ESG Lab Review

Extending Protection Capabilities with Acronis Backup 12.5

Date: October 2017 **Author:** Vinny Choinski, Senior Lab Analyst

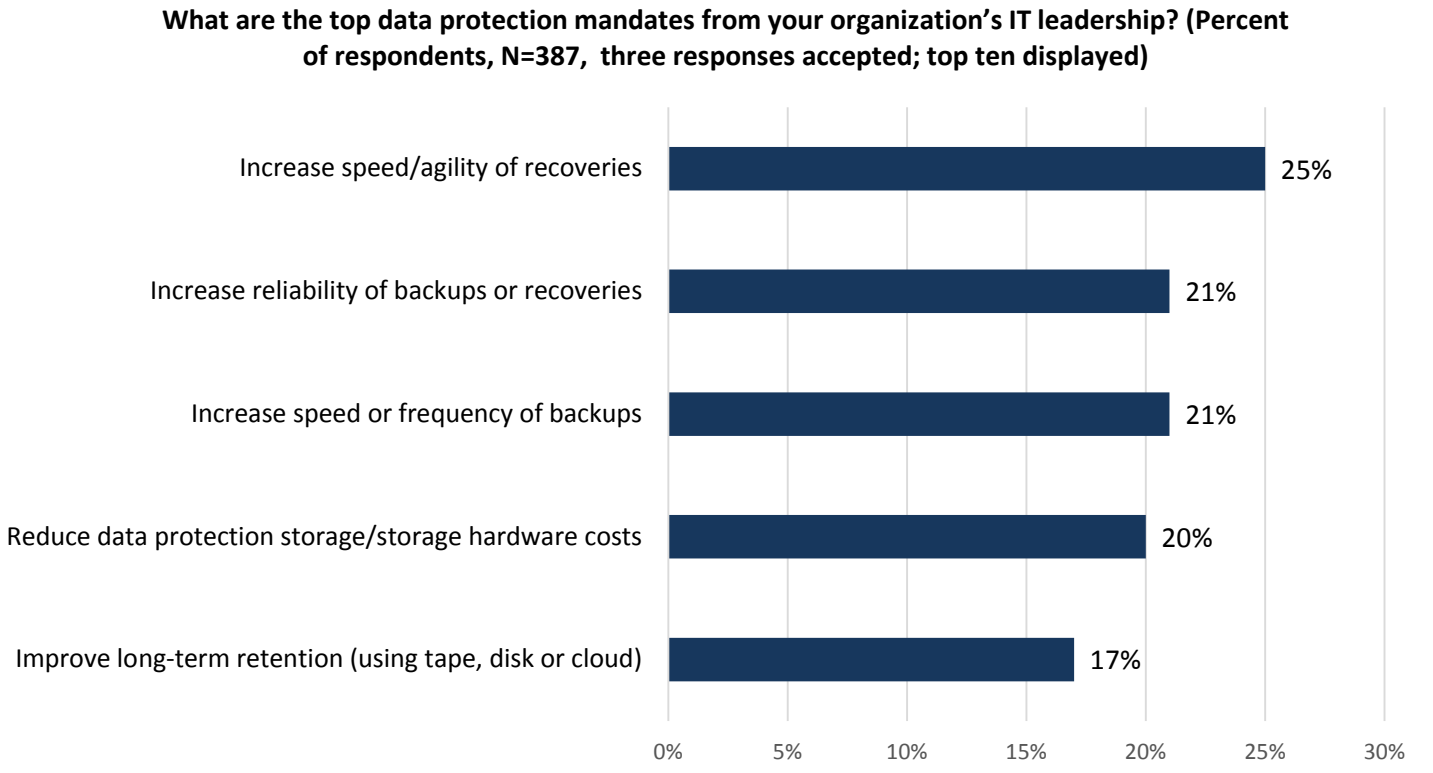
Abstract

This ESG Lab Report documents hands-on validation of the Acronis Backup 12.5 data protection solution. Validation was designed to demonstrate how the solution's agile backup, restore, and extended protection capabilities help customers easily and efficiently protect and recover business-critical systems and data.

The Challenges

A business cannot survive without its data, no matter where it lives, and hybrid cloud IT environments are putting pressure on data protection solutions to keep pace. Today's solutions are often expected to deliver not only backup and restore, but also disaster recovery and availability for physical, virtual, remote, and cloud systems and workloads. In a recent ESG research survey, 25% of respondents identified increased speed/agility of recovery as one of the top data protection mandates from IT leadership, making it the most-cited response (see Figure 1).[1] However, this same ESG research also indicates a strong desire by IT leadership to improve the reliability of both backup and recovery.

