Osterman Research

WHITE PAPER

White Paper by Osterman Research
Published **July 2021**
Sponsored by **OpenText**

The Case for Policy-Based Enterprise Endpoint Backup

Executive Summary

Employees engage with enterprise data through a myriad of endpoints—laptops, smartphones, and tablets. They create enterprise data, store it, share it, access it, and make modifications to it. An endpoint is a facilitator of productive work and the gateway to the intellectual property storehouse of the organization. Many work processes in the modern organization have been designed based on the availability and capabilities of endpoints.

Endpoints are also a risk and threat vector. Lost or stolen devices result in loss of capability to work—and data breaches. Ransomware attacks lock data and documents from usage, rendering devices useless and unique data inaccessible. Data responsive to eDiscovery requirements and internal investigations is scattered across network servers, cloud services, and endpoint devices, and while the first two are generally easy to search, securing physical access to a custodian's endpoint device is a more difficult and expensive proposition. Safeguarding the endpoint as an enabler of productive work and protecting the data stored on endpoints are critical considerations in enterprise IT strategy.

Endpoints enable productive work and connect employees to the organization's intellectual property. Endpoints are also a risk and threat vector.

KEY TAKEAWAYS

The key takeaways from this white paper are:

- **Modern World, Elevated Threats**
  Insider threats, the risk of lost and stolen devices, and ransomware incidents (among others) continue to threaten the integrity of endpoints. The health pandemic of the past year has worsened the situation. Failing to protect endpoints through a comprehensive backup approach is dangerous.
- **Similar Services, Significant Differences**
  New cloud-based file sync and share services targeted at enterprise customers are a valuable addition to the capabilities available to employees for productivity and collaboration. While these new services offer some similarities to enterprise endpoint backup solutions, significant differences remain in areas such as data protection, process assurance, eDiscovery, and insider misdeeds.
- **Enterprise Responsibility vs. End User Responsibility**
  Endpoint backup is an enterprise responsibility, not an end user one. The core drivers for endpoint backup are ones that benefit the organization: data retention, disaster recovery, legal hold and eDiscovery, and counteracting insider threats, among others. End users should be responsible for performing their work with excellence, not creating backups.
- **Opting for No Enterprise Backup**
  Organization rejecting the implementation of a strong backup approach for endpoints and instead preferring to sync only some data with OneDrive must be willing to pay the productivity loss and help desk costs every time devices are compromised, lost, or stolen.

ABOUT THIS WHITE PAPER

This white paper is sponsored by OpenText. Information about OpenText is provided at the end of the paper.

Situation Analysis

Endpoints play a pivotal role in the delivery of enterprise IT services that facilitate productivity for employees. Without an endpoint of some kind, employees revert to manual processes, pen and paper, and printed notices on the bulletin board in the lunchroom. While few organizations deliberately embrace this approach in 2021, many are not enacting the protections required to keep endpoints healthy and employees productive.

This white paper reviews the differential capabilities of two solution categories that deliver protections for endpoints and employees: policy-based enterprise endpoint backup solutions, and enterprise file sync and share services. One overarching emphasis of both solution categories is meeting compliance requirements for enterprise data, and a second is the ability to safeguard productivity when a device is lost, stolen, compromised, or otherwise destroyed. Although these areas of emphasis are the same, there are significant differences in the efficacy of each solution category in meeting the associated requirements.

In this section, we review the situational context with endpoints and how people, teams, and organizations work.

NEW TOOLS, NEW POSSIBILITIES

The IT landscape is dynamic and new style offerings from new (and established) vendors create possibilities for IT approaches that did not previously exist. Enterprise file sync and share (EFSS) tools carved a new line in enterprise IT, offering the consumer-friendly capabilities of Dropbox and SugarSync-style services for employees. OneDrive for Business, due to its tight integration in the globally used Microsoft 365, has become a very broadly adopted EFSS tool.

Enterprise file sync and share tools carved a new line in enterprise IT, and OneDrive has become very broadly adopted.

INSIDER THREATS REMAIN

Accidental and malicious insider threats remain an issue for organizations to acknowledge, mitigate, and address when identified. Insider threats are a significant causal factor for cyberattacks.[1] Although new tools create new opportunities for doing enterprise IT, they also create new security and compliance challenges. How easily can an employee abuse a new tool to deliberately hide wrongdoing? How easily can an employee make an honest but devastating mistake, such as sharing a confidential list of high-value customers with the wrong recipient? How easily can an employee move or copy protected data to non-authorized locations for surreptitious access and sharing?

