INSIDER THREAT BUYERS GUIDE
Detect, Investigate, & Respond
THE RISK: INSIDER THREAT
Insider threat is the fastest growing risk your organization faces, with insider threats growing more than 50% over the last four years and now accounting for nearly half of all data loss incidents.

WHO: THE USUAL SUSPECTS
First off, the obvious: It’s people with access to your most valuable and vulnerable data. And more often than not, it’s quitters. Departing employees account for half of all insider threat incidents. Sometimes, it’s driven by a specific event—an M&A, for example, that leads to voluntary and involuntary departures. Most of the time, it’s just people leaving for “greener pastures”—which is happening more frequently than ever, as average employee tenure continues dropping across the U.S. workforce.

WHAT’S AT RISK: YOUR TRADE SECRETS. YOUR BUSINESS VALUE. YOUR DIGNITY.
Employees are walking out the door every day with the valuable trade secrets—from source code to customer lists—that make your business work. Worse, they’re frequently bringing these trade secrets directly to your competitors. You’re losing your competitive advantage. You’re losing business value. It’s damaging. And it’s embarrassing.
THE PROBLEM: PREVENTION WILL FAIL

Insider threat is the top-of-mind challenge for security teams today. Yet 90% of insider threats go undetected, and the problem keeps growing. Why? Because most organizations are still focused exclusively on traditional data loss prevention. But relying on prevention is futile. Data is more portable than ever, and there are simply too many clever ways for employees to take your trade secrets. Prevention inevitably fails, and organizations don’t realize it until the damage is done.

THE REALITY: YOU’RE FLYING BLIND

Because traditional insider threat programs focus on prevention, most security teams are flying blind when it comes to detecting and responding to the threats that inevitably get past their prevention tools. Relying on legacy DLP, security teams can’t answer these basic data security questions:

- What data do you have?
- Where does that data live?
- Who has access to that data?
- Has data left?
- What data left?
- When did data leave?
THERE’S A GAP IN THE STACK

Legacy DLP represents a preventative approach. But when prevention fails (and it will), legacy DLP fails to provide the data visibility that security teams need to enable a true Zero Trust approach. They need security tools that let them see where their data lives (all of it) and how it moves (any way and anywhere) in order to rapidly identify and effectively respond to insider threats before the damage is done.

LACK OF VISIBILITY
- What data you have
- Where you have data
- Who has or had what data
- When data is leaving
- What data is leaving
**THE SOLUTION: FILL THE GAP**

Code42 fills the detection and response gap, taking a data-centric approach to the insider threat problem. Code42 collects and protects all of your data—every file, automatically, continuously and in near-real time. This gives security teams comprehensive visibility into all files and all file activity—driving faster and more effective response.

<table>
<thead>
<tr>
<th>Data</th>
<th>Identity</th>
<th>Prevent</th>
<th>Detect</th>
<th>Investigate</th>
<th>Respond</th>
<th>Recover</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Identification &amp; Data Classification</td>
<td>DRM + Encrypt</td>
<td>Data Loss Prevention (DLP)</td>
<td>Data Loss Detection, Investigation and Response</td>
<td>SEE THE LOSS. GET THEM BEFORE THEY GET YOU. Fill the data visibility gap. Know when data leaves. See where it goes. Respond immediately. Stop the damage.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Identity</td>
<td>Prevent</td>
<td>Detect</td>
<td>Investigate</td>
<td>Respond</td>
<td>Recover</td>
</tr>
<tr>
<td>Firewall</td>
<td>Network DLP</td>
<td>Next-Gen Firewall Network DLP</td>
<td>Identity &amp; Access Management (IAM)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application</td>
<td>Application</td>
<td>Prevent</td>
<td>Detect</td>
<td>Investigate</td>
<td>Respond</td>
<td>Recover</td>
</tr>
<tr>
<td>Cloud Gateways</td>
<td>Cloud Access Security Brokers (CASB) Integrated DLP (Gmail, O365, etc.)</td>
<td>Cloud Access Security Brokers (CASB) Integrated DLP (Gmail, O365, etc.)</td>
<td>Cloud Access Security Brokers (CASB) Integrated DLP (Gmail, O365, etc.)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Endpoint</td>
<td>Endpoint</td>
<td>Prevent</td>
<td>Detect</td>
<td>Investigate</td>
<td>Respond</td>
<td>Recover</td>
</tr>
<tr>
<td>Endpoint Anti-virus (AV)</td>
<td>Endpoint Detection &amp; Response (EDR)</td>
<td>Endpoint Detection &amp; Response (EDR)</td>
<td>Endpoint Detection &amp; Response (EDR)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
A COMPREHENSIVE SOLUTION

The comprehensive data collection, protection and visibility of Code42 gives you a powerful platform for addressing the full range of data loss threat vectors—both inside and outside the organization.