Figure 1. Top Five Data Protection Mandates from IT Leadership



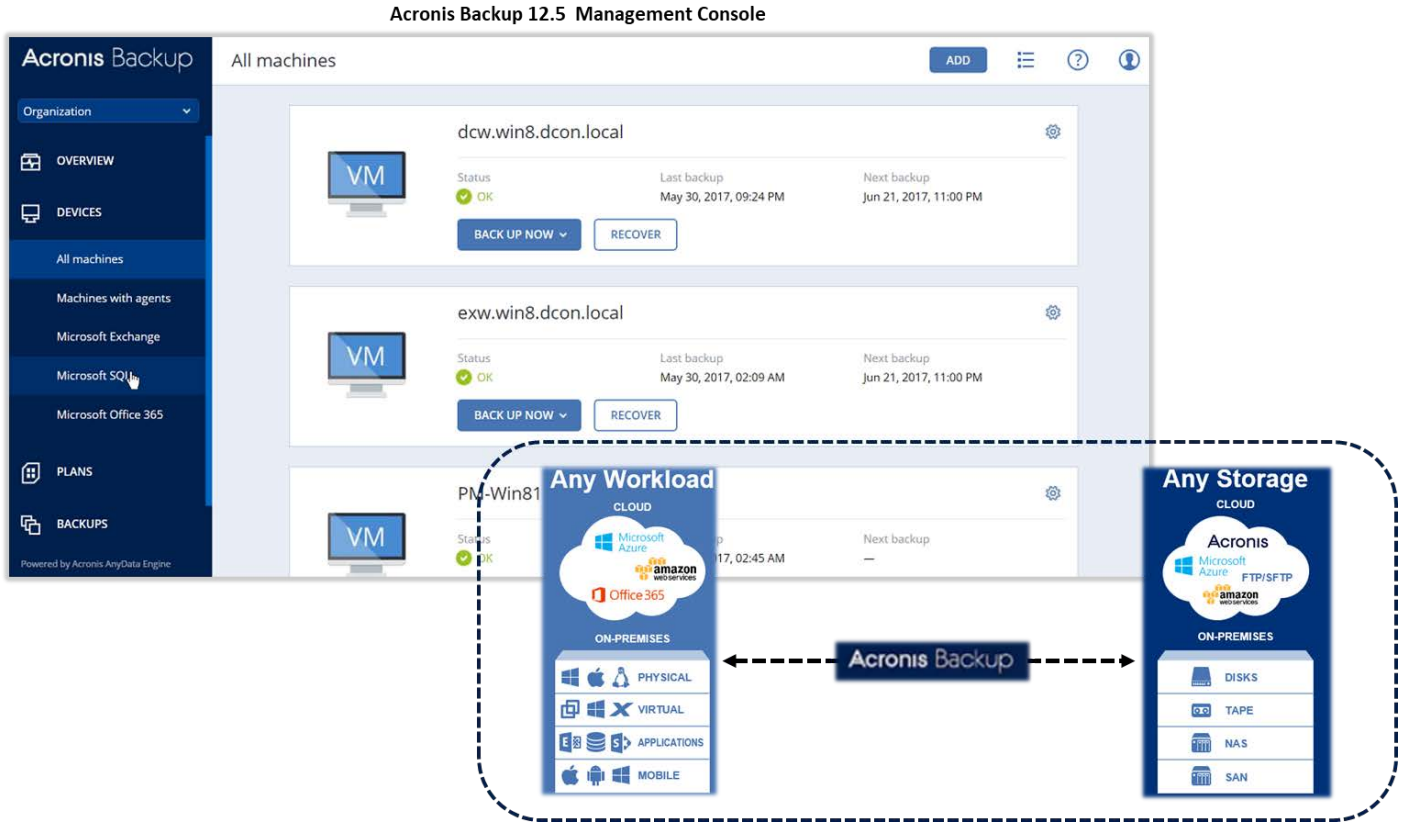
Source: Enterprise Strategy Group, 2017

[1] Source: ESG Research Report, *2017 Trends in Data Protection Modernization*, to be published.

The Solution: Acronis Backup 12.5

Acronis Backup 12.5 converges cloud and on-premises data protection into a unified solution designed for quick and reliable recovery of business-critical applications. It is managed through an intuitive, easy-to-use web console. As shown in Figure 2, it protects the entire business by including physical and virtual servers and workstations, public/private cloud infrastructure, and mobile applications and devices. It supports local and cloud-based backup storage, allowing complete control over the location of your data, systems, and backups.

Figure 2. Solution Overview



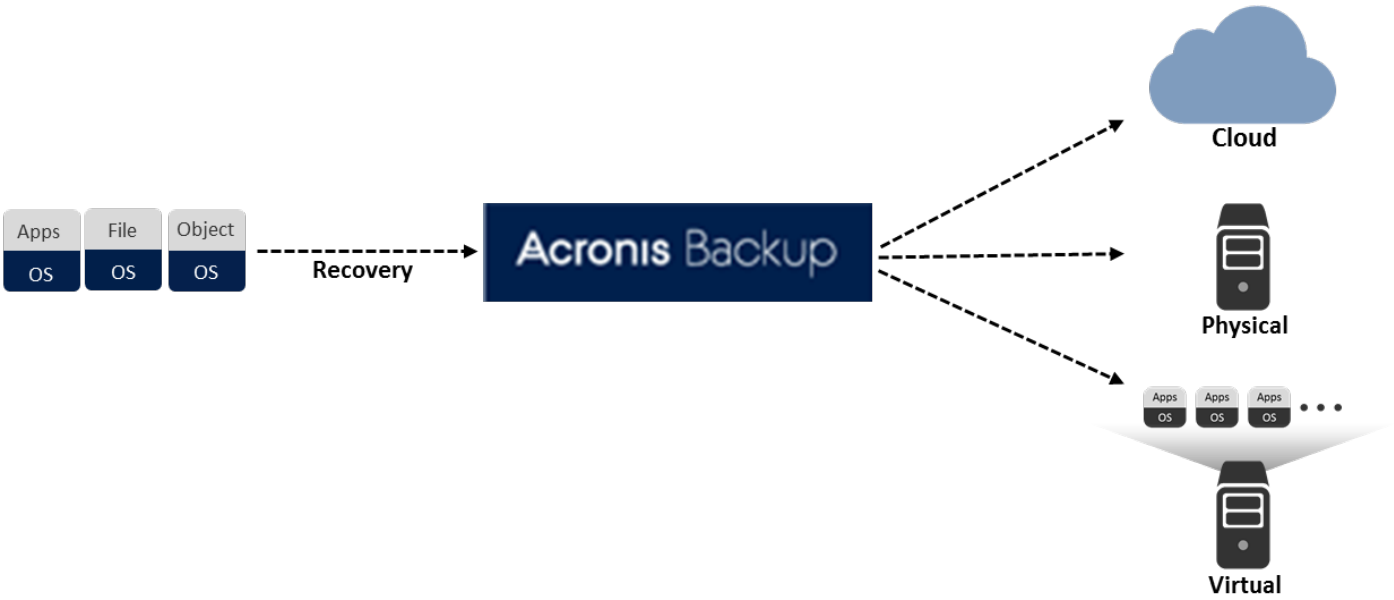
Source: Enterprise Strategy Group, 2017

Key solution features include:

- Image-based backup for entire physical, virtual, and cloud systems.
- Agentless and agent-based VM backup for VMware vSphere and Microsoft Hyper-V.
- Scale up to 2000 machines per installation.
- Backup for user endpoints, such as desktops, laptops, and mobile devices.
- Wide area network (WAN)-optimized, VMware virtual machine (VM) replication, failover, and failback.
- Easy-to-use, on-premises and cloud-based web console to manage all physical systems, VMs, cloud workloads, application backups, and endpoint backups.
- Acronis Active Protection that enables proactive ransomware protection.
- Acronis Notary that uses blockchain technology to authenticate and validate backup data.
- SAN storage snapshots that reduce hypervisor resource utilization by leveraging snapshots for backup.
- Off-host backup processing that reduces system utilization by performing backup tasks on separate machines.

Acronis Backup 12.5 enables SMEs to back up data to direct-attached disk, NAS, and SAN, or to Acronis Cloud Storage or Microsoft Azure. This backup flexibility enables extensive recovery agility. With Acronis Backup 12.5, customers can recover their data, where they want it and when they want it, from the most efficient copy to the most practical location. As seen in Figure 3, application, file, and object data can easily be recovered to cloud, physical, and virtual locations.

Figure 3. Recovery Overview



Source: Enterprise Strategy Group, 2017

Key recovery features include:

- Acronis Startup Recovery Manager for fast restore of Windows systems.
- Recovery of Windows or Linux machines to the same or dissimilar hardware, including virtual and cloud environments.
- Physical-to-physical backup and recovery of Mac systems.
- Acronis Instant Restore for flexible, complete recovery options with RTOs of seconds or minutes.
- Leverage changed block tracking (CBT) to focus recovery on data updated since last backup.
- Recovery of files, folders, databases, mailboxes, emails, and other items.
- Granular recovery from Exchange and SharePoint backups.
- Automated bare-metal recovery with customizable boot media.
- Ability for remote sites and systems to achieve bare-metal recovery on WAN to reduce recovery time.
- Backup replication in multiple locations to reduce risk of recovery failure.
- Acronis Notary's data authentication to fortify the integrity of data recovery.

