CrashPlan™

Data in the Dark

The Unseen Endpoint Data Challenge

Key data points from the 2024 SANS Endpoint Data Survey

The SANS Institute, in partnership with CrashPlan, conducted the 2024 Endpoint Data Survey to uncover how organizations manage and protect their endpoint data. For security leaders, the survey shines light on the persistence of uncontrolled data on endpoints including intellectual property, customer data and more. It also explores how this problem is inextricably linked to operational challenges both on the end-user side and the IT side.

Where Policies Fall Short

Despite having policies and/or technical controls to limit data stored on endpoints, users often create and store valuable, sensitive data on these devices. This issue has worsened with the rise of hybrid and remote work environments.

Personally Identifiable Information

62% have policies prohibiting users from copying PII onto endpoints, and **54%** have technical controls in place to prevent it

80% of organizations believe their users are bringing PII onto their endpoints regardless of policy

Only **6%** stated they were sure their users didn't have PII on their devices

Intellectual Property

52% have policies prohibiting users from copying IP onto endpoints, and **54%** have technical controls in place to prevent it

78% of organizations believe their users are bringing IP data onto their endpoints regardless of policy

Only **8%** stated they were sure their users didn't have any IP on their devices

The Compliance/Productivity Equation

While the majority of companies try to enforce special handling for PII and compliance-related data, end users often store this data on endpoints to maintain efficiency and productivity—indicating a need for better security measures that do not hinder employee productivity.

78% of organizations store, process, or transmit data that requires special handling because of externally imposed regulations or other standards

Only **55%** of respondents have a backup policy and believe it's working as intended

The **top 2 reasons** people break backup policies:
1) Too hard to enforce, and
2) Policies make it too hard for users to get their work done

Reputation at Risk

Data leaks can severely damage an organization's reputation, especially when customer information or critical IP like product roadmaps are exposed. Because not all breaches can be prevented, it's essential to have visibility into what data is stored on endpoints.

Across all types of data, respondents agreed reputational risk was the greatest concern when it comes to data breaches

