CODE42

EMPLOYEES QUIT. DATA LEAVES.

Be sure your trade secrets don’t go with them.

QUITTERS ARE YOUR BIGGEST INSIDER THREAT

People quit jobs.
Shocking? Hardly. Problematic? Usually not. Here's what's concerning:

Last year,
24 MILLION
quitters took data from their previous employers.[1]

Of those insider threats
90%
went undetected.

Departing employees account for more than half of all insider threat incidents. Ask three quitters, and two of them will openly admit to taking data with them when they leave.[2] The third one might just be less honest about it. Quitters are walking out the door with valuable information — from source code and CAD files, to financial documents and customer lists. Worse, organizations aren't realizing it until months later — often when a competitor comes out with a copycat product or steals clients.

It's embarrassing and damaging for businesses.

And yet, only 1 in 5 enterprise organizations have dedicated insider threat response plans. The other 4 in 5 are counting on traditional data loss prevention (DLP) to solve the problem. But legacy DLP won't stop the quitters from taking data — and it can't give you the visibility you need to detect the data theft and respond to it before the damage is done.

CODE42

1. Precision Discovery forensic investigations, 2018
2. Code42 Data Exposure Report, 2018

THE BRUTAL TRUTH

Quitters take data. Prevention will fail.

YOU NEED A BETTER SOLUTION.

CODE42

MEET ALEX

Alex is a mid-level sales rep at your company. Everyone knows Alex: He's 32, one kid, one dog, loves kayaking, came from one of your biggest competitors and has quickly earned respect around the office. But here's one thing you don't yet know about Alex:

Alex is a quitter.

He's about to join the more than 40 million people that quit their jobs in the last year.[3] Alex has landed a new sales gig at another competing company — lured by a promotion and a nice raise — and he's drafting his resignation letter right this minute.

Alex quits a lot — and he's not unique.

Alex has hopped around to four different companies in the past 10 years. It's not because he's a bad employee, and he's not particularly unique. Employee departures have been steadily rising for the last decade,[4] and the typical U.S. employee doesn't even make it past the three-year mark anymore.[5] In fact, right now, half of your employees are actively looking for a new job — and half of those job-seekers haven't even been with your company for a full year.[6]

Why are quitters quitting more frequently?

Alex, like the typical employee aged 22-34, doesn't have the same notion of employer loyalty as previous generations. He sees switching jobs and switching employers as the route to growth, challenge and fulfillment. Moreover, he's got the benefit of a solid job market: He knows companies are looking for people like him, so he feels confident and empowered to explore his options and pursue his self-interest.

3. U.S. Bureau of Labor Statistics
4. U.S. Bureau of Labor Statistics
5. Gallup poll data
6. Gallup poll data

ALEX IS TAKING YOUR DATA

Alex has another surprise coming your way: He's already preparing to take some files with him when he leaves. Here are just a few of the valuable and sensitive things he might take:

Pitch Decks | Sales Tools | Customer Lists | Contract Templates

He's copied a few pitch decks onto DropBox — they helped him land his new gig. Now, he's pulling together some contract templates, an ROI calculator tool, and his customer lists. This is all happening before you have any reason to keep an eye on him, of course.

Alex isn't just a "bad apple."

Alex is part of the majority — 66%, actually — of departing employees that admit to taking data when they leave their employer.[7] That number rises as you move up the chain of command: nearly three-quarters of executives say they take data when they leave.[8] And the vast majority (70%) of that data-thieving happens before quitters give their notice.[9]

66%

of departing employees admit to taking data when they leave their employer

7. Precision Discovery forensic investigations, 2018
8. Precision Discovery forensic investigations, 2018
9. Precision Discovery 2018

QUITTERS LIKE ALEX ARE EMBARRASSING THE BIGGEST NAMES IN SECURITY

It's making headlines every week: another big-name company burned by a quitter walking out the door with high-profile data. Even the DLP "market leaders" are getting embarrassed by quitters taking data. Just look at McAfee:

WHO	Finance and sales employees
WHAT	Pricing info, marketing plans, customer lists, negotiating methods and other proprietary info — putting tens of millions of dollars in business at risk
WHEN	Surprise, surprise — on the last day of employment
HOW	No sophisticated schemes here — they just put the files on thumb drives or emailed them to personal accounts

Tough questions — and uncomfortable truths — for security teams.

When quitters take valuable data, it's embarrassing for the organization. But it's really embarrassing for a security team. Not just that it's happening — but that they had no idea for weeks or even months. Moreover, when news breaks that a quitter took valuable data, the security team is forced to answer tough questions from business leaders.

HOW DID THIS HAPPEN?

And why did we not know sooner?

YOU'RE NOT PREPARED TO STOP ALEX.

