



PROACTIVE CYBER PROTECTION OPERATIONS

**Leveraging Comprehensive Backup Monitoring
& Reporting Automation To Get Ahead Of
Cyber Attacks**

INTRODUCTION

News stories abound of major organizations' data held hostage by cybercriminals. In just the past few years, this has included international newsworthy events like Colonial Pipeline paying nearly \$5 million USD in ransom to retrieve their data. However, there have been several significant yet under-the-radar ransoms like US travel services company CWT paying \$4.5 million, travel insurance provider Travelex paying \$2.3 million, and chemical distribution company Brenntag paying \$4.4 million in data ransom payments.

It's all too easy to think legacy backup operations and protocols will safeguard enterprises against ransomware events. This is grossly misguided. Data is growing at astronomical rates and it can take days or weeks to troubleshoot data protection issues, assuming they are uncovered in the first place. Relying on traditional data protection oversight practices and assuming all backup assets are properly protected leaves enterprises ripe for attacks.

Proactive backup operation automations address this head on. With improved monitoring, alerting, and data protection integrations, organizations not only safeguard unprotected assets but also enjoy proactive measures that keep them on step ahead of cyberattacks. Teams adopting these practices enjoy the same outcome as Fujifilm, an organization that successfully got their operations up and running after a ransomware attack...with zero ransom fees paid.

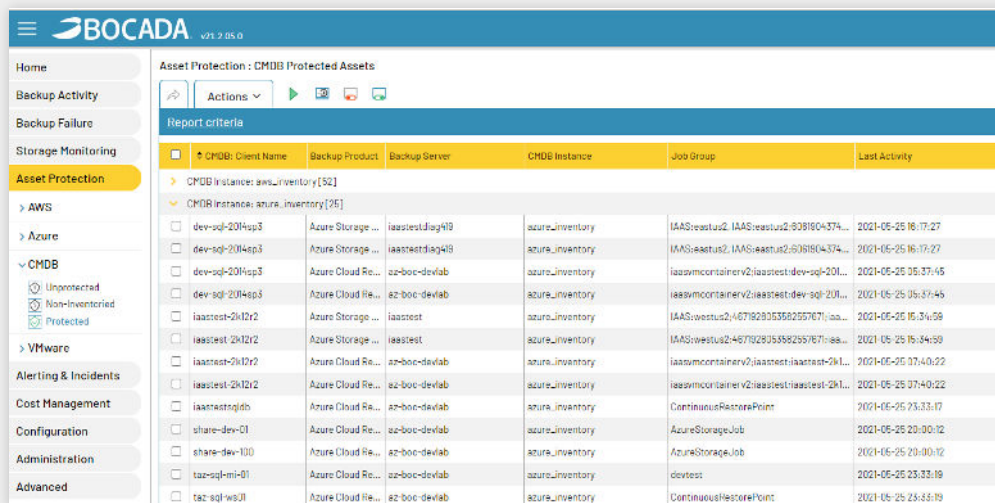
Backup Operations Automations To Safeguard Data Against A Cyberattack

The average time to identify a data breach is 196 days.¹ This tells us that while a cyberattack is in progress an organization is still generating new data. As a result, ongoing activities that streamline getting assets fully protected play a key role in holistic cyber-protection and data resilience.

Automate Unprotected Asset Discovery

Most organizations have low confidence that all of their organization's key resources have the correct backup protections in place. This is not surprising. A wide breadth of teams have authority to create new assets meaning new assets appear at breakneck speeds. The result is critical resources and assets left wholly unprotected.

Getting ahead of this through traditional procedures, however, is unwieldy. Teams would first need to collect a complete list of all key assets in their organization. They then need to collect a record of all backup job records from every backup solution in use. A full reconciliation of these two lists must follow to first identify assets missing from the backup records and then determine if they require backup protections. It's so time intensive that teams perform the task just one or two times per year, often still missing key unprotected assets.



