box

How to secure your content in the cloud with Box

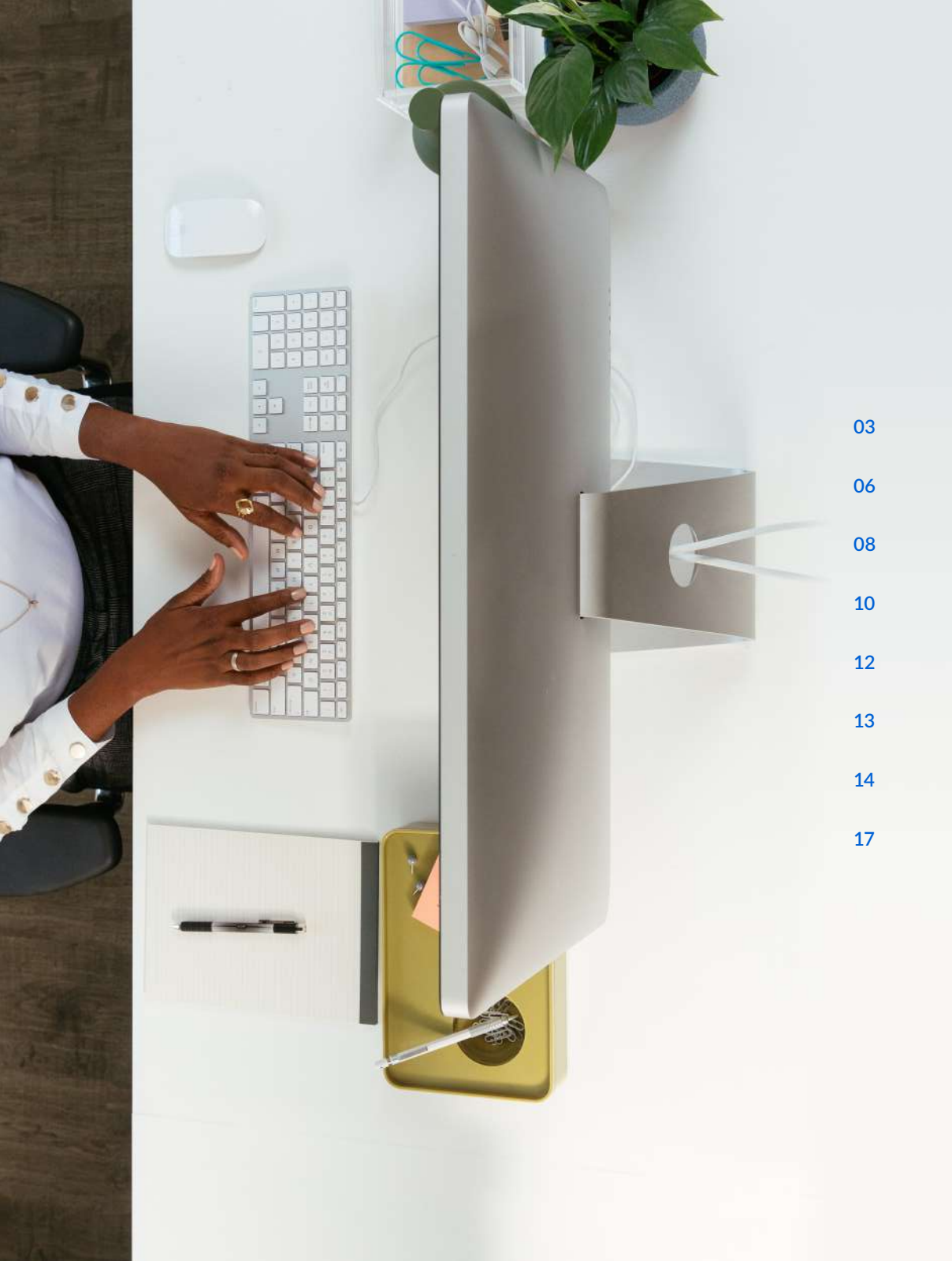


Table of contents

Digital-first companies need digital-first security

With the rise of digital transformation, companies are facing unprecedented challenges to secure their work and maintain compliance across their business ecosystems. As technology and computing processes have changed, IT services have steadily moved from a centralized computing model to a highly decentralized one. Mobility, cloud services and consumer apps have all fueled the need for employees to be able to work anytime, anywhere and from any device.

