



Beyond Sync and Share

How Druva Outshines OneDrive and Google Drive for
Endpoint Protection and Cyber Resilience

Introduction

As organizations increasingly adopt cloud storage solutions to support remote work and digital transformation, the need for robust Endpoint protection has become more critical than ever. While platforms like Microsoft OneDrive and Google Drive offer cloud storage, file synchronization and collaboration capabilities, they fall short when it comes to comprehensive data protection, security, and recovery. These cloud storage solutions are not designed for addressing the complex challenges of modern enterprises that require advanced data integrity, ransomware resilience, and compliance management.

With cyber threats on the rise and regulatory requirements growing more stringent, businesses must seek solutions that go beyond basic sync and share functions. They need automated backup, granular recovery options, ransomware defense, and full-scale compliance management to ensure the continuity of operations and the security of critical data. Druva, a leader in cloud data protection, provides a unified platform that safeguards endpoints and offers enhanced protection against evolving cyber threats.

This whitepaper explores why Druva is the superior choice for businesses looking to strengthen their endpoint protection. By comparing Druva's capabilities against OneDrive and Google Drive, we highlight how Druva's comprehensive cloud-native solution ensures data security, compliance, and resilience—helping organizations stay ahead of emerging threats while optimizing their data protection strategy.

Understanding the Need for Endpoint Protection

Given the rising number of cyber threats, businesses today are more vulnerable than ever. Endpoints - laptops, desktops or remote systems - are the most vulnerable entry points for cyberattacks. According to the [IBM Security Report](#), **90% of successful cyberattacks stem from endpoint vulnerabilities**, making them prime targets for ransomware, malware, and data breaches. In fact, the average **cost of a data breach reached \$4.88 million in 2024**, emphasizing the severe financial impact of inadequate endpoint protection.

Modern businesses are confronted with a range of risks, including:

- **Ransomware Attacks:** Malicious actors encrypt and hold company data hostage.
- **Data Loss from Human Error:** Accidental deletions and file overwrites are common.
- **Compliance & Regulatory Requirements:** Organizations must comply with data governance laws such as GDPR, HIPAA, and SOC 2.
- **Device Theft or Damage:** Lost or stolen devices can result in irreversible data loss.
- **IT Management Complexity:** Managing backups, access controls, and compliance across multiple endpoints is challenging.

As more businesses adopt cloud-based solutions, many assume platforms like OneDrive and Google Drive provide adequate protection. However, these platforms are primarily designed for file synchronization and collaboration—not comprehensive endpoint protection and cyber resilience. Without a robust backup and security strategy, organizations risk exposure to operational disruption, regulatory fines, and permanent data loss.

The rise of ransomware is particularly concerning, with [Cybersecurity Ventures](#) predicting that **ransomware attacks will occur every 2 seconds by 2031, costing victims an estimated \$265 billion annually**. This underscores the urgent need for specialized endpoint protection solutions that provide proactive security, automated recovery, and compliance enforcement.

The Shortcomings of OneDrive and Google Drive

Microsoft OneDrive and Google Drive are popular for personal and business file storage, but they lack comprehensive endpoint protection. While they excel in file synchronization and collaboration, they fall short in safeguarding critical business data with robust security, backup, and recovery features. Organizations relying solely on these platforms face challenges like ransomware protection, compliance assurance, and maintaining business continuity in case of cyberattacks or data loss.

1. Lack of True Backup & Recovery

- **Limited Data Protection:** While OneDrive and Google Drive offer versioning and recycle bins, they are not true backup solutions. They lack essential features like full data redundancy, long-term retention, and ransomware protection. Additionally, not all files and folders from endpoints are synced to these platforms, leaving critical endpoint data unprotected and vulnerable to cyberattacks.
- **Limited File Retention:** OneDrive and Google Drive have strict file retention policies—93 days for OneDrive and 30 days for Google Drive. Once these limits are reached, deleted files become unrecoverable, leaving organizations exposed to the risk of permanent data loss from accidental deletions or cyberattacks.
- **No Automated Point-in-time Recovery:** There's no point-in-time recovery feature to restore data to a specific state before an attack, leaving organizations vulnerable to ransomware and significant downtime.

