box

Securing Business Information in the Cloud

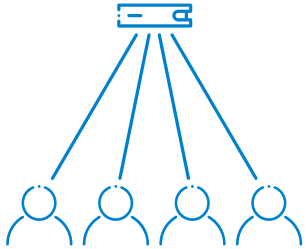
For security and IT pros concerned with protecting sensitive information across multiple endpoints and applications. Explore how cloud can enable us to go back to basics of security to address the challenges of distributed computing and make our organizations more secure.

Address the Security Challenges of Distributed Computing

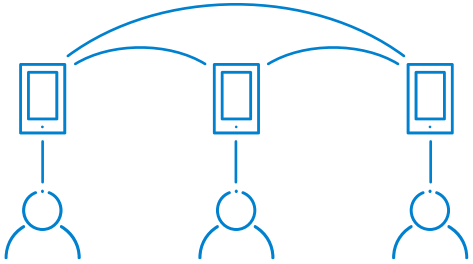
Since the days of the mainframe, IT has steadily moved from a centralized computing model to a highly decentralized one. This shift accelerated in the last decade, fueled by mobility, cloud services and service-oriented platforms. This has created immense value for IT and end users, but adapting security controls and tools to a decentralized architecture has proven difficult.

As a result, the modern enterprise is burdened with challenges like insecure devices and communications, content proliferation inside and outside the company, and the constant risks associated with human error.

Mainframe Centralized Model

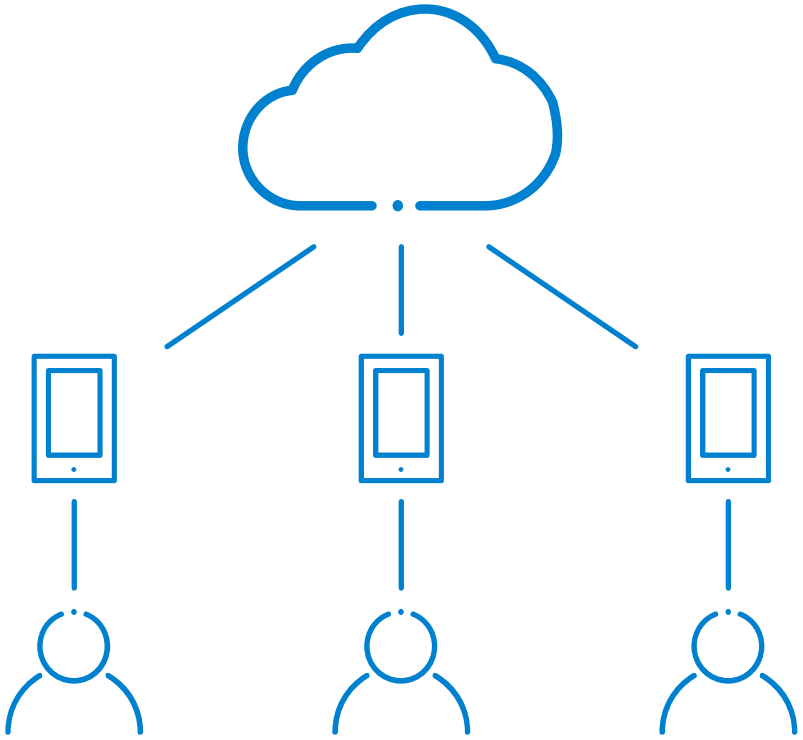


Mobile De-Centralized Model



Restoring Centralization, Control and Security

Cloud-Based Re-Centralized Model



However, a new generation of secure, enterprise cloud services creates the opportunity to mitigate many of these security challenges by centralizing documents onto a single cloud platform.

Today's Challenges

Distributed Computing Security

Insecure Devices

Stolen devices

Lost devices

Insecure backups

4.3% of phones used by or issued to employees are lost or stolen annually.

McAfee and Ponemon Study

Insecure Communication

Email attachments

FTP

Mailing CDs / USBs

58% of Sr. managers have sent sensitive information to the wrong person.

CSO Magazine, Study by Sroz Friedberg

Content Proliferation

Duplication of files

Use of online apps

19 file sharing services are used on average in a single company.

Skyhigh Networks, Study of 100 companies

Human Nature

Smart people / dumb actions

Organized crime

State / Corp. espionage

54% of security breaches are due to human error.

CompTIA, Study 2012

Centralization of Content is Critical to Cloud Security

Why is centralization in the cloud so critical?

Many organizations associate more risk with putting business information in the cloud. But in actuality, cloud technology (and secure providers of cloud services) can be a safer and more secure choice. And using cloud services to centralize and manage information can significantly boost security and mitigate risk.

To begin with, a smaller, well-managed attack surface is easier to monitor and secure than a highly distributed one. Centralization also makes it easier to manage multiple layers of defense, log every event and implement consistent access controls across endpoints. Even things that are difficult to accomplish today are attainable through centralization. With the proper reporting and control mechanisms, we can find out who has access to any piece of content, control access to content by outside parties and on mobile devices, and achieve full transparency across every event, user and administrative action.


Smaller Attack Surface


Layered Defenses


Comprehensive Logging


Consistent Access Controls

Centralization is critical for business processes because it supports the multi-party cross-firewall communications scenarios that are required for the extended enterprise to operate. Because the centralization is occurring, not on the corporate network but on the Internet as SaaS, we can finally apply identity, authentication and authorization beyond the confines of a single organization. As a result we allow for the security of content to align with how the business actually works — sharing information beyond borders.