Meanwhile, the emergence of the extended enterprise means that IT now needs to create a seamless and secure experience not only for onsite workers, but also for remote employees, suppliers, partners and customers. While increased worker mobility and collaboration across the extended enterprise has created immense value for businesses, it has also posed challenges for IT and C-Suite leaders to secure content across a distributed ecosystem.

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

The impact to a company's bottom line after a breach can be high. The global average cost of a security breach today is $3.62 million,[3] and the average cost in the US is $7.4 million.[4]

In terms of a company's relationship with consumers, the damage to brand reputation after a breach is long-lasting and not easily repaired.

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

Fragmented content strategies, shadow IT and overreliance on email can all too easily lead to these damaging vulnerabilities. Of the companies examined by the 2018 Verizon Data Breach Investigations Report, for example, 66% of malware experienced by the companies examined came in via email.[6] Meanwhile, just as threats are on the rise it has become increasingly difficult for security professionals to process the large number of security alerts that come across their desks.

You can't afford to wait to secure your content

Evolving global legislation and regulations only ups the ante for IT leaders to take an active role in managing content and setting security strategies.

After a security breach, the average company

↓ Has a 5% drop in stock price

↓ Loses 31% of relationships with consumers

Ponemon Institute[5]

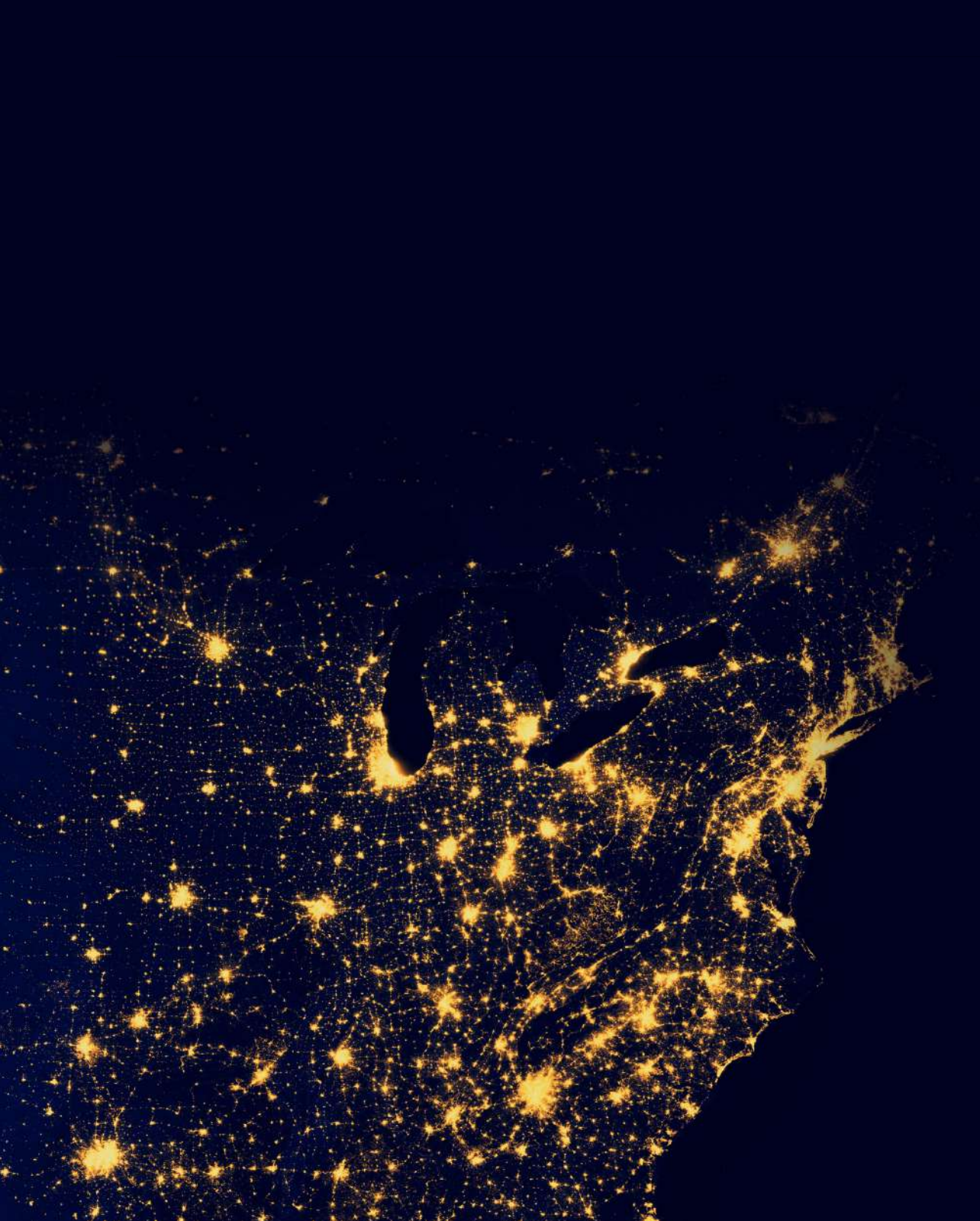
[5] bit.ly/2zvSXWr
[6] vz.to/2qihidi
[7] bit.ly/2n9aVK0