2. Limited Data Security Measures

- **Basic Encryption:** While OneDrive and Google Drive offer encryption at rest and in transit, they do not provide zero-knowledge encryption. This means they have access to the encryption keys, allowing them to decrypt user data if required by law enforcement or for service maintenance purposes. The absence of zero-knowledge encryption increases the risk of unauthorized access, as anyone with access to these keys could decrypt sensitive information.
- **No Immutable Storage:** Files in OneDrive or Google Drive are not air-gapped or immutable, leaving them vulnerable to tampering or ransomware attacks without a secure, recoverable copy.
- **Vulnerability to File Synchronization Issues:** OneDrive and Google Drive are designed primarily for file syncing and sharing, which makes them vulnerable to infections. If a file is deleted or corrupted on one device, it is likely to be synced and replicated across all connected devices.

3. Compliance & Governance Gaps

- **Lack of Compliance Reporting:** OneDrive and Google Drive lack built-in compliance reporting, making it hard to track data access and security incidents, which complicates regulatory adherence and auditing.
- **No Built-in eDiscovery or Legal Hold:** OneDrive and Google Drive does not offer built-in eDiscovery or Legal Hold functionality. Although Google Vault supports certain retention policies, it doesn't offer complete legal hold functionality, particularly for data stored outside of Google Workspace. Similarly, Microsoft Purview has limited capabilities and typically requires costly add-ons for full functionality.

4. Poor Scalability & Management

- **Fragmented Backup Management:** OneDrive and Google Drive struggle to provide scalable, centralized management across multiple endpoints in large, global enterprises. With no unified platform for managing backup scheduling, policy enforcement, or device-specific security, businesses face significant challenges in maintaining consistent protection and compliance across diverse devices and locations. This fragmented approach leads to inefficiencies and gaps in data protection, making it harder to ensure complete and secure backup coverage for critical business data.
- **Unreliable Recovery Times:** Recovery from data loss or system failure can be slow and unpredictable with OneDrive and Google Drive, especially for large-scale operations. These platforms often lack granular, point-in-time restore options, leading to extended downtimes, operational disruptions, and potential financial losses

Druva's Competitive Advantages

Druva addresses the challenges posed by OneDrive and Google Drive by offering a purpose-built solution that ensures enterprise-grade data protection, security, and recovery. Druva offers end user protection and data security that combines protection of Microsoft 365 or Google Workspace data along with end-user devices seamlessly. Unlike traditional cloud storage services, Druva provides true backup capabilities, including automated point-in-time recovery, air-gapped immutable storage, and advanced compliance features. By leveraging zero-trust security, AI-driven anomaly detection, and global deduplication, Druva empowers businesses to protect their endpoints against cyber threats, data loss, and compliance risks while improving storage efficiency and IT management.



Comprehensive Data Backup & Recovery

Druva offers **automated, continuous backups** with **long-term retention** for all endpoints, ensuring that no critical data is left unprotected. Unlike OneDrive and Google Drive, which lack true backup solutions, Druva provides **point-in-time recovery**, allowing organizations to restore data to a state before ransomware attacks or accidental deletions. Additionally, Druva's **cross-region disaster recovery** and seamless failover capabilities ensure that businesses can maintain operations even in the event of regional outages, providing unmatched protection against data loss.



Advanced Security and Compliance

Druva employs a zero-trust security model with role-based access controls and multi-factor authentication (MFA), ensuring that only authorized users can access sensitive data. With **zero-knowledge encryption**, Druva ensures it cannot access encryption keys, providing an additional layer of privacy. Druva's **air-gapped backup solution** protects against ransomware and insider threats by isolating backup data from production systems.

Druva's compliance management supports regulations such as GDPR, HIPAA, and SOC 2, ensuring that businesses can meet strict compliance requirements without the need for additional tools. Furthermore, Druva's **built-in eDiscovery and legal hold** capabilities allow organizations to preserve and retrieve critical data for regulatory investigations or litigation.



Intelligent Data Management & Storage Efficiency

Druva leverages **global deduplication** and compression technologies to minimize storage costs by up to 40% while maintaining data integrity. Its scalable, cloud-native architecture ensures enterprise-wide data protection, making it easy for businesses of any size to scale their backup operations as needed. **AI-driven anomaly detection** provides **proactive threat identification**, allowing organizations to address potential data loss risks before they become significant issues. Druva's intelligent data management ensures storage efficiency while safeguarding against evolving security threats.