Centralization of Content is Critical to Cloud Security

Moreover, by actively managing a centralized cloud platform, instead of playing defense against a constantly shifting threat landscape we take the offensive with smarter approaches to tackling challenges like:

Secure business process communications

Data Loss Prevention (DLP)

eDiscovery support

Incident response

We see an emerging opportunity.

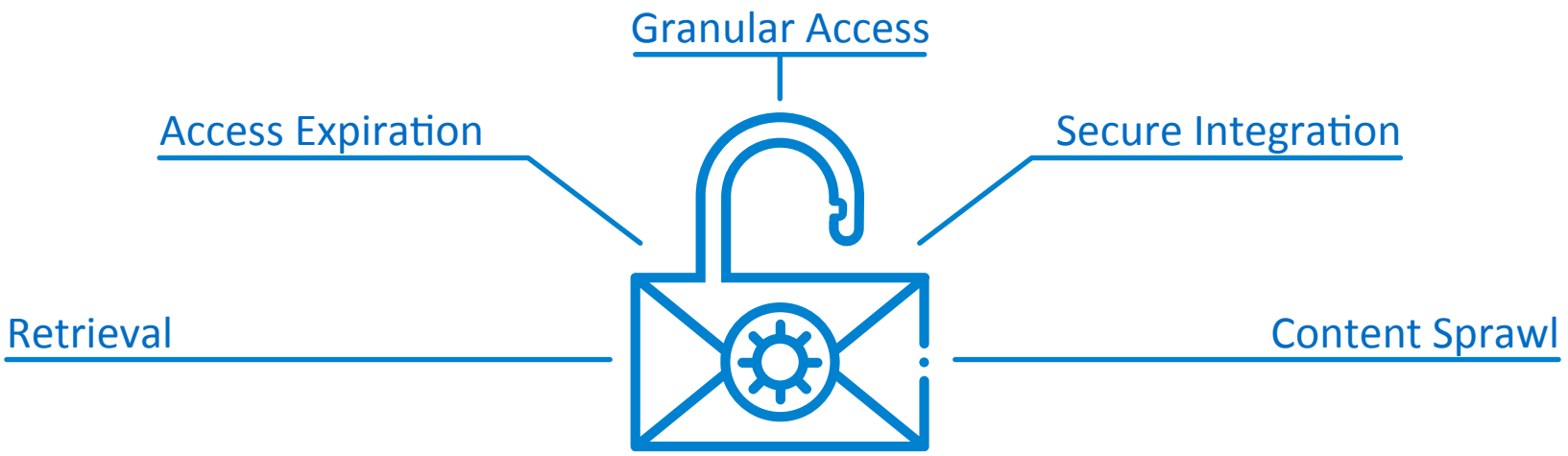
Secure cloud platforms like Box enable companies to better centralize, control and secure their documents and unstructured data than legacy, on-premise systems have enabled. Let's look at how Box can help you tackle some of the traditionally "unsolvable problems" related to business content.

Secure Business Process Communications

Getting work done requires communication with multiple internal and external parties. However, content management systems that meet the needs of many inside-the-firewall scenarios fail at external communication. Before Box, many companies were forced to set up externally hosted instances of on-premise systems in order to collaborate with a supplier or go through the lengthy process of justifying the addition of an outside party to the company's internal applications. Due to the complexity of these solutions, workers resort to other tools such as email and consumer file sharing tools, which offer easy ways to share with anyone and highly useful user interfaces.

> *"The idea that organizations can increase security by centralizing control of their content in the cloud is far from obvious. But when organizations carefully extend existing controls into a security-conscious cloud service like Box, it may be possible.*
>
> **John Oltsik, Terri McClure**
> **Enterprise Strategy Group**

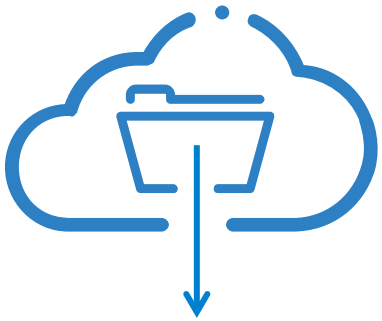
The Problem with Email Solutions



Unfortunately, email is insecure.

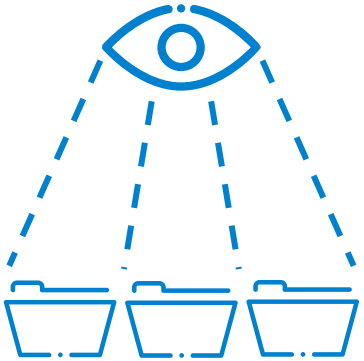
Most implementations lack encryption in transit. Once a file is sent, you can't retrieve it. You can't expire access to an attachment. You can't define granular access rights for different recipients. And you can't securely integrate email with business process applications because the bolt-on security solutions for email do not integrate with common business process applications. Most importantly, email accelerates content sprawl across applications and endpoints, with each app and endpoint storing yet another copy. Enforcing security controls becomes a non-stop game of whack-a-mole.

Insecure File Sharing Tools



There are 24 cloud file-sharing tools in the average organization, according to data collected by Skyhigh Networks.