Here are the uncomfortable truths on why even the top security teams can't stop quitters like Alex:

1. Most organizations have no defined insider threat response plan.

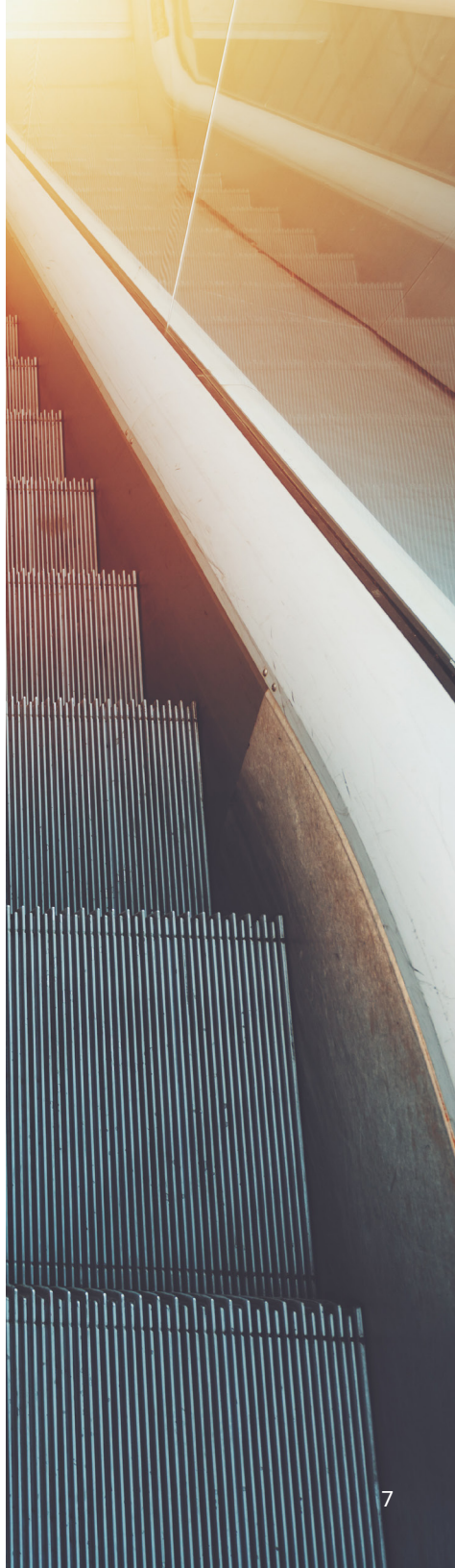
Less than 20% of enterprise organizations have a well-defined incident response plan for insider threat scenarios like quitters.[10] Most focus on external threats — until they experience a major insider threat.

2. Employee offboarding (if it exists) leaves out security.

Just about every company has an onboarding program for new hires. The rare companies that do have defined offboarding programs generally limit them to HR — not including security workflows around data protection. In other words, they're making sure a quitter doesn't take a stapler — but doing nothing to stop them from taking intellectual property.

3. They're expecting legacy DLP to stop every insider threat.

As more organizations embrace so-called Zero Trust (ZT) architectures to enable innovation without sacrificing security, the vast majority (87%) are investing in traditional data loss prevention (DLP) tools as part of ZT strategies.[11]



10. Gartner How to Build Incident Response Scenarios for Insider Threat
11. Forrester TLP Report

LEGACY DLP WON'T SAVE YOU

To enable a Zero Trust environment, security teams need tools that protect data — and empower innovation. The harsh reality is that legacy DLP products no longer achieve either of those goals — and most companies say DLP has created challenges for them.[12] Forrester puts it in more technical — and perhaps harsher — language: "Legacy DLP is a prohibitive and technically limiting solution for businesses." [13]

DLP forces a lose-lose choice.

Legacy DLP forces you to make a choice between security and productivity:

Protect Data — and Impede Your Employees

Maximizing the data loss prevention capabilities of your legacy DLP product mean creating rigid policies that ultimately present significant barriers and limitations to productivity, collaboration and innovation — stifling the lifeblood of the business the solution is meant to protect.

Enable Employees — and Let Data Walk Out the Door

Choosing to fully enable productivity, collaboration and innovation means creating lax DLP policies and endless policy exceptions — invalidating the entire purpose of the solution and leaving you with toothless data protection.

12. Forrester TLP Report
13. Forrester TLP Report

DLP OVERWHELMS YOUR SECURITY TEAM.

Traditional DLP tools continue to strain the time, budgets and patience of IT and security teams with burdensome features:

Full-Scale Data Classification

To be effective, legacy DLP requires a painstaking full-scale data classification exercise.

Ongoing Policy Management

Three-quarters of IT and security teams say they're struggling to adapt DLP policies to keep pace with dynamic business needs.

Alert Fatigue

Sifting through the endless deluge of alerts, winnowing out all the false positives, leaves security teams in a dangerous state of alert fatigue.

Security teams know they need a better way — so why does legacy DLP persist?

A recent Forrester survey found that 81% of data security decision-makers agree they're not happy with their existing DLP solution.[14] The irony is that the tremendous costs of legacy DLP solutions — lengthy implementations, painstaking data classification exercises, ongoing management burdens — have left many organizations without the time or budget to risk trying a new solution.

