CyberGrant
SECURITY MADE EASY

WHITE PAPER

Data Loss Prevention. Next Level

Are your company’s data truly secure?

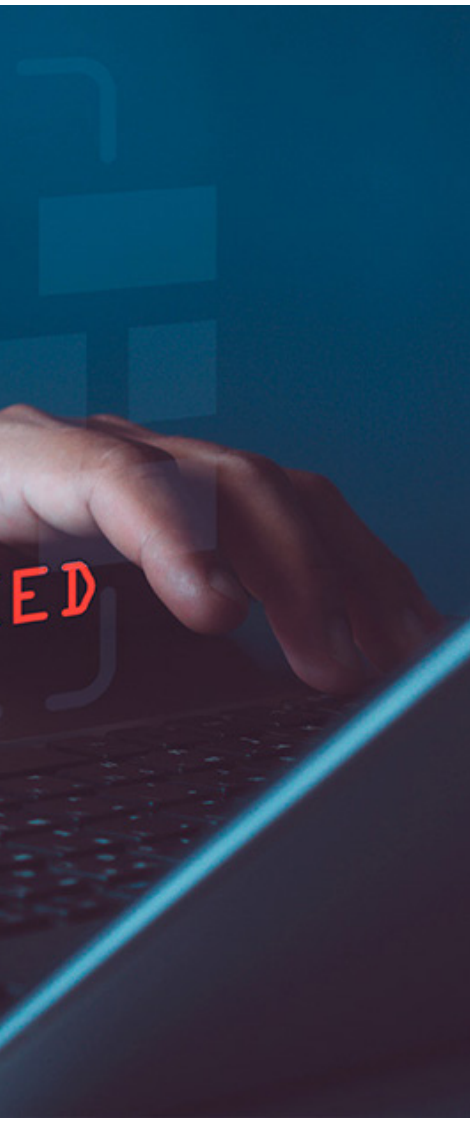
Economic and reputational risks

The answer might surprise you.

Data Loss Prevention (DLP) is often underestimated or misapplied. But with the increasing complexity of IT infrastructures and regulatory pressure, organizations can no longer afford to ignore it.

Solutions like **FileGrant Enterprise and RemoteGrant** offer a new way forward—by automating classification, securing endpoints, and containing the reputational and financial fallout of sensitive data loss.

Index



Overview

10.626 data breaches in 2024

The 2024 Data Breach Investigation Report by Verizon paints a sobering picture:

10,626 confirmed data breaches, nearly doubling the 5,199 incidents from 2023.

This sharp rise stems from a combination of:

- Increased attacker sophistication
- Expanding digital footprints of organizations

Key insights from the report:

- **68% of breaches involved human error**, typically through social engineering or accidental mistakes.
- **15% involved third parties**, such as software supply chains, hosting partners, or data custodians.

Image Source: "2024 Data Breach Investigation Report" by Verizon

AI used as an attack vector

Human error and third-party risk remain dominant causes of data breaches.

Moreover, **artificial intelligence has entered the threat landscape**—not just as a tool for defense, but also as a vector for attack. Deepfakes, AI-generated phishing, and fully automated malware are already being exploited.

SaaS platforms and major cloud providers are also under siege. The past year has seen an uptick in cloud-based attacks, including incidents involving Snowflake and other high-profile vendors.