Greatest Risk if Data is Exposed

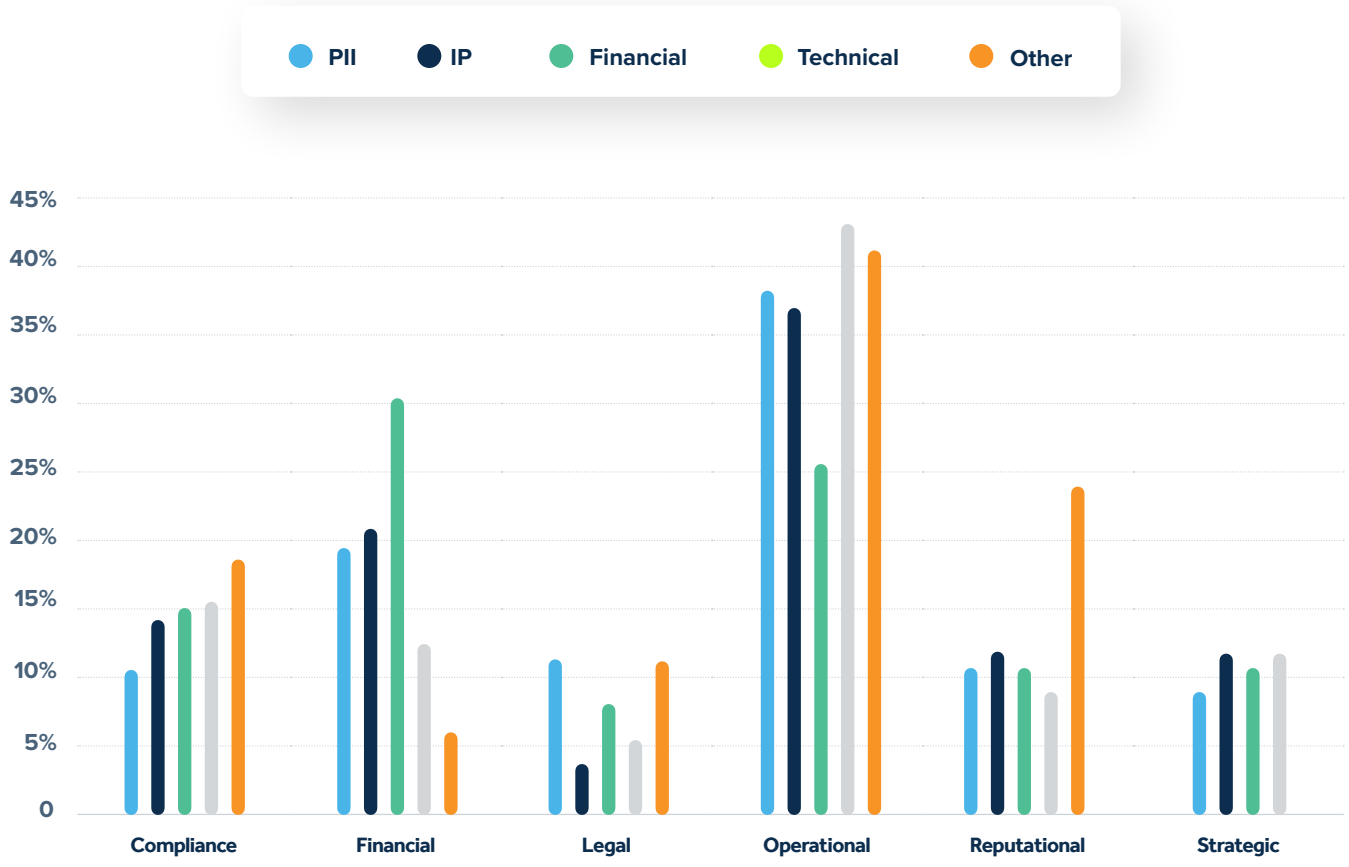
 | crashplan.com

Data Loss Disruption

IT leaders reported operational disruptions are the most significant consequence of endpoint data loss. These disruptions—such system downtime, lost employee productivity, and the need for extensive incident response—can severely impact day-to-day business operations.

Respondents reported operational risk was the greatest concern in the event of data loss. The only exception was for financial data, where the greatest risk was (understandably) financial.

Greatest Risk if Data is Deleted



“Regardless of policies, users are always going to work in the ways that they find fastest and easiest. Organizations need to consider the business needs that are driving users to store data on their local devices and take a human-centric approach to solving the problem.”

— Todd Thorsen, Chief Information Security Officer, CrashPlan

Discover more insights and access the full report at crashplan.com/resources/video/do-you-know-where-your-data-is-sans-endpoint-data-survey-2024.

Don’t Let Your Data Go Dark

Close the Endpoint Data Resiliency Gap with CrashPlan

1. **Complete, Continuous Backup:**

   15-minute incremental backups require no user action.

2. **Ransomware and Disaster Recovery:**

   CrashPlan protects your data integrity, enabling seamless recovery from even the most sophisticated ransomware threats.

3. **Remote Workforce Management:**

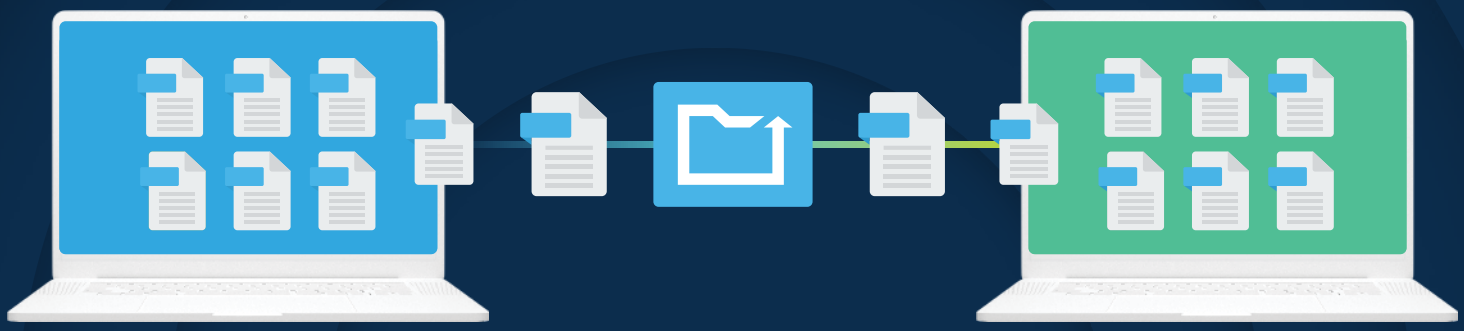
   Effectively manage data loss risks and ensure data integrity during employee transitions and device migrations.

4. **Unlimited Storage and Version Control:**

   Eliminate storage limitations and easily restore any document directly to the user’s desktop.

5. **Legal Hold and Compliance:**

   Meet rigorous auditing requirements worldwide with limitless version retention and secure electronically stored information (ESI).



CrashPlan™

1.4M+
devices protected

900K+
users

100B+
files recovered annually

Trusted by over 50,000 businesses

CrashPlan has given our organization the peace of mind that our data is being backed up. As much as we try to have individuals use cloud or network sites to store their work documents, they still will store items locally."

— Scott O, Executive Director of Network Applications and Security at Maryville University of Saint Louis

Start your free 14-day trial

visit crashplan.com/enterprise