ENDPOINT DEVICES LOST OR STOLEN

Endpoint devices get lost or stolen. Various research studies have found that the average adult in the United Kingdom has lost two smartphones during their lifetime,[2] 70 million devices are lost per year in the United States,[3] and even among industry sectors where standards should be much higher, thousands of smartphones, laptops, and tablets are lost every year.[4] Public locations are not even the most common place to lose devices, with homes, businesses, and schools representing the riskiest locations—the places we feel most comfortable and secure.[5]

RANSOMWARE THREATS

Ransomware has become a significant threat in recent years, with the WannaCry attack in 2017 a pivotal illustration. Major ransomware events in May 2021 included the Colonial Pipeline attack and several hospital systems around the world. In the first four months of 2021, nearly 300 enterprises were compromised by one of only six of the ransomware variants in the wild.[6] Ransomware gangs are adding other nasty tricks to their arsenal, including data exfiltration prior to encryption, extortion of ransom payments through the threat of publishing breached data, and even financially motivated outreach to the consumers whose data was breached. A protected backup of data is the quickest and least expensive way to recover data compromised by ransomware.

NEW WORKFORCE DESIGNS

The health pandemic of the past year forced new workforce designs, including widespread working-from-home arrangements in 2020 and newer hybrid workforce approaches in 2021. Endpoint devices and data are under increased threat when employees no longer work in secured locations over known and protected networks. Threats include poorly secured home routers and free Wi-Fi networks, increased variation and usage of whatever endpoints are available (from a policy viewpoint, non-standardized equipment that is unlikely to be enterprise-class), and heightened likelihood that endpoints are not regularly patched. In addition, with fewer employees commuting to an office location regularly—if at all—it has become ever more difficult for enterprise IT teams, compliance professionals, and legal staff to gain physical access to an endpoint for IT assurance and compliance assessments.

Endpoint devices and data are under increased threat when employees no longer work in secured locations over known and protected networks.

CONCLUSION: A DANGEROUS TIME

As the situational context changes in line with the risks and trends outlined above, the need for real security over endpoints and edge devices becomes more critical, not less. It is a dangerous season of life to be throwing caution to the wind and decreasing the protections enacted over endpoint devices and data.

Differences

This section explores the differences between a policy-based enterprise endpoint backup solution and enterprise file sync and share (EFSS) tools, of which OneDrive is a prime example. Whenever OneDrive is mentioned in this section, the intent is to refer to a well-known example of an EFSS tool rather than putting OneDrive in the crosshairs. We avoided writing “OneDrive (or equivalent)” or “OneDrive (or similar)” each time because that makes a white paper hard to read, but we ask the reader to please note the reference is to a category instead of a single product.

A DIFFERENCE OF ESSENCE

One service offers snapshots for restoration and the other quick links for collaboration. This is a difference of essence between the two solution types:

- Policy-based enterprise endpoint backup solutions safeguard all the data on an enrolled endpoint, offering a succession of historically accurate restore points. If data on an endpoint becomes corrupted or even if the entire endpoint is lost or destroyed, the most current restore point can be used to recreate what was there previously on new physical hardware.

- OneDrive provides quick links for collaboration on current documents, as well as simple access to a selection of data across multiple endpoints. OneDrive enables users to share documents for real-time multi-person input and review, instead of sending documents as email attachments and then having to deal with the resulting versioning chaos. OneDrive has revolutionized document-based collaboration.

DATA RETENTION: ONE-TIME DECISION VS. A MILLION OR MORE

For organizations subject to data retention requirements, the decision to be compliant is essential. The two solution types offer a different decision profile:

- Embracing a policy-based enterprise endpoint backup solution is a one-time decision to be compliant. By design, the solution captures and preserves all endpoint data, providing professionals with data protection, archiving, and compliance responsibilities with the capabilities they need to safeguard the organization. Such professionals—with the responsibility and training to decide—can therefore ensure that data retention requirements across the organization's endpoint estate are met automatically by policy.
- Replacing an enterprise endpoint backup solution with OneDrive to synchronize documents in the correct folder hierarchy between the cloud and the endpoint substitutes a one-time compliance decision by trained professionals with a proverbial million individual decisions spread across the employee workforce. An employee with OneDrive alone must decide for every document whether to act in a compliant way by storing the document in OneDrive.