81%

of security buyers are not happy with their DLP solution

14. Forrester TLP Report

THE BIGGEST PROBLEM:
IF YOU CAN'T SEE ALEX, YOU CAN'T STOP ALEX

Insider threats happen when you 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 data left?**

But legacy DLP really only answers one of those questions — some of the time: has data left? Because you don't know who has (or has access to) what data, your DLP rules fail to catch all the creative ways that quitters take data. And when you do catch it, you can't always tell exactly what's happened, what's been taken, and what you should do about it.

YOU DIDN'T SEE ANYTHING ALEX DID.

Going back to dear Alex, we can see how these visibility gaps play out:

ALEX TOOK SALES PITCH DECKS

Your DLP solution didn't see anything odd about a sales rep moving pitch decks to Dropbox.

ALEX TOOK THE ROI CALCULATOR

Even though you had specific rules set up to protect the proprietary ROI calculator, Alex changed the file name — a pretty simple workaround that flew under DLP radar.

ALEX TOOK A CUSTOMER LIST

Since it happened after he gave his notice, your DLP solution caught Alex moving a file named EastCoast_Contacts.xlsx to Dropbox. But without access/visibility into that file, you couldn't properly determine if action was necessary.

THE BRUTAL

TRUTH

When it comes to stopping quitters,

YOU'RE FLYING BLIND.

PREVENTION WILL FAIL. RESPONSE IS WHAT COUNTS.

It's time to acknowledge that you'll never stop Alex from finding creative ways to take data. But you can stop him from embarrassing your security team and damaging your company. And that's ultimately what your business needs from your security team: protection against the actual business risks of data loss.

Think of it this way: If you tell your C-suite that Alex took a customer list, they're going to ask, "What did he do with it — and what are you doing about it?" They innately know that it's not the act of data theft that matters — it's what happens next that defines the risk and determines the outcome.

1 You need simpler detection.

2 You need faster response.

3 You need next-gen data loss protection.

CODE42 NEXT-GEN DATA LOSS PROTECTION

ELIMINATE BLIND SPOTS

See all your files. See all your users.

Protection depends on response. Response depends on visibility. Code42 continuously monitors all file behavior across all devices and the cloud in real time. No painful data classification here — Code42 works automatically, silently and without slowing down your employees.

TARGET YOUR BIGGEST RISKS

Narrow your focus. Make a bigger impact.

“Stop everything” isn’t just unrealistic, it’s an impractical way to allocate your resources. Quitters are your biggest (and fastest growing) threat, so Code42 gives you a purpose-built workflow that fits into any employee offboarding process and makes it easy to focus on quitters like Alex.

SEE ALEX. STOP ALEX.

See what Alex is doing.

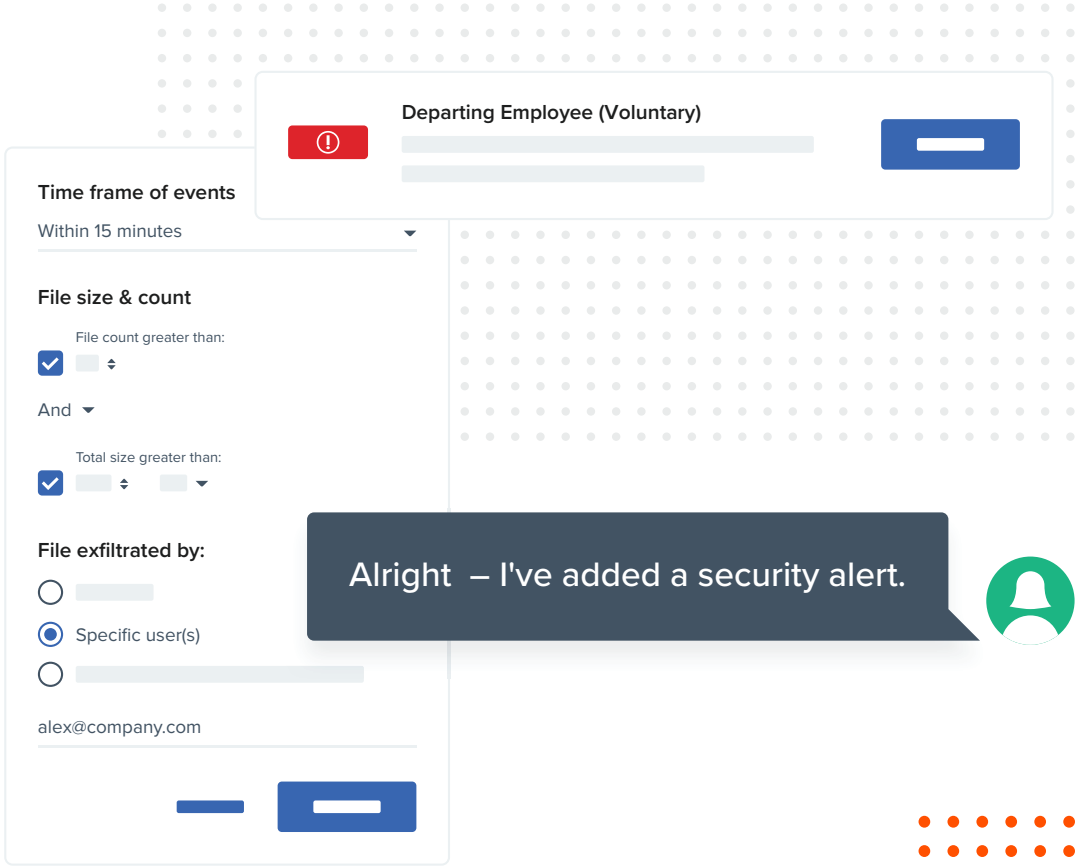
See what Alex has done.