BOCADA v1.7.05.0						
Asset Protection : CMDB Protected Assets						
Report criteria						
<input type="checkbox"/>	CMDB Client Name	Backup Product	Backup Server	CMDB Instance	Job Group	Last Activity
CMDB Instance: aws_inventory [52]						
CMDB Instance: azure_inventory [25]						
<input type="checkbox"/>	dev-sql-2014sp3	Azure Storage ...	iaasestdiag40	azure_inventory	IAAS:iaasus2:IAAS:iaasus2:6081604374...	2021-05-25 16:17:27
<input type="checkbox"/>	dev-sql-2014sp3	Azure Storage ...	iaasestdiag40	azure_inventory	IAAS:iaasus2:IAAS:iaasus2:6081604374...	2021-05-25 16:17:27
<input type="checkbox"/>	dev-sql-2014sp3	Azure Cloud Re...	az-boc-devlab	azure_inventory	iaasvmcontainerv2:iaasestdev-sql-201...	2021-05-25 05:37:45
<input type="checkbox"/>	dev-sql-2014sp3	Azure Cloud Re...	az-boc-devlab	azure_inventory	iaasvmcontainerv2:iaasestdev-sql-201...	2021-05-25 05:37:45
<input type="checkbox"/>	iaasest-2k12r2	Azure Storage ...	iaasest	azure_inventory	IAAS:iaasus2:467828353582557671:iaa...	2021-05-25 16:34:58
<input type="checkbox"/>	iaasest-2k12r2	Azure Storage ...	iaasest	azure_inventory	IAAS:iaasus2:467828353582557671:iaa...	2021-05-25 16:34:58
<input type="checkbox"/>	iaasest-2k12r2	Azure Cloud Re...	az-boc-devlab	azure_inventory	iaasvmcontainerv2:iaasest:iaasest-2k1...	2021-05-25 07:40:22
<input type="checkbox"/>	iaasest-2k12r2	Azure Cloud Re...	az-boc-devlab	azure_inventory	iaasvmcontainerv2:iaasest:iaasest-2k1...	2021-05-25 07:40:22
<input type="checkbox"/>	iaasestdiag40	Azure Cloud Re...	az-boc-devlab	azure_inventory	ContinuousRestorePoint	2021-05-25 23:33:17
<input type="checkbox"/>	share-dev-01	Azure Cloud Re...	az-boc-devlab	azure_inventory	AzureStorageJob	2021-05-25 23:00:12
<input type="checkbox"/>	share-dev-100	Azure Cloud Re...	az-boc-devlab	azure_inventory	AzureStorageJob	2021-05-25 23:00:12
<input type="checkbox"/>	taaz-sql-mi-01	Azure Cloud Re...	az-boc-devlab	azure_inventory	devtest	2021-05-25 23:33:19
<input type="checkbox"/>	taaz-sql-ws01	Azure Cloud Re...	az-boc-devlab	azure_inventory	ContinuousRestorePoint	2021-05-25 23:33:19

Image 1.
Bocada
Automated
Unprotected
Asset Report

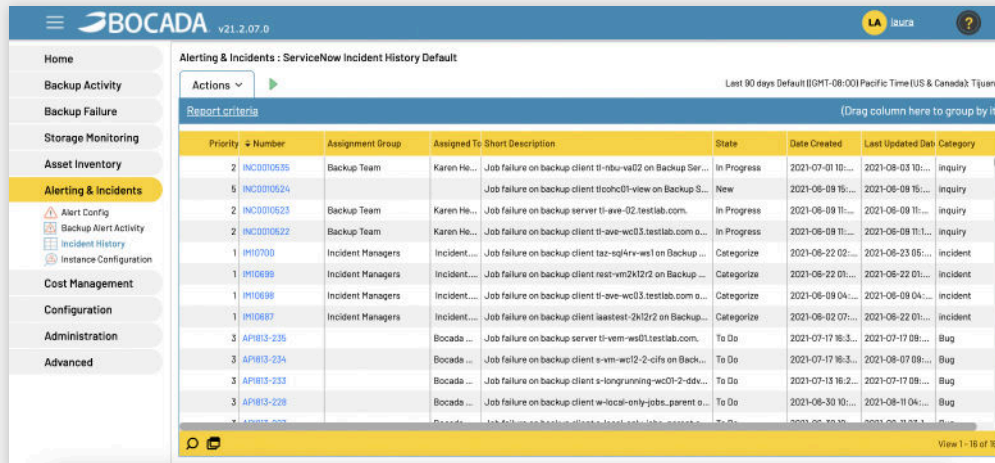
¹ Technavio. Backup-As-A-Service Market 2020-2025. Published May 2021.