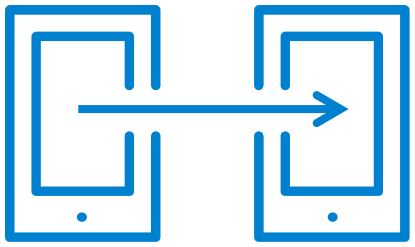
Over 54% of the more than 380 different services examined don't support encryption at rest and 15% still don't support encryption in transit. More than 81% also don't support two-factor authentication. And unfortunately, federated identity is still lagging overall with only 15% of cloud providers supporting SAML or OAuth. And some tools have privacy policies that give them ownership of your business data.



Even the tools that claim to support business needs usually lack granular access and sharing controls.

Once you let someone from outside your organization into a folder, they have full rights to everything. These same tools also often fail to preserve file metadata like date and time stamps on upload as well as lack global search capabilities and other functionality required to support a defensible eDiscovery process. Other limitations include lack of mobile controls, integration with common security and IT management tools, and compliance certifications like SOC 1 and ISO 27001.

Insecure File Sharing Tools



Consumer file sharing tools not only fail to provide the centralized administration and visibility you require,

but they also increase the risk of attacks against your organization and intellectual property. Most firms are aware of the most popular offenders and often block the well-known names. The problem is that new players are constantly popping up. We can keep trying to patch the leak, or we can deal with the root of the problem by offering the end-users a secure, easy-to-use alternative that also provides the centralized control that IT and security teams need to their jobs.

What if we could stop using insecure consumer tools to exchange sensitive files,

and stop using email as a document management system for attachments? We can remove sensitive IP from insecure channels, reduce risks associated with PST files and consumer-focused cloud repositories, and drive security controls into communications.

Creating Secure Business Process Communications

Centralizing content and collaboration in the cloud can:

Assure encryption at rest and in transit.

Box supports 256 bit AES at rest. In transit, Box supports SSL 3.0, and TLS 1.0 through 1.2 for the web application and API. We use 2048-bit public keys in our certificates, and support only high-strength symmetric ciphers.

Monitor, revoke and expire access.

Comprehensive audit trails show who accessed each file, when and whether they've viewed, downloaded, or updated a document. With a secure link, you can add a password, set an expiration date, and revoke access at any time.

Define granular access rights.

You can invite partners to collaborate inside a folder and chose from 7 different access rights - from upload only, to view only, to full folder control. With secure links, pick from 10 options by determining the audience and their access rights.

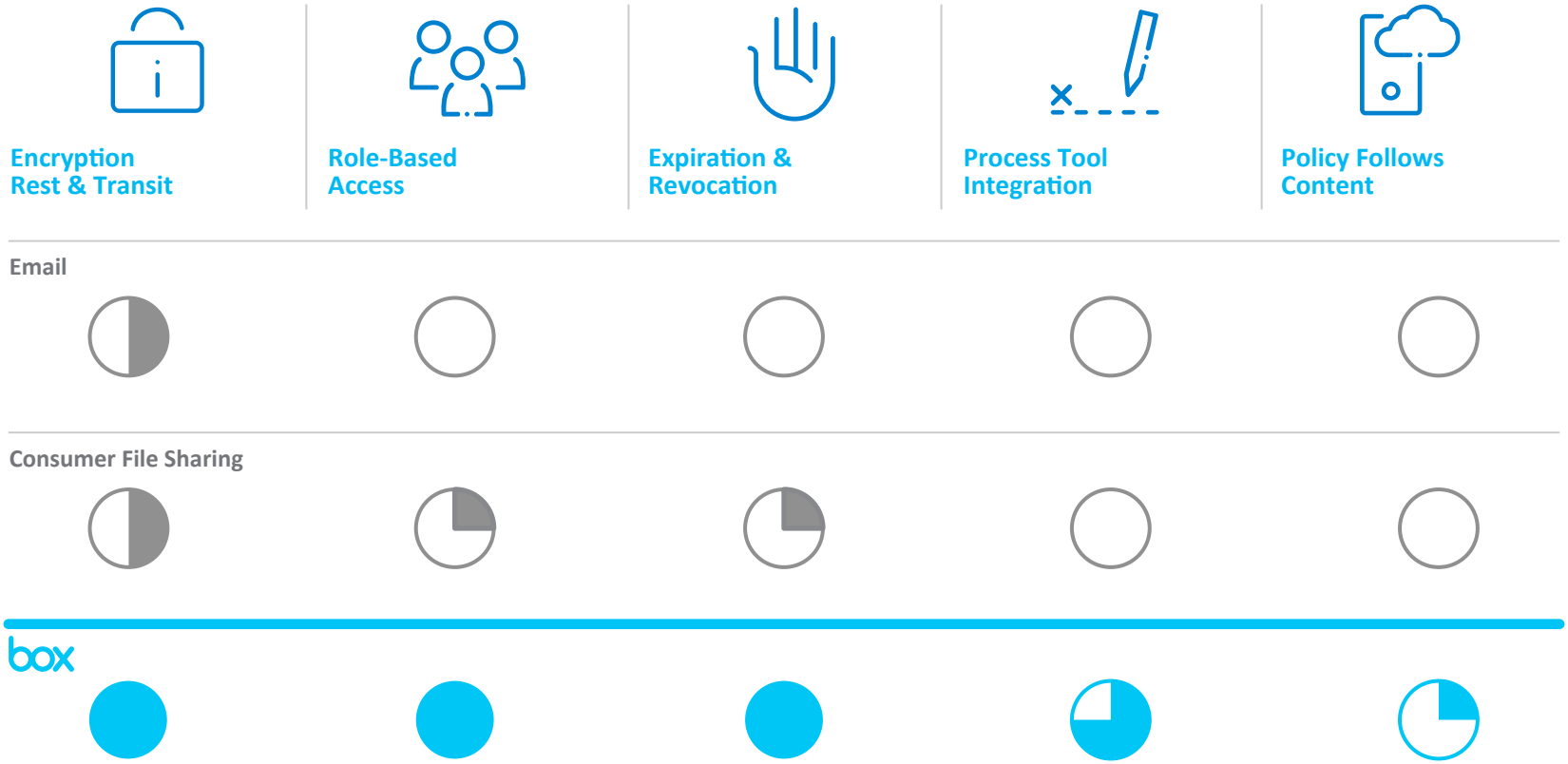
Extend your security policies to outside parties.