Cost of a Breach in 2024: Rising Fast

> **$4,88 million**
>
> **average global cost of a data breach**

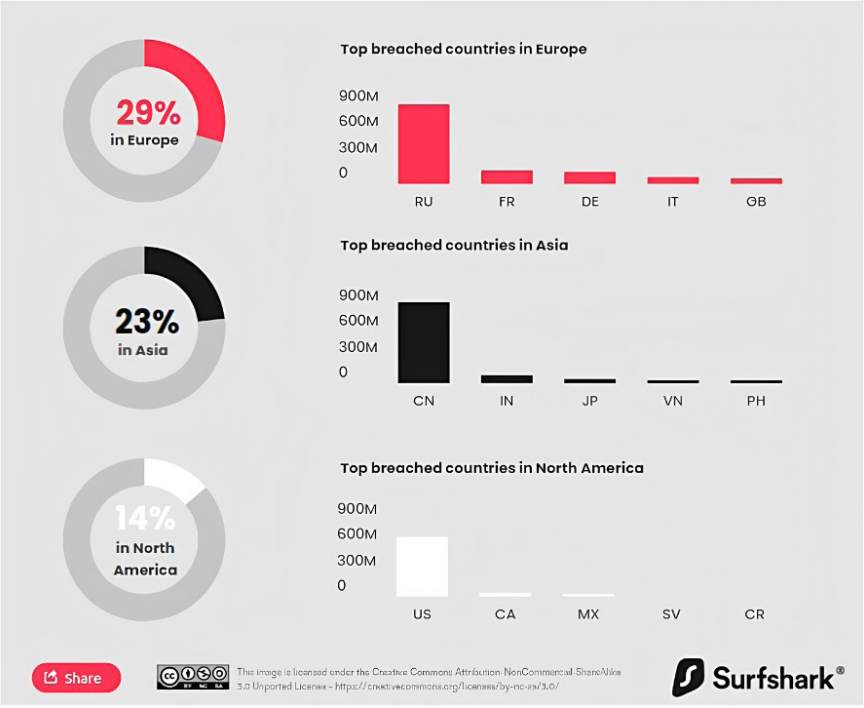
According to the Cost of a Data Breach Report 2024 by IBM and the Ponemon Institute:

- **$4.88 million** – the average global cost of a data breach in 2024, up 10% from last year.
- **1 in 3 breaches involve "shadow data"** – untracked data that resides in multiple environments, complicating visibility and protection.
- **$2.22 million saved on average** by organizations that use AI-driven security and automation extensively.
- **292 days – time needed on average to detect and contain breaches** involving stolen credentials. Phishing takes ~261 days, and social engineering ~257.

Where Are Breaches Happening?

According to **Surfshark's Data Breach Recap 2024**, data breach exposure by region is as follows:

- **Europe: 29% of breached accounts** (1.6+ billion), with Russia leading.
- **Asia: 23%** (nearly 1.3 billion), led by China.
- **North America: 14%** (approx. 770 million accounts), mainly in the U.S.



Fonte immagine – Surfshark - "Data Breach Recap 2024"

What’s Causing These Breaches?

External attacks and internal weaknesses

Data breaches in 2024 stem from both external attacks and internal weaknesses. The main culprits:

- **Stolen or compromised credentials (16%)**
- **Phishing attacks (15%)**
- **Human error and system misconfigurations (45%)**
- **Malicious insiders (7%)**
- **Ransomware attacks (23%)**
- **Outdated or unpatched software**

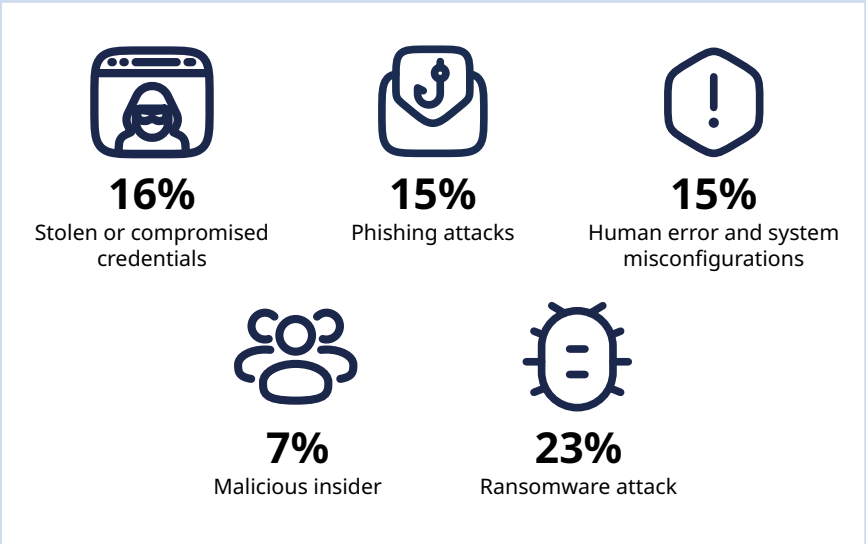


Image created with icons and percentages reflecting data collected from IBM and Verizon reports.

