need frictionless security

We all know that security is non-negotiable in today's world. Our work is much more complex than it used to be, and organizations are facing unprecedented challenges to protect their content and maintain compliance. As technology has evolved along with the way we work, IT services have steadily moved from a centralized computing model to a highly decentralized one. Mobility, cloud services, consumer apps, and the widespread acceptance of e-signatures have all fueled the need for employees to be able to work anytime, anywhere, and from any device.

Meanwhile, IT has to create a seamless and secure experience not only for onsite teams, but also for remote workers, suppliers, partners, and customers. While increased mobility and collaboration has created immense value for businesses, it has also posed challenges for IT and C-suite leaders to protect content across a distributed ecosystem.

Maintaining security is critical, given the major impact that data breaches can have on your company's finances and brand reputation. Without tight IT controls, the risk of human error — resulting in data loss — is incredibly high. Three out of every four employees think it's fine to transfer confidential work documents to personal devices. That increases the risk of exposure if you're moving files back and forth between personal devices,[1] consumer applications, and shared drives. Mobile teams also lack security when operating outside of a managed cloud architecture: 87% of people don't notify anyone when a USB drive is lost, and 52% don't notify security teams quickly when a computer (and the files on it) go missing.[2]

A breach can have a huge impact on your company's bottom line. After all, the average global cost per data breach is $3.86 million.[3]

With many companies storing millions (or even tens of millions) of sensitive records, the financial risk of a data breach is higher than ever. And in terms of your relationship with your consumers, the damage to your brand reputation after a breach is long-lasting and not easily repaired.

[1] *bit.ly/2zvoxnc*
[2] *bit.ly/2k6LdHH*
[3] *ibm.co/2rLVOKR*

Fragmented content strategies, shadow IT, and relying on email can lead to these damaging vulnerabilities. Of the companies examined by the 2018 Verizon Data Breach Investigations Report, for example, 66% of malware came in via email.[5] And just as threats are on the rise, it's become even more difficult for security professionals to process the large number of security alerts that come across their desks.

You can't afford to wait to ensure compliance

Evolving global legislation and regulations only raise the stakes — IT leaders need to take an active role in managing content and setting security strategies.

What causes a breach?

52% malicious attack

23% human error

IBM[4]

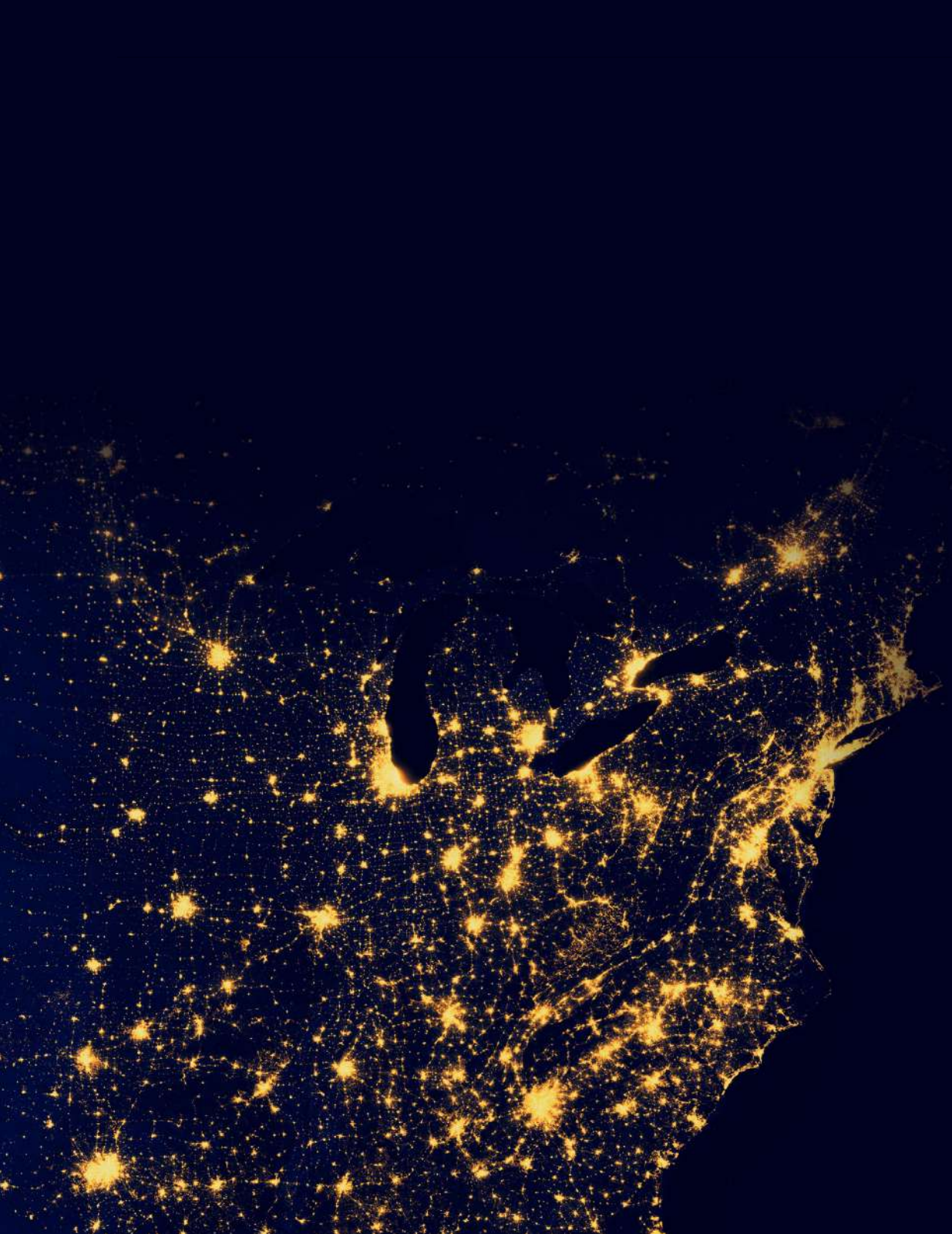
Compliance management requires tackling complex industry, line-of-business, and geography-specific standards. The European Union's General Data Protection Regulation (GDPR) for example, went into effect in 2018 and tightens regulations around any company handling the data of European citizens and residents, irrespective of whether or not the company is based in the E.U. Similarly, in 2020, the California Consumer Privacy Act (CCPA) went into effect — and other privacy regulations in countries like Brazil and India are expected over the next couple years.