Automated reconciliation and identification streamline this process and shore up unprotected assets on an almost daily basis. Backup monitoring automation tools like Bocada let enterprises take any kind of asset list—CMDB, CSV file, propriety in-house databases—and compare them to backup job logs. The end result is a punch list of assets that need protection intervention. This streamlined approach equips organizations with the backups they need should a ransomware event require data restoration.

Streamline Ticketing Operations

It's one thing to lose data during a ransomware or cyberattack because it was never protected in the first place. It's another to lose it because data protection teams could not resolve backup impediments before the attack took place. This is where automating key steps in the ticketing and backup failure resolution process come into play.

Conventional backup resolution procedures are hyper-manual and demand a great deal of time. A backup failure must first be identified. A ticket summarizing the failure and its details is then populated and submitted into a ticketing system. Personnel then monitor the ticket's status and close it when the underlying issue resolves. It's a time-tested process, but one whose manual steps make the resolution process take longer than necessary.



Priority	# Number	Assignment Group	Assigned To	Short Description	State	Date Created	Last Updated	Category
2	INC0010635	Backup Team	Karen He...	Job failure on backup client ti-nbu-va02 on Backup Ser...	In Progress	2021-07-01 10:...	2021-08-03 10:...	Inquiry
5	INC0010624			Job failure on backup client ti-toohc01-view on Backup S...	New	2021-06-09 15:...	2021-06-09 15:...	Inquiry
2	INC0010623	Backup Team	Karen He...	Job failure on backup server ti-ave-02.testlab.com.	In Progress	2021-06-09 11:...	2021-06-09 11:...	Inquiry
2	INC0010622	Backup Team	Karen He...	Job failure on backup client ti-ave-wc03.testlab.com o...	In Progress	2021-06-09 11:...	2021-06-09 11:1...	Inquiry
1	IM10700	Incident Managers	Incident...	Job failure on backup client taz-sql4rv-ws1 on Backup ...	Categorize	2021-06-22 02:...	2021-06-23 05:...	incident
1	IM10699	Incident Managers	Incident...	Job failure on backup client rest-vm2k12/2 on Backup ...	Categorize	2021-06-22 01:...	2021-06-22 01:...	incident
1	IM10698	Incident Managers	Incident...	Job failure on backup client ti-ave-wc03.testlab.com o...	Categorize	2021-06-09 04:...	2021-06-09 04:...	incident
1	IM10697	Incident Managers	Incident...	Job failure on backup client laatest-2k12/2 on Backup...	Categorize	2021-06-02 07:...	2021-06-22 01:...	incident
3	APIB13-235		Bocada ...	Job failure on backup server ti-vev-ws01.testlab.com.	To Do	2021-07-17 16:3...	2021-07-17 09:...	Bug
3	APIB13-234		Bocada ...	Job failure on backup client s-vm-wc12-2-cifs on Back...	To Do	2021-07-17 16:3...	2021-08-07 09:...	Bug
3	APIB13-233		Bocada ...	Job failure on backup client s-longrunning-wc01-2-ddv...	To Do	2021-07-13 16:2...	2021-07-17 09:...	Bug
3	APIB13-228		Bocada ...	Job failure on backup client w-local-only-jobs-parent o...	To Do	2021-06-30 10:...	2021-08-11 04:...	Bug

Image 2.
Bocada
Automated
Ticket Monitoring

Backup operations automation software like Bocada remove these manual touchpoints. Automated ticket creation based on pre-defined criteria eliminates the need to identify a failure and then create, submit, and route a ticket to the correct team member. Further, consolidated monitoring under a single pane and auto-ticket closure based on resolution criteria enables improved oversight, cleaner operations, and reduced manual intervention.