ESG Lab Validated

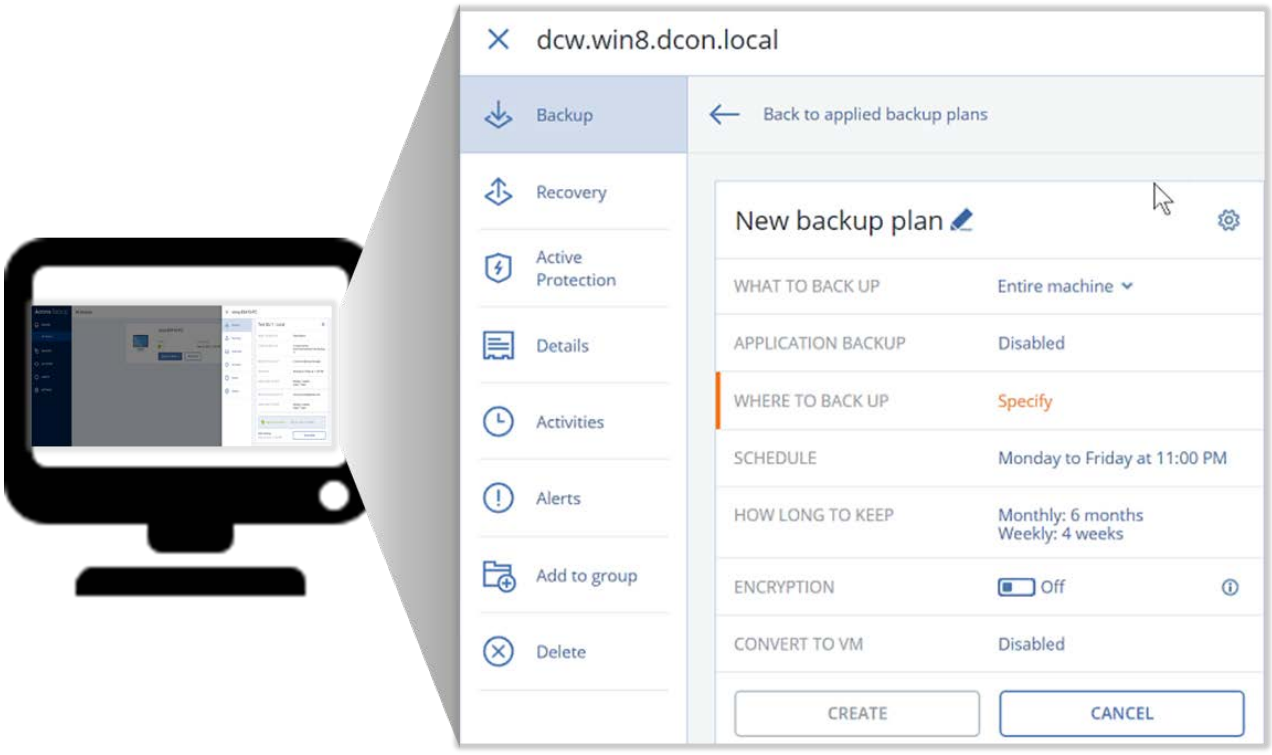
ESG Lab performed remote, hands-on evaluation of Acronis Backup 12.5 using an Acronis Cloud demo environment, and by leveraging an Acronis trial license option, at the ESG corporate office in Milford, MA. Validation was designed to demonstrate how the solution's agile backup, restore, and extended protection capabilities help customers efficiently protect and recover business-critical data and systems with ease.

Ease of Use

The usability section of this report focuses on using the Acronis Backup 12.5 administrator interface to configure and run multiple backup and recovery scenarios. This included simple file level backup and restore, MS-Exchange message level restores, and Acronis Instant Restore of virtual machines. For validation, ESG Lab leveraged an Acronis Cloud demo environment and a local install on a small Windows server with USB-attached high-capacity disk storage. The Acronis Cloud demo environment allowed us to test the more complex scenarios, while the local deployment allowed us to take an extended dive into the management interface features.

As shown in Figure 4, ESG Lab leveraged the Acronis Cloud demo environment to configure a backup plan for a Microsoft Exchange server called *dcw.win8.dcon.local* in the test environment. The interface made it easy to configure key settings including what to back up, where to back it up, the schedule, and the retention. More advanced options can be configured by clicking on the gear icon to the right of the edit ***New backup plan*** field.

Figure 4. Backup Plan Configuration

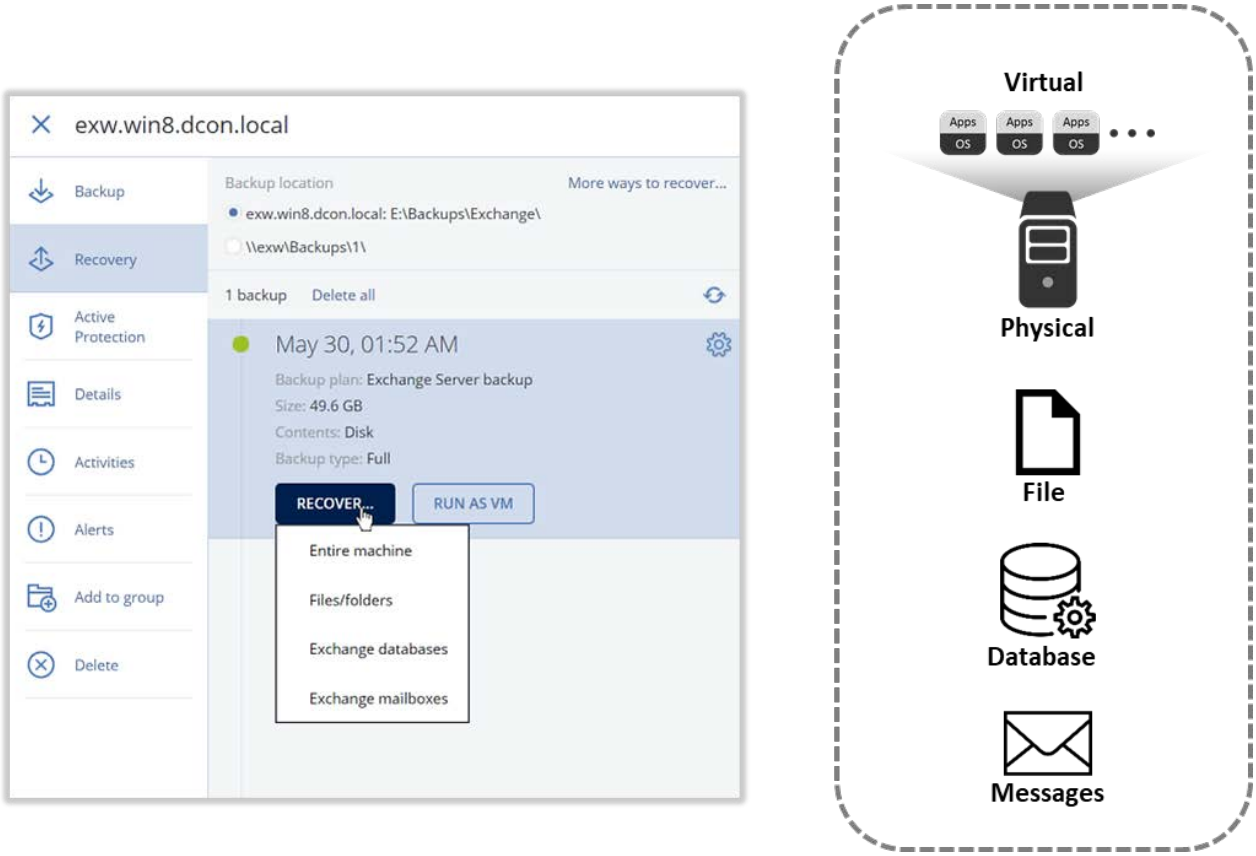


Source: Enterprise Strategy Group, 2017

We also leveraged the 30-day trial license to configure one terabyte of Acronis Cloud Storage to our local test environment. We also configured a local backup repository on a 250GB SSD device. The local backup repository was simply a directory created on the external SSD drive that we named *Acronis Backup Storage*. We leveraged both the local storage and the cloud storage in different backup plans. ESG Lab successfully conducted directory level, file level, and system state backups and restores using the local device and the Acronis Cloud storage.