Compliance management requires tackling convoluted industry, line-of-business and geography-specific standards. The European Union's General Data Protection Regulation (GDPR), for example, takes effect in 2018 and tightens regulations around any company handling the data of European citizens and residents, and any company managing such data needs to be ready to comply.

As companies serve increasingly global customer bases and work with global partners across the extended enterprise, they need to be ready to meet regional data governance and residency requirements, or face significant penalties associated with failure to adhere. GDPR violations, for example, can cost companies up to €20 million or 4% of their total worldwide annual revenues, whichever is higher.[7]

At Box, we refer to bringing all of your people, information and applications together in the cloud to transform the way you work as Cloud Content Management (CCM). With security and compliance baked into your content strategy, you get a single, secure system to manage all of your content to prevent these kinds of vulnerabilities and quickly and accurately respond to threats. It's a radically simplified and far more secure way for teams to work together across the extended enterprise.

In the rest of this eBook, we will explore how Cloud Content Management solutions like Box reduce security risks while empowering everyday users, and ultimately provide a modern content platform to help enterprises succeed in the digital age.



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

With the rise of digital transformation, enterprises must rethink how they protect, control and govern data. Mitigating risks means finding ways to manage all the data flowing at higher speeds and volumes than ever seen before. But while trying to protect corporate data, enforce privacy and maintain compliance, companies are also looking for solutions that enable innovation. The challenge before the modern enterprise 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 instead operate on a zero-trust model and never assume that a user or a network is safe. That means we don't just protect a laptop, for example, to protect the data on it. We also protect the data directly. That way, if the machine gets compromised the data doesn't get compromised, too. We also 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 experiences of end users. If users have a bad experience, they're that much more likely to abandon IT-sanctioned solutions and turn to insecure consumer tools. At Box, we aim to make our product seamless and delightful to use, and for security to operate in the background where users don't even notice it.

3

Provide a centralized content layer in the cloud

Centralizing your content in the cloud makes it easier to secure, manage and govern. While many IT organizations rely on a decentralized model of computing, this results in fragmented content and a larger attack surface. Even if you operate on a modern cloud stack, if you don't leverage the cloud as a central content layer you can end up with a massive fragmentation problem. By providing a single content layer centralized in the cloud, Box helps you better protect and govern your content.