You can't dictate email password policies of your business partners, but you can require compliance with your Box policies and acceptance of your terms of use.

Integrate content into business process applications.

Box Embed creates a secure view onto Box content inside other applications like Netsuite, Jive, and Salesforce, and DocuSign. This eliminates content sprawl and provides one secure place to manage confidentiality and integrity of your business information.

Box vs. Consumer Solutions



Data Loss Prevention

Data loss in a distributed environment is a complex and expensive problem.

With the average cost of data breaches reaching as high as $5 million, we need to consider different approaches. Centralization in the cloud can help alleviate the three main reasons for data loss: good people doing bad things, device loss or theft and attacks by malicious actors.

> *“Box has mitigated the risk of having the company’s Intellectual Property in many cloud services without appropriate security controls. Box has blazed the trail on how to handle desktop documents in the cloud securely.”*

Doug Harr
CIO, Splunk

Good People **Doing Bad Things**

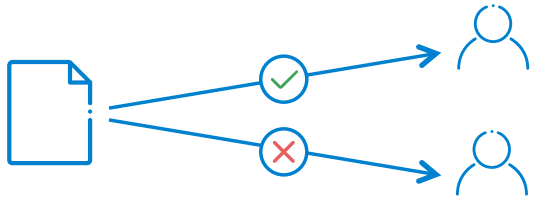
Device Loss or Theft

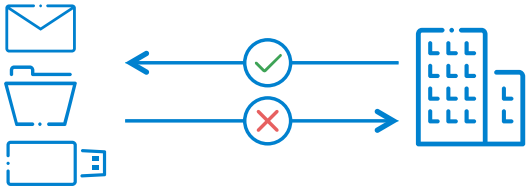
Malicious Actors

Good People Doing Bad Things

Revoke Access of Unintended Recipients.

Prevent breaches before they happen. A mistyped email address is a common reason for a breach, but it doesn't have to be. With Box you can remove the shared link and see whether anyone accessed the file.





Address Root Cause of Bad Behavior.

Poor usability (e.g. complex products, file size limits, slow VPN connections) of enterprise-sanctioned products is the root cause of reliance on personal email, USB sticks and consumer file-sharing services. These are often used to take files home from work or to collaborate externally. Box overcomes these issues by providing an enterprise-grade service with a consumer-quality UI and ubiquitous access to the work files.

Prevent Accidental Leaks of Sensitive Data.

Box Content Security Policies can detect and quarantine files containing SSN #, Credit Card and specific terms. Additional data loss prevention capabilities, including industry-specific and international templates, are available via integration with Skyhigh Networks, CipherCloud, and CodeGreen Networks. Through these integrations you can connect Box with DLP solutions from companies like Symantec and other vendors that support the ICAP protocol.

Device Loss and Theft

Here is a common scenario: An employee leaves their device in a cab or at an airport. IT now has a problem because the employee doesn't know what data was sitting on the device. Should they issue a breach notice? Can they wipe the device? Moreover, significant work products and valuable IP can be irrecoverably lost if they weren't backed up.

Take informed action.

Because the content is centralized in the cloud, you can use our Content Manager tools to find out exactly what files were accessible to the user and determine whether breach notices are necessary.

Work doesn't stop, data isn't lost.

Your employees shouldn't have to stop being productive due to a lost or misplaced device. Because content is centralized, employees can access an important presentation on another device. Another benefit is the ability to quickly sync files to a new device and recover an employees documents.

Protect data on a lost device.

Box allows you to enforce a pin code to access the mobile application, turn off offline access and remotely log out users. Additional controls like enforced device encryption and remote wipe are available through our pre-integrated MDM partners.

Malicious Actors

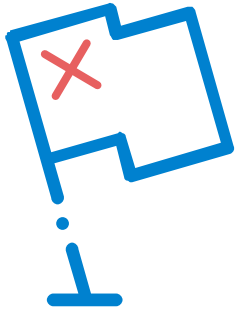
Recover important files.

Some organizations experience disruptive attacks like CryptoLocker. This is a particularly nasty type of ransomware that locks all of your files with high-grade encryption and demands a ransom for the decryption keys. Because Box creates a new version of the file each time it is saved, the CryptoLocker attack simply creates another version without affecting all previous versions. Box customers can do a quick restore by deleting the affected version and reverting back to their last good version, without losing data. File versioning also provides recovery in case of malicious insiders or accidental overwrites.

Protect your data against some types of APTs.

A common approach for APT (Advanced Persistent Threat) attacks is to use a spear phishing campaign to compromise an endpoint, get access to PST files and other sensitive information on the device and then exfiltrate the data. You can reduce risks and eliminate attachments, by quickly sending shared links via our email client and desktop integrations. For further protection, prevent downloads of specific files or folders, forcing users to view files online. Box is not a solution to all APT attacks on its own and should be used in combination with other security tools, but Box can reduce risks associated with highly sensitive data commonly stored on endpoints.

