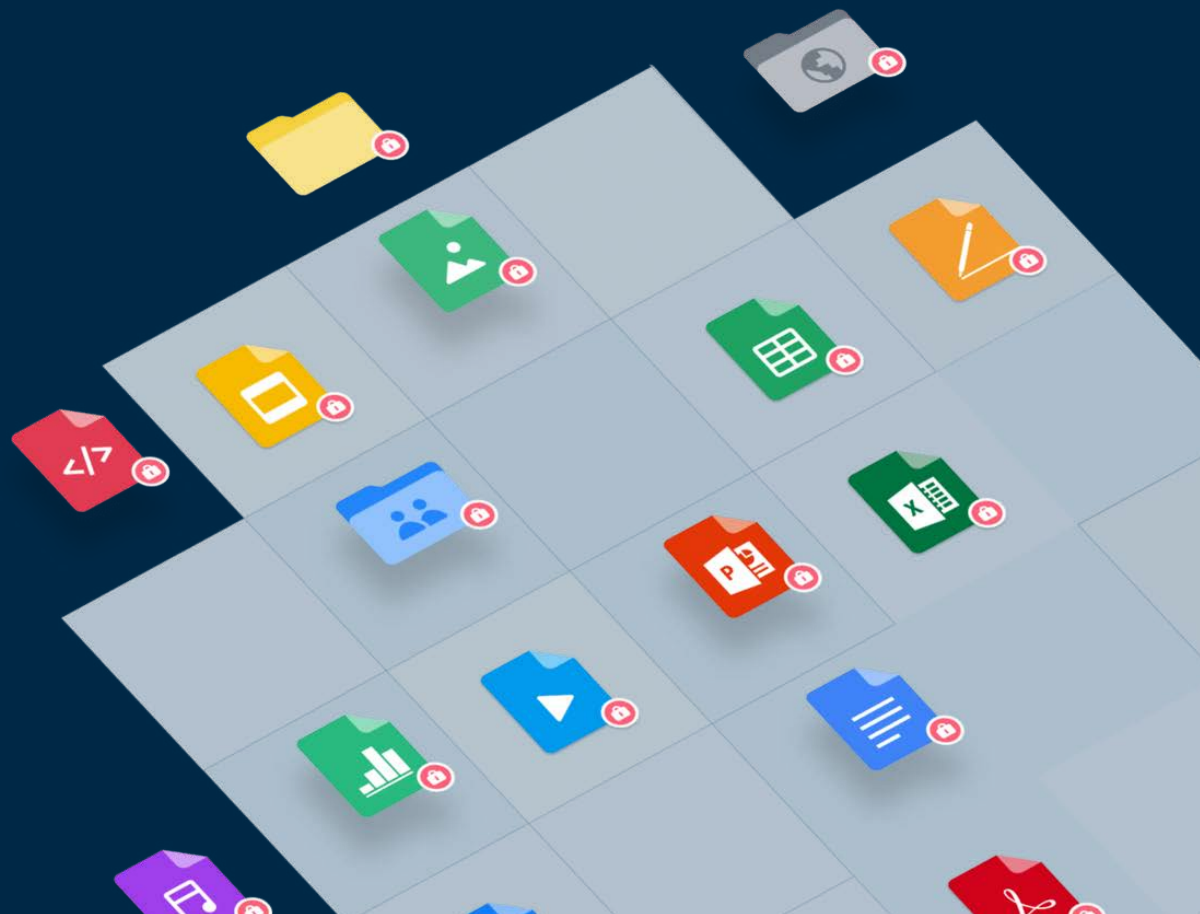
box

Protecting your content against cyber threats and data loss



Content is your business

Valuable assets like sales contracts, product specs, marketing assets, and videos are at the heart of every process, no matter your industry. But your content faces constant threats from malicious hackers and even well-meaning employees.

Access to corporate networks tended to be more controlled pre-Covid as employees were either in the office and secured via local and network credentials or used VPN to access systems. In both cases, employees are accessing content through corporate-controlled mechanisms. Now, this is not their sole access point with transition to a hybrid work environment.

You need an entirely new approach to protecting the content that supports your customers and enables your teams — anytime, anywhere, and on any device.

$20 billion

Estimated global damage from ransomware recovery cost in 2020, up from $8 billion in 2018.[1]

Today's threat landscape: Inside and outside the organization

Threats to your content can come from both external and internal sources. One way to think of these threat types are content- and user-centric, respectively. They create different, yet overlapping, kinds of risk.

External threats

Content-centric external threats create operational risk.

Malware

Cybercriminals seek out security vulnerabilities to install malicious software (malware) designed to exploit a private device, service, or network and steal content for financial gain (for example, by selling it). Content they target may include:

- Sensitive financial and legal records that have operational and reputational implications
- Employee and customer personally identifiable information (PII) covered by regulations such as GDPR
- Protected health information (PHI) covered by regulations such as HIPAA

$2.6 million

Average cost of a malware attack on a company in 2019.[2]

Ransomware

Criminals in this subset of malware recognize your content's value and hold it hostage. They know that without it, your business will grind to a halt. Ransomware has quickly grown in volume and resulting damage — and is now considered the number one cybercrime threat[3], due to its lucrative nature and relative simplicity (thanks to "ransomware-as-a-service" on the dark web).