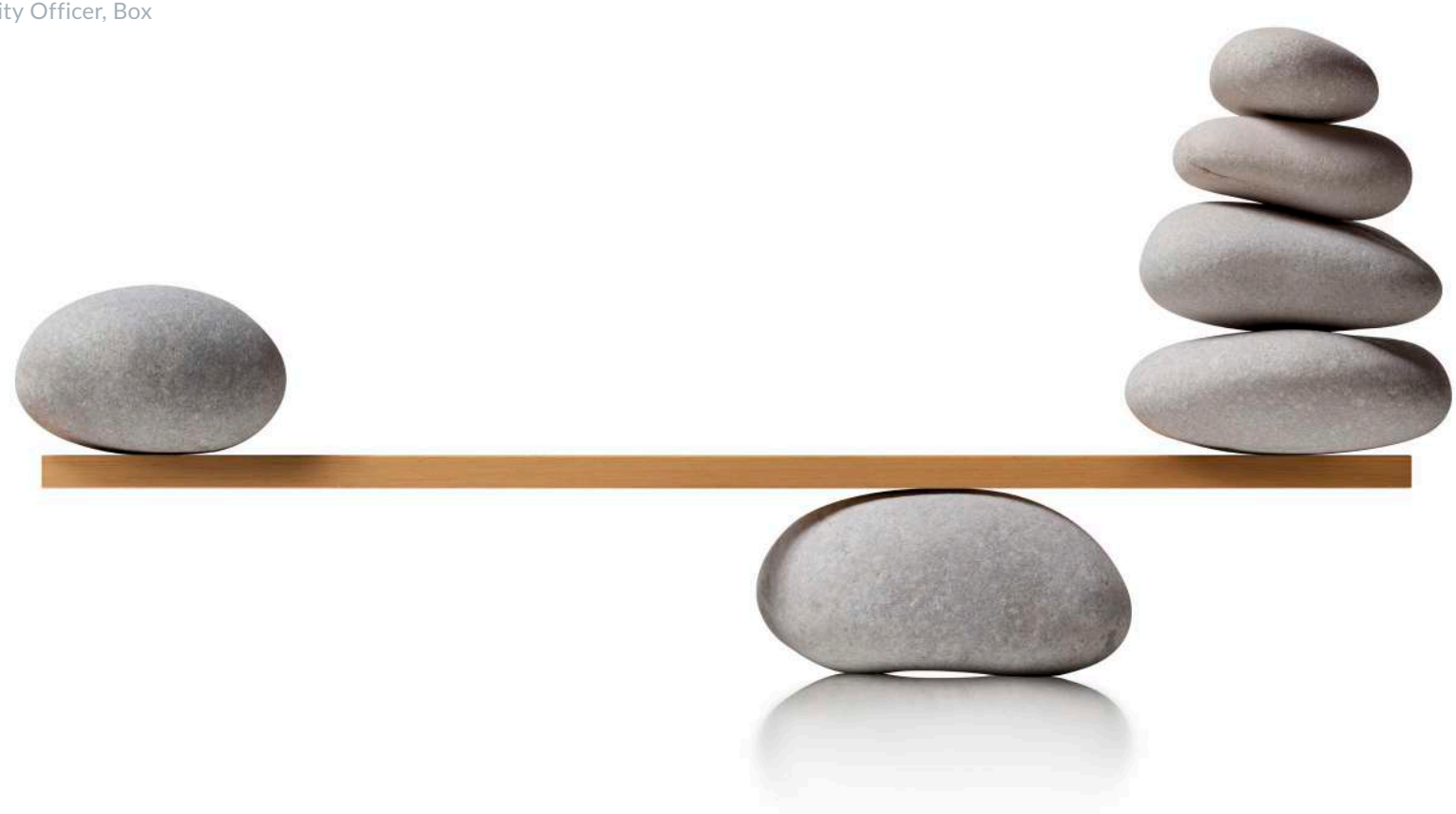
4

Security that travels with your content

Security as a bolt-on, afterthought solution rarely works — you need controls built in to the very fabric of how you manage your content. Not only is your data protected, but that same level of security travels with your content when you work in other applications using Box as your content layer. That means when you work in Slack, Salesforce or any other application while using the Box integration to manage your content, you get Box-level security to go with it.

"The challenge before is similar to the challenge behind us: we need to find a way to balance innovation and security, with a focus on visibility and analytics instead of data control. Only building such controls in from the beginning will allow us to strike this balance. Security as an afterthought never works."