See the weird data events.

See the files.

Take action — before the damage is done.

THE CODE42 QUITTERS WORKFLOW



We saw how Alex flew under the radar of traditional DLP, working around rules to take several sensitive files. Now let's see what happens when Alex tries to beat the targeted Code42 departing employee workflow:

Alex is quitting.

As soon as Alex gives his notice, your security team adds him to the departing employee alert profile.

Next-Gen Capability: High-Risk Alert Profiles

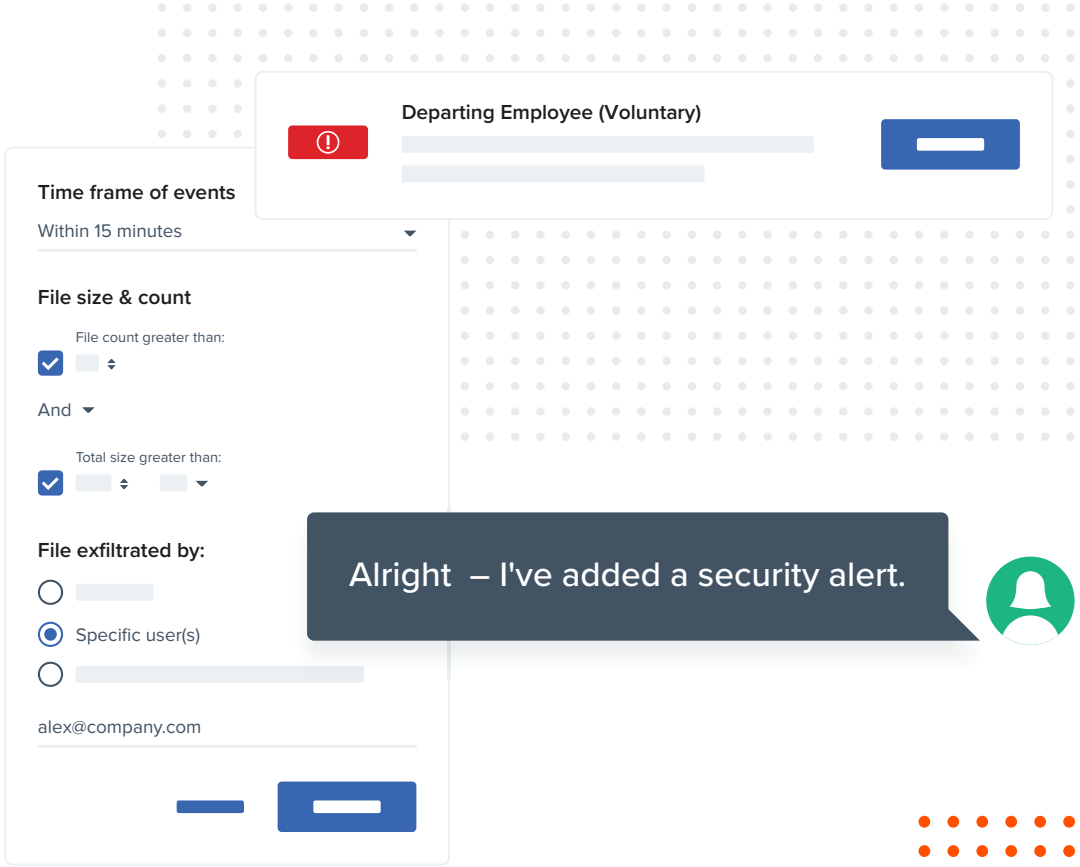
Leverage pre-built alert profiles for your most high-risk scenarios, including departing employees.

A Smarter Outcome:

Focus on your biggest risks.

Your security team is honed in on the specific and unique risk presented by Alex — and any other quitters.

THE CODE42 QUITTERS WORKFLOW



We saw how Alex flew under the radar of traditional DLP, working around rules to take several sensitive files. Now let's see what happens when Alex tries to beat the targeted Code42 departing employee workflow:

Alex is quitting.

As soon as Alex gives his notice, your security team adds him to the departing employee alert profile.

