Barracuda
Your journey, secured.

Mitigating the risk of ransomware in the education sector with Barracuda Backup.

As documented by the Department of Education and the National Cyber Security Centre (NCSC) there has been an alarming increase in Cyber-Attacks involving Ransomware infections affecting the UK Education Sector, this has led to a programme of education around the subject to help advise Schools on how to get the basics right to minimise the risk and be prepared to be able to recover from a Ransomware attack.

Fundamental to this strategy is having the right Security and Data Protection plan in place that has been researched and tested, to prevent or minimise the risk of a Cyber attack taking place, and if you are unfortunate enough to have a Ransomware attack, how to deal with the situation and recover the affected systems quickly. *

** (Source) https://www.gov.uk/government/publications/school-governance-update/school-governance-update-october-2020#cyber-security-for-schools*

The plan includes:

- Have an incident plan and test it.
- Make sure your data is backed up offline and test the recovery of it.
- Regularly review your defenses and controls.
- The Department of Education has worked with the NCSC on cyber security questions for governors and trustees to help inform conversations with school leaders.

It is important to have an effective Data Protection and Recovery plan in place, simply put having confidence that you have tested the ability to restore complete physical and virtual servers and all associated Data and applications/ Databases that support the Schools IT systems. This should also include Windows Desktop and Laptop devices that can be re-imaged to ensure no trace of the Ransomware can come back to re-infect any system.

When a system becomes infected by Ransomware and data is encrypted, you need to have confidence that your chosen Backup Solution can recover the system back to a point in time - prior to any infection taking place, you should never be in a position that you have no means to recover your data, and you should never pay the Cyber-criminals a ransom to get your data unencrypted; doing this allows the Cyber Criminals to re-encrypt your data at any future point in time as they know you would be susceptible to paying a ransom and repeat this process at will.

Many Ransomware attacks also target your backup infrastructure, 85% of Ransomware attacks target Windows

Servers, and if you run a Backup product on a Windows Server it puts you at greater risk as there is code in the payload that will try to seek out your backup service account passwords in your AD, the attack will also encrypt backup config files, delete registry keys and render your backup service unusable, we have seen cases that AD servers have been interrogated to ascertain backup service account passwords, so a cyber criminal can log into your Backup Manager and delete backup sessions on disk, There have even been cases where offsite (Disaster Recovery) Backup servers holding a second copy of the backups also been targeted and backup data has been deleted.

There are steps you can take to minimise any of this happening:

- Ensure you have strong end point security to protect your servers and desktop devices against Virus and Malware attacks, this should also include security for non-windows tables such as iPads. The software should be able to detect ransomware real-time and be able to quarantine attacks before they even start.

- Strong Education for staff and students not to open email attachments or links that they do not recognise where email has come from, 90% of ransomware attacks are initiated through Phising and Spear Phising emails, enticing the recipient to click on an attachment or open a link to enter information.

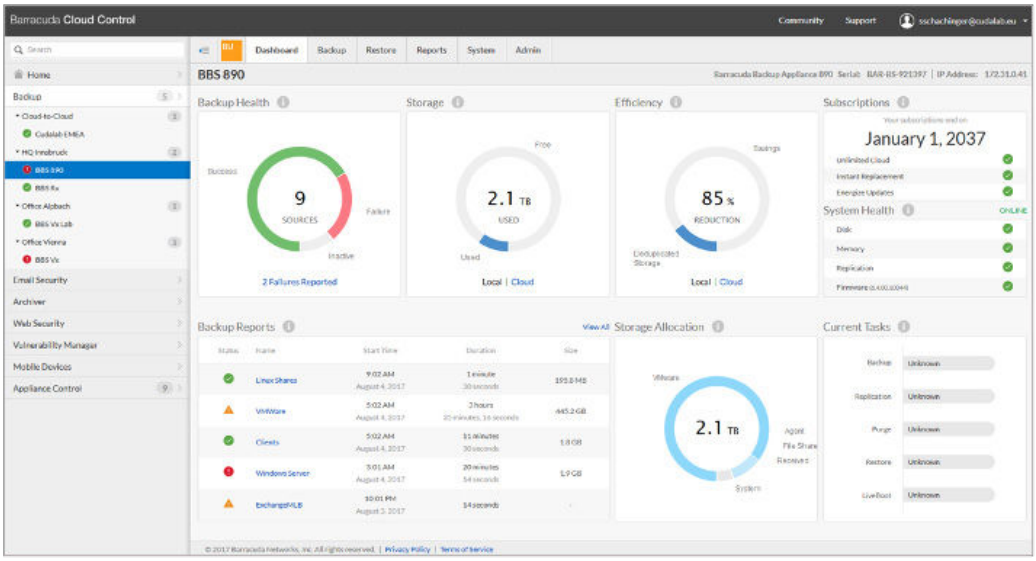
- Look at non-Windows Data Protection solutions, they are less likely to be compromised.