Poor password hygiene, misrouted emails, and improperly configured databases are all examples of small oversights that lead to big consequences.

Additionally, cloud misconfigurations, unsecured endpoints, and communication over unmonitored mobile channels expose data in ways most companies don’t anticipate.

Breach Impact by Industry

Each sector faces unique cybersecurity challenges based on the type of data they manage, their operating models, and their regulatory landscape. Here are the highlights from the **IBM 2024 report**.

Healthcare: The Costliest Industry

$ 9,77 million

average cost per breach

For the 13th consecutive year, healthcare remains the most expensive industry for data breaches:

Le ragioni principali per cui il settore sanitario è particolarmente vulnerabile includono:

- **$9.77 million – average cost per breach**
- **Increasing reliance** on digitized patient records
- **Strict regulatory penalties** for non-compliance (HIPAA, GDPR, etc.)

Why healthcare is particularly vulnerable:

- Highly sensitive patient data (e.g., medical history, diagnostics)
- Service disruption = life-threatening impact
- Ransomware delays treatment, risking lives and hospital trust

Financial Services: Under Constant Siege

$ 6,08 million

average breach cost

Financial institutions continue to be prime targets due to their access to monetary assets and sensitive financial records:

- **$6.08 million – average breach cost, higher than the cross-industry average**

Top risks include:

- **Regulatory penalties from frameworks like GDPR, DORA, PCI-DSS**
- **Operational downtime and financial theft**
- **Loss of customer trust, impacting retention and acquisition**

Manufacturing & Industrial: Rising Risk

This sector—covering production, utilities, and critical infrastructure—has seen the **steepest increase in data breach costs**.

Key trends from 2024:

- **+ $830,000 average increase per breach**
- **219 days to detect**, 85 days to contain – both above average

Why industrial operations are especially at risk:

- **IT/OT convergence expands the attack surface**
- **Downtime = revenue loss and supply chain delays**
- **Legacy systems lack modern protections**
- **Cyber-physical risk –** attacks can damage equipment and endanger safety

Why Data Loss Prevention (DLP) Matters

Direct consequences

Data breaches trigger significant consequences—financial, reputational, legal, and operational.

The top five reasons to prevent data loss:

1. **Financial losses** – both direct (fines, recovery) and indirect (downtime, churn)
2. **Brand reputation damage** – customer trust takes years to rebuild
3. **Legal and regulatory sanctions** – penalties and audits are getting stricter
4. **Service disruption** – affects business continuity and delivery commitments
5. **Third-party risks** – vendors and supply chains multiply exposure

Recognizing these factors is the first step toward building an effective data protection strategy.

What is Data Loss Prevention (DLP)?

DLP is a **set of technologies, policies, and procedures that detect and prevent the unauthorized access, transfer, or exposure of sensitive business data**.

It plays a critical role in safeguarding sensitive information and maintaining regulatory compliance.

Key pillars of DLP

- **Data discovery & classification –** Know what you're protecting
- **Data visibility –** Track data flows and interactions
- **Access control –** Limit data usage based on user roles and privileges

Types of DLP

DLP solutions are typically divided into three categories:

1. **Endpoint DLP** – Protects data on user devices like laptops and desktops. E.g., blocks file transfers from a company laptop to an external USB drive.
2. **Network DLP** – Monitors data in motion across the corporate network. E.g., prevents email attachments with sensitive info from being sent externally.
3. **Cloud DLP** – Secures data in cloud services such as Google Drive, Dropbox, or AWS. E.g., restricts unauthorized downloads from shared folders.