Seamless IT Administration & User Experience

Druva simplifies IT administration with **centralized policy management**, automation, and orchestration, allowing teams to streamline operations across a global enterprise. **Self-service recovery** for end-users reduces the burden on IT support teams and accelerates recovery times for individual users. Additionally, Druva ensures **multi-device protection**, securing data across all endpoints—whether laptops, desktops or remote systems—providing a comprehensive, unified data protection solution for the modern workforce.

Here's how Druva compares with OneDrive and Google Drive:

	 Druva's Endpoint Backup Solution	 OneDrive	 Google Drive
Primary Use Case	Backup, security, and recovery	File sharing and collaboration	File sharing and collaboration
File Size Limit	Unlimited	250 GB	5TB
Platform Capability	Windows, macOS, and Linux	Windows, macOS, iOS, Android	Windows, macOS, iOS, Android and Linux
Granular Backup	Granular backup allows selective syncing of files/folders to Druva Cloud. Druva can even backup system files or configurations	Limited control over syncing specific files or folders	Limited control over syncing specific files or folders
Deduplication	Global deduplication across all users, systems, and data sources, reducing storage needs	✗ No	✗ No
Curated Snapshots	✓ Yes (Create a "golden copy" from backup snapshots)	✗ No	✗ No
Intelligent Tiering	✓ Yes (Optimizes storage costs & ensures compliance)	✗ No	✗ No
Long Term Retention	✓ Yes (Supports long-term retention for compliance & business continuity).	Limited; Microsoft 365 Archive is only for SharePoint sites	Limited; Google Vault is for eDiscovery/legal holds, not long-term backup
Zero-knowledge Encryption	✓ Yes (Druva does not have access to encryption keys)	✗ No (Microsoft holds encryption keys)	✗ No (Google holds encryption keys)
Data Lock (Immutability)	✓ Yes (Prevents modification, deletion, or tampering)	Personal Vault available but not fully encrypted	✗ Not Available
Ransomware Protection	Air-gapped, immutable backups ensure secure recovery	Malware spreads through synced devices, affecting all files & making recovery difficult	Malware spreads through synced devices, affecting all files & making recovery difficult
Recovery of Deleted Data	✓ Supported	Deleted files retained for up to 93 days, but users can permanently delete them	Deleted files retained for up to 30 days, but users can permanently delete them
Point-in-time Restore	Quick point-in-time restoration of files, databases, or entire environments	Difficult to recover specific file versions or restore full systems at a specific point-in-time	Difficult to recover specific file versions or restore full systems at a specific point-in-time
Anomaly Detection	Detect suspicious data modification on a resource and provides instant alerts	✗ Not Available Limited to the Standard Defender Antivirus	✗ Not Available

Why Customers Love Druva

Today, over [7,000 customers, including 65 of the Fortune 500](#), trust Druva's Data Security Cloud for its comprehensive data protection, cyber resilience, and compliance capabilities. Druva's automated backups of endpoints and SaaS apps (including Microsoft 365 and Google Workspace) combined with faster recovery times help reduce downtime, ensuring continuous business operations. Additionally, by eliminating the need for on-premise backup infrastructure, Druva delivers a lower total cost of ownership (TCO), providing organizations with a more cost-effective and efficient data protection solution.

Hitachi America Limited Uses Druva for Endpoint Backup and Governance for Cyber Resilience

[Learn more >](#)



2000+

Endpoints protected 24x7 with the Druva Data Resiliency Cloud

20%

Reduction in the volume of IT support tickets leveraging Druva for self-service restore

Regeneron Partners With Druva and AWS for SaaS Data Protection Across Their Enterprise

[Learn more >](#)



16,000

Endpoints around the world protected and recoverable via Druva

18,000

Microsoft 365 accounts protected 24x7 and recoverable in minutes

Medallia Lowers Risk by Moving Data Resilience to the Cloud for VMware and AWS Workloads

[Learn more >](#)