- **User-based risk**: Full visibility for rapid detection and response to insider threats.
- **Organization-based risk**: Continuous data collection and protection to mitigate risk during M&A, litigation or other organization restructuring events.
- **Device-based risk**: Instant file recovery that protects from lost or stolen devices, ransomware and other disasters.
- **Cyber risk**: Comprehensive visibility that enables proactive threat-hunting of external cyber threats lurking within the organization.
HOW DOES IT WORK?

Code42 delivers this full range of data loss protection through one simple, highly automated workflow:

COLLECT & MONITOR

Automatically monitor all files and file activity for every user and every device.

DETECT & INVESTIGATE

Quickly and easily identify suspicious behavior and rapidly investigate.

ASSESS & RESPOND

Access the exact file(s) in question, determine risk and respond in seconds.

COLLECT
all endpoint & cloud data

Device Risk

User Risk

Organization Risk

COLLECT
all endpoint & cloud data

What data is at risk

Where data is located

Who has/had what data

How & when data moved

RETRIEVE
files for content analysis

Take Legal / HR action

Investigate further

Close case
PRODUCT OVERVIEW

COLLECT & MONITOR

Automatically monitor all files and file activity for every user and every device.

- Track creation, modification and movement of files on Windows, Mac and Linux computers
- Collect file content and associated metadata to speed insider threat investigations
- Monitor file movement within corporate cloud environments such as OneDrive, Google Drive and Box

DETECT & INVESTIGATE

Quickly and easily identify suspicious behavior and rapidly investigate.

- Detect when files move to devices, web browsers, web applications and cloud file sync & share folders
- Identify files shared publicly via corporate OneDrive, Google Drive and Box accounts
- Define custom alerts based on users, data exfiltration vector and file count or size
- View file details including file hash, owner, path, size, category and device information such as hostname and IP address
- All file activity is indexed and made searchable to reduce the time it takes to investigate insider threats
- Review file event activity in seconds—even when user devices are offline

ASSESS & RESPOND

Access the exact file(s) in question, determine risk and respond in seconds.

- Quickly access file contents to determine their sensitivity and value
- Restore files that have been deleted or ransomed
- Recover files from lost and stolen devices

One Endpoint Agent

Mac, Windows, Linux OS feature parity
Lightweight – no disruption to users

for multiple exfiltration vectors
NEXT-GENERATION CAPABILITIES

The unique capabilities of Code42 deliver smart outcomes that drive this powerful combination of efficiency, efficacy and speed:

- FILE BREADTH
- FILE DEPTH
- FILE ACCESS
FILE BREADTH

Detect suspicious file behavior using one window into the past 90 days of file activity from computers to cloud while having unlimited access to historical file versions on endpoints no matter how old.

- Detect trends and anomalies in file movement across endpoint, cloud, email and web browser data exfiltration vectors via a single data exposure dashboard.
- Detect data loss risk due to suspicious file creation, modification and movement across Windows, Mac and Linux computers, removable media devices, web browsers/applications and cloud accounts, without the need for policies.
- Detect data loss risk within corporate cloud environments and identify sensitive files shared publicly via corporate OneDrive, Google Drive and Box accounts.
- Detect data loss by type of activity (removable media, web browsers/apps, cloud sync applications or file sharing) as well as by file size and count.

Customer Validation: “Code42 gives me a complete view of everything that happens to our data, including ... vulnerable endpoints such as PCs and laptops. And if people upload to the cloud, we can see what they took and with whom they share it.”

- David Chiang, IT Systems Engineer, Macom
FILE DEPTH

Investigate suspicious file activity by name, path, size, owner, category, MD5, SHA256, date, type, source, device hostname, username, IP address and that’s just the start. Collect file content and associated metadata to speed insider threat investigations.