- Always make sure you have multiple copies of your backup data, you do not want to have all your eggs in one basket, the second copy should be held offline (such as Tape) or in a secure Cloud (completely detached from your on-premise Infrastructure). Using a Cloud copy can be easier to manage as the tasks to replicate your backups are completely automated to get your second copy off-site for full protection.

- Test, Test and Test again, having confidence that you can restore in every scenario is important so you know if something happens, you have confidence the backup can be restored easily.

Barracuda Backup overview

Protecting your data in today's complex school infrastructures—often combining on-premises, virtual, cloud-hosted, and SaaS environments—presents challenges that competing backup solutions can't adequately meet. At best, you'll spend a lot more time and money managing and maintaining multiple solutions. At worst, gaps in coverage leave your data vulnerable. Barracuda Backup Appliances run on a Hardened Linux OS and have automatic rollback configuration to fully protect against Ransomware and Cyber attacks to ensure your data is always safeguarded.



Barracuda Backup is designed from the ground up for Hybrid protection you depend on today. It gives you the flexibility to easily back up data wherever it resides at different School sites/locations, and to replicate the data offsite to the Barracuda Cloud, Amazon Web Services (AWS), or a private location of your choice. Simple to configure and manage, and totally automated, Barracuda Backup is truly a "set it and forget it" solution for total peace of mind.

Built for the cloud—Simple and scalable

The job of managing data across multiple environments is complex, but backup and disaster recovery doesn't have to be. Deployment, configuration, and ongoing management are fast and easy, thanks to a centralised cloud-based console that gives you complete, single-pane-of-glass visibility into all Barracuda solutions in the global network.

Rapid recovery of your data and systems

Barracuda Backup supports all popular Server types including VMware, Hyper-V, Windows Server, Desktop (Windows 7-10), Linux and MAC OSX Systems, it provides Complete Virtual Machine Recovery and the ability to recover selected file systems/folders and individual files, also SQL Databases and applications and Physical Windows Server Disaster Recovery.

Reliable and predictable

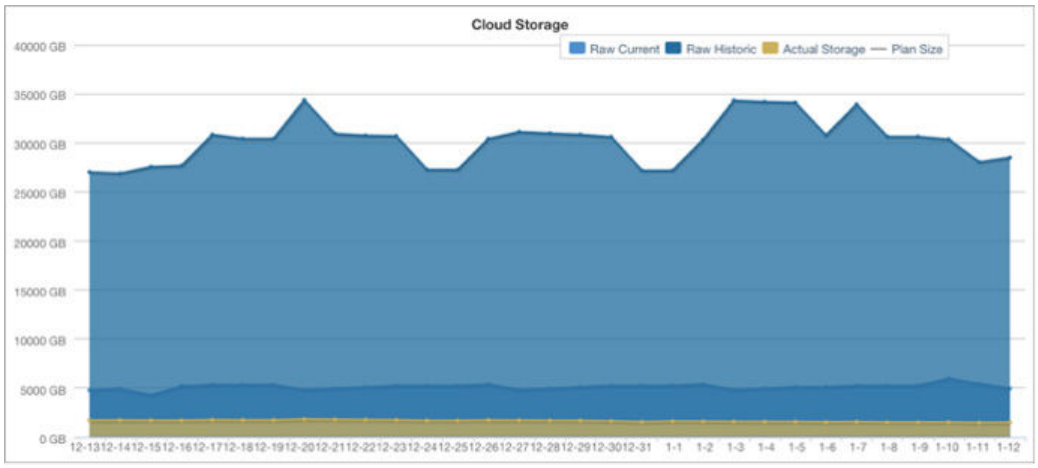
To protect your backup systems from failures, all Barracuda Backup products include Energize Updates that automatically apply software updates to improve performance and keep you protected from the latest threats. Updates are sent as frequently as needed to protect you from zero-day security threats.