99%

Faster restores with the Druva Security Cloud

4.4x

Global deduplication storage savings

The Future of Endpoint Protection

As cyber threats become more sophisticated, cybercriminals are increasingly targeting backup systems to compromise data integrity and disrupt business operations. Businesses must adapt to new challenges by adopting advanced data security measures that go beyond traditional file synchronization. Legacy backup solutions often lack the advanced data security features necessary to defend against these evolving threats. Implementing an extra layer of security, ensures that backup data is isolated from production systems, making it significantly more challenging for attackers to access or manipulate critical information. The future of endpoint protection is poised to focus on several critical technologies that will help organizations safeguard their data, mitigate risks, and maintain compliance. With the

rapid pace of change in the cyber threat landscape, proactive solutions are more essential than ever. The next generation of endpoint protection will include:

- **Zero-trust architectures:** Implementing stricter access controls by assuming no user or device can be trusted by default.
- **AI-driven threat detection:** Leveraging artificial intelligence to proactively detect data anomalies and address emerging risks.
- **Immutable backups:** Protecting data integrity by preventing unauthorized alterations or deletions, especially during ransomware attacks.
- **Unified security and compliance frameworks:** Streamlining security measures to ensure seamless adherence to evolving regulatory requirements.

Druva offers these features out-of-the-box so that businesses don't have to use multiple tools or rely on multiple vendors to protect, secure and recover their business critical data. With Druva's ongoing innovation and investment in AI, businesses are equipped with the tools necessary to stay ahead of emerging threats and effectively manage the complexities of modern compliance challenges.

Endpoint and SaaS Applications Better Together

Druva extends endpoint protection by combining advanced endpoint security with SaaS application protection for Microsoft 365 and Google Workspace, offering a unified approach to data security. This comprehensive solution ensures that end-user data is secured across devices and cloud applications, mitigating risks associated with data loss, ransomware attacks, and compliance breaches.

By integrating endpoint protection with SaaS app security, Druva provides seamless data backup, recovery, and governance, all managed through a single, centralized platform. This unified approach reduces complexity and eliminates the need for multiple tools or vendors, enhancing operational efficiency and security. Druva's platform incorporates zero-trust architectures, AI-driven threat detection, immutable backups, eDiscovery, ransomware recovery and unified compliance frameworks, delivering robust protection against evolving cyber threats.

Protect End User Data Across Endpoints and SaaS Applications.

Secure every piece of end-user data — across devices and SaaS applications — with Druva's comprehensive solution. One unified platform, complete peace of mind.

[Explore Now >](#)

Conclusion

While Microsoft OneDrive and Google Drive excel in file synchronization and collaboration, they fall short when it comes to providing the comprehensive endpoint protection that modern enterprises need. These platforms focus on syncing and sharing files, but lack the advanced data security features required to guard against today's sophisticated cyber threats. With no true backup solutions, limited compliance tools, and inadequate protection against ransomware, organizations relying solely on OneDrive and Google Drive leave their critical data exposed.

In contrast, Druva offers a purpose-built, cloud-native solution designed specifically for data security, compliance, and resiliency. By combining enterprise-grade security measures, continuous backup, compliance management, and advanced threat detection in one unified platform, Druva ensures businesses can protect their data at the endpoint and beyond. As cyber threats and regulatory requirements continue to evolve, Druva provides the adaptability and protection that businesses need to stay secure and compliant, now and in the future.

Next Steps

Take the next step in protecting your business data with Druva. Experience powerful endpoint data protection, cyber resiliency and compliance features with a [free trial](#). Sign up today to discover how Druva can safeguard your critical data, ensure business continuity, and reduce risk.

druva Sales: +1-800-375-0160 | sales@druva.com

Americas: +1-800-375-0160
Europe: +44 (0) 20-3750-9440
India: +91 (0) 20 6726-3300

Japan: japan-sales@druva.com
Singapore: asean-sales@druva.com
Australia: anz-sales@druva.com

Druva is the leading provider of data security solutions, empowering customers to secure and recover their data from all threats. The Druva Data Security Cloud is a fully managed SaaS solution offering air-gapped and immutable data protection across cloud, on-premises, and edge environments. By centralizing data protection, Druva enhances traditional security measures and enables faster incident response, effective cyber remediation, and robust data governance. Trusted by over 6,000 customers, including 65 of the Fortune 500, Druva safeguards business data in an increasingly interconnected world. Visit druva.com and follow us on [LinkedIn](#), [Twitter](#), and [Facebook](#).