Next, as shown in Figure 5, ESG validated the ability of Acronis Backup 12.5 to recover individual MS-Exchange messages. We leveraged the Acronis demo environment, which had an existing Exchange server running. We deleted two messages from a test user Outlook account and used the Acronis Backup 12.5 management interface to recover the messages back to the original mailbox. The interface enables easy search of the backups for deleted messages and even allowed us to preview the message and attachments before recovery.

Figure 5. Backup Policy Configuration



Source: Enterprise Strategy Group, 2017

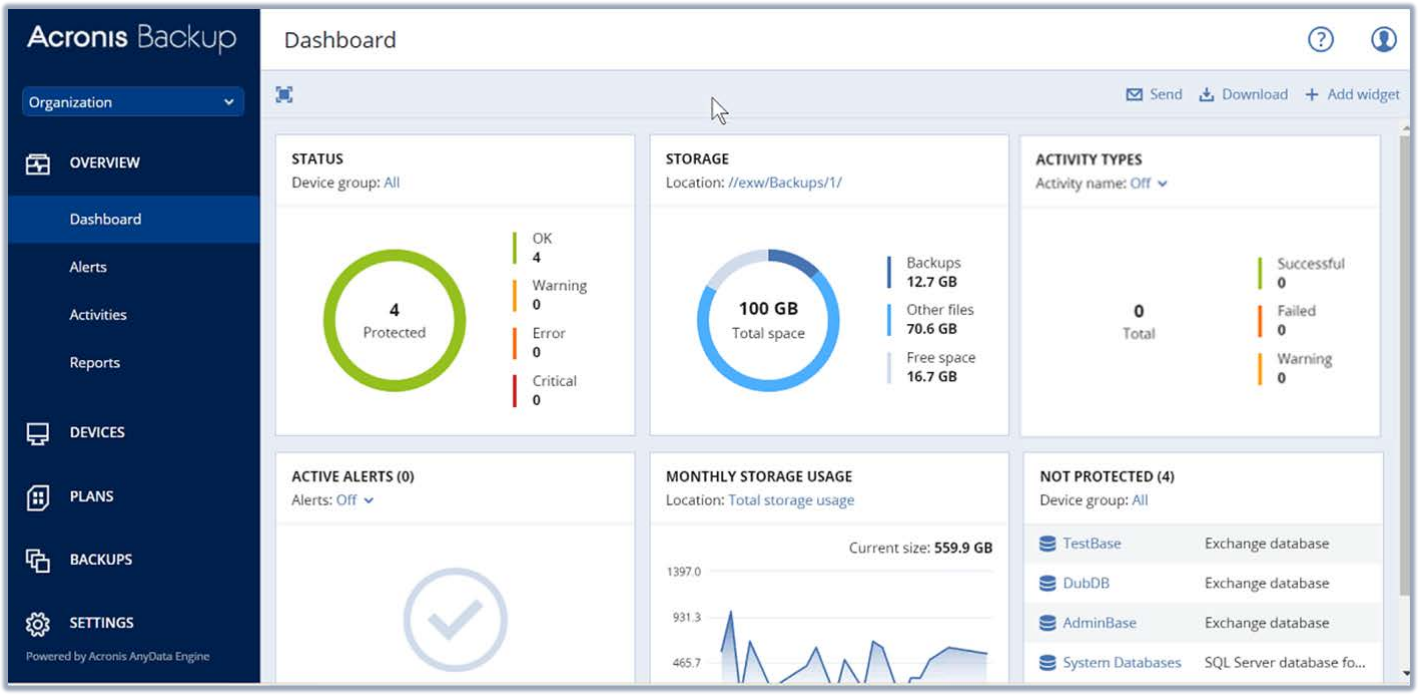
We leveraged the same demo environment to conduct an instant recovery of a virtual machine from an Acronis Backup image. We selected a Windows Hyper-V machine that had a complete system backup and chose the option to run it as a VM. From the Windows Hyper-V server, we monitored the process and confirmed the virtual machine showed up and started the boot process. This took approximately 12 seconds. A few seconds later, it was up and running and we were able to log in to its console.

Next, ESG Lab leveraged the local test environment to further explore the management interface by reviewing more of the advanced backup configuration options. It should be noted that for each device you add to the environment, Acronis creates default settings for backup to make getting started easier. These settings, including backup plan name, backup type (e.g., file, application, and complete system), backup target, data storage location, schedule, retention, and replication can be easily adjusted to match your business requirements. The replication option allows different retention periods to be set for replicated data. The interface provides very granular control of backup attributes. The default settings enable you to quickly get up and running.

Finally, as shown in Figure 6, we explored the new solution visibility features available in version 12.5 of Acronis Backup. These features can be found under the ***OVERVIEW*** icon located in the left side navigation pane. The features can be accessed from the new ***Dashboard*** view that provides a customizable visual display of the backup infrastructure. Solution

information can be easily added to the view as table, chart, graph, and list widgets such as the *STATUS*, *STORAGE*, and *ACTIVITY TYPES* widgets shown in the top row of Figure 6. They can be dragged and dropped in the dashboard view to create the desired order. Alerts and activities with detailed lists are made available as separate pages to help with drill down troubleshooting and monitoring. This detailed information can also be packed into preconfigured or custom PDF or MS-Excel rendered reports that can be easily emailed out on scheduled intervals to appropriate recipients such as organizational, departmental, or remote office administrators. It's also worth noting the *Organization* dropdown tab just above the *Overview* icon. This is where the solution can be configured for multi-site or multi-department management. Under the *Organizations* tab, units with specific administrators can be created for different business departments, locations, or remote branch offices. A unit administrator has the access required to manage the devices assigned to that unit. Organization administrators have access to manage the entire environment.

Figure 6. Solution Visibility



Source: Enterprise Strategy Group, 2017

Why This Matters

Ease of use is an important element in the SME space, where IT professionals often have to wear many hats, but it is only one piece of the overall usability equation. It is just as important that the data protection solution supports the entire environment and provides the flexibility to meet an organization's business requirements for data protection.