As companies serve customers around the world and work with global partners, they need to be ready to meet regional data governance and residency requirements — or face significant penalties. GDPR violations, for example, can cost companies up to €20 million or 4% of their total worldwide annual revenues, whichever is higher.[6]

At Box, security is woven into our DNA. And it's an integral part of the Content Cloud: a single secure platform for the entire content lifecycle, from file creation to sharing and e-signature to retention. With security and compliance baked into your content strategy, you get one secure place to manage all of your content to prevent these kinds f vulnerabilities and quickly and accurately respond to threats. It's a radically simplified and far more secure way for teams to work together.

In the rest of this ebook, we'll explore how the Content Cloud provides frictionless security and compliance, helping you reduce risk without impacting productivity or slowing down the business.

[4] *ibm.co/2rLVOKR*
[5] *vz.to/2qihidi*
[6] *bit.ly/2n9aVK0*



S&P Global

"Security is key in everyone's business. We have the ability to downgrade sovereign nations, so it's an imperative for us. We have to be really thoughtful about putting the right controls in place, and ensuring that information is not accessible where it shouldn't be."

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

The four key tenets of Box security

Every company is adjusting to this new way of work: the need for faster processes across more dispersed teams, with a modern cloud stack to match. And that means companies like yours must rethink how to protect, control, and govern data. Mitigating risk means finding ways to manage all the data flowing at higher speeds and volumes than ever before. But while trying to protect corporate data, enforce privacy, and maintain compliance, you also need solutions that enable innovation. The challenge is finding a way to balance innovation and security, and to gain visibility and analytics into the flow of data — instead of striving for data control.

1 Zero trust infrastructure

Conventional security models assume that all users inside the network are trustworthy. But this doesn't protect against insider threats. At Box, we operate on a zero-trust model and never assume that a user or network is safe. That means we don't just protect a laptop or mobile device, for example, at the machine level. We protect at the more granular data level. That way, if the machine gets compromised, the data doesn't also get compromised. Plus, we take steps to protect all content with security bots, advanced authentication techniques like one-time passwords, and out-of-band approval for sensitive tasks.

2 Zero tolerance for a poor user experience

Security shouldn't interfere with the user experience. People will likely abandon IT-sanctioned solutions with bad user experiences, and instead turn to consumer tools that lack security. At Box, we aim to make our product seamless and delightful to use, and allow security to operate in the background where the user doesn't even notice it. This means being able to take actions right where your content lives and not having to log in to a standalone tool just to complete the e-signature step of a business process. Or, this means creating simple ways for people to send files via shared links, choosing between link controls such as "people with the link," "people in your company," or "invited people only." For IT, it means having the right guardrails in place while empowering people to get work done.

3 Provide a centralized content layer in the cloud

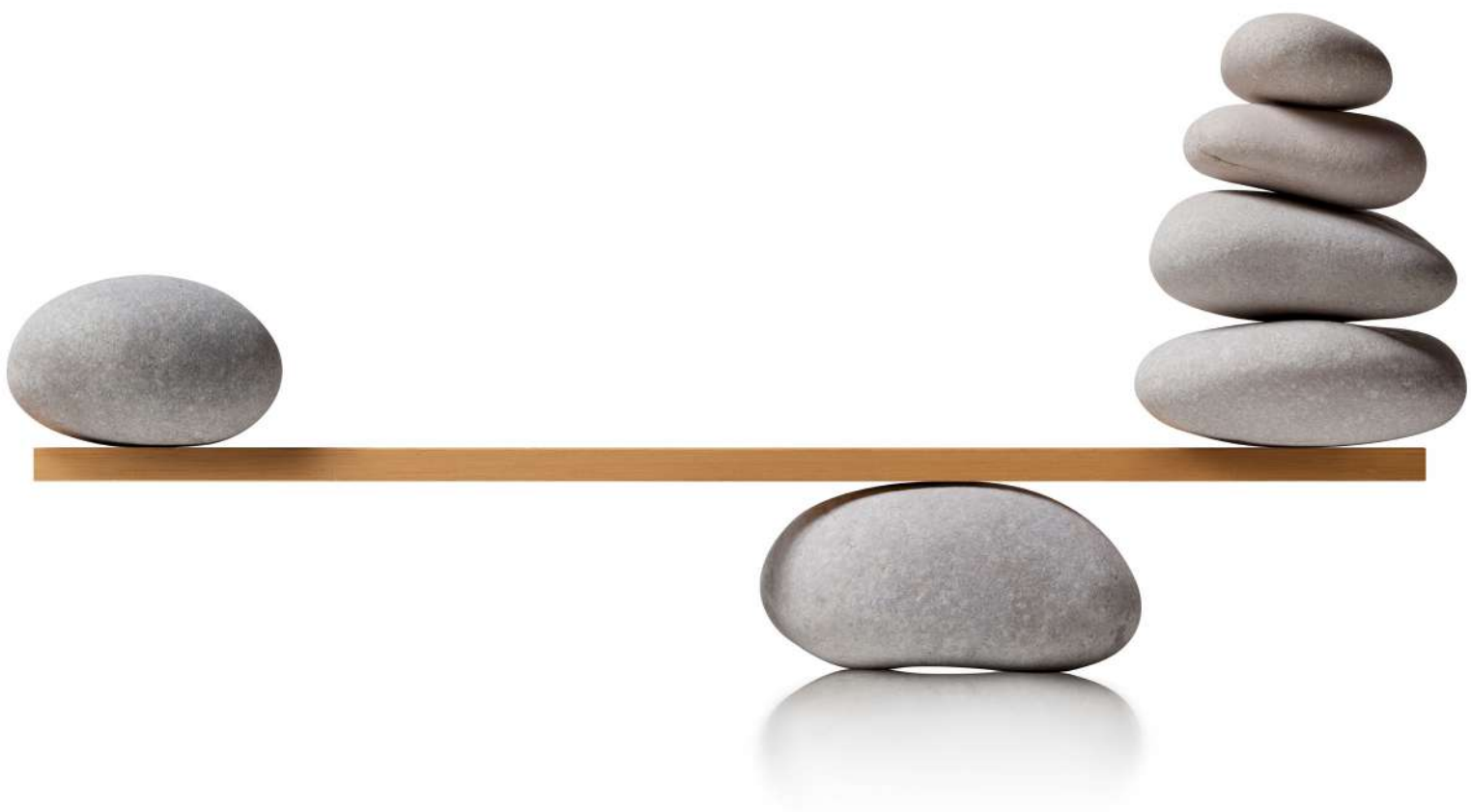
Centralizing your content in the cloud makes it easier to secure, manage, and govern your files. While many IT organizations rely on a decentralized model of computing, this results in fragmented content and a larger attack surface. But even if you operate on a modern cloud stack, failure to use the cloud as a central content layer can create a massive fragmentation problem. By providing a single content layer centralized in the cloud, Box helps you better protect and govern your content.

