CODE42

Code42 Security Tools

Regardless of the threat trigger, Code42 sheds light on the data moving to and from endpoint devices to give IT and InfoSec personnel a single point of visibility and control across every employee in the enterprise.

Threats to data from inside the organization can happen accidentally when employees make mistakes or lose their laptops, or maliciously when employees intentionally steal, sell or sabotage data—but both behaviors can result in operational, financial or reputational harm to an organization.

Get more from your backups

Code42 customers already have the ability to respond to and remediate data loss, no matter the cause. Automatic and continuous Code42 backups also allow businesses to know with certainty what data was on a lost, stolen or compromised device.

Now with the Code42 Security Tools feature set, enterprises can identify and respond to threat indicators. Administrators can see what files users had, when they had them and what they did with them.

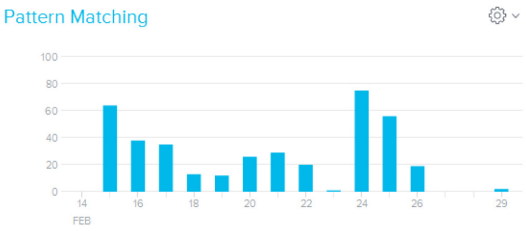
The ability to see the full life cycle of data on endpoints means IT, legal, security and compliance professionals can pinpoint the movement of highrisk data, and monitor when data is moved to clouds or removable media. Endpoint monitoring functionality reveals anomalous behaviors that could signal threat, such as an unusual restore activity, which may suggest compromised user credentials.

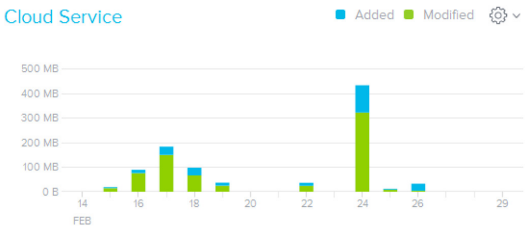
9.3 Number of insider threats the average organization experiences per month.[1]

>$5M[3] Potential loss from an insider threat.

75% Unreported insider crimes.

26% Number of companies citing lack of evidence as the reason.[2]





Respond and investigate faster

With Security Tools enabled, designated Code42 administrators gain access to a web app that allows them to:

- Review end-user data activity within a chosen timeframe
- Visualize instances of high-risk data or threatening end-user behavior
- Export reports for detailed analysis, or integrate with Splunk Enterprise for advanced monitoring

Code42 endpoint monitoring in action

Endpoint monitoring identifies five types of risk-related activities on devices running a Code42 client.

Code42 endpoint monitoring indicates when data is:

- Transferred to removable media devices
- Transferred to cloud storage applications
- Restored via the web
- Attached to webbased email
- A match to patterns of sensitive data

ENDPOINT MONITORING TYPE	ACTIVITY IDENTIFIED	USE CASE EXAMPLE
Removable media	A user transfers files onto a removable media device such as a USB drive, external hard drive or SD card.	A user plugs a USB drive into her computer, copies a proprietary file and removes the drive.
Personal cloud	A user syncs files using a cloud storage application such as Box, Dropbox, Google Drive, iCloud or OneDrive.	A user uploads a sensitive file to the Google Drive desktop application.
File upload (Windows only)	A user opens or sends files in a web browser.	A user attaches a confidential file to a Gmail email.
Restore	A user restores files with Code42.	A web restore is initiated by someone who has gained access to a user's credentials.
Pattern matching	Using Yara rules, a pattern of sensitive data is discovered on the device.	A user saves a file containing Social Security numbers to her hard drive.

Leveraging the Code42 client, enterprises gain the ability to recognize suspicious employee activities, mitigate the impact of data leak, and identify negligent or problematic behaviors that reveal the need for more end-user education.

References:

[1] bit.ly/1UmaaJM [2,3] bit.ly/1QfiQh9

CONTACT CODE42 SALES:
code42.com/contact

CORPORATE HEADQUARTERS | 100 WASHINGTON AVENUE SOUTH | MINNEAPOLIS, MN 55401 | 612.333.4242 | CODE42.COM

FEBRUARY 2017 / OV021739