Joel de la Garza, Chief Security Officer, Box



Box security at a glance

End user

Device controls
- Device trust / pin
- Device controls (mobile, sync)
- Remote logout
- Encryption

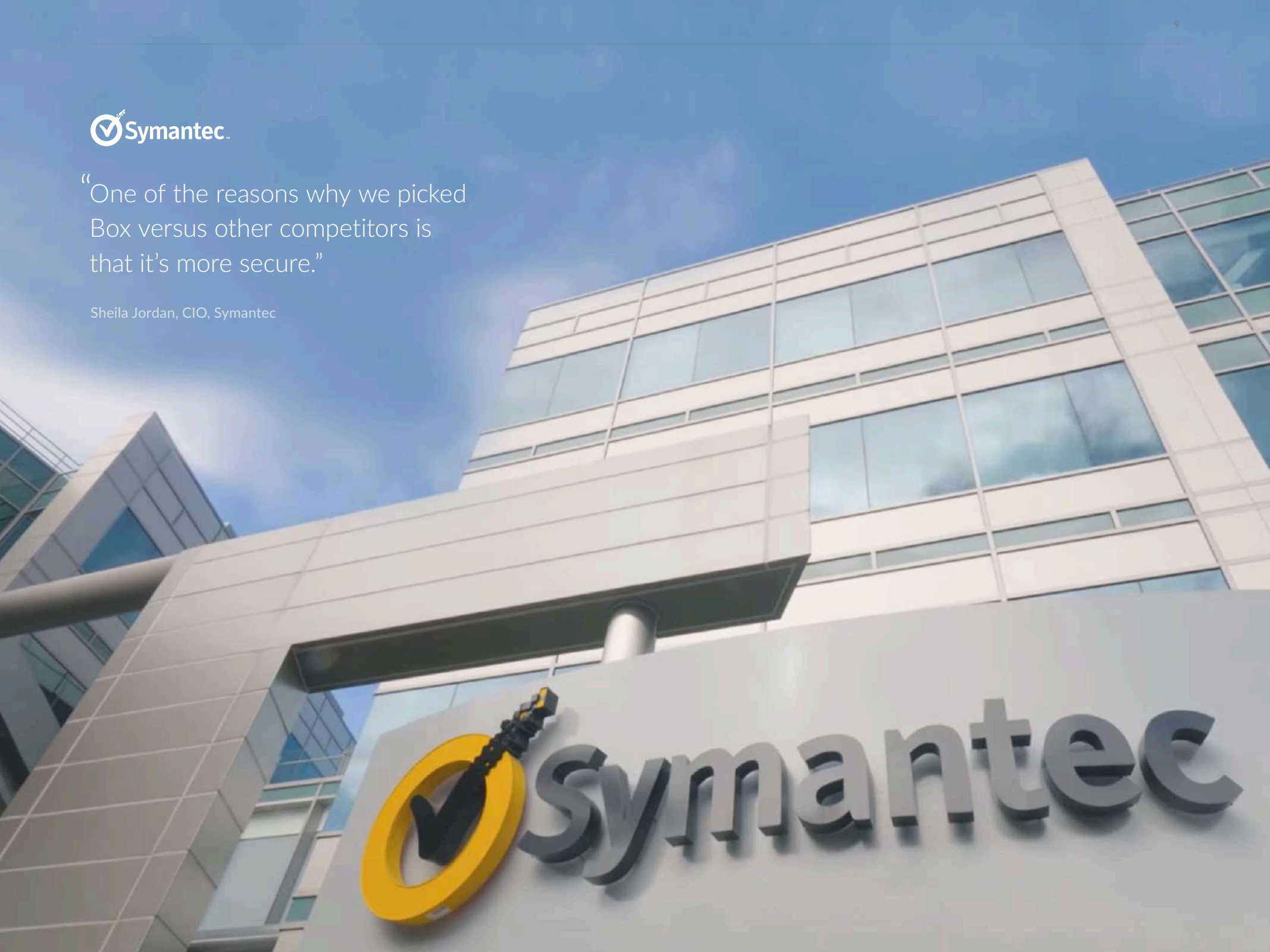
Connection controls
- 256-bit TLS
- HSTS secuirty headers
- IP whitelisting

Authentication controls
- Single sign-on
- Multi-factor authentication
- Password controls
- Domain whitelisting

Content controls
- Granular permissions
- Access control (Trust Viewing)
- Document watermarking
- Content policies (DLP)
- Legal holds
- Retention & deletion
- Content manager & discovery
- Classification-driven policies

Customer infrastructure controls
- Box KeySafe (key management)
- Box Zones (In-region storage)
- Network connect
- Trust ecosystem integrations (CASB, DLP, eDiscovery)