ESG Lab found this solution not only easy to manage, but also feature rich. It includes all the attributes needed to conduct enterprise-class data protection with ease-of-use features that make it ideal for SMEs. During our validation, we were able to easily define protection attributes such as the storage location (e.g., cloud versus local), the frequency of protection, and data retention at a very granular level. We also used the new dashboard, alerts, activities, and reports features to easily and intuitively monitor the status of the entire data protection environment.

Resource Efficiency

In this section of the report, ESG explores two new capabilities that impact the overall resource efficiency of an Acronis Backup 12.5 solution: SAN storage snapshots and off-host backup processing. These elements help improve overall solution scalability and RPOs by removing protection workloads from the production systems that are being protected.

ESG started resource efficiency validation by reviewing the SAN storage snapshot process for protecting a virtual environment. For this configuration, the Acronis Backup 12.5 solution leverages API communication with both the virtual machine hypervisor and the SAN storage system. As shown in Figure 7, for this environment, the SAN storage solution that contained the VM datastore was a NetApp filer NFS connected to the VM host server.

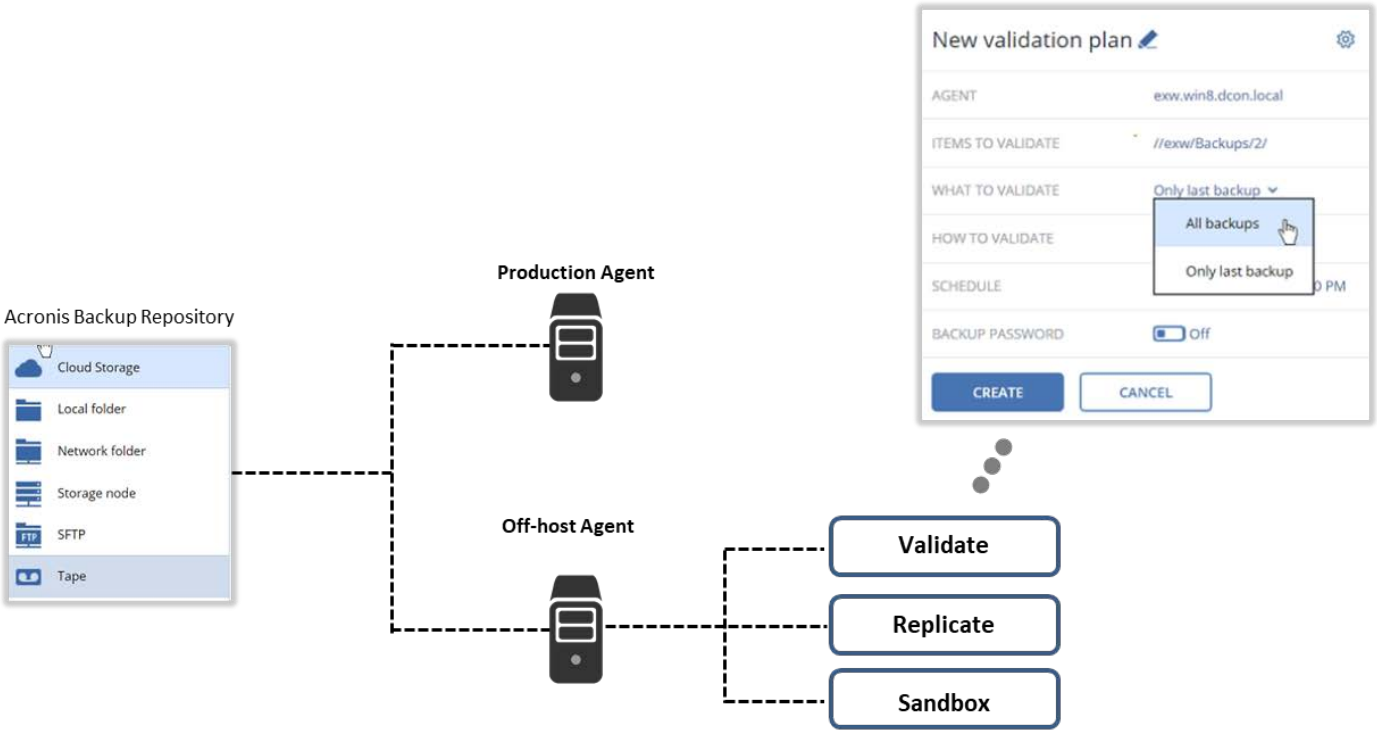
To execute the SAN storage snapshot backup, the Acronis Backup software first made an API call to the hypervisor host that created a VM level snapshot. Then an API call was made from the Acronis Backup software to the storage system to instantaneously make a storage snapshot of the volume that contained the VM datastore. Once the storage snapshot was created, the VM level snapshot was closed. The volume snapshot was then presented to a server running the Acronis backup agent. The backup data was transferred from the Acronis agent server to the backup repository. There was no impact to the production VM environment during the transfer of backup data, and the VM level snapshot was only open for a brief time to put the datastore in a consistent state before the storage snapshot was created. To control snapshot sprawl, the storage snapshot was deleted immediately after the backup job completed. It should also be noted that the entire process was orchestrated through intuitive Acronis configuration menus. We simply needed the name and credentials to the NetApp storage system to complete the configuration. The Acronis agent machines with access to the NFS storage were preconfigured in the storage network infrastructure for access and were presented as a list of options in the menu. API access to the hypervisor was also previously configured in the Acronis Backup 12.5 solution for a different backup job. We simply had to check a configuration box to enable the initial ESXi consistent snapshot.

Figure 7. SAN Storage Snapshots

Source: Enterprise Strategy Group, 2017

We also explored the ability within the Acronis Backup solution to move data protection management tasks such as validation, replication, deduplication, and even sandboxing to a non-production host. This ability improves system resource availability for production applications by reducing the amount of resources needed for data protection operations. As shown in Figure 8, off-host processing tasks such as validation can be easily configured using Acronis Backup user interface menus. ESG used the *New validation plan* menu to set up off-host checksum verification for a production server being protected by Acronis Backup 12.5. Here, the off-host agent simply needed access to the production server's backup images stored in the backup repository to run the checksum process. The same process can be used for replication, deduplication, and D2D2C, or even to bring up a VM in a sandbox environment for validation or test/dev operations as long as the infrastructure supports the process.

Figure 8. Off-host Backup Processing



Source: Enterprise Strategy Group, 2017

Why This Matters

We often forget how big a role agility and flexibility can play in a data protection solution's overall performance. It's not just about how fast a chunk of data can be moved from point A to point B at any given time. Arguably, it's rare for an organization to have all the hardware resources at its disposal to hit maximum performance when a backup job is run. It's really about being able to apply the right resources where they are needed to quickly get a protection copy off the production host as fast as possible.

ESG Lab validated that with the Acronis SAN storage snapshots and off-host backup processing capabilities, Acronis Backup 12.5 customers can efficiently apply protection resources where they are needed with less impact on the system resources needed by production applications. We found that the combination of these features significantly improves the overall efficiency of Acronis Backup 12.5 data protection capabilities.