Instant Replacement Service

Barracuda Instant Replacement provides next-business-day replacement in case of failure or malfunction. In the event of a complete site disaster, Barracuda will migrate Data from the Cloud onto your New Appliance to recover the data and configuration settings stored in Barracuda Cloud Storage onto a replacement unit for emergency restores. And an included complementary hardware refresh every four years will keep you on the latest platform at no additional cost.

Unlimited Barracuda Cloud Storage

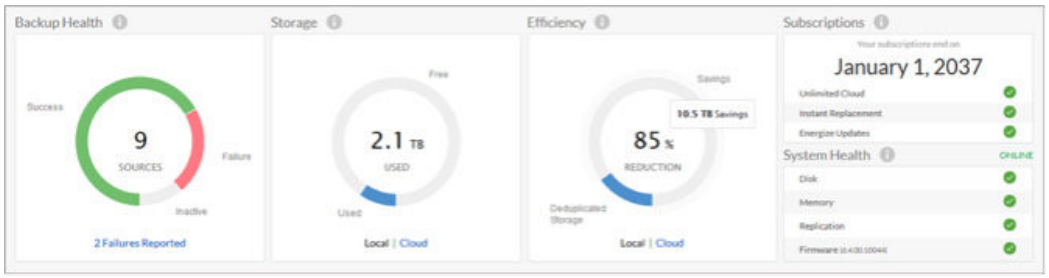
Unlimited Barracuda Cloud Storage provides storage to replicate Barracuda Backup to the cloud. Unlimited Barracuda Cloud Storage subscriptions allow replication of data on Barracuda Backup, up to the capacity of your Backup product, to our geographically distributed enterprise-grade datacentres to store your data safely. The included offsite vaulting allows extended retention by moving multiple revisions off Barracuda Backup and into Barracuda Cloud.



Key features

Inline deduplication

Barracuda inline deduplication, an inherent capability of all Barracuda Backup products, lets organisations significantly reduce storage needs, bandwidth requirements, and backup costs. By deduplicating data as it is received, Barracuda Backup minimises the time for completion of the full backup and replication process. Barracuda's advanced variable block deduplication analyses the data type and chunk size, setting a block size to obtain the greatest level of deduplication. For organisations protecting multiple sites, Barracuda's global deduplication and cloud storage technology help distributed networks stay protected while reducing the backup storage footprint.



Encrypted appliance

Barracuda's got you covered for security and data protection but protecting against exfiltration and theft of data shouldn't be overlooked. Barracuda Backup ships with encrypted disk drives which render data useless when removed from the appliance. When coupled with a power-on password for the appliance, this prevents sensitive and critical data from falling into the wrong hands if disk drives or appliances are lost or stolen. Barracuda Backup appliances uses Software Encryption to Encrypt all Data Volumes on the Appliance and a TPM Chip to hold all randomly generated encryption Keys, avoiding the significant performance and efficiency degradation that software-based encryption solutions suffer.

