Replacing Legacy Enterprise Backup Solutions with Druva in Today's Cloud- and Mobile-First World

Published: June 2018

What You Need to Know

In the world of the globally distributed and mobile workforce, the needs of backing up enterprise data are constantly evolving and becoming more complex. Organizations must ensure that corporate information is not only recoverable in the event of system failure, but they must do so across a variety of endpoints such as laptops, tablets, and mobile devices as well as Software as a Service (SaaS) applications at any location around the globe.

As they work to ensure these capabilities, business decision-makers must balance concerns around encryption, varying data privacy regulations in certain geographic regions and delivering the service in a way that is minimally disruptive to end users. Further, IT must consider how to provide these services without overtaxing the limited administrative bandwidth at their disposal.

Existing legacy solutions such as HP Connected or Microsoft Data Protection Manager were not originally designed to deliver on the business needs of today's mobile-first and cloud-centric workforce. To this end, Blue Hill conducted deep qualitative interviews with five organizations that felt these pain points and navigated the solution selection process to invest in their enterprise endpoint backup capabilities.

Ultimately, each participant selected inSync from Druva, a California-based endpoint data protection and governance provider, to address their needs. By distilling common challenges, investment drivers and resulting business impacts, Blue Hill expects that the experience of these five organizations will provide guidance to business decision-makers in similar situations.

AT A GLANCE

Business Challenges

Inefficient endpoint and applications backup requiring significant administrative oversight and causing disruption in end-user productivity

Legacy Solutions in Place

- HP Connected
- Microsoft Data Protection Manager
- Mozy

Solution Selected

Druva inSync

Benefits

- Enhanced IT efficiency
- Reduced costs
- Eliminated IT administration and oversight
- Increased uptime of line-of-business employees

About the Subjects

Subjects in this initiative represent mid- to large-sized firms across a variety of industry verticals. This includes a Canadian food-services provider with over 900 restaurants and $1 billion in annual revenue, one of the United States' largest medical equipment providers, a global electronics manufacturer, a prominent global consultancy with more than 6,500 employees and a supplier of digital radio and smart audio devices.

Drivers for Investment

Prior to selecting Druva, each of the subjects had in place an existing endpoint backup solution that included HP Connected, Microsoft Data Protection Manager and Mozy. Blue Hill also observed Accellion, a managed file transfer vendor rather than a designed endpoint backup provider, which supported backups as well.

> "We pay less than $150 a year per user and we charge our consultants out at at least $150 an hour. Anything beyond saving them one hour is a bonus. It's easy to justify the cost, especially when employees are in a revenue-generating role. Keeping our employees able to bill is paramount. Restoring lost laptops and removing the need to reboot or reconstruct files is critical. The time we save is time we can bill."
>
> *Director of IT, Global Consultancy*

A number of factors precipitated the research participants' decision to seek an alternative solution provider. In the case of both the global electronics manufacturer and healthcare equipment provider, their existing solutions were unable to function properly at an enterprise scale. For the electronics manufacturer, an acquisition dictated their prior solution. In each instance, their attempts at backing up endpoints consistently failed, and required oversight that was far in excess of what was deemed reasonable. For the digital radio and smart audio supplier, endpoints were not the only backup concern. The entire company had moved to the cloud and SaaS applications such as Microsoft Office 365, and the shift spotlighted the need for guaranteed data protection and governance that the applications themselves could not provide. Indeed, as organizations move more data into SaaS apps, IT is still responsible for protecting the data and make sure it remains accessible in case of a legal or HR issue. With a legacy applications-backup approach, operating remote locations or using SaaS applications translates into less IT control.

In addition, participants reported that their legacy solutions required a level of maintenance and oversight that was too taxing on their time and resources. Participants said it was not uncommon to spend multiple hours each week managing their endpoint backups and data protection. The solutions also were slow at accomplishing backups, which impeded employee device usage or discouraged end users from running backups at all.

Global expansion amounted to another common investment driver. The majority of companies that Blue Hill analyzed – including the global consultancy, the electronics manufacturer and the digital radio and smart audio devices supplier – have globally distributed, highly mobile workforces. These companies needed a way to maintain endpoint backups regardless of where their employees were located. Having an end user back up their device to a data center halfway across the globe can present a number of issues with performance and logistics, especially if that person needs to log into a VPN connection. Further, there are significant challenges with varying data privacy laws, especially in the European Union, which now enforces General Data Protection Regulation compliance. Organizations backing up data for their Europe-based employees often must use data centers based in specific countries and comply with more nuanced regulations.

Ultimately, these challenges drove the studied organizations to evaluate new solutions that could meet their requirements associated with performance, ease of management and global workforce needs.