- Automatically index file activity across computers and cloud to assess data loss risk from insider threats.
- Retain 90 days of historical file activity by employee to quickly replay events and assess data loss risk.
- Preserve copies of files for as long as needed to support security investigations, legal hold and eDiscovery processes.
- View detailed information on files, devices, cloud destinations and exposure events. Find as much or as little information as you need to do the job—from file owner to the removable media serial number.

Customer Validation: “Through one holistic view, File Forensic Search gives us near real-time visibility to where data lives and moves across all endpoints. We speed up our time-to-response for a wide range of cyber threats. It’s a game changer for security professionals.”

- Mark Ruchie, VP and CISO, Entrust Datacard
FILE ACCESS

Assess data loss risk by viewing the contents of any file version whether it was created one hour or one year ago, respond quickly and always recover in the event files are lost, stolen, deleted, or ransomed.

- Simple: Security teams can review event activity in seconds—even when user devices are offline
- Fast: View file contents in seconds to determine their sensitivity and value
- Comprehensive: Query file details including file hash, owner, path, size, and category alongside device information such as hostname and IP address across computers and cloud services.

Customer Validation: “If it wasn’t for the Code42 ability to actually see the files, we wouldn’t really understand what the person is doing... It provides us both speed and thoroughness of investigations.”

- Tim Briggs, Incident Response Analyst, Crowdstrike
MAKE YOUR SECURITY TOOLS SMARTER

Code42 seamlessly integrates with the full range of best-in-class security and IT tools your teams are already using. The comprehensive data visibility—all files and all file activity—of Code42 makes everything in your existing security ecosystem work better. Make detection and investigation instantaneous. Automate your response.
Insider threat is a complex problem—and there will never be a single, one-size-fits-all solution. However, while several categories of tools have emerged to address insider threat, it's important to understand exactly what kind of protection they offer—and at what cost.

<table>
<thead>
<tr>
<th>Technology</th>
<th>Sample Vendor Used</th>
<th>Primary Deployment Model</th>
<th>Exfiltration Vector Coverage</th>
<th>User Productivity</th>
<th>File Depth</th>
<th>Historical File Breadth (Retain)</th>
<th>File Access (Restore)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Loss Detection &amp; Response (DLDR)</td>
<td>CODE42</td>
<td>Cloud</td>
<td>Endpoints, cloud services, cloud applications, web browsers</td>
<td>Low</td>
<td>Automatically indexes and makes searchable: file name, path, size, owner, category, MD5, SHA256, event date, type, source, device hostname, username, IP address</td>
<td>Continuous always-on collection with 90 days file activity retention and unlimited days file &amp; file version retention</td>
<td>Yes</td>
</tr>
<tr>
<td>Data Loss Prevention (DLP)</td>
<td>Symantec</td>
<td>On-premises</td>
<td>Endpoints, email, network</td>
<td>High</td>
<td>Dependent on policy-driven file events</td>
<td>Generated based on incidents incurred. Unlimited based on storage capacity</td>
<td>No</td>
</tr>
<tr>
<td>Cloud Access Security Brokers (CASB)</td>
<td>Netskope</td>
<td>Cloud</td>
<td>Cloud services, cloud applications</td>
<td>Low</td>
<td>Focused on cloud application, network and user activity not file events</td>
<td>Continuous always-on collection with 90 days file activity retention</td>
<td>Yes</td>
</tr>
<tr>
<td>Data Centric Audit &amp; Protection (DCAP)</td>
<td>Varonis</td>
<td>On-premises</td>
<td>Enterprise servers &amp; storage</td>
<td>High</td>
<td>Collects data on users, permissions, device access activity, AD &amp; perimeter telemetry, and content classification</td>
<td>90 days log data</td>
<td>Files can be quarantined for direct review</td>
</tr>
<tr>
<td>User Activity Monitoring (UAM)</td>
<td>ObserveIT</td>
<td>On-premises</td>
<td>Endpoints</td>
<td>High</td>
<td>Focuses on user-based activity events not file activity events</td>
<td>Admin-triggered collection, retention based on available storage capacity</td>
<td>No</td>
</tr>
</tbody>
</table>
Zero User Burden
Code42 is purpose-built to be extremely lightweight, with automatic data collection and protection that doesn’t slow down users’ devices and productivity. Maximum CPU allowances can be set for when users are present and away from their devices to further minimize impact. The agent can be fully hidden from users, as well.