Centralised management

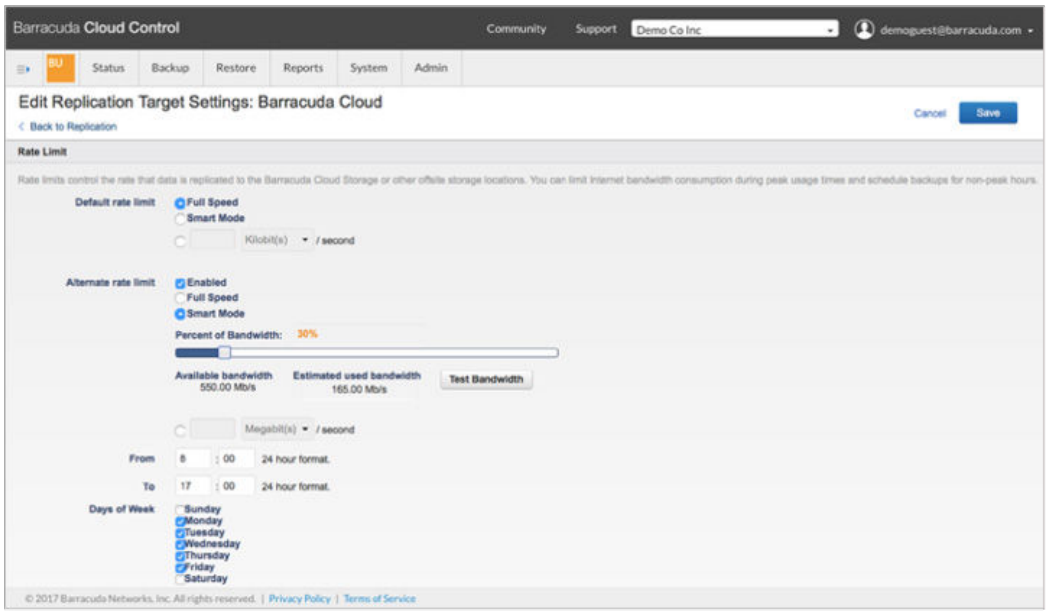
Barracuda's robust central management allows organisations to manage multiple sites from a clean and simple-to-use interface. Administrators can define roles in their organisation for access to each location.

Data recovery

Barracuda offers a wide range of restore options: Organisations with physical servers are able to perform bare metal restores in case of catastrophic failure, while virtual environments benefit from fast image-based restores. For customers with Instant Replacement: In the event of a complete site disaster, Barracuda will preload the most recent data and configuration settings stored in Barracuda Cloud Storage onto the replacement unit for emergency restores.

Replication

Barracuda Backup lets you protect against local disasters and data loss by using the cloud to simply and cost-effectively get data off-site. It lets you securely and efficiently replicate data to the Barracuda Cloud, a remote physical backup appliance, a remote virtual backup appliance, or Amazon Web Services (AWS) for off-site protection. 256-bit AES encryption of all data in transit and at rest ensures security.



Offsite vaulting

Organisations with conservative retention policies can use Offsite Vaulting to minimise the cost of backup storage. With Offsite Vaulting, organisations can move local copies of their monthly and yearly backups off their local appliance to the Barracuda Cloud or another Barracuda appliance.

Flexible deployments

Barracuda Backup is available as both an all-in-one physical appliance or as software that can be deployed in virtual environments to leverage existing compute and storage infrastructures.

FEATURES	
Deployment Options	Physical Appliance, Virtual Appliance
Offsite Replication	Remote Physical Appliance, Remote Virtual Appliance, Barracuda Cloud Storage, Amazon Web Services (AWS)
Management Interface	Barracuda Cloud Control Centralised Administration
Backup Agents	Microsoft Windows (Windows Server, Hyper-V, Exchange, SQL) Linux, macOS
Network Backups	Network Attached Storage (NAS)
Host-Level Virtual Environments	VMware vSphere, Microsoft Hyper-V
Guest-Level Virtual Environments	Citrix XenServer, Kernel-Based Virtual Machine (KVM), Oracle VM, Red Hat Virtualisation
Deduplication	Global, Inline, Block-Level, Source- and Target-Based
Rapid Recovery	LiveBoot, Cloud LiveBoot, Physical-to-Virtual (P2V), LiveBrowse
Long-Term Retention	Offsite Vaulting to Barracuda Cloud, Export to Amazon Web Services (AWS), External Disk, Tape, Autoloader, Robotic Library