Overcoming the Challenges of DLP Implementation

While DLP is essential, many organizations struggle to implement it effectively. Below are the most common barriers—and the strategies to overcome them.

Identifying Sensitive Data

Challenge: Many companies lack a clear inventory of what constitutes sensitive data, especially when it comes to personally identifiable information (PII), financial data, and critical business IP.

Solution: Use AI-powered DLP tools that **automatically classify and tag** sensitive data across file types and locations. These systems improve visibility and reduce the risk of overlooking high-value information.

Monitoring Data Movement Across Environments

Challenge: With hybrid and remote work, data lives across multiple platforms—on-premise, cloud, SaaS, mobile—and visibility becomes fragmented.

Solution: Deploy multi-environment DLP solutions that provide real-time monitoring across:

- File storage
- Email and collaboration platforms
- Cloud services

Managing Access Rights

Challenge: Balancing security with operational flexibility. How do you ensure users can access what they need—without exposing too much?

Solution: Implement r**ole-based access control (RBAC)** with **least privilege principles**. Modern DLP platforms support:

- Fine-grained access policies
- Multi-factor authentication (MFA)
- Regular auditing of access logs

This ensures that only authorized users access sensitive content, without slowing productivity.

Mitigating Insider Threats

Challenge: Insiders with valid access can still cause damage—intentionally or accidentally.

Solution:

- Segment data access by role
- Conduct background checks
- Implement continuous behavioral monitoring
- Define exit protocols for departing employees
- Use “on-behalf” access features for internal audits

Creating a transparent and accountable work culture is key.

Mini Roadmap for Rolling Out DLP Successfully

Here's a strategic sequence of actions to implement a modern DLP solution:

1. **Understand Your Data**

   Collaborate across departments to identify what needs protection—customer data, financial records, source code, etc.

   Use interviews and data discovery tools to map critical assets.

2. **Develop Global DLP Policies**

   Build policies that cover:

   - Data classification
   - User roles and access levels
   - Data handling rules (storage, sharing, encryption)

   Ensure these policies are clear, documented, and updated regularly.

3. **Train Employees and Build Awareness**

   DLP starts with people. Run regular workshops, simulate phishing attempts, and demonstrate DLP tools.

   When users understand their role in data stewardship, compliance improves dramatically.

4. **Enable Real-Time Monitoring and Incident Response**

   Deploy tools that detect anomalies and trigger automated workflows.

   Have an incident response plan ready to isolate breaches and mitigate damage fast.

5. **Audit and Iterate**

   Run regular audits to assess effectiveness.

   Update policies and technologies based on:

   - Internal changes (new teams, tools)
   - External trends (emerging threats, new regulations)

DLP as a Strategic Lever for Regulatory Compliance

From GDPR in Europe to DORA, NIS2, PCI-DSS, and the upcoming AI Act, global regulations are tightening around data protection, privacy, and operational resilience.

DLP solutions are no longer optional—they are a foundational layer for compliance. Let's explore how.

ISO/IEC 27001

A globally recognized standard for information security management systems (ISMS), ISO 27001 outlines specific controls relevant to DLP:

- A.8.8 – Protect sensitive information
- A.9.4.1 – Monitor and control access to data

These controls are core features of modern DLP platforms.

GDPR

The EU's General Data Protection Regulation requires strict technical and organizational safeguards to protect personal data.

DLP enables compliance by:

- Identifying and classifying personal data
- Monitoring data flows and user behavior
- Logging and documenting access and transmission events
- Supporting "data minimization" and "right to erasure" principles

PCI-DSS

Applies to any organization handling payment card data.

DLP helps enforce the confidentiality of payment records and prevents cardholder data from leaking via unprotected channels.

DORA (Digital Operational Resilience Act)

This EU regulation focuses on financial entities and ICT providers. It requires:

- Risk assessments
- Security controls to prevent data exfiltration
- Audit trails for sensitive data access

DLP solutions that monitor endpoints and cloud storage are essential to fulfilling DORA's technical compliance requirements.