PEACE OF MIND: DEEP CALM VS. HIGH STRESS

Assurance of compliance with organizational policies means the organization is compliant by design. The two solution types result in very different experiences for compliance and data protection professionals charged with safeguarding the organization:

- A common way of describing a benefit of policy-based enterprise endpoint backup solutions is "set and forget." An administrator connects a new endpoint to the backup solution, and everything stored on the device at that point in time and from then onward is captured. No one needs to remember to put documents in a particular place. The employee does not have to connect an external drive every Friday night and run a backup script. If there is a problem with the device being offline for too long or the backup agent failing, the administrator is alerted so remedial action can be taken.
- With OneDrive only, "set and forget" gives way to "set and worry continually." Data not stored in OneDrive is not captured for access or restoration, and data loss is almost certain if the endpoint is compromised by ransomware, lost, or destroyed. The potential for data loss becomes a weak link in the security and compliance strategy for an organization.

Without an enterprise endpoint backup solution, "set and forget" gives way to "set and worry continually."

DATA RETENTION: SEAMLESS VS. CHAOTIC

Capturing and storing the data that needs to be retained is seamless with one service and chaotic with the other:

- Policy-based enterprise endpoint backup solutions assure seamless compliance with data retention requirements because all data stored and created on the endpoint is automatically captured whenever the backup process runs. If the endpoint is connected to the backup solution, everything is captured all the time, irrespective of where an employee chooses to store a given file or document on the device.
- Assurance for compliance with OneDrive is chaotic, with variations possible by department, employee, day, data type, and even type of device. Some information will be stored in OneDrive, and much will not. Understanding the risk profile of a compromised, lost, or stolen device is much more difficult when a complete inventory of recent data is unavailable.

PHISHING ATTACKS: TWO ACCOUNTS TO COMPROMISE VS. ONE ACCOUNT

The rise in phishing attacks against Office 365 is worrying because a compromised account gives access to multiple productivity apps, data sources, and file storage locations in Office 365. Once an account is compromised, the threat actor can move quickly to review the victim's Exchange email, browse SharePoint sites, snoop around in Teams workspaces, and read OneDrive files (among others), either for quick data exfiltration or a quiet extended dwell time with an eye towards business email compromise attacks at an opportune time. There are differences between the two solution types:

- Organizations forcing a hard line on storing everything in OneDrive unwittingly increase the attack space when Office 365 accounts are compromised. A greater proportion of the organization's data is available for a threat actor to access with each compromised account.
- Organizations using a policy-based enterprise endpoint backup solution do not have to take such an inflexible stance on storing everything in OneDrive to retain it. Irrespective of whether content is stored in OneDrive or elsewhere on the endpoint, it is all captured by policy for access and restoration. A phishing attack that compromises the credentials of an Office 365 account will therefore secure access to fewer documents, because everything else is protected in a separate account accessible with different credentials.

Policy-based enterprise endpoint backup solutions assure seamless compliance with data retention requirements.

EDISCOVERY AND ENTERPRISE SEARCH: COMPREHENSIVE VS. LIMITED

Finding content responsive to eDiscovery cases or necessary for an enterprise search query is required by law on the first and mere best practice on the second. The two solution types offer a different experience:

- A policy-based enterprise endpoint backup solution enables the defensible and systematic capture of data to support eDiscovery and enterprise search. Legal and compliance professionals can search a complete inventory of endpoint data to ascertain responsive content, and with appropriate rights, administrators can initiate an enterprise search query across the same data corpus. Searches query a comprehensive set of data that is not dependent on whatever data end users have chosen to retain.

- eDiscovery and enterprise search are also possible with OneDrive, but the data set available to be queried only includes data stored in OneDrive and other Office 365 workloads (including any third-party data uploaded to Office 365 via connectors). The data available for search is highly dependent on end user actions. Data stored on endpoints outside of the OneDrive sync hierarchies are excluded from eDiscovery and enterprise search, creating areas of dark data. Without the ability to assess all data on endpoints, the actual legal exposure of the organization is unknown and unquantified.