4 Security that travels with your content

Security as a bolt-on, afterthought solution rarely works — you need controls built into the very fabric of how you manage your content. That way, not only is your data protected; that same level of security travels with your content when you work in other apps by using Box as your content layer. So when you work in Slack or request a Box Sign-powered e-signature on a client contract in Salesforce (or use any of our other 1,500+ integrations), you get Box-level security along with it.

"We are all in this journey towards frictionless security and compliance. The advantage will go to those who are consolidating their content, securing it with built-in controls, and maintaining a 'single-pane-of-glass' view of risks to their highly valued information."

Julien Soriano, Chief Information Security Officer, Box



Box security at a glance

Users

- Strong user authentication
  via SSO and MFA
- 2FA for external collaborators
- Password controls
  set requirements for internal/external users
- Advanced user management
  de-activiation, login activity, and force-logout
- Signer authentication (via email, SMS, or access code)

Devices

- Device posture check
  sets device security and ownership requirements
- Device pinning
  limits number of devices with Box access
- MDM and MAM
  secure access with Box for EMM integrations
- Domain block and allow-listing
  restricts Box use to approved IPs

Applications

- 1,500+ integrations
  maintain single source of truth through secure APIs
- Permissions sync
  maintains permissions for Slack, Teams, Salesforce, and NetSuite
- Granular application scopes
  enforce least privilege good practices
- Classification-based app controls*
  based on sensitivity of file

Content

- Granular permissions
  with 7 levels of access
- Shared link expiration
  sets auto expiry for public vs. non-public links
- Dynamic watermarking
  for 120+ file types
- Malware detection
- Retention, deletion, and legal holds*
- Classification-based access controls*

Visibility

- Reporting
  and centralized audit logs for 7 years
- One view
  of all internally and externally shared content, including those sent for e-signature
- ML-powered threat detection*
- CASB and SIEM partners
  provide unified view across apps and network

Infastructure

- In-region storage*
  meets data residency requirements
- Encryption key management*
  lets you manage your own encryption keys

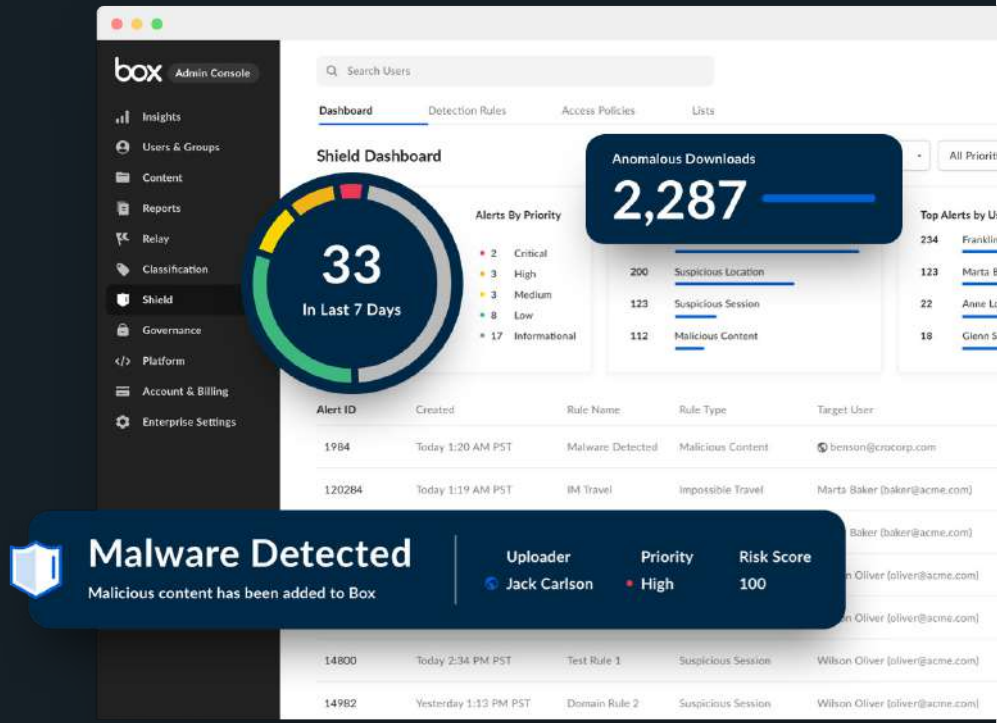
Box operational controls

- Encryption at rest
- 99.9% SLA
- Secure software development lifecycle
- Globally compliant certifications
  e.g., FINRA, HIPAA, FedRAMP, GxP, ISO 27001/27018
- Global Security Operations
- SSAE 16 Type 2 datacenters