Choosing Druva

As the participants moved through their solution evaluation process, they weighted the comparative merits of a number of solutions alongside Druva, including HP Connected, Microsoft Data Protection Manager, Box, Mozy Pro and Code 42. Ultimately, the participants selected Druva inSync. Blue Hill observed common differentiators that gave Druva the competitive edge over the other solutions considered. Most frequently, the factors that lead to Druva's selection were:

> "Within 20 minutes of them giving me credentials, I was running backups on multiple devices. …Druva has an automated provisioning process. For 90 percent of our user population, no one in IT even touches it. Automatic provisioning is an absolute must now."
>
> *Senior Manager of IT Infrastructure, Electronics Manufacturing*

Global Presence: Druva's cloud includes data centers located in North America, Europe and Asia, backed by Amazon Web Services. This was one of the strongest differentiators for Druva, as the other considered solutions, including HP Connected and Code 42, did not have such an option at the time of the organizations' decisions. This was important to the IT decision-makers for two reasons. First, it presented a significant logistical advantage. Subjects with a global footprint were concerned with the inefficiencies of users backing up their endpoints to North America-based data centers, as well as the burden that this would place on their network and the time it would take to complete backups. The proximity of Druva's cloud to their workforces mitigated these concerns.

Secondly, Druva's data centers in Europe allow organizations to comply with GDPR requirements and other stringent data privacy laws. When faced with this decision, the unappealing alternative to selecting Druva was for organizations to build their own data centers in these countries, or find another way to comply with regulations.

SaaS Application Backup: More applications now reside in the cloud, making it imperative that organizations back up that data, not just data in endpoints. The apps themselves are not built to ensure data protection or governance. In fact, several SaaS vendors, including Salesforce.com, recommend that users employ a third-party tool for backup. In the corporate-mandated move to Office 365, the digital radio and smart audio devices supplier, in particular, knew it needed the holy grail of endpoint and SaaS applications data backup and management, including long-term retention and the ability to immediately identify and remediate at-rest sensitive data risks.

> "Companies do need to back up their cloud data."
>
> *Director of IT and Cloud Operations, Digital Radio and Smart Audio Devices Supplier*

Ease of Scalability: Research participants reported that Druva presented the solution that was most easily scalable throughout their organizations. Druva's cloud-based delivery model meant that organizations did not have to build new data centers if they wanted to increase the amount of endpoints or SaaS applications they were backing up just because it surpassed their current storage capacity thresholds. This benefit became quite valuable, especially in the case of the global consultancy. The consultancy had recently acquired a competitor that expanded headcount by almost 1,500 employees overnight. As these employees were located around the world, provisioning them with an endpoint backup solution would have been an arduous task if the firm had stuck with its original on-premises solution. Doing so would have required building new data centers and hiring more people to manage the servers internationally. On that note, participants identified Druva's ability to automatically provision new users as a significant productivity improvement. Overall, Druva was identified as the best solution to deal with growth, as provisioning new employees required no additional infrastructure and little extra administrative responsibility.

Data Encryption: Druva's data encryption capabilities, both in transit and at rest, were also a competitive differentiator for research participants to ensure that corporate data was being protected when employees were actually backing up their data, regardless of the path the data took to go back into the public, hybrid or private cloud backup destination. Druva's approach both for data encryption and data security led to perceived differentiation and added value. For encryption, Druva encrypts the data both in transit using 256-bit Secure Sockets Layer, or SSL, and at rest through Advanced Encryption Standard (AES). Additionally, Druva uses both two-factor encryption key management and two-factor authentication to ensure no party – including Druva itself – has access to unencrypted data. When making a holistic assessment of overall security, an important point of differentiation arises in Druva's purposeful approach to preclude Druva employees from having any access to customer data stored in the cloud. Druva's access is limited only to administrative tasks of patching and upgrades, which minimizes customer's data risk profiles even to potential vendor influence.

> "Their support is the best I've seen and I've worked with a lot of different support teams. They are very responsive. The phone barely rings and they pick up."
>
> *Network Systems Manager, Medical Equipment Provider*

Data encryption further was important when considering protecting applications in the cloud. For example, Druva can detect when malware, human intervention or some other threat may have breached an application and deleted, changed or uploaded files. Druva notifies IT and provides complete visibility into all endpoints and SaaS applications from its single-pane-of-glass interface.

Licensing and Multi Device Support: Druva licenses on a per-user, rather than a per-device, basis. In contrast, Blue Hill found that HP Connected charges additional fees for each device an employee uses. Research participants noted that this was an important factor in choosing Druva over the competition, as employees either have, or are planning to have, multiple endpoints that require backup, including tablets, phones and/or laptops. Participants perceived this as an indicator of a lower total cost of ownership.

In a similar vein, some of the evaluated solutions (such as Microsoft Data Protection Manager) were not optimized for other operating systems and devices. Research participants, even those that were traditionally a Microsoft shop, wanted a solution that could support whatever hardware and software decisions they needed to make in the future.