LEGAL HOLD: ALL ENDPOINT DATA VS. ONLY SOME ENDPOINT DATA

Responsive data for eDiscovery and internal investigations must be protected from deletion and modification to avoid charges of spoliation. Both solution categories enable legal hold, but with differences:

- Policy-based enterprise endpoint backup solutions support legal hold across all data created and stored on endpoint devices. An eDiscovery search can be used to identify all responsive data across the corpus of backup data, and a legal hold can then be put in place without having to gain physical or real-time remote access to each endpoint device.
- Legal hold capabilities for services such as OneDrive depend entirely on what legal hold capabilities are offered in each service, but the core principle remains the same: only the data stored in OneDrive can be put on legal hold. Accessing all other data stored outside of OneDrive on an endpoint requires gaining physical or real-time remote access to the custodian's endpoint.

DELIBERATELY HIDING DATA: HARD TO DO VS. EASY TO DO

Keeping data secret that should not be hidden offers an easy way for employees to use organizational resources for wrongdoing. Both solutions approach this issue in different ways:

- An employee, manager, or executive who wants to deliberately hide data that should be subject to wider visibility, such as in regulatory supervision circumstances or in harassment cases, will find it much harder to do when a policy-based enterprise endpoint backup solution is in place. Since all data across the entire endpoint is captured for access, restoration and search, there is no hiding of data. An administrator with appropriate access to the corpus of data on the backup of the endpoint can execute a search to find potentially offensive material.
- Deliberately hiding data is a much easier act when merely saving the document to the desktop—let alone another nested folder hierarchy outside of OneDrive—will suffice. If the document is not saved into OneDrive, no one else will ever know of its existence until the physical endpoint is examined directly. Without the ability to search and discover across all endpoint data, early case assessment in eDiscovery or internal investigations has a significant blind spot, raising the specter of uncovering smoking guns at the most inopportune time.

Deliberately hiding data is a much easier act when merely saving the document to the desktop—let alone another nested folder hierarchy outside of OneDrive—will suffice.

MIGRATING TO A NEW DEVICE: TWO STEPS VS. A HUNDRED OR MORE

With enterprise endpoints having a lifespan of two to four years—depending on the usage characteristics and the organizational policy—users will need to migrate to a new device, even if their device is never lost, stolen, or compromised. There is a different experience on offer with the two solution types:

- The ability to access an up-to-date and comprehensive backup image of an endpoint means migrating from one device to another is a streamlined and simple two-step process: log into the device and connect to the desired image. Files, documents, settings, preferences, and everything else from the previous device flow to the new one, enabling the user to focus on their work and contribution rather than how to configure their new device to enable them to do so. In a disaster recovery situation, getting employees back on their feet with a new endpoint is an easy proposition.
- The use of OneDrive without a comprehensive backup image incurs a more laborious process when migrating to a new device. The user must log into the device, reinstall their apps, reestablish connections to multiple on-premises and cloud services, and attempt to piece together settings, preferences, passwords, and browser favorites, among others, from memory. If the new device is required because the previous one was lost, stolen, destroyed by ransomware, or otherwise inaccessible, permanent data loss is extremely likely. In a disaster recovery situation, the emphasis will remain on the "disaster" part, not the "recovery" aspect.

The use of OneDrive without a comprehensive backup image incurs a more laborious process when migrating to a new device.

REMOTE ACCESS: ALL ENDPOINT DATA VS. ONLY SOME DATA

Gaining remote access to files, documents, and other content stored on an endpoint but not from the endpoint itself is a useful productivity feature for employees. Both solution types enable remote access to the data stored on endpoints:

- Since a comprehensive backup of all data is created with policy-based enterprise endpoint backup solutions, an employee can remotely access all data via a web browser session. Everything on the endpoint is available for review and access without requiring the physical presence of the endpoint.
- While it takes a different approach to enabling remote access and includes capabilities to support real-time collaboration, OneDrive also provides beyond-the-endpoint access to whatever endpoint data was correctly stored in the designated folder structure. Users can log into OneDrive on the web to browse, search, and access data stored in their OneDrive account.

BACKUP FOR RISK MITIGATION: EMBRACED VS. SYSTEMICALLY IGNORED

Creating backups of any type of data is a risk mitigation strategy. If there was no risk, no backup would be required. Both solution types deal with this differently:

- Continuous backup of the endpoint estate is embraced as a risk mitigation strategy when a policy-based enterprise endpoint backup solution is in use. The benefits we have explored in this white paper are easily available to organizations doing so.