Extended Protection

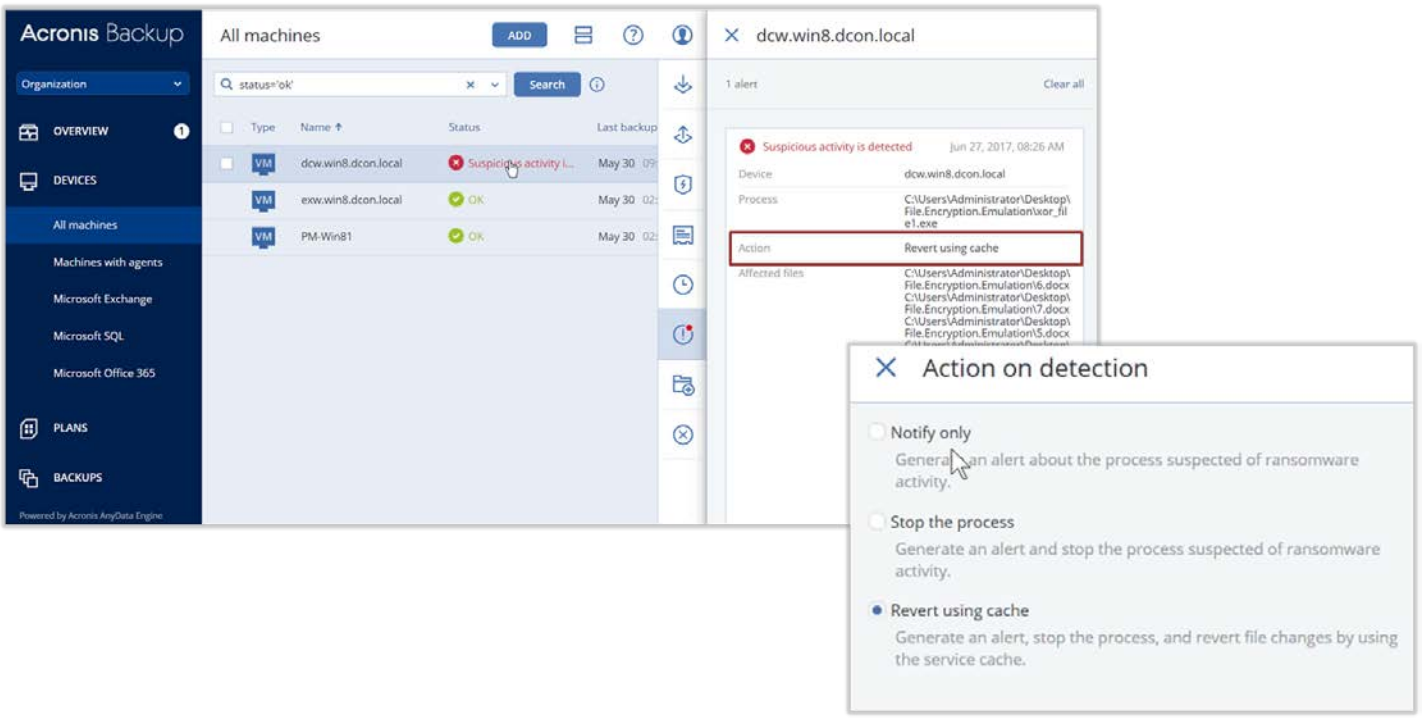
The extended protection section of this report focuses on Acronis Active Protection and Acronis Notary, two new features in Acronis Backup 12.5 that go beyond the traditional backup and restore functionality typically associated with data protection solutions. The first feature, Acronis Active Protection, complements existing security solutions by helping organizations detect, stop, and instantly recover from malicious activity that can render corporate data inaccessible. The second feature, Acronis Notary, helps ensure the authenticity of corporate data, a task that is typically the responsibility of the corporate compliance officer.

ESG started its extended protection feature validation by exploring the capabilities of Acronis Active Protection. This feature is included in the Acronis Backup 12.5 client agent software and can be run on any licensed device that is part of the data protection infrastructure. Once enabled, the software monitors the device in real time for malicious activity, which is usually exposed through unexpected bulk file encryption or file extension changes. If malicious activity is detected, the software takes action based on the defined configuration. For validation, we used a script that simulated malicious file encryption on a set of test files and directories.

Once the script was executed, as shown in Figure 9, we clicked on the red color-coded suspicious activity alert on the test device to display detailed information about the event. This information included the device affected, the name and directory path of the file that caused the alert, the action to be taken, and the files that were affected by the event. For this test scenario, we used Acronis Active Protection cached data to revert to the original files.

The Acronis Backup configuration menu displayed on the lower right side of Figure 9 shows the available action options that can be taken in the event malicious activity occurs. These actions include offering simple notification, stopping the process, and stopping the process and reverting to a cached copy.

Figure 9. Acronis Active Protection



Source: Enterprise Strategy Group, 2017

Finally, ESG Lab explored the Acronis Notary feature now available in the Acronis Backup 12.5 solution that leverages a distributed ledger and trust infrastructure for data and transaction immutability and authenticity called blockchain. Blockchain technology was first capitalized on by the financial industry to record and validate transactions in a permanent way. It is quickly becoming a worldwide standard across industries such as finance, banking, supply chain, and manufacturing for validating and auditing data immutability. Acronis Notary uses blockchains to ensure file validity with timestamp fingerprints and links to previous blocks in the chain.

As shown in Figure 10, we enabled the Notary feature in an Acronis Backup 12.5 backup plan to validate a set of files during the backup operation. For this backup job, Acronis Notary, in the background, handled the complex tasks of creating unique data hashes (SHA-2) and organizing the information into special data structures (Merkle Patricia tree). It also registered the transaction, in the Ethereum public blockchain, to validate the backup file existed at the time it was notarized. This data authenticity schema enables great flexibility in how and where long-term archive data is managed and stored.

Figure 10. Acronis Notary

Source: Enterprise Strategy Group, 2017

Why This Matters

Things move and change fast in today's always-on, always-up business environments, especially quickly when it comes to infrastructure and information protection and security. The lines between IT disciplines such as data protection, security, and compliance become more blurred every day. And, after several very high-profile data breaches over the last few years, the ascension of improved security and risk management as an investment justification metric for the entire IT organization is not surprising.