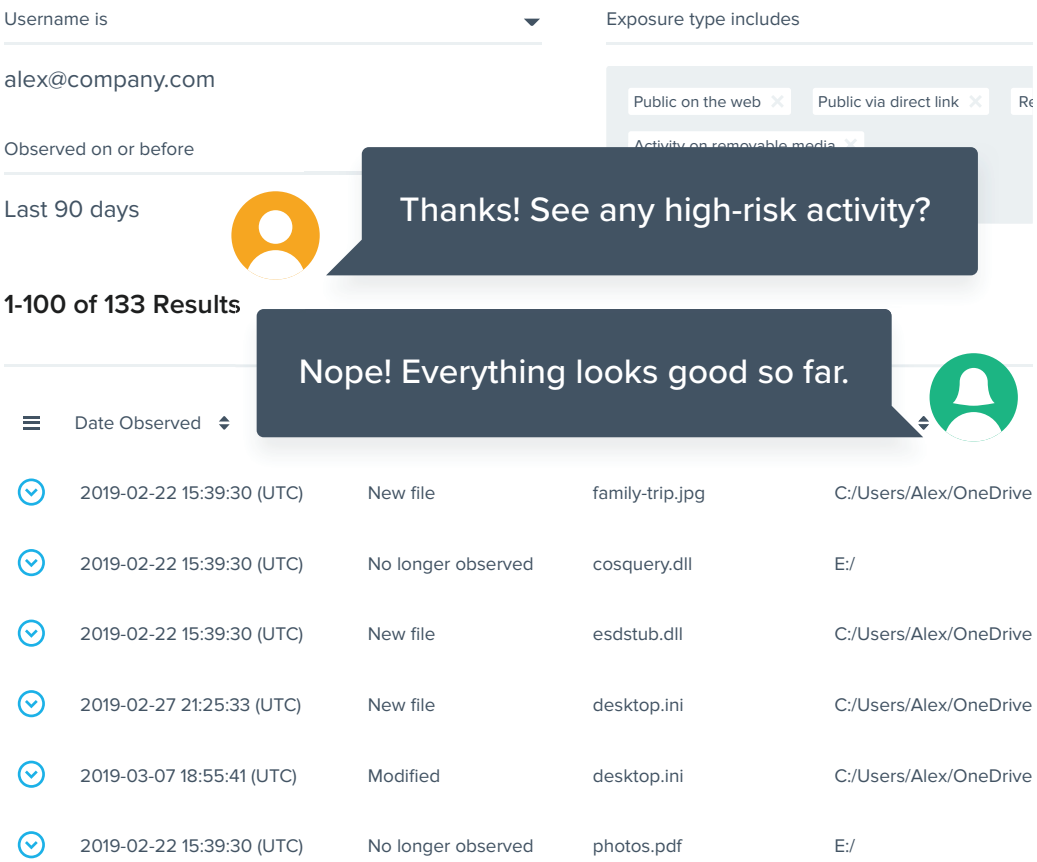
Next-Gen Capability: High-Risk Alert Profiles

Leverage pre-built alert profiles for your most high-risk scenarios, including departing employees.

A Smarter Outcome:

Focus on your biggest risks.

Your security team is honed in on the specific and unique risk presented by Alex — and any other quitters.



You take a closer look at Alex.

Adding Alex to the departing employee profile also triggers an automatic 90-day historical review. Your security team looks back at the last 90 days of Alex's file activity. Fortunately, the review shows nothing unusual happened.

Next-Gen Capability: Historical Breadth

Because you're constantly monitoring file activity for all employees, you can instantly conduct historical analysis of file activity for any employee. Narrow your investigation by timeframe, exposure type, file category, file name, file hash and more.

Next-Gen Capability: Forensic Depth

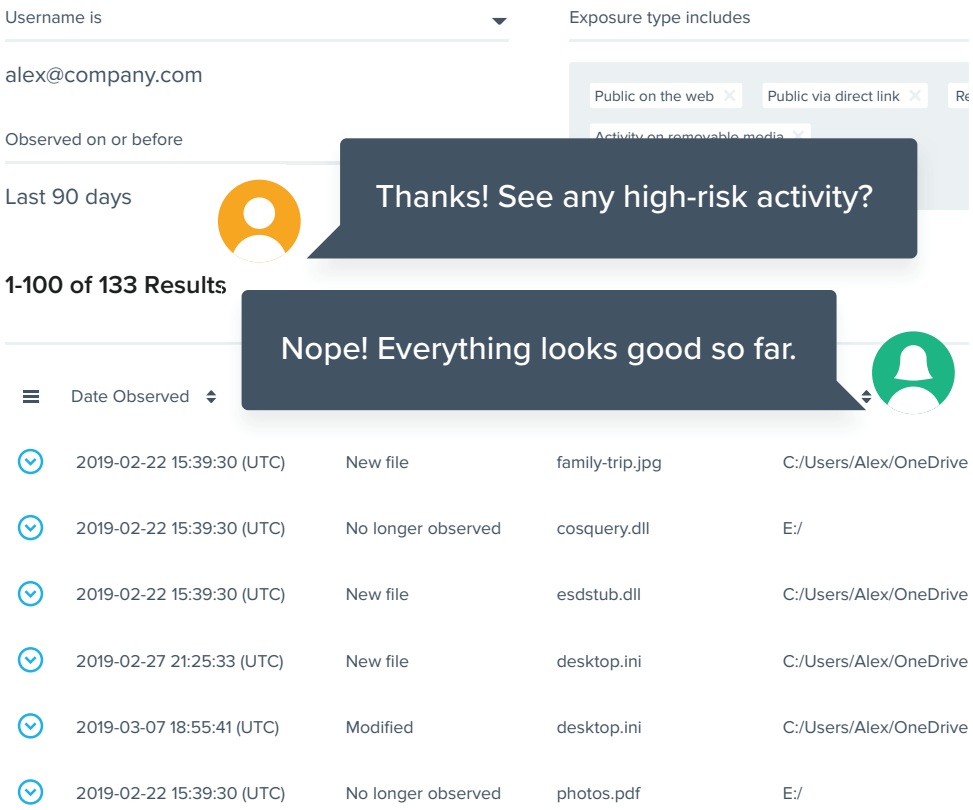
Detect when your employees move files to removable media devices, web browsers, web applications and cloud sync folders, as well as when they share files externally via corporate OneDrive, Google Drive and Box environments.