*Available in Box Enterprise Plus plan

"With Box Shield, we can roll out a well-thought-out strategy for data classification and policies. Shield is going to give us greater telemetry on user behavior in Box, better protecting our data while enabling a great user experience."

JT Jacoby, CISO, International Rescue Committee



Prevent data breaches with Box Shield

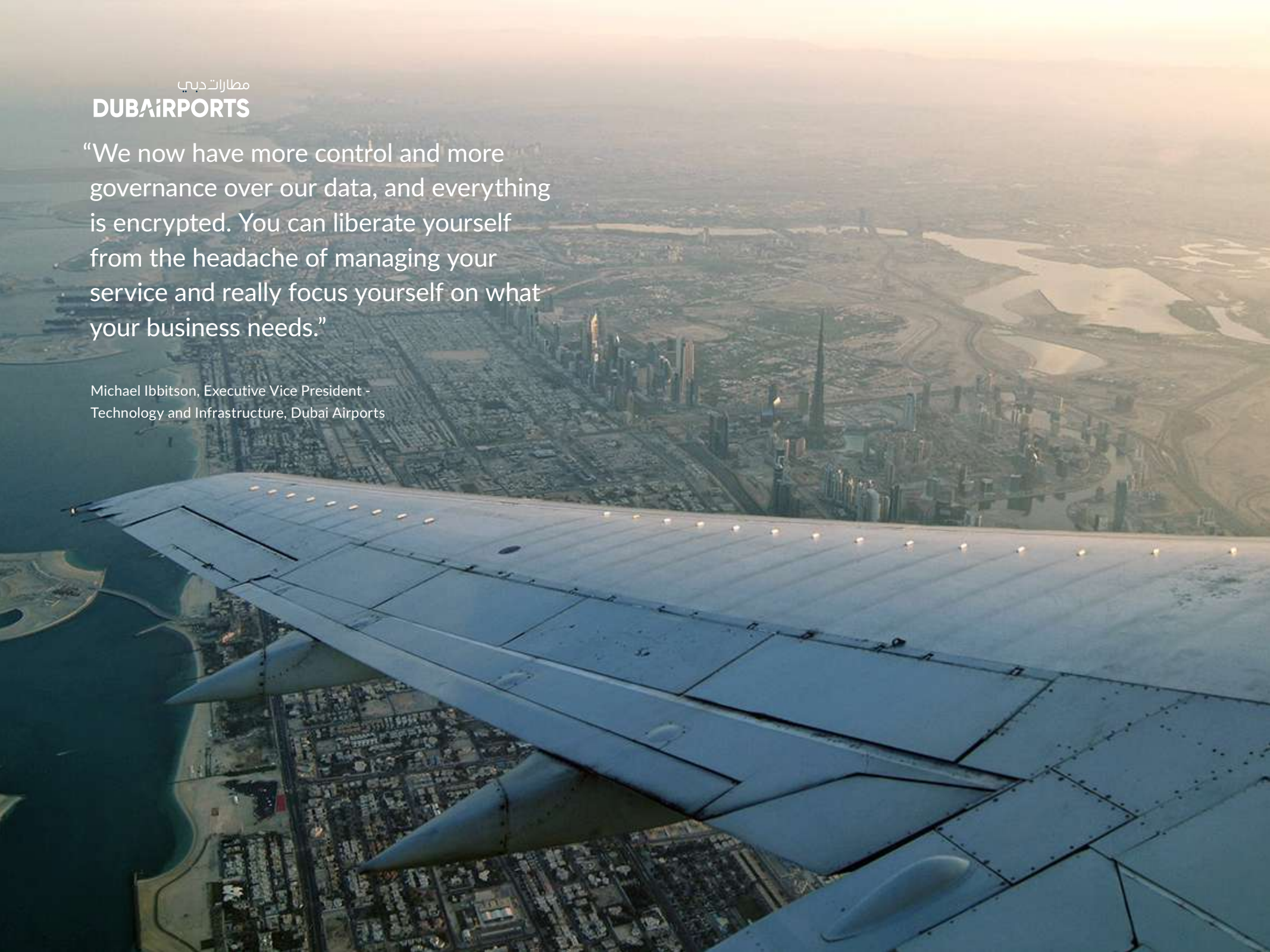
As your valuable information flows in and out of your organization, the old-school approach to information security doesn't get the job done. Box Shield helps you reduce risk and protect your most valuable information without slowing down your business.

Prevent data leaks with precision

Box Shield lets you classify files and folders your way: manually or automatically. Shield can now identify PII and custom terms within files, and automatically classify them based on your policies. And through built-in access controls based on the classification, you can prevent leaks in real time.

Empower your security team with intelligent detection

Box Shield uses machine learning and a deep understanding of how people collaborate on Box to bring you timely, accurate alerts on insider threats, account compromise, and malware. Quickly evaluate alerts in Shield, or send them out to your existing SIEM or CASB for further analysis.



"We now have more control and more governance over our data, and everything is encrypted. You can liberate yourself from the headache of managing your service and really focus yourself on what your business needs."