Customer Support: Customer support was consistently mentioned by each of the participants as meaningful in their choice of Druva. Overall, during the evaluation process, Druva's response times to inquiries and willingness to work with the participants was notably superior to that of the competition, and factored into the final decision. It is worth noting that ongoing support after implementing Druva was rated exceptionally well by the research participants.

While research participants initially selected Druva inSync with a focus on cloud backup, the available data governance and eDiscovery capabilities interested several of the companies. Druva provides an opportunity for organizations to audit their file archives, monitor activity and manage data governance policies from a central platform. This represented a significant advantage over incumbent processes for accomplishing these goals, and Blue Hill found that existing Druva customers appreciated this value proposition to a greater extent after they purchased the inSync solution. After growing comfortable with Druva's endpoint backup capabilities, the organizations that Blue Hill studied took the next step of exploring additional compliance and governance value that these additional features provided.

> "Backups used to be our worst nightmare. They failed all of the time. Now, I have only seen one failed backup in two years and it was our fault. If data loss protection is important to you, then Druva's is really good."
>
> *Desktop IT Lead, Food Services*

Selection Spotlight: Choosing Druva inSync over HP Connected

The global electronics manufacturer presented a particularly compelling case as it navigated the choices for an endpoint backup solution. After experiencing a number of challenges with its existing environment, the manufacturer launched a thorough evaluation process of viable alternatives. In the process of doing so, the IT and business decision-makers made direct, head-to-head comparisons between Druva inSync and HP Connected.

In preparing for this analysis, the IT infrastructure manager and his team compiled a list of features they considered necessary to a successful implementation. The team identified that the new backup solution must do the following: present a low total cost of ownership; work seamlessly with employees who experience infrequent connectivity; have sufficient security and encryption capabilities; and support users in European locations.

As the firm went through the evaluation process, it became clear that Druva presented the only viable option for its particular business needs. In the direct comparison with HP Connected, the global electronics manufacturer highlighted several instances where Druva differentiated itself as the superior solution from a technical capabilities standpoint.

The three most prominent differentiating factors were:

- Superior deduplication capabilities
- Better network usage
- More robust encryption and security

The IT infrastructure manager identified Druva as having far more advanced deduplication capabilities than HP Connected. Druva has the ability to deduplicate information on a more granular level than just the device level, meaning that Druva does not backup redundant information from multiple devices across the entire enterprise. For example, if the same file existed on 500 devices, HP Connected would back up this file 500 times whereas Druva would only back up this file once. The impact is that Druva is able to drastically enhance the efficiency of backups. In contrast, HP Connected was found to unnecessarily back up large quantities of redundant data. The team identified Druva's advantages in deduplication as leading to smaller, faster, and overall better backups than what HP Connected could provide.

Along with more efficient backups, Druva not only placed less strain on bandwidth limitations, but also more intelligently balanced network usage rates than HP Connected. This further provides an opportunity to reduce demands on IT infrastructure and allows for faster backups while minimizing potential bottlenecks and other instances that would require manual oversight.

The manufacturer was drawn to Druva inSync's:

- Superior deduplication capabilities
- Better network usage
- More robust encryption and security

In the evaluation, the electronics manufacturer also noted that Druva's ability to encrypt data at rest and in transit was an important differentiator. The IT infrastructure team evaluated Druva's overall security as superior to what HP Connected offered. This had a two-fold impact on compliance needs and peace of mind.

It should be noted that the electronics manufacturer also placed great importance on the presence of European data centers and the advantageous licensing model that Druva provided. Consistent with the broader themes discussed in the prior section, Druva's advantages in these areas were material in the decision-making process. This served to further solidify their position when holistically evaluating the value offering of Druva in comparison to HP Connected.

Resulting Business Impact

Since choosing and implementing Druva, the studied organizations reported a number of impacts on their business of tangible magnitude. The benefits realized could primarily be attributed to IT efficiency gains and their resulting financial implications.

> "Now my guys can spend their time doing more interesting stuff than patching servers and running around doing big forklift upgrades."
>
> *Director of IT and Cloud Operations, Digital Radio and Smart Audio Devices Supplier*

IT Efficiency: The efficiency savings that participants experienced after deploying Druva were both significant and measurable. This study demonstrates that Druva provided a reduction in administrative resources required to run successful endpoint backups. The global electronics manufacturer went from requiring nearly full-time attention of a dedicated employee to almost no administrative oversight. To this end, the global consultancy also experienced measured efficiency gains. Prior to Druva, the organization hosted the information on its own internal servers. Upkeep of the endpoint backup process traditionally required 2-3 hours a week, but as its infrastructure aged, this time requirement ballooned to 2-3 hours each day. With Druva, the participant reported that administrative oversight was almost non-existent. Similarly, the medical equipment provider and digital radio and smart audio devices supplier both reported that they were able to take an almost completely hands-off approach to endpoint backup administration after deploying Druva.