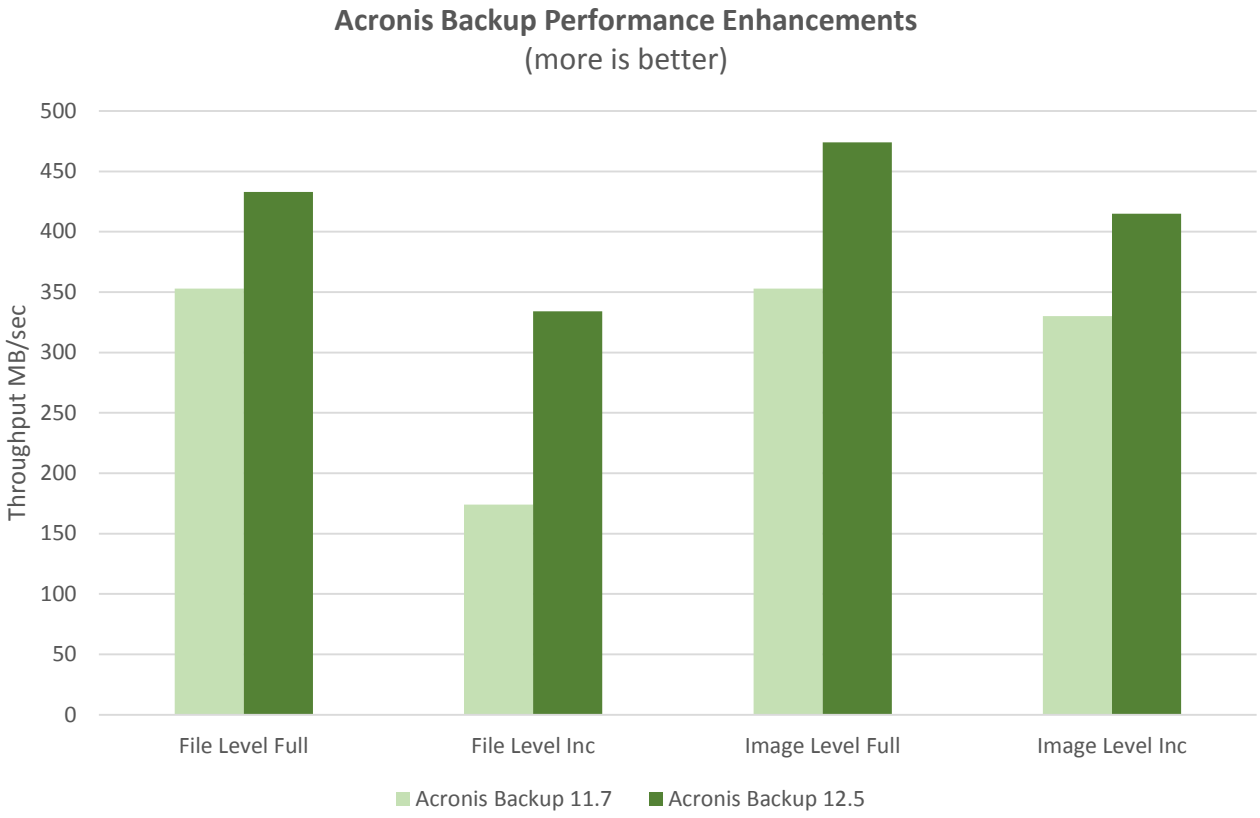
ESG confirmed that with the addition of Acronis Active Protection and Acronis Notary, Acronis Backup 12.5 has moved well beyond the expectations of traditional backup and recovery solutions. ESG validated that Acronis Active Protection augments the protection capabilities of the solution and works seamlessly with existing antivirus applications. And the Acronis Notary data authenticity capabilities add the information validation functionality needed when designing compliance and long-term data retention strategies.

Enhanced Performance

Performance is an important component of any data protection solution, and the latest version of Acronis Backup offers its customers significant performance improvements. To validate these improvements, ESG reviewed the Acronis development testing environment and audited the results of three different performance testing scenarios. The scenarios included Acronis version over version performance enhancements, Acronis versus competitors file level backup and restore performance, and Acronis versus competitor image level backup and restore performance.

As shown in Figure 11, ESG started its performance exploration by reviewing and auditing the results of Acronis Backup 12.5 versus Acronis 11.7 performance testing. Figure 11 shows the results of full and Incremental file level backups and full and incremental image level backups between the two versions. The test data set included real-world user data harvested from a production environment.

Figure 11. Backup Performance Enhancements



Source: Enterprise Strategy Group, 2017

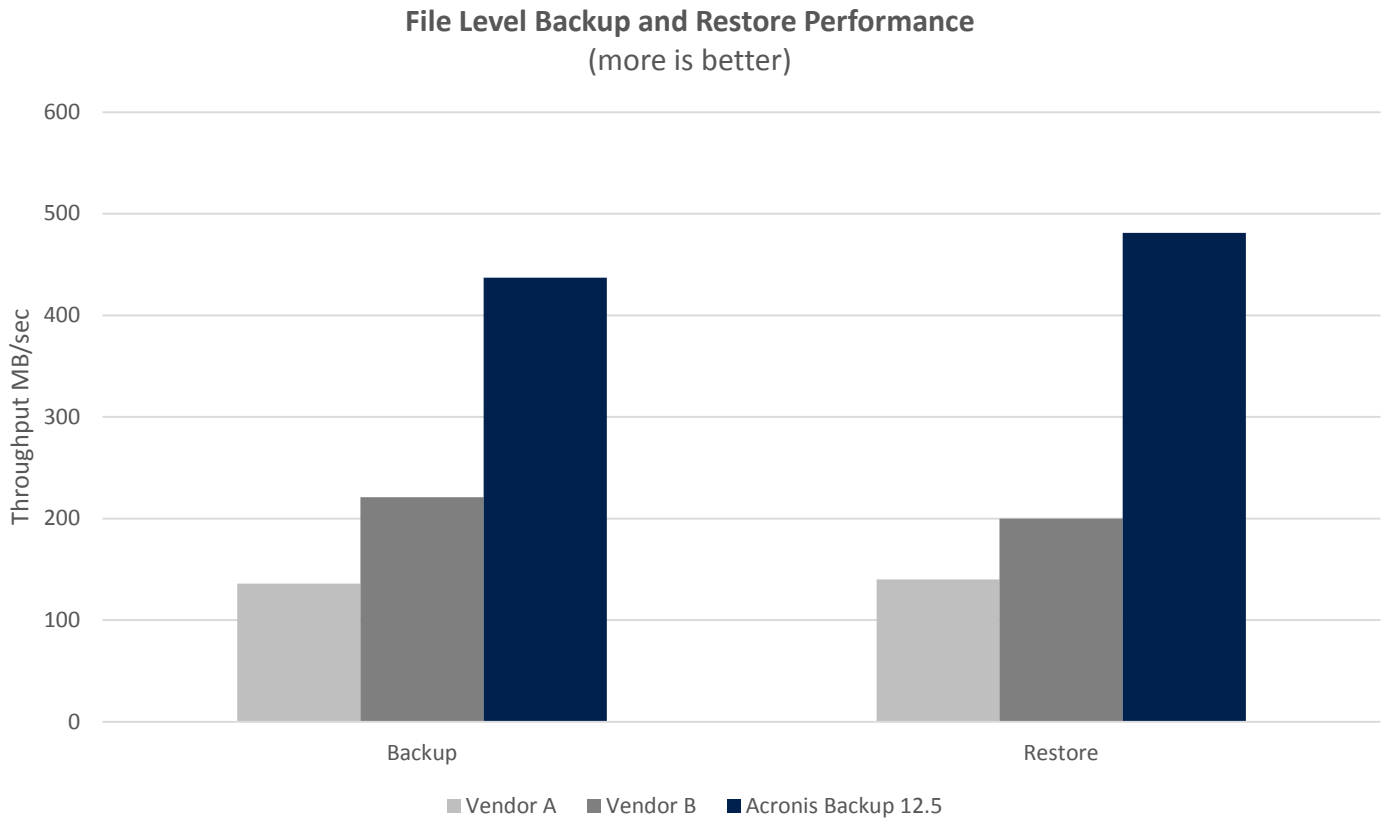
What the Numbers Mean

- Acronis Backup 12.5 demonstrated 18% more throughput than version 11.7 for a full file level backup.
- With a file level incremental backup, version 12.5 achieved 48% more throughput than version 11.7.
- Acronis 12.5 delivered 26% more throughput for a full image level backup over version 11.7.
- Version 12.5 also delivered 20% more throughput over Acronis 11.7 for an image level incremental backup.