Michael Ibbitson, Executive Vice President - Technology and Infrastructure, Dubai Airports

Securing collaborative work

By providing a secure platform to manage all of your content in the cloud, Box protects your valuable content and collaborative processes without impeding end-user productivity. Box's security controls are designed with the end user in mind, work in-line with the flow of information, and extend to third-party applications. By having a central content layer integrated with over 1,500 best-of-breed applications, employees can keep content secure in a single source of truth — without resorting to workarounds or consumer solutions.

Here are some of the ways Box protects your content:

- **Entitlement management** encompasses the controls that grant, resolve, enforce, revoke, and administer detailed access entitlements (also known as "access rights" or "permissions"). Entitlement management procedures let IT enforce access policies for enterprise content across the organization, and thus boost cloud security and reduce the risk of data breaches.

What Box offers:

- Granular permissions controls: Choose from a broad range of file and folder permissions for collaborators
- IP/domain block and allow-listing: Allow administrators to restrict collaboration to specific domains
- Device posture check: Establish a minimum set of software or hardware requirements for devices accessing Box
- Access expiration: Expire privileges to content after set periods of time (e.g., shared link expiration for public and non-public links)

- **Identity and access management** addresses the mission-critical need to ensure appropriate access to enterprise resources across increasingly diverse and complicated technology and workforce environments, while also meeting rigorous compliance standards.

What Box offers:

- Strong authentication via single sign-on (SSO), TTOP, multi-factor authentication, and integrations with identity partners (e.g., Okta, Microsoft Azure AD, OneLogin, Ping Identity)
- Two-factor authentication (2FA) for external collaborators
- Advanced user management: Deactivation, login activity, force-logout
- Signer authentication with email, sms, and access code with Box Sign

- **Data-loss prevention** technologies inspect content and analyze data at rest in cloud applications. This helps businesses discover sensitive data throughout the organization and reduce the risk of losing that data.

What Box offers:

- Box Shield: Includes a native capability to classify files and folders with sensitive content, and define access policies containing multiple security controls to prevent data leaks via improper sharing, collaboration, and downloads
- Box Trust: An ecosystem of security and governance partners, including data-loss prevention (DLP) and cloud access security broker (CASB) vendors, that extend Box's native cloud security with industry- and region-specific data-loss prevention policies

Morgan Stanley

"Box empowers our clients to collaborate with their financial advisers seamlessly while adhering to the highest standards of data privacy, protection, and security."

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

Information governance, compliance, and privacy

- **Governance** capabilities are key for organizations that need to manage sensitive content.

What Box offers:

Box Governance provides enhanced protection for sensitive content, enables defensible eDiscovery for litigation, and lets you automatically set up retention and disposition schedules for files in Box.

- **Encryption key management** technologies allow you to control your own encryption keys without the cloud provider also managing the encryption keys. This adds an extra layer of privacy and protection to your content.

What Box offers:

Box KeySafe gives you independent control over your encryption keys — without compromising the usability, mobility, and integrations that work with Box. All key usage is tracked in an unchangeable and detailed log so you can see exactly why and how your organization's keys are being accessed. And if you ever experience suspicious activity, your security team can cut off access to the content at any time.

- **Data residency** concerns are impacting virtually any business that wants to operate on the global stage. Certain countries and regions require that data based in that country or region also reside there. By addressing data residency concerns, Box is removing regulatory and compliance barriers to cloud adoption so that businesses around the globe can better manage and protect their content.

What Box offers:

Box Zones provides in-region data storage to help customers address data residency and privacy concerns. Box Zones offers in-region data localization by separating all the powerful collaboration, productivity, and ease-of-use features of Box from the storage layer. In fact, the content storage location is invisible to end users. This allows end users to go on with their day without ever having to think about where their data needs to be stored. We offer in-region storage in one or more of the following regions, all on the same Box instance.