Box operational controls
- Encryption at rest
- SSAE 16 type 2 datacenters
- Access control
- 99.9% SLA
- Compliance program
- Secure SDLC
- Global sec operations
- Intelligence sharing


Symantec
"One of the reasons why we picked Box versus other competitors is that it's more secure."
Sheila Jordan, CIO, Symantec
Symantec

Secure mobility and collaboration

By providing a secure hub to manage all of your content in the cloud, Box makes it possible to secure your employees' collaborative efforts and work product without damaging the end-user experience. Because employees don't have to move back and forth between secure, sanctioned on-premises tools and insecure consumer solutions, they can save time jumping between systems, work more productively and ultimately work more securely by leveraging Box's security while working in other integrated apps. Having a single central content layer embedded across all of your applications also makes Box easier to use, and thereby fosters widespread adoption and prevents the rise of shadow IT.

Here are some of the ways Box enhances user security, mobility and collaboration:

- **Entitlement management** at Box 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 enterprise, and thus boost 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 whitelisting: Allow administrators to restrict collaboration to whitelisted domains
- Device trust: Meet security standards by establishing a minimum set of software or hardware requirements for devices accessing Box
- Remote logout: Admins can log out users remotely
- Access expiration: Expire access privileges to enterprise content after set periods of time

- **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:

- Single sign-on (SSO) with support for SAML 2.0 and ADFS 2
- Two-factor authentication (2FA)

- **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.

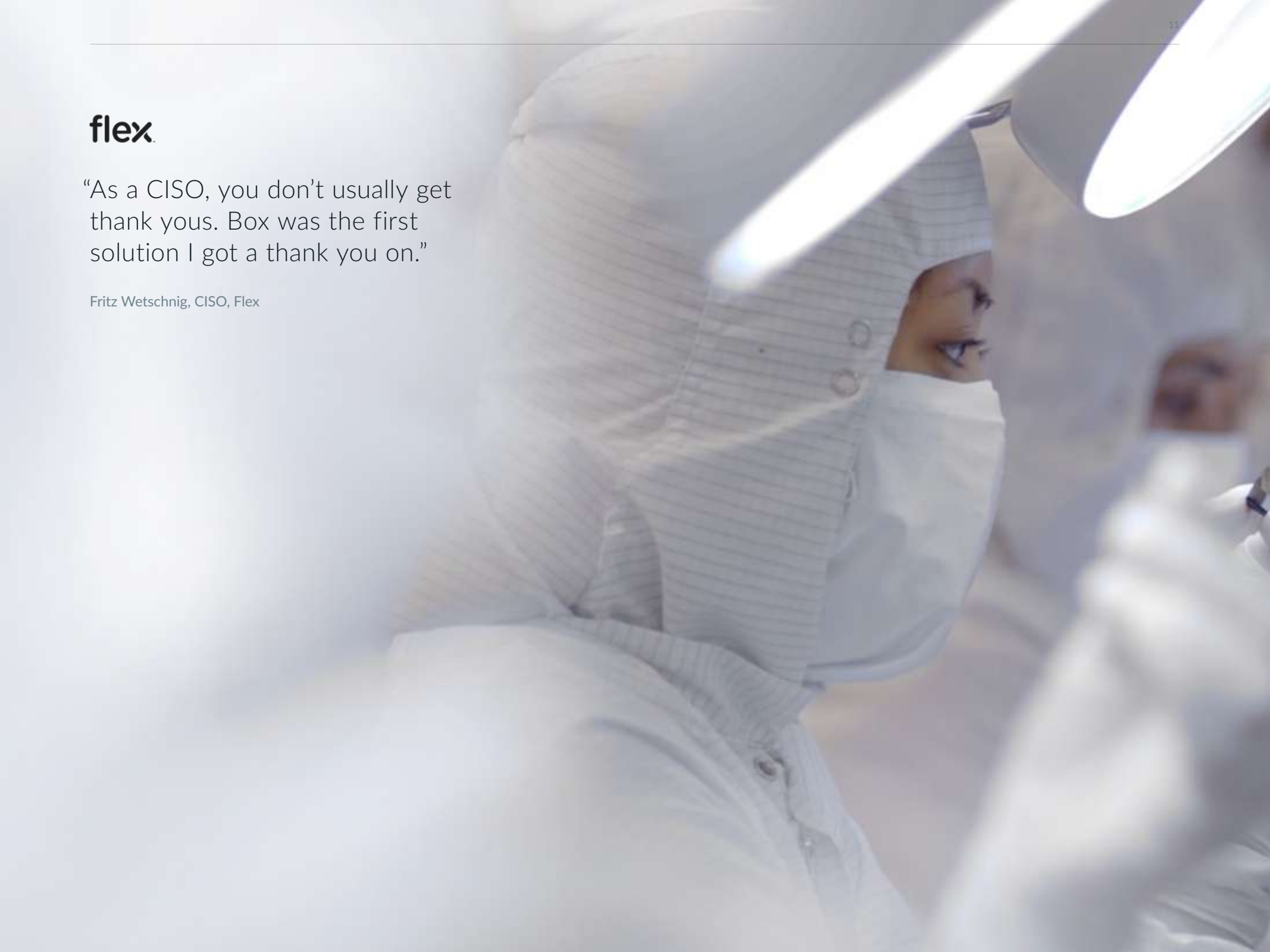
What Box offers:

- Box Governance: Includes a feature to classify sensitive content and enforce policies to prevent users from sharing confidential information inappropriately
- Box Trust: Is an ecosystem of security and governance partners, including data-loss prevention (DLP) and cloud access security broker (CASB) vendors, that extend Box's native security with advanced, industry- and region-specific data-loss prevention policies

flex

"As a CISO, you don't usually get thank yous. Box was the first solution I got a thank you on."

Fritz Wetschnig, CISO, Flex



Information governance, compliance and privacy

- **Governance** capabilities are key for enterprises looking 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 enterprise 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 secure their content.

What Box offers:

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

To learn more about Box Zones, visit www.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, insecure 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:

- **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.

- **TCDP 1.0**
  The Trusted Cloud Data Protection Profile (TCDP) for cloud services is the testing standard for data protection certification in accordance with the German Federal Data Protection Act (BDSG). It represents the legal requirements for subcontracted data processing as a testing standard.

- **SOC 1**
  The Box System and Organization Controls (SOC) 1 Report covers processes and controls relevant to customers' financial reporting.

- **SOC 2**
  The Box SOC 2 report covers security and availability controls defined by the American Institute of Certified Public Accountants (AICPA).

- **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.

- **FedRAMP**
  Box is compliant with the Federal Risk and Authorization Management Program (FedRAMP), the cloud security standard of the US government. This certifies Box to meet additional security and compliance controls to manage sensitive non-classified data for federal civilian agencies.

- **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.

- **GDPR**
  The Global Data Protection Rule (GDPR) harmonizes data-privacy laws and regulations across the EU, protects EU citizens in the area of data privacy and reshapes the way organizations across the region (and beyond) approach data privacy. Box is committed to fulfilling GDPR requirements and has Binding Corporate Rules (BCRs) to enable GDPR compliance.

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

- **TÜV Rheinland**
  German certification body has awarded Box the status of Certified Cloud Service. TÜV Rheinland certifies that Box has implemented and maintained effective processes and controls that meet the data privacy and security objectives as defined by TÜV Rheinland's inspection catalog, which is based on requirements from the German Federal Data Protection Act, EU Data Protection Regulation, ISO 27001, IT Infrastructure Library and ISO 20000.

- **BSI C5**
  Box has achieved Cloud Computing Compliance Controls Catalog (C5) certification as awarded by the German Federal Office for Information Security (BSI). C5 defines the bar that cloud providers should meet when dealing with German data, and combines existing security standards like ISO 27001 with increased transparency in data processing.

- **Department of Defense Cloud Computing SRG Impact Level 4**
  Box has received the Department of Defense SRG Impact Level 4 authorization from the Defense Information Systems Agency (DISA). This allows Box to support the Department of Defense in managing sensitive non-classified data.

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

How Box can help with Cloud Content Management

Corporate history and mission

Box was founded in 2005 to help businesses bring all of their people, information and applications together to transform the way they work. After humble beginnings being born out of a college research project and developed by its four founders in a Berkeley cottage, Box has grown to now serve 82,000 customers and 69% of the Fortune 500. Our in-house consulting arm, Box Consulting, helps companies implement and get the most out of Box, and our nonprofit, Box.org, provides nonprofits with the technology resources they need to innovate and achieve their goals.