A Smarter Outcome:

Take a look back — see all activity.

Your security team has the historical breadth to follow the best practice of looking back at the last 90 days of file activity — since most data theft happens before an employee gives notice.

CODE42



You take a closer look at Alex.

Adding Alex to the departing employee profile also triggers an automatic 90-day historical review. Your security team looks back at the last 90 days of Alex's file activity. Fortunately, the review shows nothing unusual happened.

Next-Gen Capability: Historical Breadth

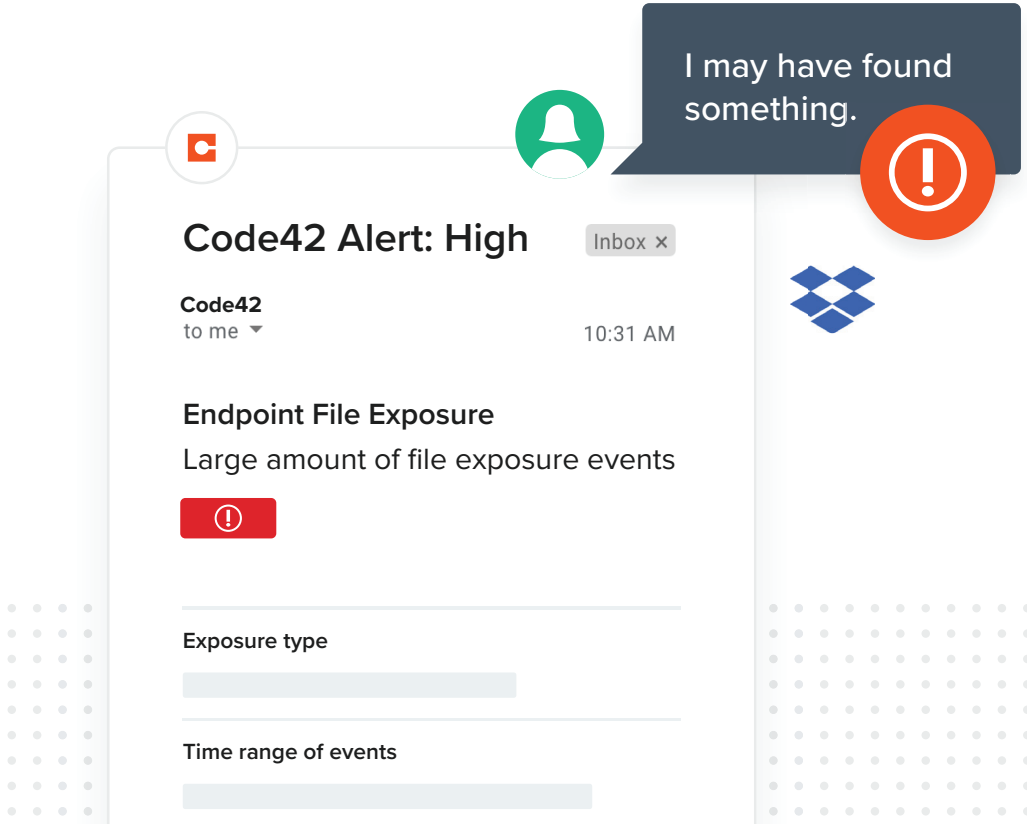
Because you're constantly monitoring file activity for all employees, you can instantly conduct historical analysis of file activity for any employee. Narrow your investigation by timeframe, exposure type, file category, file name, file hash and more.

Next-Gen Capability: Forensic Depth

Detect when your employees move files to removable media devices, web browsers, web applications and cloud sync folders, as well as when they share files externally via corporate OneDrive, Google Drive and Box environments.

A Smarter Outcome:

Take a look back — see all activity.
Your security team has the historical breadth to follow the best practice of looking back at the last 90 days of file activity — since most data theft happens before an employee gives notice.



Alex moves files to DropBox — and you see it.

Three days after giving his notice, your security team receives an alert that Alex added several files to a DropBox account minutes ago.

Next-Gen Capability: Customizable Alerts

Easily customize alerts for near-real-time notification of risky activity based on the type of activity (removable media, web browsers/apps, cloud sync applications or file sharing) as well as by file size and count. Alerts don't depend on data classification, because Code42 automatically assigns file categories to help you identify your most important data at a glance.