To learn more about Box Zones, visit box.com/zones

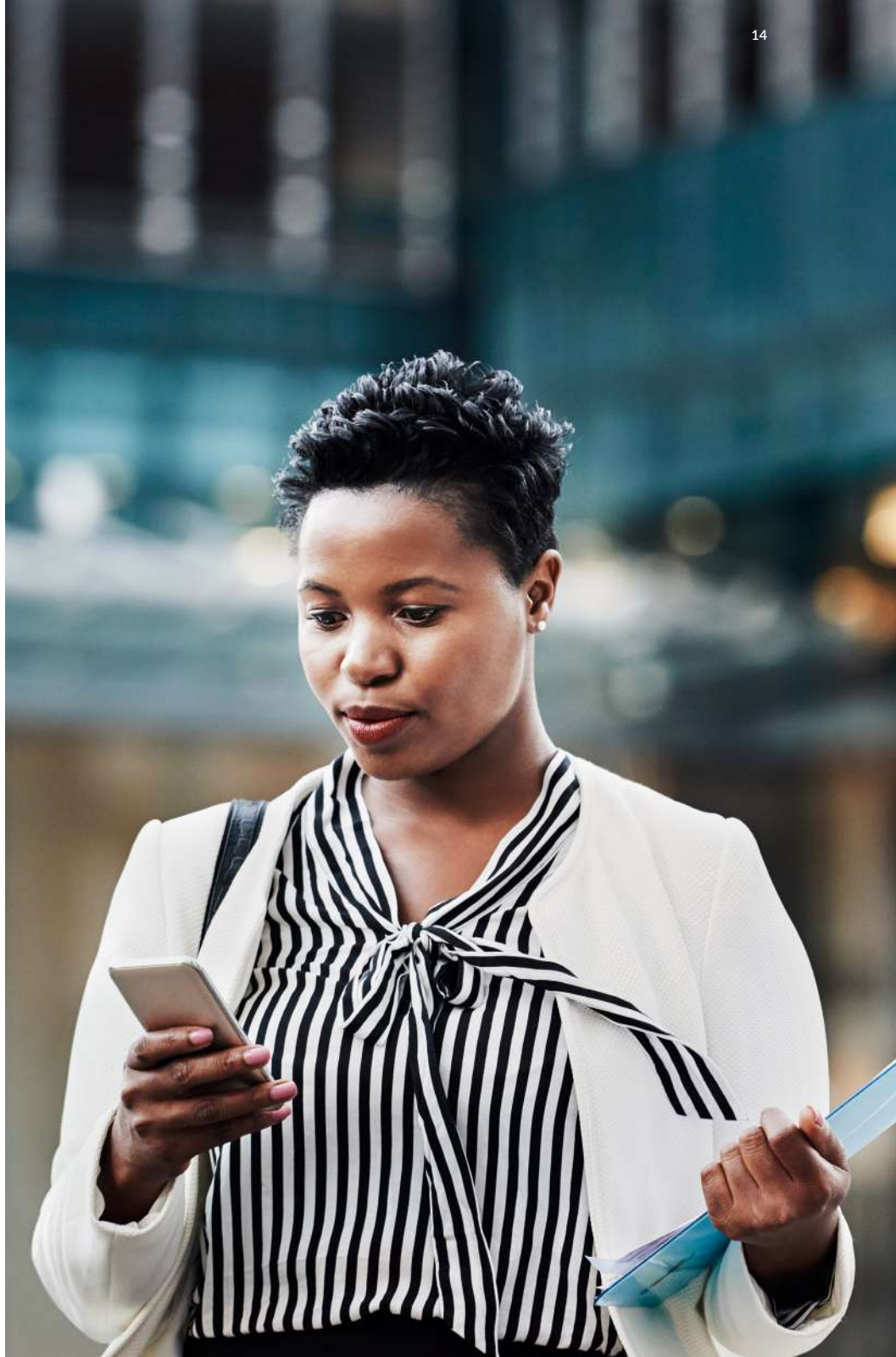
Infrastructure security and threat management

Managing your content with Box enables you to work in a secure, resilient environment where you can prevent and manage threats. When your end users are on Box, they operate within a single redundant, integrated, and centralized architecture with security embedded throughout the infrastructure and processes. This means employees access and share content directly and securely from the cloud, eliminating the incentive to use unauthorized methods and services, and have access through a highly available software solution.

- Infrastructure security and assurance is the bedrock on which Box operates. Box processes over one billion files every single day, and has multiple data centers with reliable power sources and backup systems.

What Box offers:

- 99.9% SLAs
- In-transit and at-rest encryption (256 bit AES)
- Customer-driven penetration testing
- Dedicated 24/7 incident response
- Right to audit
- Hardware security modules (HSMs)
- Automation of Intrusion Prevention Systems (IPS) and Intrusion Detection Systems (IDS) into firewalls
- Only US citizens have access to critical production areas (a FedRAMP requirement)



Certifications and audits

You don't have to take our word on Box's content security. We know our customers expect the best, and we go through regular independent certifications and audits to make sure we meet the toughest security standards today. Here are some of the certifications and audits Box has completed:

- **SOC 1, SOC 2, and SOC 3**
  Box maintains SOC 1, SOC 2, and SOC 3 reports issued by independent third-party assessors. The SOC 1 enables companies that use Box to support their financial reporting requirements (e.g., Sarbanes-Oxley) and gives them assurance that Box has appropriate internal controls in place. The SOC 2 and SOC 3 reports validate the controls and processes Box has implemented to make Box secure and highly available while protecting the confidentiality of customer data.

- **ISO 27001**
  ISO 27001 is a globally recognized security standard that provides a guideline of the policies and controls an organization has in place to secure data. The standard sets out internationally agreed upon requirements and best practices for the systematic approach to the development, deployment and management of a risk/threat-based information security management system. Box has achieved ISO 27001 certification for our Information Security Management Systems (ISMS), covering the Box product and all supporting infrastructure.

- **ISO 27018**
  ISO 27018 focuses on protecting personal data in the cloud. Based on ISO 27002, it provides guidance for controls around personally identifiable information (PII) in the public cloud. It also provides additional protections not encompassed by ISO 27002.

- **Asia-Pacific Economic Cooperation (APEC) Cross Border Privacy Rules (CBPR) and Privacy Recognition for Processors (PRP)**
  The APEC CBPR and PRP build consumer, business, and regulator trust in cross-border flows of personally identifiable information (PII) and associated processing. These certifications confirm that Box meets international best practices with regards to privacy and is one of few SaaS providers that has demonstrated this level of commitment to users' privacy.

- **GDPR, CCPA, C5, and TCDP**
  The General Data Protection Regulation (GDPR) harmonizes data-privacy laws and regulations across the E.U., protects E.U. citizens in the area of data privacy, and reshapes the way organizations across the region (and beyond) approach data privacy. Box is GDPR-ready and has the following certifications to enable GDPR compliance: Processor Binding Corporate Rules, Controller Binding Corporate Rules (BCRs), the E.U.-U.S. Privacy Shield and the Swiss-U.S. Privacy Shield Frameworks provide legally recognized ways to transfer data across European borders.

  The California Consumer Privacy Act (CCPA) was created to give California residents more control over their personal information (PI) and requires that businesses provide greater transparency on how they may collect, share, or process such data. Box is CCPA-ready and can help you along your journey through easily finding PI, maintaining strong cloud security controls, and enforcing the right retention/deletion policies.

  We've also received the Cloud Computing a Compliance Controls Catalogue (C5) and the Trusted Cloud Data Protection Profile (TCDP) certifications from Germany. The C5 and the TCDP show we've been independently audited by German organizations for meeting their high bar for adequate security and data protection.