Barracuda Backup appliance technical specifications

MODELS COMPARISON	190	295	290	390	490	690
CAPACITY						
Usable Storage	1 TB	2 TB	2 TB	4 TB	6 TB	12 TB
Recommended Environment	500 GB	1 TB	1 TB	2 TB	3 TB	6 TB
SPECIFICATIONS						
Form Factor	Desktop	Desktop	1U Micro	1U Mini	1U	1U
Dimensions (inches: W x H x D)	10.0 x 2.0 x 8.3	10.0 x 2.0 x 8.3	16.8 x 1.7 x 10.2	16.8 x 1.7 x 14.0	16.8 x 1.7 x 19.8	17.2 x 1.7 x 27.0
Weight (lbs)	6	6	9	12	26	26
Network Interface	1Gb RJ45	1Gb RJ45	1Gb RJ45	1Gb RJ45	1Gb RJ45	2 x 10Gb RJ45
Optional 10Gb Fibre	-	-	-	-	-	-
Disk Arrangement	1 x 1 TB	1 x 2 TB	1 x 2 TB	2 x 4 TB	4 x 4 TB	4 x 6 TB
Redundant Disk Array (Primary Array)	-	-	-	SW RAID 1	SW RAID 10	HW RAID 10
Dedicated Database and OS Disks	-	-	-	-	-	-
Redundant Disk Array (Database/OS Array)	-	-	-	-	-	-
Swappable Disks	-	-	-	-	Hot Swappable	Hot Swappable
Redundant Power Supplies	-	-	-	-	-	-
AC Input Current (Amps @ 120V)	0.25	0.25	0.30	0.40	0.65	1.3
Site-to-Site Replication	Sender	Sender	Sender	Sender	Sender/Receiver	Sender/Receiver

MODELS COMPARISON	790	890	895	990	995	1090
CAPACITY						
Usable Storage	18 TB	24 TB	36 TB	48 TB	80 TB	112 TB
Recommended Environment	9 TB	12 TB	18 TB	24 TB	40 TB	56 TB
SPECIFICATIONS						
Form Factor	2U	2U	3U	3U	3U	4U
Dimensions (inches: W x H x D)	17.4 x 3.5 x 25.8	17.4 x 3.5 x 25.8	17.4 x 5.3 x 23.8	17.4 x 5.3 x 23.8	17.4 x 7.0 x 27.9	17.4 x 7.0 x 27.9
Weight (lbs)	45	52	70	76	114	121
Network Interface	2 x 10Gb RJ45	2 x 10Gb RJ45	2 x 10Gb RJ45	2 x 10Gb RJ45	2 x 10Gb RJ45	2 x 10Gb RJ45
Optional 10Gb Fibre	2-port SFP+	2-port SFP+	2-port SFP+	2-port SFP+	2-port SFP+	2-port SFP+
Disk Arrangement	6 x 6 TB	8 x 6 TB	10 x 6 TB	16 x 4 TB	14 x 8 TB	32 x 4 TB
Redundant Disk Array (Primary Array)	HW RAID 10	HW RAID 10	HW RAID 60	HW RAID 60	HW RAID 60	HW RAID 60
Dedicated Database and OS Disks	-	-	-	-	2 x 2 TB	4 x 2 TB
Redundant Disk Array (Database/OS Array)	-	-	-	-	HW RAID 1	HW RAID 10
Swappable Disks	Hot Swappable	Hot Swappable	Hot Swappable	Hot Swappable	Hot Swappable	Hot Swappable
Redundant Power Supplies	Hot Swappable	Hot Swappable	Hot Swappable	Hot Swappable	Hot Swappable	Hot Swappable
AC Input Current (Amps @ 120V)	1.7	2.5	2.6	6.9	7.8	8.4
Site-to-Site Replication	Sender/ Receiver	Sender/ Receiver	Sender/ Receiver	Sender/Receiver	Sender/Receiver	Sender/Receiver

24/7 technical support and management of your data in our cloud

Barracuda provides Global Technical Support with UK first line support available as standard, we have different support centres around the world with follow the Sun support depending on what time of day help is required. We also assist you with Data Migration from the Cloud in the unlikely event your local Backup Appliance has a hardware failure or there has been an environmental issue such as loss of Air conditioning/Fire to ensure your critical data can be recovered quickly.

Barracuda
Your journey, secured.