This end-to-end ticketing automation keeps organizations one step ahead of cyberattacks. Faster overall resolutions aided by automation mean data is restorable, no matter what.

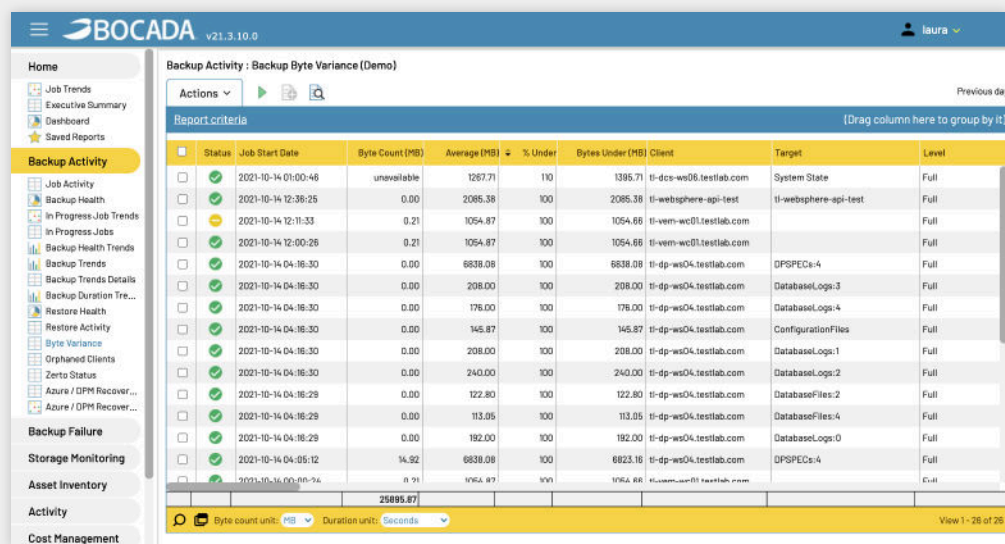
Backup Operations Automations For Proactive Cyberattack Monitoring

Backup operations frequently play the role of being the last line of defense in the event of a cyberattack. However, enacting backup monitoring automation protocols changes this dynamic. With the right protocols in place, backup professionals play a key role in safeguarding organizations against cyberattacks in the first place.

Identify Unusual Backup Patterns

The amount of data backed up over the course of several days or even weeks rarely varies that much. This is why a variance in the bytes of data backed up over a short period of time can be cause for concern and, sometimes, a signal of an in-progress cyberattack.

Ransomware impacts backup byte volume in a variety of ways. One of the most common scenarios is ransomware completely removing files. This results in a backup file suddenly having no bytes at all. A related ransomware practice is the changing of a file name or extension. Malware replicates the file and gives this new file the original file's name, all while deleting or altering the contents of the original file. Through this process, the original file's byte count changes.