A Smarter Outcome:

Alerts you can trust

Your security team has alerting that means something. No more alert fatigue; just focused alerts that you know deserve your full attention.

Yup – there's a file that looks like a risk.

1-6 of 6 Results

Date Observed (UTC)	Event Type	Filename	File Category
2019-02-22 15:39:30 (UTC)	Modified	SalesProposalTemplate.pptx	Presentation
2019-02-22 15:39:45 (UTC)	**Modified**	**EastCoast_Customers.xlsx**	**Spreadsheet**
2019-02-22 15:40:02 (UTC)	Modified	2019_AlexResume.docx	Document
2019-02-22 15:40:30 (UTC)	Modified	Family-Vacation.jpg	Image
2019-02-22 15:40:45 (UTC)	Modified	Alex Johnson W-9.xlsx	Spreadsheet
2019-02-22 15:41:15 (UTC)	Modified	Project Summary.docx	Document

You see exactly what Alex moved.

Looking at the list of files Alex moved to DropBox, most look harmless — a W-9 form, his resume, a few photos — but the file named EastCoast_Contacts.xlsx sounds like it could be a customer list.

You open that file.

There's no guesswork about whether the file in question is sensitive or valuable. You simply open the file and immediately see that, yes, it's a list of all of Alex's customer contacts on the east coast.

Next-Gen Capability: File Access

When you're alerted of risky file activity, you can quickly access the file(s) in question — even restoring files that users have deleted.

A Smarter Outcome:

See the file in question.

Make an informed decision.

Access to the file in question enables you to make a fully informed decision about whether it's acceptable, harmless activity — or if it warrants a response.

Restored the file. It's definitely proprietary and needs to be removed.

EastCoast_Customers.xslx

Company Name	Client Name	Email Address	Phone Number
Reception Hub	Catherine Pierce	c.pierce@receptionhub.com	+1 (212) 555-9450
Cloud Coder	Joel Fox	joel.fox@cloudcoder.com	+1 (803) 555-1219
NestEasy	Patrick Poole	patrick.poole@nesteasy.com	+1 (215) 555-3415
Ivy Ladder	Annie Ross	annie.ross@ivyladder.com	+1 (212) 555-8589
Nuvallo	Beulah Reeves	beulah.reeves@nuvallo.com	+1 (401) 555-9813

You make Alex permanently delete the file from DropBox.

You call Alex's manager with a clear and confident response plan. Alex's manager tells Alex that we know exactly what he's taken — and his manager watches as Alex permanently deletes the file from his DropBox account.

Next-Gen Capability: Fast Response

Armed with full visibility into exactly what has happened, you can quickly take action to address the specific, identified risk. This generally begins with requiring the files be returned or deleted, but may also include escalating to management, taking disciplinary action through HR, or sending a legal notice to the employee.

A Smarter Outcome:

Take confident action sooner.

You're getting all the facts — and getting them in near-real-time. You can respond quickly and confidently to protect against the identified risk(s).

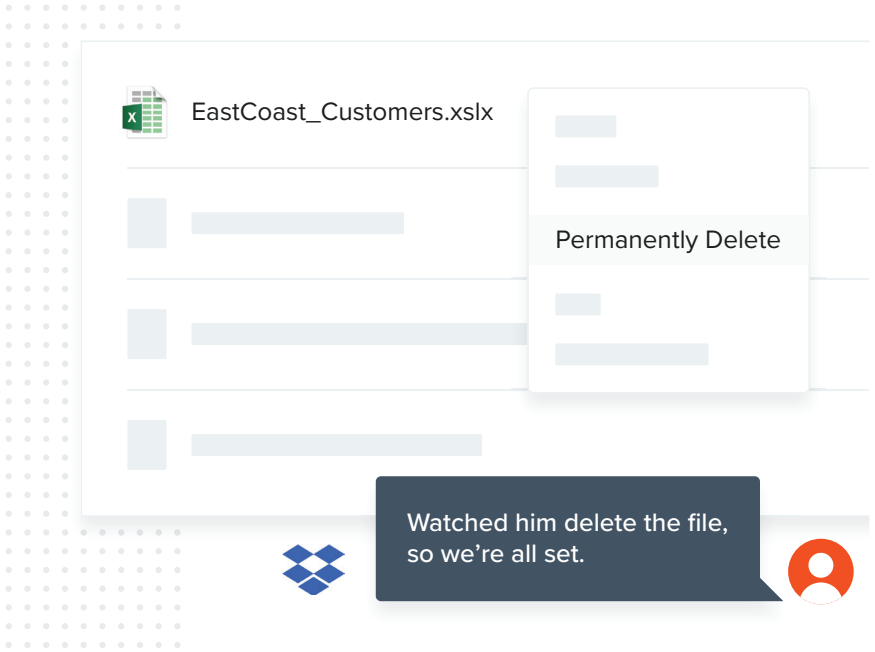
THE SMARTEST OUTCOME:

You stopped Alex before damage was done.

You didn't stop Alex from taking the data — but neither did your legacy DLP.

