dataJAR
Beyond Device Management

Product Guide

Code42 - Data Loss Protection

Insider threat solution for cyber security

What is it?

Code42 has a proven track record with regards to protecting organisation data. In an ever-growing mobile world, the right technology is required to manage the risks of a remote workforce. Protecting data, while enabling the flexibility for a remote workforce, is a fine balance to strike. Our partnership with Code42 cloud service brings best-in-class data loss protection and insider threat analysis enabling simple, fast detection and response.

Optionally, and combined with our device management platform, datajar.mobi or Jamf Pro, your customer's data will be protected while they continue to work to full capacity, safe in the knowledge their files are visible and can be retrieved efficiently and securely at any time.

Who is Code42 - Data Loss Protection for?

Most organisations could benefit from data loss protection but it could be especially beneficial for:

- Organisations that work on sensitive data, and a loss of data or intellectual property could substantially impact the value of their business.
- Organisations who are concerned about employees taking data when they leave.
- Organisations going through a merger or acquisition. Loss of data at this time could prove catastrophic to a deal, and the risk of data loss is higher due to mergers and acquisitions often coming hand in hand with increased employee turnover or layoffs.

Requirements:

- **Code42 app system requirements:** https://support.code42.com/CrashPlan/6/Get_started/Code42_app_system_requirements
- **IP addresses and ports used by the Code42 platform:** https://support.code42.com/Administrator/Cloud/Planning_and_installing/IP_addresses_and_ports_used_by_the_Code42_platform

dataJAR
Beyond Device Management

How does it work?

This is a cloud-based, annual subscription service that can be purchased as an add-on for datajar.mobi or Jamf Pro. A lightweight agent is installed on your supported devices which integrates into the operating system. All data created, moved or deleted is tracked to a forensic level of detail.

Integrating into common cloud storage products such as Microsoft OneDrive™, Box™, Google Drive™, DropBox™ and iCloud Drive™, you will see and be alerted, from a central dashboard, of any suspicious activity. With Code42 you will be able to gain visibility of off-network file activity and quickly detect, investigate and respond to data exfiltration. Code42 makes sure you take no chances with your data, with a mandatory remote professional services engagement ensuring you have the best of every feature enabled for your organisation.

Imagine keeping a copy of every file ever created within your organisation - now you can with unlimited revisions of files even stored outside your central collaboration areas. Employees can recover previous versions of their file without the need to raise support requests and can even migrate their data to a new device removing the need for IT involvement.

FAQs

Q: Is this a managed service dataJAR can offer?
A: No. Due to the sensitivity of the data collected this is a product that, once set up, can be used by IT professionals or Human Resources.

Q: Does Code42 integrate into external Identity Services Integration?
A: Yes. Code42 can be configured to integrate into any SAML based identity system. It can be configured to use the Lifecycle Management module from Okta.

Q: Which cloud sync applications can Code42 monitor?
A: Code42 detects when files are added to installed cloud sync applications such as Dropbox, iCloud, Google Drive, Google Backup and Sync, OneDrive and Box. Code42 can also identify and differentiate between files sent to personal and corporate Slack accounts.

Q: What information does Code42 provide on web upload activity?
A: When files are accessed by web browsers or other web-based applications, such as FileZilla and FTP. Most notably, Code42 provides the browser tab/window title and the tab URL for the event so security teams can quickly identify where files are sent.

Q: Can Code42 detect improper sharing from corporate accounts?
A: Yes. Code42 has built integrations with corporate cloud services to monitor employee file activity in Microsoft OneDrive, Google Drive and Box. You can receive alerts when files are shared outside your trusted domains, when sharing settings are elevated or when public links are generated.

Q: How are file types categorised?
A: Code42 uses a variety of file metadata, including MIME type and file extension, to assign files to categories. Categories include archive, audio, document, executable, image, PDF, presentation, script, source code, spreadsheet, video and virtual disk image.

Ready to find out more about dataJAR?
We would love to hear from you.

Chat with our experts

dataJAR
Beyond Device Management

0800 368 9330 | International: +44 (0) 1273 023700 | enquiries@datajar.co.uk