Multiple Exfiltration Points

Device
- Devices—such as flash drives, hard drives and cards—that connect via USB, eSata, Thunderbolt and SD Card ports. Code42 collects the vendor, name and serial number of all devices used.

Cloud
- Installed cloud sync applications for Dropbox, iCloud, Google Drive, Google Backup and Sync, OneDrive and Box. API integrations with corporate cloud services support monitoring of activity in Microsoft OneDrive, Google Drive and Box.

Web
- Internet Explorer, Chrome, Firefox, Safari, Edge, Chromium and Opera, as well as processes and applications such as FileZilla, Winscp, Slack, SFTP, FTP, Curl and SCP.

Email
- Browser detection tracks the number and size of files uploaded or downloaded—including when a user attaches a file to a web-based email—including file name, IP address, file path, file size, MD5 and SHA256 hashes.

Comprehensive Monitoring & Alerts
Customizable alerts can be set for near real-time notification of risky activity. Code42 also assigns categories to files in order to help you identify your most important data at a glance. Monitored categories include archive, audio, document, executable, image, PDF, presentation, script, source code, spreadsheet, video and virtual disk image. When you’re alerted of risk, you can quickly access the file(s) in question to make an informed decision about whether that file needs to remain private. Finally, most organizations further narrow their focus by prioritizing alerting during times where data is put at the most risk, such as during employee departure and M&A.
DEPLOYS IN DAYS. RESULTS IN MINUTES.

### Rapid Deployment
Most Code42 customers are able to start using the product within 2 weeks. From there, they continue to work with our deployment team to implement full product capabilities and best practices over the course of 1-2 months.

### Time to Deploy
You don’t have to move mountains to get Code42 up and running. Code42 is 100% in the cloud so deployment doesn’t take months and seamlessly fits into your existing security environment.

**Customer Validation:**

“In support of our campus wide digital transformation effort, Cornell has been on the bleeding edge and early adopter of Code42’s cloud offering. Since we deployed, we have seen valuable client upgrades, new features, and most of all exceptional responsiveness from Code42.” Bob Talda, System Engineer IV at Cornell University

### Time to Manage
Unlike traditional DLP solutions, Code42 delivers client release parity across Windows and Mac. And since we are in the cloud, patches and bug fixes happen in real time.

**Customer Validation:**

“The global deployment went very smoothly. It was complete within about a month, which was a fast turnaround for us.” David Chiang, Systems Engineer at MACOM

“‘Our deployment happened on a very tight timeline and was executed without a hitch. We’re so pleased with the deployment that we’re discussing how to leverage the other benefits.’ Scott Rabjohn, Systems Analyst at Viasat

### Time to Maturity
Code42 is not another security tool. It’s a complete data loss protection solution designed to elevate your insider threat security posture today and well into the future.

**Customer Validation:**

“Our data security needs have expanded significantly in recent years due to acquisitions. It’s important to our business that the data security programs we deploy makes it easy to protect our intellectual property portfolio as it grows.” Jeff Zuniga, Senior IT Operations Manager at Shape Technologies Group.

“Today, we have gone a step further, and integrated Code42 and Splunk. Together, these solutions not only help us monitor data activity, but also consolidate that information for a clear snapshot of what’s happening at an individual and organizational level. Having these tools provides efficiencies and enhanced security beyond what we had before.” David Chiang, Systems Engineer at MACOM

### Global Data Centers
Code42 offers a variety of data center destinations to support the requirements of global businesses.
PROVEN VALUE. MEASURABLE ROI.

You know the potential damage that insider threat can cause. But mitigating this risk can seem like an intangible, hard-to-quantify value. Fortunately, Code42 gives you the compelling metrics you need to gain buy-in. Hard numbers that you can point to—proving the value you bring to your business. Hard numbers your business leaders can point to—showing they’re helping move the organization forward.

230% ROI

Forrester calculated a risk-adjusted Return on Investment (ROI) of 230% over three years.

$925,000 NPV

(Net Present Value)

PAYBACK in 3 Months

(That’s more than two dollars earned for every dollar spent.)

THE BOTTOM LINE:

Code42 stops your biggest insider threats for just 33 cents a day.
TAKE THE NEXT STEP

Visit www.code42.com/contact/sales to get started on the path to stopping insider threat.
FILL THE GAP. SEE THE THREAT. PROTECT YOUR TRADE SECRETS.