Malicious Actors



Defend against compromised credentials.

Stolen credentials are another common method for sophisticated attackers to obtain your intellectual property. Unfortunately, most enterprises still don't use 2FA (two-factor authentication). Box offers native 2FA capabilities and allows you to enforce these. We also partner with SSO providers like Okta, Ping and others who offer 2FA solutions like time-based passwords generated by a smartphone app to reduce risks associated with compromised credentials.

Protect against insider threat.

Box includes alerts of unusual download activity specific to your organization and alerts of folder collaborators with domains on watch lists. Full activity logging captures all actions of users and administrators. In addition, security reports capture every security settings change, who made it and when. By integrating Box logs into your SIEM system or MSSP, you can get complete visibility and alerts of suspicious activity around your content.

eDiscovery Support

eDiscovery requests happen to every organization.

As the volume of ESI (electronically stored information) continues to grow, so is the frequency and cost of eDiscovery. Box provides a secure, auditable repository that can be integrated into a defensible eDiscovery process. With centralization in the cloud you can simplify the identification, preservation and collection steps to reduce costs and shorten time to resolution.

A recent study of preservation costs by a University of Chicago Law School professor found that collaboration tools have fewer incidences of "preservation-related problems" than email and hard drives and that this difference is statistically significant.[1] The average expenditure can reach $1.8MM in 2012 and involve about 30 GB of data per matter on average.[2]

> *"Among data types, email and hard drives are the most common source of preservation difficulties for companies of all sizes."*[1]

1. Source: http://www.ediscoverylaw.com/files/2014/02/Hubbard-Preservation_Costs_Survey_Summary_of_Findings.pdf

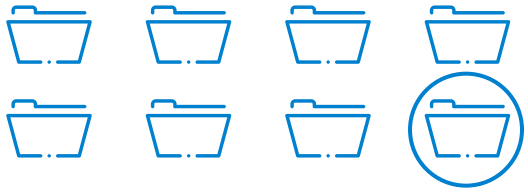
2. Source: Institute for Civil Justice, A Rand Law, Business, and Regulation Institute, 2012

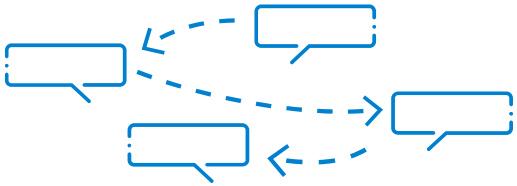
Note: Provided for illustration purposes only and shall not be deemed legal advice.

How Box Helps Your eDiscovery Efforts

Identification.

Instead of searching hard drives and multiple file servers, Box allows you to search across all Box content owned by your custodians using various combinations of filters. Unlike other cloud services, Box preserves file metadata on upload and also provides access to comprehensive audit reports so you know who created, edited, downloaded or viewed a particular piece of content and when.



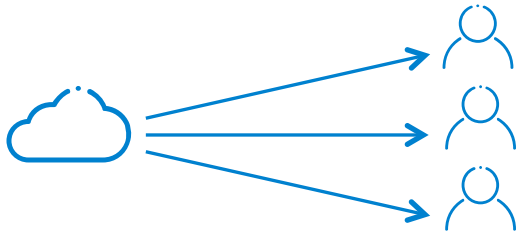


Preservation.

With Box, you can turn off deletion of content to preclude custodians from destroying relevant information. You can also capture every notification email sent by Box with our Compliance Email Archive. This gives you a contextual audit trail of comments, notifications, and action items that were shared via email notifications.