How Box can create value for your company

No matter your industry, Box can help 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.

A study by Forrester Research[8] based on surveys and interviews with Box customers found that customers can see up to a 405% return on investment (ROI) and a productivity improvement of over 20% in its first three years with Box.

Try using the Box ROI Calculator (box-roi.com) to learn how your company can save costs, boost productivity and reduce risk with Box.

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

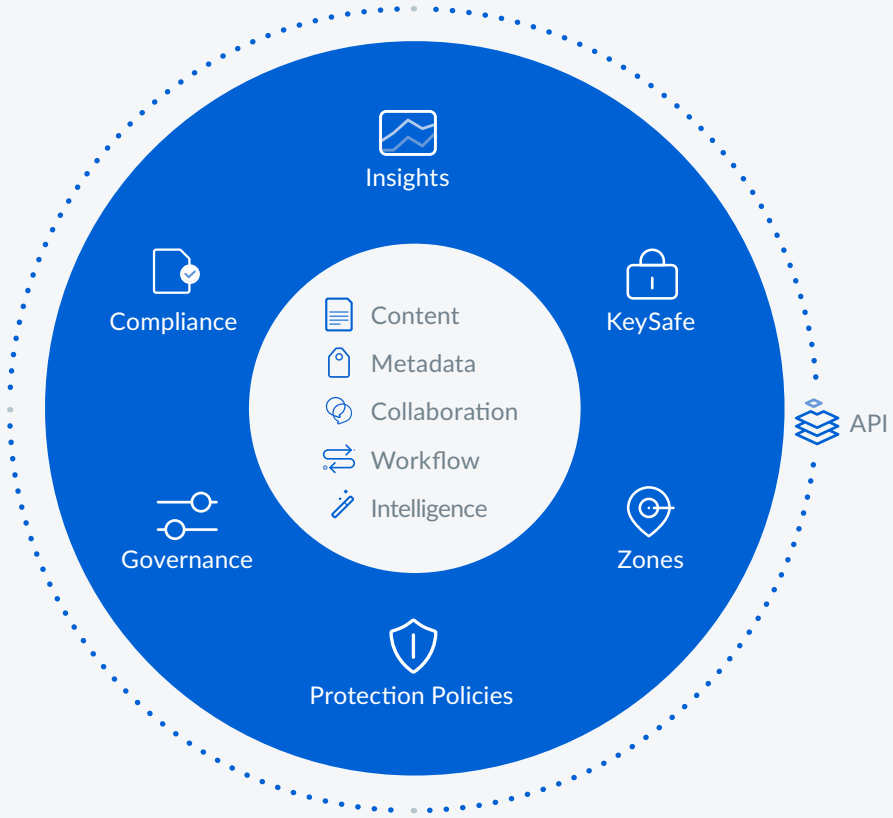
The Box offering

Over the past 10 years at Box, we've continuously striven to build and improve our product to better serve our customers.

Designed for the needs for end users, IT and developers, Box lets you securely manage, share, and organize in the digital workplace.

Meanwhile, you can also efficiently manage the metadata, collaboration and workflows (Box Relay) related to that content to enable your digital business.

We've enhanced the security and hosting services and added a range of features design to meet the needs of enterprises for governance (Box Governance), compliance with a broad range of certifications from ISO to GDPR, encryption key management (Box KeySafe) and data sovereignty (Box Zones). We've also defined and published APIs that enable developers to build their own applications, and are rolling out two innovative machine-learning technologies (Box Skills and Box Graph) to make content more actionable and useful. 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 for Cloud Content Management.



We believe that every company can and should work like a digital company, and that Cloud Content Management is essential to achieving this.

With Cloud Content Management, manual processes become digital and automated. Employees no longer have to spend hours each day or week hunting for information, and productivity soars. Collaboration across the entire extended enterprise becomes seamless, and the latest machine learning technologies help you maximize the value of every piece of content you have. No more siloed content, no more searching for information.

With Cloud Content Management by Box, you can finally work as one.

To learn more about Box, visit www.box.com/security