Next, as shown in Figure 12, ESG reviewed and audited backup and restore performance of Acronis Backup 12.5 as compared with two industry recognized backup solutions. Figure 12 shows the results of agent-based, file level backup and restore testing. The test data set included the same harvested real-world user data previously used in the Acronis Backup 12.5 versus 11.7 testing. The supporting infrastructure included a Supermicro server with a Xeon E5-2640 processor and 128 GB of RAM to host each backup application during testing. The backup target was a 7.2TB RAID-0 set with a stripe size of 256 KB made up of four 7200RPM disk drives.

In Figure 12, Vendor A is a legacy, midmarket, agent-based solution that started out as a physical-host-only data protection application. It now supports both physical and virtual machine environments. Vendor B started as a virtual-only backup solution that now supports physical system data protection with the addition of Linux and Windows backup agents.

Figure 12. File Level Backup and Restore



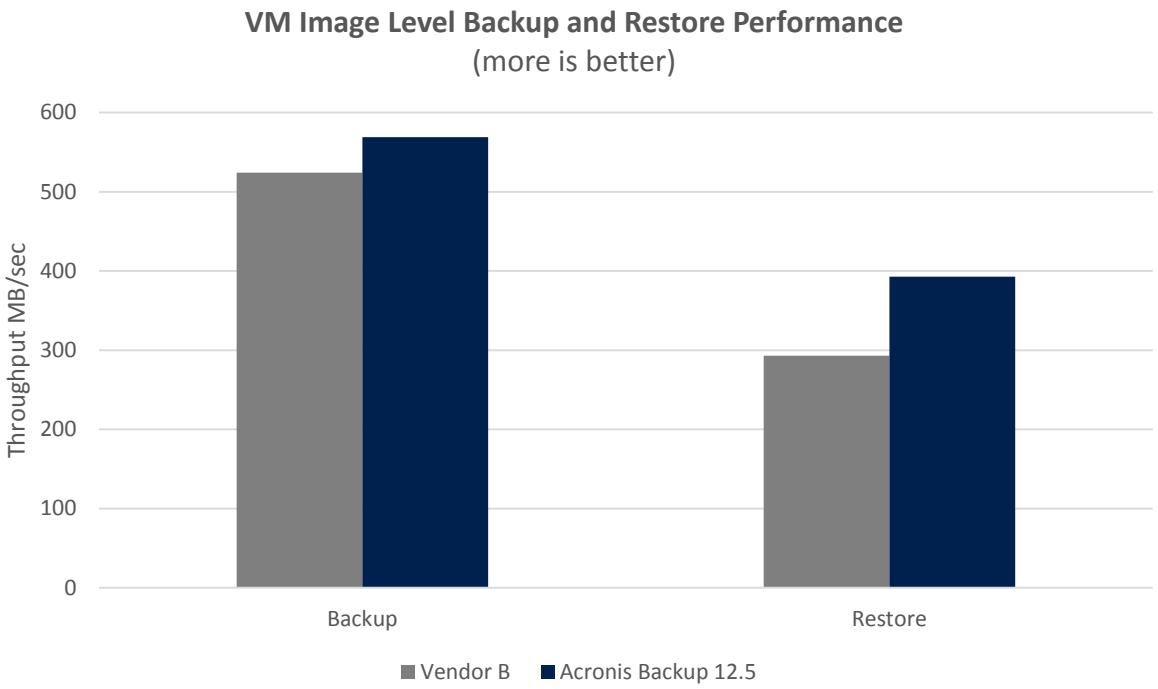
Source: Enterprise Strategy Group, 2017

What the Numbers Mean

- For file level backups, Acronis demonstrated 69% more throughput than Vendor A.
- For file level restores, Acronis Backup 12.5 demonstrated 71% more throughput than Vendor A.
- Acronis Backup 12.5 delivered 49% more throughput than Vendor B for file level backups.
- Acronis Backup 12.5 also delivered 58% more throughput than Vendor B for file level restores.

Finally, as shown in Figure 13, ESG audited Acronis Backup 12.5 performance results for image-based virtual machine backup and restore as compared with the virtual environment data protection capabilities of Vendor B.

Figure 13. Image Level Backup and Restore



Source: Enterprise Strategy Group, 2017

What the Numbers Mean

- Acronis Backup 12.5 delivered 8% more throughput than Vendor B for image level backup operations.
- Acronis Backup 12.5 demonstrated 25% more throughput than Vendor B for image level recoveries.

Why This Matters

According to ESG research, the top three most identified storage challenges—data protection, hardware costs, and rapid data growth rate—have stayed the same from 2015 to 2017. While 2017 finds data protection atop the list of challenges, the overarching issue that drives data storage concerns is relatively unchanged—data growth is accelerating and the resulting infrastructure required to store and protect that data is costly and complex.[2] To meet these challenges, data protection solution providers must be on a consistent path to innovate and improve solution efficiency.

ESG Lab validated that with each release, Acronis invests significant effort in improving the performance and efficiency of its data protection solution. ESG confirmed version over version backup performance improvements to Acronis Backup and a significant effort to keep pace with industry challenges and stay ahead of the competition.

[2] Source: ESG Brief, *2017 Storage Trends: Challenges and Spending, August 2017.*

The Bigger Truth

Today's IT environments are changing; these days, you would probably be hard pressed to find an environment that is not highly virtualized and using some form of cloud compute or cloud storage. However, it would not be unusual to find these same environments running certain business-critical applications on physical servers or local storage because certain applications are better suited for that type of environment.

Legacy applications that cannot be migrated in the foreseeable future, and applications that require specific onsite infrastructure to run a critical business process can make it difficult for IT to implement an easily managed data protection solution. Similarly, IT may struggle to support physical, virtual, and cloud initiatives, and multiple workflows such as protection, disaster recovery, replication, and migration.

ESG confirmed that Acronis Backup 12.5 is much more than a data backup solution. It also enables full system recovery, ranging from instant restore of virtual and physical machines to bare-metal recovery, migration capabilities, cloud-based disaster recovery, replication, off-host backup processing, SAN storage snapshots, and high availability.

ESG was pleased to see the new visibility features in version 12.5 that included dashboard, alerts, and activities views, along with reporting, that make it easy and intuitive to monitor the status of the entire data protection environment. We were also pleased with the addition of Acronis Active Protection and Acronis Notary, two new features that go beyond the traditional backup and restore functionality typically associated with data protection solutions.

If mandates from IT leadership have you evaluating your current data protection environment, and you're considering a faster, more agile, flexible, and comprehensive solution, ESG Lab believes Acronis Backup 12.5 should be on your list. It's a solution for the SME that has numerous features found in data protection tools designed for the enterprise. And, with very little investment in time and system resources, you can easily test drive it for yourself.