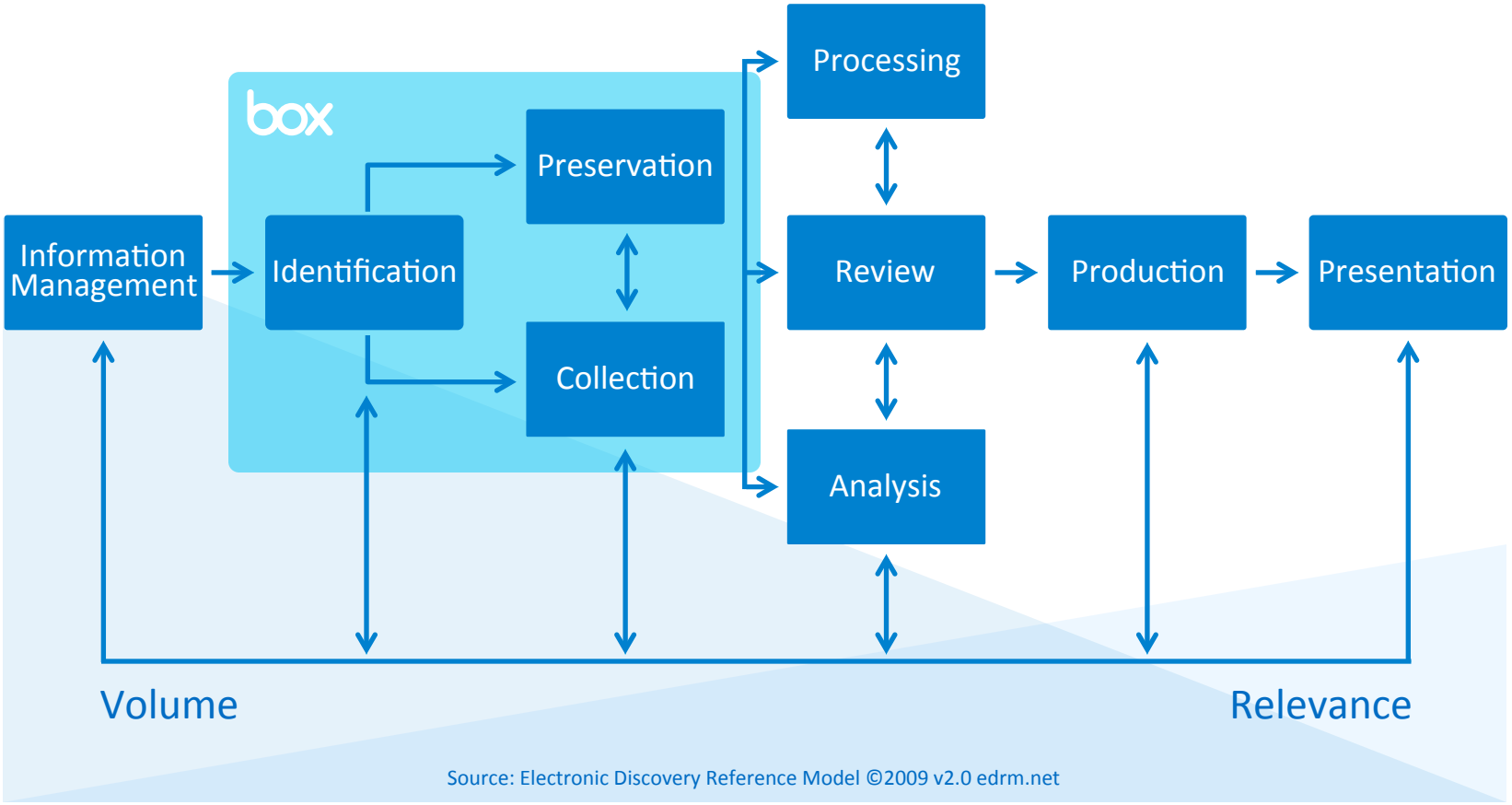
Collection.

Instead of copying hard drives, you can export a user's entire file tree with up to 50 levels; the user doesn't even have to be in the office. Or you can export all content of a specific folder. In addition, the pre-built integration with EnCase eDiscovery from Guidance Software provides a powerful set of tools to identify, preserve and collect ESI stored in Box. This is especially helpful for customers who manage multiple matters that involve data stored in Box.



Where Box Helps eDiscovery

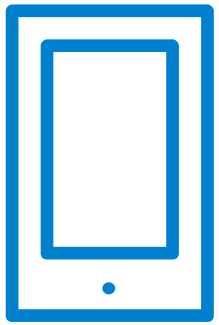
Electronic Discovery Reference Model:



Source: Electronic Discovery Reference Model ©2009 v2.0 edrm.net

Untether Your eDiscovery

You can also mitigate challenges that are difficult to address with on-premise solutions:



Overcome privacy & technical challenges of BYOD.

How do you find files on a mobile device that belongs to an employee? Because Box has mobile applications for all major platforms and syncs the data to the cloud, you don't need access to the device to view and search the files. You also avoid concerns of violating employee privacy because you search only those files that reside inside the corporate Box application.

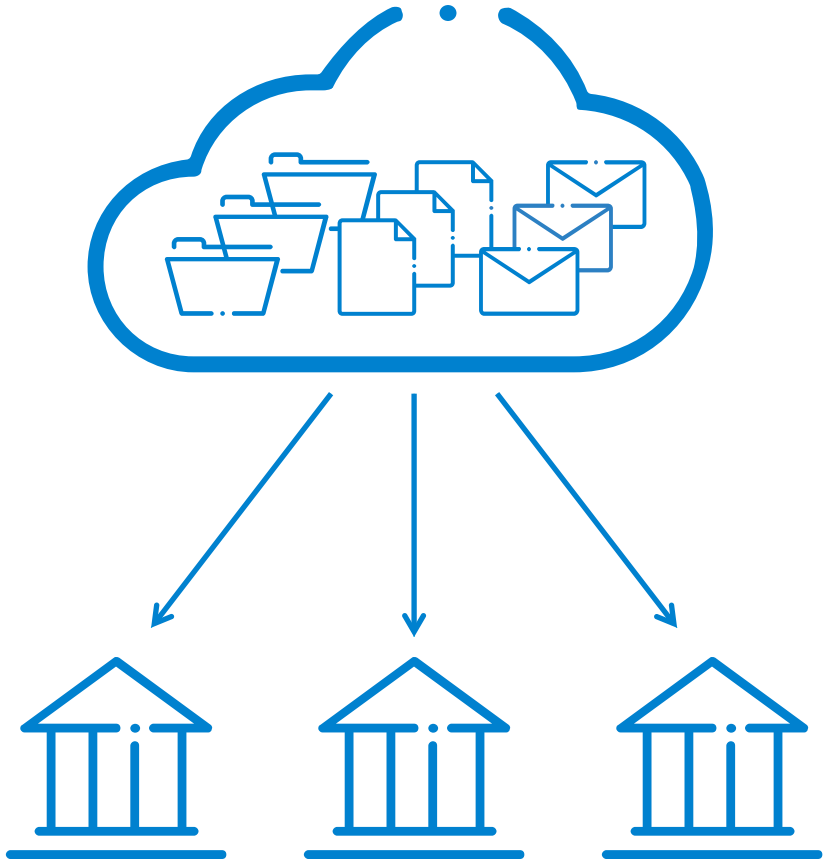
Leverage outside resources for discovery.