For example, in the spring of 2021, ransomware attackers struck Colonial Pipeline, the largest petroleum pipeline in the U.S., demanding (and receiving) $5 million. The attack shut down operations for over a week, resulting in gasoline shortages and price spikes.

$1.85 million

Average ransomware recovery cost in 2021, a 2x increase over 2020.[4]

Internal threats

User-centric internal threats create financial and reputational risk.

Data loss or compromise, even when accidental, reduces your content's net value, causing financial and reputational losses. The typical target is PII that can be resold on the dark web.

Global brands such as Alibaba (1.1 billion pieces of user data), LinkedIn (700 million users), Facebook (533 million users), and Marriott (500 million customers) have suffered embarrassment and legal woes due to data leaks in the past three years. And that pipeline shutdown? It was caused by a leaked password on a VPN account.

Email attacks

Email attacks are a type of social engineering breach that exploits human behavior. This is why collaborating on content using email attachments poses risks. Attachments from seemingly reputable emails can inject malware into a user's device that then spreads quickly across enterprise systems.

70%

of companies anticipate harm by an email-borne attack in 2021[5]

Negligence

Negligence occurs even in the best organizations. Despite regular reminders about safe practices, mistakes — like sending a sensitive document to the wrong email recipient — happen.

$307,111

Average cost of incidents related to employee or contractor negligence

Malicious activity

Malicious activity by employees or contractors intent on stealing content is also a serious internal threat.

$756,760

Average cost of criminal and malicious insider breaches

How Box solves for content-centric risk

The Content Cloud takes a four-level, automated approach to securing content against external threats

Prevent access to sensitive content

Malicious files on your computer may be synced to other users, but ransomware can't spread further once it's within Box cloud storage. All files are encrypted at rest and don't have an executable environment from which to run. Box lets users collaborate while maintaining data compliance — and without exchanging highly vulnerable email attachments. Moreover, Box Shield Smart Access features let you classify your content with a permanent label that restricts sharing content outside your organization.

Detect malicious activity

Research shows that automation and security artificial intelligence (AI), when fully deployed, reduce the average cost of a breach by 79%[6]. Box Shield uses context-aware machine learning (ML) to scan external content shared by third parties as well as internal content upon upload and when users perform an action such as share, preview, and download. Shield recognizes malicious traits (even that of more sophisticated malware) within the content in near real time and automatically labels the file as malicious. Box Shield's deep learning technology makes it possible for IT and security teams to address potential threats in an efficient and structured manner.

Shield will also generate a detailed security alert so security and IT teams can act quickly. You can see these alerts in the Shield dashboard or have Box send them to your SIEM with built-in integrations. The alert will show you who uploaded the file, any threat intelligence about the malware, and file-related activities to date, so your team can choose the best response. To minimize disruption, Shield allows admins to mark the threat verdict for low-risk content as safe.

The Content Cloud takes a four-level, automated approach to securing content against external threats