In addition to reduced administrative time, participants reported that Druva made performing the backups themselves considerably more efficient. In the case of the Canadian food services company, backups took sometimes in excess of a week to complete. Since Druva, this was reduced to approximately two hours a week. A crucial aspect driving these efficiency gains is Druva's ability to automatically provision new users, since this allows IT teams to broaden the scope of their endpoint backups without incurring additional time commitments.

> "For Druva we spend zero time. There is no administration. When we hire someone, it is all automated. We update the directory and it automatically provisions the accounts on Druva and emails the user. Sometimes we get a request, but it is negligible."
>
> *Director of IT, Global Consultancy*

Participants in IT organizations also noted another benefit in peace of mind. While this may not qualify as an explicit efficiency gain, its impact on IT's relationship to the endpoint back-up process was meaningful. Prior to Druva, participants were constantly monitoring their backup processes, which frequently broke, worked incorrectly or otherwise required maintenance. Participants reported that Druva eliminated these concerns by effectively running in the background without the need for monitoring.

Financial Impact: From a financial perspective, Druva was found to have both an implicit and explicit impact. Explicitly, Druva was generally found to reduce the total cost of ownership of endpoint backup. This stemmed largely from Druva's licensing model, cloud delivery model and increased personnel efficiency. Participants found that licensing on a per-user basis, which Druva does, rather than on a per-device basis, proved advantageous to the participants. Additionally, Druva lets organizations reassign licenses from employees who leave the company rather than requiring the organization to purchase a new license. Further, the cloud delivery model allows organizations to disassociate themselves from the cost of maintaining and building physical infrastructure. As previously discussed, the reduction in backup and monitoring personnel costs also freed companies to reallocate employees to higher-value tasks.

An interesting counterpoint from a financial perspective is that maintaining physical infrastructure can have a cost advantage from an accounting and reporting view. Data centers can be depreciated as an asset, which has certain advantages over recurring expenses spent on recurring monthly cloud expenses. However, in practice, participants found that the overall gains in efficiency from Druva, costs of licensing, and the upfront and ongoing costs of building and maintaining infrastructure were enough to overcome this argument. As one example, the Canadian-based food services company analyzed by Blue Hill reported that switching to Druva resulted in a roughly two-thirds cost savings over its prior solution.

Implicitly, Druva made a financial impact through the efficiencies and time savings it enabled. Because Druva reduced administrative oversight, IT team members shifted from a reactive to proactive roles and no longer had to worry about putting out recurring fires.

Another indirect financial impact comes into play when considering Druva's effect on line-of-business productivity. Backups can affect employee productivity in a number of ways. Business users know that backups that slow down or crash their devices or applications have a net negative effect by adding downtime throughout the working day. More importantly, if a device is lost or stolen, or an unprotected application is breached, the ease of restoring relevant information can impact productivity as well. In short, the faster employees are able to get the information they need to begin working again, the sooner they can start being productive again.

Especially in organizations that charge out their employees via billable hours, every hour of uptime provided by a superior backup solution can be directly traced to additional revenue. In the case of the global consultancy where employees typically bill clients hundreds of dollars an hour, even the first hour of additional uptime more than covers the licensing costs.

Conclusions and Key Takeaways

Blue Hill offers the experiences of these five research participants so that business and IT decision-makers can identify pain points and business opportunities relevant to their own organizations. Legacy endpoint backup solutions that were not created to reflect the reality of a changing mobility landscape and distributed workforce can create real challenges in enterprise scalability and IT efficiency. It is clear from the experience of the studied organizations that Druva presented an opportunity to not only provide the technical requirements necessary for modern endpoint backups, but also the opportunity to protect applications, and reduce oversight, infrastructure, data footprint and headaches traditionally associated with the backup process.

IT staff should audit the amount of time they are spending on managing and provisioning their endpoint and applications backup processes each week. In considering the cost of investment in Druva or competing endpoint and applications backup solutions, potential buyers should also consider the implicit financial benefits of reallocated time to more value-added activities. In the case of line-of-business productivity, there may be an opportunity to draw a direct line between reduced downtime and firm revenue. IT decision-makers who can quantify the hourly cost associated with line-of-business employees will craft a compelling argument when presenting the business case for investment. By considering the holistic financial and technical experiences of these five studied organizations, Blue Hill expects that organizations investigating enterprise-wide endpoint and applications backup solutions will be better prepared to make a decision that aligns both with the new needs of mobile and cloud-based IT, and to increase IT efficiencies to encourage greater technical innovation and improved technical support.