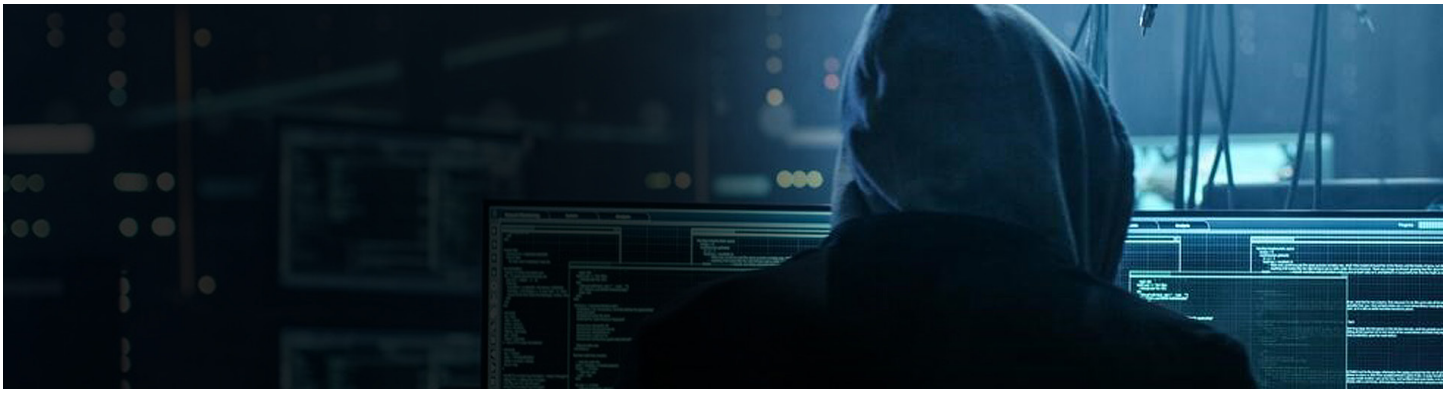


Ransomware Data Recovery

When malicious code infects an organization's system and extorts it for monetary gain, the overall impact can be dire. Meanwhile, the FBI advises against paying a ransom as this encourages the ransomware business model and offers no guarantees that the data will be successfully decrypted. When time is of the essence and next steps are uncertain, organizations should consult with experienced professionals to determine their best course of action.

Data recovery experts are ready to help.

KLDiscovery's global data recovery business, Ontrack, has developed a specialized collection of proprietary tools to recover data from ransomware-encrypted systems, virtual machines, backup files, tapes, and other storage media. With labs located around the world, help is available 24/7 from our knowledgeable team with vast experience in all types of data loss situations.

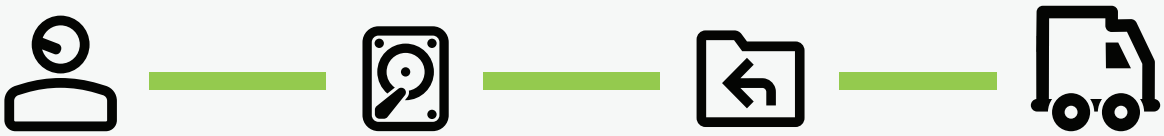
Industry experts and a specialized collection of proprietary tools developed to recover data encrypted by ransomware.

If your organization might be affected by ransomware:

- Contain the attack by disconnecting infected machines from the network.
- Contact us as early as possible. Our team will provide a free consultation and advise on options for data recovery and how to prevent further potential data loss.
- Avoid do-it-yourself attempts to decrypt the affected data. Doing so could make future recovery attempts impossible.

Recovery Process Overview

Though each ransomware incident is unique and varies in complexity, data recovery is possible. Success depends on the type of payload that has been executed, the hardware it has affected, and the initial actions taken upon discovery.



Consult

Immediate phone consultation with data recovery specialists.

Evaluate

Media is evaluated to determine what files can be recovered.

Recover

Recovery carried out by our expert data recovery engineers.

Return

Data is recovered remotely or returned on encrypted media.

Ransomware Case Studies

- **Phishing Attack**
  A multinational chemical corporation experienced a ransomware attack that took over a server using administrator privileges obtained through phishing. The ransomware formatted all the hard drives and created a new aggregate. Ontrack was able to rebuild the RAID and the original volumes, and restore the customer's data.
- **CryptoLocker Ransomware**
  A single user's laptop at a large pharmaceutical company was infected with CryptoLocker ransomware. The laptop was connected to the corporate network, which allowed the malware to infect 46 shares. Leveraging NetApp's proprietary OS (OnTap) and file system (WAFL), Ontrack engineers used multiple consistency points to "walk back" in time to a point before the attack to find and recover unencrypted copies of the critical data to return to the customer.
- **Erased Backups**
  Ransomware attacked a company server, encrypted the Microsoft Dynamics 365 data, and demanded payment. Recent backups of the server were stored on multiple LTO-6 backup tapes, which had been erased by the malware. Working in conjunction with the R&D department, Ontrack developed a custom hardware and software-based solution to recover 46TB of data from 18 of the LTO-6 erased backup tapes.

About Ontrack

Ontrack has vast experience dealing with data loss scenarios ranging from routine to extreme. With 35 years in business, a suite of proprietary hardware and software recovery tools, and a highly qualified data recovery team of engineers and developers, Ontrack delivers world-class data recovery for all types of storage including: hard drives, solid-state drives (SSD), servers, NAS, SAN, virtual machines, cloud, mobile devices, and tape.

SLS KLD US_Ransomware_Mar 2023

KLDiscovery™
9023 Columbine Road
Eden Prairie, MN 55347
952.937.1107
www.kldiscovery.com