Status	Job Start Date	Byte Count (MB)	Average (MB)	% Under	Bytes Under (MB)	Client	Target	Level
unavailable	2021-10-14 01:00:48	unavailable	1287.71	110	1385.71	ti-dcs-ws06.testlab.com	System State	Full
✓	2021-10-14 12:38:25	0.00	2085.38	100	2085.38	ti-webosphere-api-test	ti-webosphere-api-test	Full
⚠	2021-10-14 12:11:33	0.21	1054.87	100	1054.88	ti-venm-wc01.testlab.com		Full
✓	2021-10-14 12:00:26	0.21	1054.87	100	1054.88	ti-venm-wc01.testlab.com		Full
✓	2021-10-14 04:16:30	0.00	6838.08	100	6838.08	ti-dp-ws04.testlab.com	DPSPECs:4	Full
✓	2021-10-14 04:16:30	0.00	208.00	100	208.00	ti-dp-ws04.testlab.com	DatabaseLogs:3	Full
✓	2021-10-14 04:16:30	0.00	176.00	100	176.00	ti-dp-ws04.testlab.com	DatabaseLogs:4	Full
✓	2021-10-14 04:16:30	0.00	145.87	100	145.87	ti-dp-ws04.testlab.com	ConfigurationFiles	Full
✓	2021-10-14 04:16:30	0.00	208.00	100	208.00	ti-dp-ws04.testlab.com	DatabaseLogs:1	Full
✓	2021-10-14 04:16:30	0.00	240.00	100	240.00	ti-dp-ws04.testlab.com	DatabaseLogs:2	Full
✓	2021-10-14 04:16:29	0.00	122.80	100	122.80	ti-dp-ws04.testlab.com	DatabaseFiles:2	Full
✓	2021-10-14 04:16:29	0.00	113.05	100	113.05	ti-dp-ws04.testlab.com	DatabaseFiles:4	Full
✓	2021-10-14 04:16:29	0.00	192.00	100	192.00	ti-dp-ws04.testlab.com	DatabaseLogs:0	Full
✓	2021-10-14 04:05:12	14.92	6838.08	100	6823.18	ti-dp-ws04.testlab.com	DPSPECs:4	Full
✓	2021-10-14 00:00:00-14	0.00	1762.87	100	1762.88	ti-dp-ws04.testlab.com		Full
		25895.87						

Image 3.
Bocada Backup
Bytes Variance
Report

These are often subtle byte variances that happen file by file over the course of long periods of time. In fact, it's their very subtlety that results in attacks going undetected for so long.

Yet backup monitoring tools like Bocada detect these variances automatically. The software first assesses historical backup byte norms. It then uses these benchmarks to measure the presence of unusual variances in backup byte volume. With a list in-hand of unusual backup byte activity, data protection professionals have a simple tool to identify potential ransomware threats.

Pinpoint Unusual Storage Usage Behaviors

Changes in backup bytes point to a related signal of ransomware and cybersecurity attacks: unusual peaks or valleys in backup storage usage. One typical malware practice encrypts server files and then leaves them unavailable for access without an encryption key. Sometimes, this encryption significantly increases the original file's size and therefore the amount of storage needed to backup up those files. Meanwhile, a slightly less common malware practice involves the insertion of extremely large malware data into files to avoid detection by anti-virus programs that focus on finding small, unexpected files. Again, backup data volume, and therefore storage usage, spike unexpectedly.

While these spikes may be detected by data protection personnel, the real question is how long will it take for that detection to happen. Even a few days lag time may mean millions of dollars in lost data and operational uptime.

Instead, imagine receiving alerts the moment these unusual storage spikes occur. Bocada's automated backup storage monitoring lets data protection personnel set specific benchmarks for such alerting. Rather than relying on personnel to remember to check and then identify unusual storage spikes, these alerts offer yet another proactive tool to get ahead of cyberattacks.

CONCLUSION

In a world where cyber and ransomware attacks are only increasing in frequency and scale, enterprise IT professionals must review the extent to which their existing tools and protocols fully protect their organizations. Leveraging tools that introduce cyberattack prevention and detection throughout their infrastructure empowers all IT personnel to be proactive participants in data protection.

When assessing backup operations automation tools' ability to get ahead of cyberattacks, be sure to assess them on the following key capabilities:

- Native integration with enterprise backup and storage solutions
- Automated unprotected asset discovery
- Streamlined bytes variance detection
- Centralized ticketing creation, monitoring, and resolution
- Customizable alert triggers

Tools that incorporate these features will not only address daily backup operations monitoring and reporting needs but also offer the added benefit of being valuable cyberattack prevention tools.



About Bocada

Bocada LLC, a global IT Automation leader, delivers backup reporting and monitoring solutions that give enterprises complete visibility into their backup performance. Bocada provides insight into complex backup environments, enabling IT organizations to save time, automate ongoing reporting activities, and reduce costs. With the largest installed customer base in the Fortune 500, Bocada is the world's leading provider of backup reporting automation.

For more information, visit [**www.bocada.com**](http://www.bocada.com)