- Embracing OneDrive as a type of backup approach fails the backup veracity test on two fronts: the original data capture is incomplete and the so-called backup is not itself backed up. On the first, only data stored in the OneDrive sync hierarchy is available for restoration to a new device, and only for data types and file sizes supported by OneDrive. On the second, Microsoft does not create backups of OneDrive and other workloads in Office 365. OneDrive offers a real-time snapshot of current and stored files, but once deleted files have been purged, the roll-back capabilities in OneDrive are unable to retrieve what an actual time-based backup snapshot is able to preserve. The lack of backup for Office 365 itself has created market demand that third-party vendors are filling with true backup solutions for Office 365 to close Microsoft's gaps. It is nonsensical to trust restoration to a backup approach that is partial at best, and one that is not itself backed up.

ACCESS TO DELETED FILES: LONG-TERM VS. SHORT-TERM

Deleted files can become important again—either for an end-user to recall what happened on a project, or more significantly to meet compliance and litigation requirements. Both solution types provide access to deleted files, with a couple of critical differences:

- Organizations can define how long deleted files should be kept available in historical backup data sets using a policy-based enterprise endpoint backup solution, providing a defensible and systematic means of supporting compliance and litigation requirements. Deleted files can be recovered years after the original was deleted.
- OneDrive automatically captures deleted files in a couple of tiered duration recycle bins, enabling files to be recovered after several months of being deleted. But once the file is actually removed from the second stage recycle bin, it is unrecoverable.

Observations

An early comment in this white paper is that two solution categories exist that deliver protections for endpoints, employees, and organizations. The previous section offers a comparative analysis of both, but to read that section with an either/or perspective misses the major point: both solution categories are valid, and both are required. In making the decision on how to proceed with these solution categories, we offer the following observations.

PLAN WITH HUMAN NATURE IN MIND

The perfect employee who always does the right thing with files and documents and never makes an inaccurate or harmful comment is a phantom; they do not exist. Even if you find one among thousands, the thousands evidence the principle more than the one. Therefore, plan with human nature in mind. Careless mistakes, an overly protective sense of ownership of nascent ideas, and deliberate misdemeanor can all be hidden on endpoints when a comprehensive backup approach is not used.

The perfect employee who always does the right thing with files and documents and never makes an inaccurate or harmful comment does not exist. Plan accordingly.

RECREATING THE 3-2-1 RULE FOR SYNC ONLY?

In the age of tape backups and less reliable computing infrastructures, the 3-2-1 rule of backup saved many careers and organizations: three copies of your data, on two different media, with one copy stored in a different physical location to the other copies. The 3-2-1 rule gave almost ironclad assurance that you could recover from pretty much anything.

The power of the cloud with auto-sync services, anywhere access from multiple device types, and rapid time-to-market attributes has dulled our collective senses to the risk of unforeseen data loss events and threatens to relegate the 3-2-1 rule to the history books. And yet, for cloud services that are auto-syncing and providing little in the way of historically accurate backups, the risk is that an unintentional corruption of the system, an attack by threat actors, or the mere passage of time for a deleted folder results in lost data. It is not on your endpoint. It is no longer in the cloud. If you are going to bet disaster recovery for your organization on the native capabilities of your cloud provider, you need to be certain that nothing that should be kept will ever be irretrievably deleted, compromised, or made inaccessible.

ENSURING THAT SYNC ONLY IS SUFFICIENT

Perhaps a sync-only approach is sufficient for your organization because your assessment of the risks faced by employees and endpoints is overshadowed by the cost of a policy-based enterprise endpoint backup solution. Before finally embarking on this approach, however, we recommend clearly defining the list of business risks with sync only. Take this list to the responsible compliance professionals, legal staff, and senior executives in your organization to get their official sign-off for the missing capabilities. Unforeseen and unprecedented data loss events are unforeseen and unprecedented, but when they do happen, it is helpful to have a strong document trail showing sign-off on the approach from the highest levels.