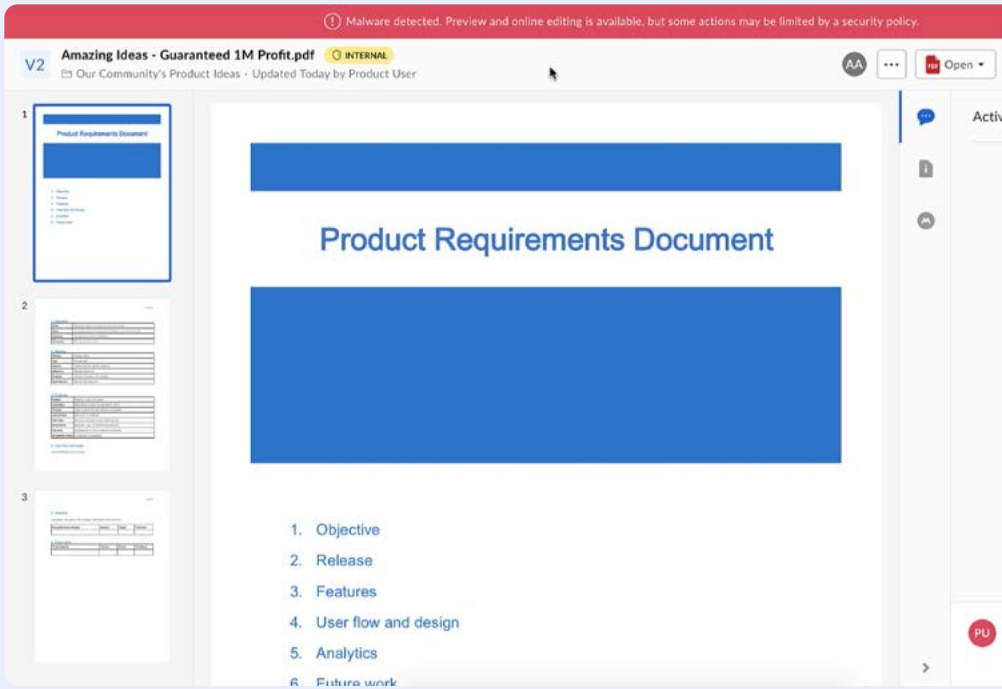
Contain content to stop spread

Once Shield identifies malicious content, it restricts downloads and local editing to prevent the spread to more users and devices. Users will see a malware notification in the Box UI, but they can still safely preview and edit the file online. This allows your teams to stay productive.

Remediate by accessing a previous version

If your systems become infected with malware, you can still preview your content in the Content Cloud while your team works to research the threat.

Because Box creates a new file version with each save, you can delete affected files without original data corruption and access previous versions of important files following a ransomware attack. If you have developer resources available, you can write a custom script that rolls back all infected files to an unaffected version using the Box API.



And remember that you can get expert support whenever you need it. Box has multiple resources available to assist you in getting access to your content.

How Box solves for user-centric risk

Box takes a multi-pronged approach to internal threats that removes the burden of security from your employees, contractors, and other users – while allowing them to continue working seamlessly.

Zero-trust infrastructure

Box allows you to protect your content using a "zero-trust" posture. Rather than assuming certain content or users are trustworthy, it uses context-aware intelligence to check for suspicious behavior during common activities, such as upload or sharing. Box Device Trust helps you enforce your company's security policies by defining a minimum set of requirements for devices used to access Box.

Zero tolerance for a poor user experience

Protection only works if your employees use it. When security degrades the user experience, users simply find ways to get around it. Box offers a highly secure experience that lets users easily share and collaborate on content without putting it at risk. With Box Shield, admins can allow users to make one-time access exceptions with admin-defined business justifications, bolstering security without impeding productivity.

Anomalous behavior detection

Box Shield leverages ML-powered anomalous behavior detection to identify potential threats such as compromised accounts and data theft and keeps security teams informed with alerts. Shield's Anomalous Download detection identifies account holders who may be stealing sensitive content. Suspicious Location detection flags access from an unusual or excluded geographic location or host IP address. And Suspicious Session detection recognizes potentially harmful access characterized by unusual user-agent strings, abnormal IDs, uncommon application types, new IP addresses, and an improbably rapid change in someone's log-in location.

Centralized content layer in the cloud

Having all your content in the Content Cloud makes secure collaboration easy, even among team members spread across geographies and time zones, no matter which device they happen to be using. Centralized content also streamlines information management and governance, keeping your content safer and always up to date.

Security that travels with your content

Box Shield adds yet another layer to the Content Cloud's core security features, which include built-in multifactor authentication (MFA), single sign-on (SSO), watermarking, and KeySafe encryption key management. Together, these safeguards ensure that you can access and collaborate on your organization's valuable content wherever and whenever you need without compromising security. Box lets you and your team work the way you want by integrating seamlessly with thousands of popular applications.

Show me the money: How Box security increases ROI

In a commissioned study, Forrester recently analyzed the total economic impact of the Content Cloud. Among the many ways in which the Content Cloud impacts the bottom line, several relate to content security directly.[7]

Total savings

$1,125,000 in net security, governance, and compliance savings, including reduced risk of data breaches and streamlined content access monitoring with Box Shield

Third-party costs

$245,000 avoided cost of third-party security and compliance solutions and certifications

User-centric risk

$580,000 savings: data breach from accidental data leakage

Data governance

$63,000 savings in improved ease of data governance

User content access monitoring

$237,000 savings: monitoring employee content access

The Content Cloud: A secure approach

Companies spend tons of time and effort eliminating security risks in their systems and applications, and rightly so. But it means nothing if they're not focused on the content at the heart of it all.

That's where the Content Cloud comes in. It's a proven approach to managing your most valuable information, with a single, secure platform for the entire content lifecycle. Every step of the way, Box is here to help.

box

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 69% 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.

To learn more about the Content Cloud and the many ways it supports sharing and collaboration without compromising security, visit box.com/shield

[1] 10 Cyber Security Trends You Can't Ignore In 2021 | PurpleSec

[2] Accenture, "Ninth Annual Cost of Cybercrime Study," 2019

[3] 10 Cyber Security Trends You Can't Ignore In 2021 | PurpleSec

[4] Sophos, "State of Ransomware 2021"

[5] Mimecast, Securing the Enterprise in the Covid World, 2021

[6] IBM, Cost of a Data Breach report, 2021

[7] Forrester, The Total Economic Impact™ of the Box Content Cloud, June 2021. All figures reflect savings over three years for a single composite organization.