With Box, you can grant your outside counsel access to search for relevant ESI or create read-only copies of specific ESI for them to review. Either way, you're taking the workload off your legal team that is usually not staffed for handling large requests and transferring it to an outside party that can be located in a lower cost region.

Data Centralization: The Key to eDiscovery

By enabling you to manage and centralize content in the cloud,

Box simplifies eDiscovery request responses while reducing the impact on your employees, IT, and legal teams. To further assist customers, the Box Consulting team has developed a service to advise customers on Box configuration and implementation options to support eDiscovery. This service includes methods for identification of content, implementation planning, configuration to support your current process, and documentation of relevant eDiscovery features.

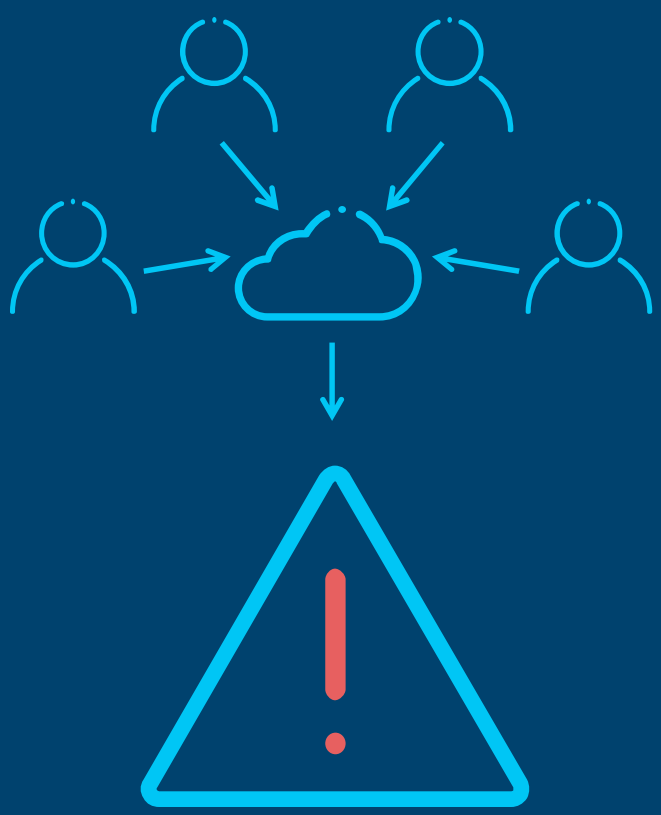


Incident Response

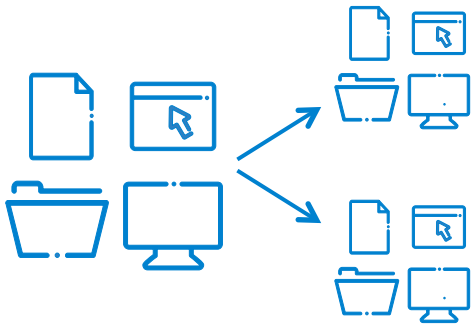
Security is not just about prevention.

It's also your ability to respond quickly when an event occurs. Rapid response is becoming more and more important as the number and sophistication of attacks continues to grow.

When incidents happen, your response team needs to come together to investigate. For critical incidents, even more parties come into the play (law enforcement, PR agencies, etc.). Box enables secure exchange of sensitive content related to the investigation and collaboration around it.

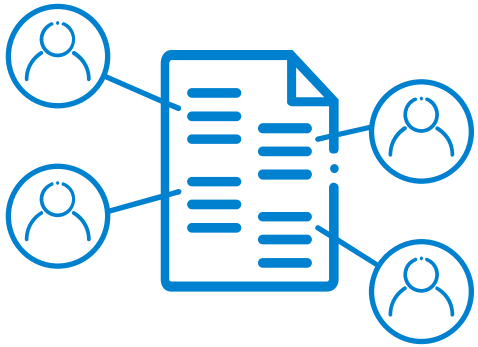


Centralization and Collaboration: The Key to Incident Response



Quickly spin up an incident response workspace.

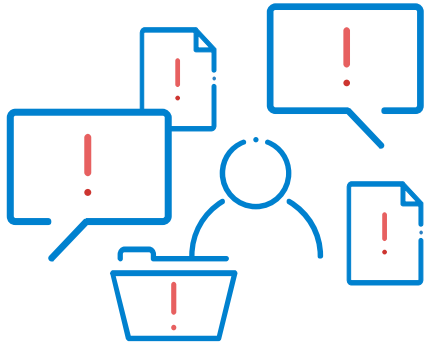
The IR (incident response) team can set up several types of instant workspace templates, which include specific folders, templates and links to resources and applications. When a new incident investigation kicks off, they can quickly create a copy of the workspace and get to work.



Keep the team on the same page in real time.