- **GxP**
  Box GxP Validation enables life sciences organizations to validate Box so they can work with, manage, and distribute all of their regulated clinical, lab, and manufacturing content.

- **HIPAA (Health Insurance Portability and Accountability Act)**
  HIPAA is a U.S. federal mandate that requires protections for Protected Health Information (PHI). Box supports HIPAA compliance, including the final Omnibus rule and Health Information Technology for Economic and Clinical Health (HITECH) Act.

- **Export-Control International Trafficking and Arms Regulations (ITAR) and Export Administration Regulation (EAR)**
  ITAR is an export control regulation run by The Directorate of Defense Trade Controls (DDTC) at the U.S. Department of State. EAR is an export control regulation run by the Bureau of Industry and Security (BIS) at the U.S. Department of Commerce. Customers can configure Box to meet the requirements of both ITAR and EAR.

- **FINRA**
  Box can store and retain data in compliance with the Financial Industry Regulatory Authority (FINRA) as established by section 17a-4 of the SEC Act. This governs how certain electronic records should be preserved in non-rewritable, non-erasable formats for specific periods of time.

- **Internal Revenue Service Publication 1075 (IRS 1075)**
  IRS 1075 provides guidance to minimize risk of loss, breach, or misuse of federal tax information (FTI). The IRS has accepted a Box implementation for IRS-1075 use and customers can configure the Box platform to store FTI in a compliant manner.

- **PCI DSS**
  The Payment Card Industry Data Security Standard (PCI DSS) is a global data-security standard established by payment card brands to guide all entities that process, store, or transmit cardholder data. This affirms that Box upholds basic security measures for the protection of payment card data.

- **Department of Defense Cloud Computing SRG Impact Level 4**
  The DoD Cloud SRG sets security requirements for the Department of Defense for Cloud Computing. Box has been accredited at Impact Level 4 which is for Controlled Unclassified Information (CUI) which includes Export Control, Privacy Information, and Protected Health Information.

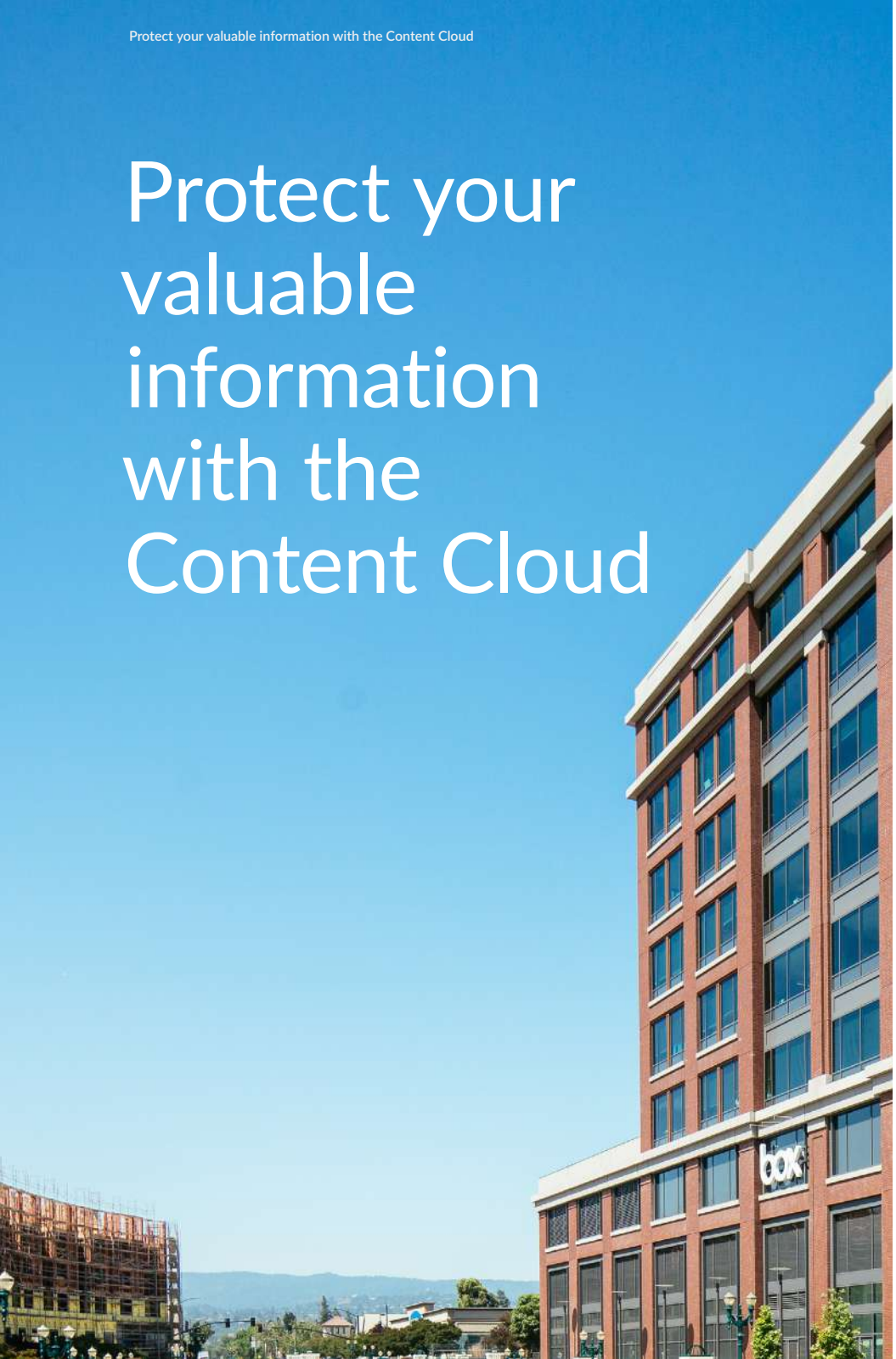
- **FedRAMP/FISMA**
  FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. Box is authorized at the FedRAMP Moderate Impact Level and is listed on FedRAMP.gov as a FedRAMP compliant system. Box is also FISMA compliant. Both FedRAMP and FISMA are based off the NIST 800-53 standard of controls.