NIS2 Directive

Aims to boost the cyber resilience of critical infrastructure and essential services across the EU.

Key mandates include:

- Real-time monitoring of sensitive systems
- Incident detection and response
- Data access logging and retention

All of which are native capabilities in leading DLP platforms like RemoteGrant and FileGrant.

AI Act

Set to become the world's first comprehensive AI regulation, the AI Act mandates that data used by AI systems must be protected throughout their lifecycle—training, inference, and storage.

- DLP solutions provide essential safeguards by:
- Blocking unauthorized AI model training on sensitive datasets
- Ensuring file-level encryption during processing
- Aligning AI data flows with existing privacy laws (e.g., GDPR)

CyberGrant's Approach to DLP

Cyber Grant Inc. (Menlo Park, California) offers two tightly integrated DLP solutions:

FileGrant

An AI-resistant, **encryption-first platform** ideal for:

- **Encrypting all file types** (PDFs, Office, media, CAD, etc.)
- **Applying AES-256 encryption** with offline protection
- **Embedding encrypted files into PDFs** for safe previews
- **Enforcing secure file downloads** (even by file owners)
- **Protecting against AI-based scraping** (e.g., ChatGPT, Copilot)
- **Role-based access** logging and complete sharing control
- **Disabling screen captures** and unauthorized printing

It supports full regulatory traceability, helping enterprises pass audits with confidence.

RemoteGrant

Focused on **endpoint protection and behavioral control**, RemoteGrant allows organizations to:

- **Block unauthorized data exfiltration** at the system level
- **Set context-aware usage restrictions** without interrupting workflows
- **Monitor file access by application, user, and network** environment
- **Lock down RDP access**, USB ports, and cloud uploads
- **Prevent AI assistants** and scripts from scraping or modifying data
- **Create custom, on-demand security policies** based on business logic

It's particularly effective in hybrid work environments and virtualized systems.

Both solutions support a Zero Trust Architecture and are engineered to meet the needs of regulated industries like finance, healthcare, and manufacturing.

Conclusion

In today's data-driven economy, Data Loss Prevention (DLP) is no longer a "nice to have"—it's a **strategic necessity.**

The stakes are higher than ever:

- **Cyber threats are more sophisticated**
- **Regulatory demands are intensifying**
- **The digital footprint of every organization continues to grow**
- **Hybrid and remote work have redefined the security perimeter**

DLP: From Reactive to Proactive

Next-gen DLP is not just about blocking threats. It's about:

- **Improving data visibility**
- **Enabling secure collaboration**
- **Enhancing incident response**
- **Ensuring business continuity**
- **Building digital trust**

Organizations that implement modern DLP solutions gain not just compliance, but a resilient posture that protects their reputation, operations, and future growth.

Why DLP is a Strategic Investment

By adopting DLP platforms like **FileGrant Enterprise and RemoteGrant**, companies can:

- **Proactively prevent data loss and breaches**
- **Secure sensitive files across all environments**
- **Align with evolving regulations (GDPR, NIS2, DORA, AI Act)**
- **Enable secure, AI-aware workspaces**
- **Maintain full control over who accesses what, when, and how**

This isn't just a cybersecurity decision—it's a business continuity imperative.

Stay Compliant. Stay Resilient. Stay Ahead.

As cyber risks and compliance requirements accelerate, organizations must act decisively. Choosing a robust DLP strategy isn't just about protecting data—it's about protecting trust.

Whether you're in finance, healthcare, manufacturing, or SaaS, CyberGrant delivers enterprise-grade tools that combine encryption, access control, user behavior analytics, and AI governance—all in one unified platform.

Ready to rethink your DLP strategy?

Contact CyberGrant today to learn how FileGrant Enterprise and RemoteGrant can help you protect what matters most.

info@cybergrant.net

Edited by **Federica Maria Rita Livelli**

www.cybergrant.net