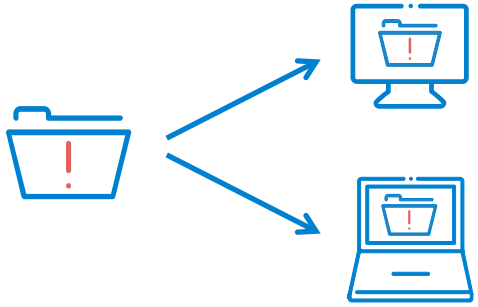
When incidents occur, the team needs a common place to share the most important updates, commonly known as IR Doc (Incident Response Doc). Box Notes – the ability to create collaborative notes in Box with other users - allows IR teams to simultaneously gather in the same place and see each other's updates in real time. No more saving and opening files or questioning whether you're looking at the right version of the document. Notes Heads (an icon of the author's profile photo) show who is editing which part of the IR Doc.

Centralization and Collaboration: The Key to Incident Response



Protect the team from distractions.

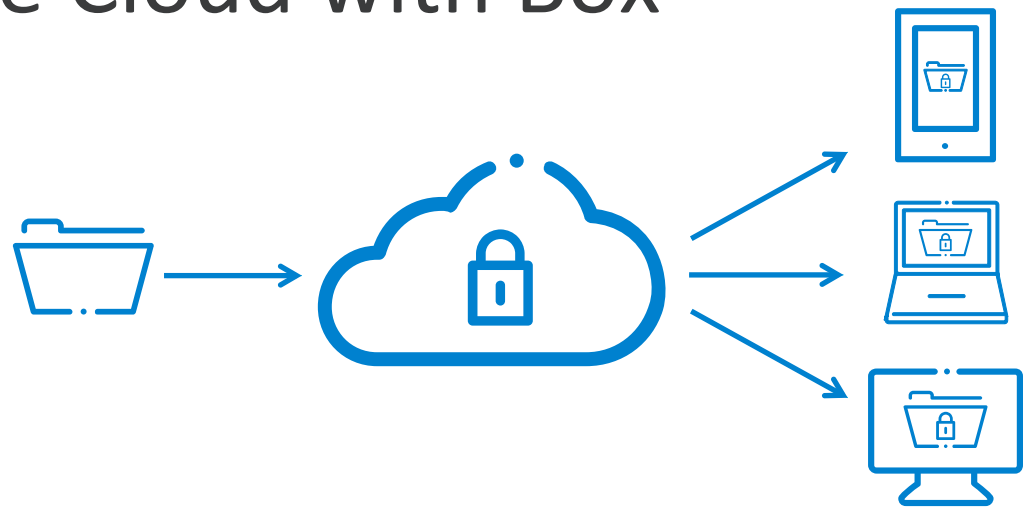
When an incident takes place, the management team will expect frequent updates. With a serious incident, the IR team will be tired, catching brief periods of sleep under their desks, and too busy to provide updates. Box gives you multiple options to reduce the possibility of missed updates. The IR team lead can share a status report and see which managers and executives have looked at it or set up proactive notifications whenever a certain file is updated. Either way, your IR team can focus on what they do best.



Collaborate and share incident data with outside parties.

Sharing screenshots, log files, and other sensitive data during an incident must be done quickly and securely. Box provides multiple methods for sharing large files, includes powerful image preview and eliminates confusion caused by email attachments, which can interfere with a course of a fast-paced investigation.

Extend Your Security Strategy into the Cloud with Box



Centralizing information allows us to convert the well-known maxim "create once, use many" into "secure once, use many."

You can manage your business content, wrap policies and controls around it and provide authorized and confidential access wherever the business needs it. This approach seems counter-intuitive at first. However, when we analyze Box's ability to secure business communications, reduce data loss, support eDiscovery and accelerate incident response, centralization of content in the cloud is not a risk. It's a risk mitigation strategy for several of the most difficult security challenges faced by modern businesses.

Box can help extend your security strategy into the cloud. You have made investments into tools and controls—our goal is to integrate with them to give you the assurance and the transparency you need to enable your business users to work securely and effectively.

That's the core of our Customer Protection framework, which is made up of five key focus areas.

Five Themes of the Box Customer Protection Framework

Content Protection

In addition to the expected encryption and content integrity Box provides, you can enforce content security policies, device compliance, and strong passwords. Box also integrates with DRM and DLP tools to secure your most confidential content.

Account Protection

At Box, identity is protected with directory integration, groups, as well as SSO and ADFS integration. Authentication controls include 2FA, custom terms of service and session expiration. Our platform also includes configurable admin roles and fine-grained authorization for collaborators and links.

Device Protection

Limit the number and types of devices that can access your content with device pinning, or enforce the use of MDM-compatible apps. Enforce application passcode locks and device encryption (on Android or via MDM), and report on device usage.

Application Protection

Leverage our resilient infrastructure, full logging and integration into security ecosystem to build your applications. Take advantage of over 1,000 mobile productivity apps and authorize which can access Box. Use Box Embed to integrate into web applications to stop content sprawl.

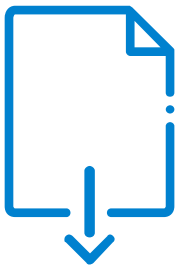
Transparency

Every action and activity is logged and available for reporting. Our reporting API supports integration with SIEM and BI systems like Splunk and ArcSight. Get immediate access to audit reports and benefit from our ongoing compliance and penetration testing.

Data Centralization: The Key to Information Security

With sensitive business content, security and transparency are critical. Talk to us to learn how Box can make you more secure without making your job more difficult and more importantly where and why you can trust us to enable your security strategy.

To learn more about how Box can help you secure business content, take a look at our whitepaper:



Redefining Security for the Cloud

(Download Now)