AstraZeneca

"Box has become the industry standard in this space, and we've chosen it to continue our drive toward efficiency, security, and simplicity for all our employees."

David Smoley, CIO, AstraZeneca

Protect your valuable information with the Content Cloud



About us

Box (NYSE:BOX) is the Content Cloud, a single platform that empowers organizations to manage the entire content lifecycle, work securely from anywhere, and integrate across best-of-breed apps. Founded in 2005, Box is trusted by 67% of the Fortune 500, including AstraZeneca, General Electric, JLL, and Nationwide. Box is headquartered in Redwood City, CA, with offices across the United States, Europe, and Asia. Visit box.com to learn more.

Get a higher ROI and a better way to work

No matter your industry, Box can accelerate your business growth and ultimately save you money. By boosting efficiency, reducing IT infrastructure costs, and significantly decreasing the chance of costly data breaches, Box is ready to help you save.

Based on surveys and interviews with Box customers, a study by Forrester Research[7] found that customers can see up to a 332% ROI and $8.8M in productivity gains in their first three years with Box.

[8] *www.box.com/resources/forrester-tei*

Learn more about what Box can do for you

Over the past 16 years, we've focused on building and improving our products to better serve our customers.

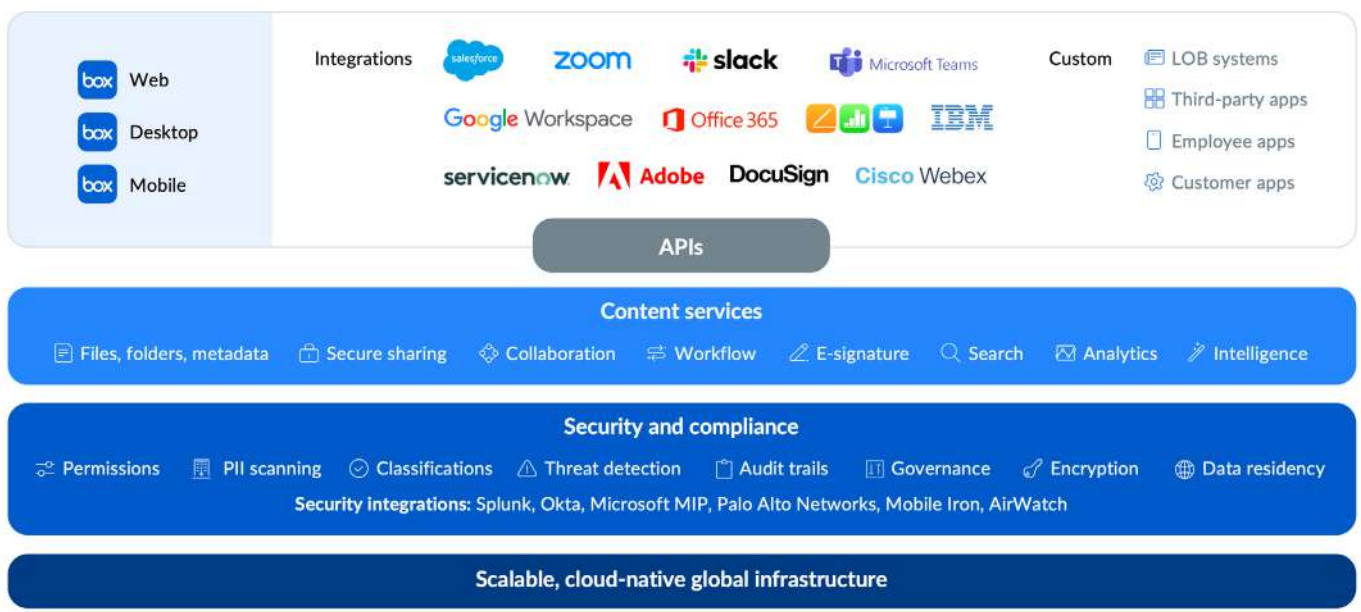
The Content Cloud lets you manage the entire content journey on a single open platform. It's designed to meet the needs of end users, IT, and developers.

The first step is getting all your information into the cloud. The all-new Box Shuttle makes content migration easy, fast, and cost-effective. Once your content is in Box, you can reap all the security benefits.

Our workflow tool, Box Relay, enables you to manage the metadata, collaboration, and workflows related to your content. And Box Sign brings natively integrated e-signature capabilities right to where your content lives in Box.

We've enhanced our security and hosting services and added a range of features for advanced security with Box Shield, governance with Box Governance, and compliance with a broad range of certifications from ISO to GDPR. Plus, we offer encryption key management with Box KeySafe and data sovereignty with Box Zones.

We've also defined and published APIs that enable developers to extend the power of Box, including e-signatures, to third-party applications. Box continues to evolve, and by leveraging cutting-edge technologies like machine learning, we bring the latest and best suite of services to our customers with the Content Cloud.



We believe that every organization can and should work like a digital organization. The Content Cloud will help you get there.

With the Content Cloud, manual processes become digital and automated. Teams no longer spend hours each day hunting for information, and productivity soars. Collaboration both inside and outside the organization becomes seamless, and the latest machine learning technologies help you monitor and detect potential threats. No more siloed content, no more searching for information. Just the freedom to get real, meaningful work done.

Protect what matters most with Box.

box

Learn more at box.com/security