box

Protect your content with Box

One platform for secure collaboration that includes intelligent, frictionless security to protect your enterprise content against ransomware and other types of malware

From contracts that close deals, to designs for your next big product launch, your business runs on content. As teams move from remote to flexible working models, keeping critical content secure and compliant is more important than ever. Ransomware incidents can severely impact business continuity and leave enterprises without the data they need to operate and deliver mission-critical services. Recently, ransomware incidents have become more frequent, destructive, and impactful in nature leading to reputational and financial risk.

Learn about malicious software

"The total cost of recovery from a ransomware attack is $1.85M."

Why is ransomware so important?

Ransomware is an ever-evolving type of malware (malicious software) designed to encrypt files on a device, rendering any content and the systems that rely on those files unusable. Bad actors then demand ransom in exchange for decryption. Malicious actors often target and threaten to sell or leak exfiltrated data or authentication info if the ransom is not paid.

There's been a 62% increase in ransomware globally since 2019, and 158% spike in North America [1]. The Accenture CIFR team observed ransom demands ranging from $100K to $50M in 2020 with the average total cost of recovery from a ransomware attack increasing from $761K in 2020 to $1.85M in 2021[2]. No wonder Christopher Krebs, former Director of the Cybersecurity and Infrastructure Security Agency (CISA), says "...ransomware is the biggest threat."

Minimize your ransomware risk

How does Box help?

Box can help with prevention, detection, containment, and remediation of ransomware and other types of malware.

Prevent

Use the Box Content Cloud with versioning, native security features (MFA, Device Trust), and external sharing controls

Contain

Configure Box Shield to automatically block the download of malicious content to your local machine or sync across other apps so it will not proliferate — without disrupting the flow of work (in addition to still being able to preview and edit online)

Detect

Employ Box Shield to scan files for malicious content, including ransomware, on "active" content (that is uploaded, edited, shared, downloaded etc) and use suspicious location and session alerts to monitor abnormal user behavior that can be fed into your SIEM

Remediate

Restore files that were locked or modified with Box backups and leverage Box Shield to classify your content with an immutable label that restricts sharing outside your organization

Save more than $1.1M on security and compliance with Box

Box commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises may realize by deploying its suite of cloud-based content management solutions.

Benefits (three-year)

$580K

Reduced risk of data breach from accidental data leakage

$237K

Cost savings on monitoring employee content access

$245K

Avoided cost of third-party security and compliance solutions and certifications

$63K

Improved ease of data governance

[1] 2021 SonicWall Cyber Threat Report
[2] The State of Ransomware 2021

Extend your security strategy into the cloud

Malware protection is just one critical element of a robust data protection strategy. We think about security holistically, and Box integrates with your existing security tools and controls to give you the continuous assurance and monitoring transparency you need.

> “We love Box Shield because it enables granular capability that cuts across Box and surfaces anomalies to a small group. It also helps me demonstrate that we are compliant.”
>
> - Chief Innovation Officer and Assistant Town Manager, Town of Cary NC

The Box security portfolio

Box Shield

Prevent data breaches with classification policies and intelligent threat detection

Box Governance

Manage document retention policies and conduct defensible discovery

Box Zones

Address data residency obligations across multiple geographies

Box KeySafe

Maintain full control of your encryption keys

GDPR compliance

GDPR-ready platform to facilitate GDPR compliance

GxP validation

Manage GxP documents and assure that Box is constantly in a validated state

Learn more about our security and compliance solutions

At Box, our top priority is the security and integrity of our customers’ data. We scan every file to identify viruses, trojans, worms, and other types of malicious code.

Virus Scan

Virus scan is carried out by sending the checksum of the file to a trusted third-party service, relying on the expertise of numerous malware signature providers like CrowdStrike, Trend Micro, SentinelOne, and McAfee. To protect our customer’s privacy and reduce the risk of data exfiltration, the file itself is not sent for analysis, and this operation does not interfere with Box’s performance.

Malware Deep Scan

Box Shield provides another layer of malware detection that leverages deep learning models to analyze the file for any malicious traits or suspicious content. Deep scan looks inside the file to identify malware in near real-time, allowing Box Shield to detect more sophisticated varieties of malware, and even ransomware. Detection happens natively within Box at the same time as virus scan.

With Box Shield, organizations receive comprehensive coverage because external content that is accessed by managed users is also analyzed, reducing third-party risk. Even better, Box admins can override threat verdicts for low-risk content so that productivity is not impeded.