Shifting your approach from prevention to protection enabled you to:

FOCUS	Key in on Alex as a unique risk
SEE	See Alex doing something unusual
ASSESS	Clearly discern the risk and the necessary response
ACT	Swiftly take action — before the damage was done



YOU'RE THE HERO.

Now, when you're called in to that executive meeting, you get to be the hero instead of the scapegoat. You get to tell your C-suite that you hunted down Alex. That you beat him at his own game. That you stopped him from poaching customers. That you protected your business from damage and embarrassment. And then, you get to ask for a raise.

YOU CAN START STOPPING ALEX RIGHT NOW.

Quitters like Alex are walking out your doors with data every day. You don't have the time (or the budget) for a months-long rollout that requires extensive tweaking and optimization before you can start using it. You need a better solution — now. Code42 built the next-gen data loss protection solution with this reality in mind. You'll see none of the time-sucking, money-wasting hassles you've experienced with legacy DLP products.

Deploys in days.

Next-gen data loss protection deploys in your environment in just a few days.

Results in minutes.

Immediately gain 100% visibility of all your files and all your file activity. Pre-built workflows for quitters and other high-risk scenarios mean you're ready to start hunting down Alex from Day 1.

One Agent — 100% Cloud

Built for the cloud, next-gen data loss protection gives you the simplicity and flexibility of a single agent and a centralized admin platform for all your devices — Mac, Windows and Linux.

YOU CAN GIVE YOUR TEAM EFFICIENCY THEY LOVE.

By shifting to next-gen data loss protection, you're not just stopping quitters like Alex — you're saving your team time, money and frustration.

Focused efforts. Simple workflows.

With your legacy DLP solution, your team was struggling to manage and adapt the complex web of policies — and buried in endless alerts. But with next-gen data loss protection, you've focused your team's efforts on your biggest risks — and you've given them simple, purpose-built workflows triggered by specific events:

CONFIGURE

Add user to a voluntary separation alert profile

LOOK BACK

Review past 90 days of activity

DETECT

Receive activity alerts via email or SIEM

INVESTIGATE

Examine flagged activity

REVIEW

Restore file(s) in question

REPORT

Close case OR report to user's manager

Escalate to HR, legal

...AND GIVE THEM MORE TIME TO HUNT DOWN THE NEXT ALEX.

The focused and streamlined workflows of next-gen data loss protection gives your team valuable time back, so they can hunt down the next insider threat.

Moving to Code42 was a transition from having multiple teams that put a lot of efforts and hours to conduct investigations, to having one person achieve better results with a few clicks."

– Senior Manager on Equipment Services Team,
Forrester Total Economic Impact Study, 2019

As an outcome of adopting Code42, organizations reduced the time spent by IT and security on data collection, recovery and investigations — giving staff capacity to support other initiatives."

- Forrester Total Economic Impact Study, 2019

YOU CAN DELIVER VALUE THE "BIG WIGS" CAN'T IGNORE.

Money talks — and business leaders listen. That's why talking risk mitigation to business leaders is typically so tough. They don't want to hear about what might have happened — they want to see what you've done. The money you've saved. The value you've added. Next-gen data loss protection gives you the compelling metrics you need. 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.[15]

$925,000 NPV

(Net Present Value)[16]

PAYBACK IN 3 MONTHS[17]

That's more than two dollars earned for every dollar spent.

CODE42

15. Forrester Total Economic Impact study, 2019
16. Forrester Total Economic Impact study, 2019
17. Forrester Total Economic Impact study, 2019

THE BRUTAL

TRUTH

Next-gen data loss protection
stops your biggest insider threats for just

33 CENTS A DAY.

CODE42

QUITTERS ARE YOUR BIGGEST RISK. SEE THEM. STOP THE DAMAGE.

Employees are more transient than ever. Data is more portable than ever. And outdated data loss prevention just can't cut it. Quitters are taking valuable data and most organizations are helpless because they can't even see what's happening. It's time to get smart about the quitter conundrum — and shift your approach from prevention to protection.

Empower your employees — unburden your team.

Stop letting legacy DLP stifle your employees' productivity, collaboration and innovation. Free your security team from the constant policy management and endless stream of false-positive alerts. Enable a true Zero Trust architecture for your business.

Focus your efforts.

Quitters account for more than half of insider threat incidents. Build simple, targeted workflows that focus your security team and your security tools on quitters — and the other small subsets of high-risk employees that account for 80% of data loss.

See all file activity.

To stop something, you have to see it first. You need visibility into all your files and all your file activity — including full historical breadth — so you can detect when a quitter takes data.

Enable faster response.

To move from alert to response quickly, you need full access to every file, so you can investigate unusual events, confidently assess the risk and swiftly take action.

AVOID THE EMBARRASSMENT. PROTECT YOUR DATA. BE THE HERO.

Quitters take data. Prevention will fail. Don't be blindsided by it. Get the visibility and access you need to detect events in real time and respond before the damage is done. Save time and money. Save frustration and embarrassment. Stop quitters — and save the day.

CODE42

DATA LOSS PROTECTION FOR WHEN PEOPLE QUIT

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