SAVE PENNIES, LOSE DOLLARS

If your organization rejects implementing a strong backup approach for endpoints in preference for syncing only some data with OneDrive, there must be a parallel organizational willingness to pay the productivity loss and help desk costs every time devices are compromised, lost, or stolen. The presence of a comprehensive backup on one hand and the threat to endpoints on the other are mutually exclusive; one does not cause the other, and one does not negate the possibility of the other.

POLICY VS. USER CHOICE

It is inconsistent to assert the organization has a mandatory policy for data retention and yet trust to user choice for moment-by-moment compliance with the policy. If all that is required to circumvent the organization's data retention policy is to store documents outside of OneDrive, the policy is meaningless.

With no endpoint backups, your organization must be willing to pay the productivity loss and help desk costs every time devices are compromised, lost, or stolen.

ACHIEVING THE BEST-CASE SCENARIO, AVOIDING THE WORST

The best-case scenario without policy-based enterprise endpoint backup is that an employee losing an endpoint (whether by ransomware, theft, or natural disaster) can get a new device, install their apps from an app catalog, and reestablish their connection to OneDrive to get to their documents. In this best-case scenario, the employee has stored all relevant and required documents in OneDrive and, apart from the several hours of lost productivity getting everything set up again, they are ready to dive into their work again.

An entire chain of events must work flawlessly in sequence to achieve the best-case scenario, but if any of the conditions are missing, the best-case scenario is compromised and could turn into the worst possible nightmare instead.

Summary and Next Actions

This white paper has reviewed the case for endpoint backup solutions as complementary to OneDrive and similar cloud-based file sync and share services. Both solution types focus on different use cases, and we encourage organizations to ensure the business, legal, compliance, and data protection benefits of policy-based enterprise endpoint backup solutions are fully realized in this era of heightened threats and business risks.

Sponsored by OpenText

OpenText™ is The Information Company. We power and protect information to elevate every person and every organization to gain the information advantage. A leader in global Information Management, OpenText offers a comprehensive portfolio of solutions across content, business network, digital experience, security, application modernization, operations management and developer APIs. OpenText solutions help customers simplify their systems, connect their data, build frictionless automation and thrive in a multi-cloud world. The company fosters inclusive environments that leverage the diverse backgrounds and perspectives of all employees, customers, suppliers and partners. For more information about OpenText (NASDAQ/TSX: OTEX), visit www.opentext.com.

OpenText™ Portfolio solutions help organizations know their data, empower their people, and drive their future. Automated compliance solutions provide real-time data analytics and privacy reports. Productive, empowered people achieve flexible, smarter, more collaborative work environments. Give remote workers the right content, for the right people, at the right time, on any device. Learn more at www.opentext.com/products/digital-workplace.

opentext™

www.opentext.com

@OpenText

[1] Jasmine Henry, These 5 Types of Insider Threats Could Lead to Costly Data Breaches, August 2018, at https://securityintelligence.com/these-5-types-of-insider-threats-could-lead-to-costly-data-breaches/

[2] Simon Chandler, Brits Boost Mobile Industry By Losing 98 Million Smartphones To Date, July 2020, at https://www.forbes.com/sites/simonchandler/2020/07/14/brits-boost-mobile-industry-by-losing-98-million-smartphones-to-date/

[3] Elaine Hom, Mobile Device Security: Startling Statistics on Data Loss and Data Breaches, November 2019, at https://www.channelpronetwork.com/article/mobile-device-security-startling-statistics-data-loss-and-data-breaches

[4] BBC News, Thousands of Mobiles and Laptops Lost by UK Government in a Year, February 2020, at https://www.bbc.com/news/technology-51572578

[5] Prey, Inc., Prey's Mobile Theft & Loss Report 2020 Finds 67% of Mobile Losses Occur in Interior Locations, 33% When Users are in Transit / Movement, March 2020, at https://www.globenewswire.com/en/news-release/2020/03/13/2000245/0/en/Prey-s-Mobile-Theft-Loss-Report-2020-Finds-67-of-Mobile-Losses-Occur-in-Interior-Locations-33-When-Users-are-in-Transit-Movement.html

[6] eSentire, Six Ransomware Gangs Claim 290+ New Victims in 2021, Potentially Reaping $45 Million for the Hackers, May 2021, at https://www.esentire.com/resources/library/six-ransomware-gangs-claim-290-new-victims-in-2021-potentially-reaping-45-million-for-the-hackers

248-000085-001