SOLUTION BRIEF

COMMVAULT

New Cyberthreats Require New Thinking: Reimagined Data Protection for Education Providers

THE EVOLUTION OF CYBERTHREATS

Cyberthreats are continuously evolving. What was once a lone wolf practice has transformed into a new form of organized digital crime, deliberately designed to exploit businesses, agencies, and institutes of every size. From sophisticated nation-state attacks to ready-made ransomware-as-a-service toolkits, today's threats have changed, leveraging myriad techniques and skillsets that silently bypass perimeter defenses and traditional security tools — and compromise even the most technically advanced organizations.

One thing that hasn't changed, however, is the pursuit of your data.

Data remains the crown jewel of your institution. It fuels operations, informs decisions, and contains the most sensitive faculty and student information. It's also the chief target of cyberattacks. In fact, 80% of lower education providers and 79% of higher education providers report being hit by ransomware in 2023 — as education programs remain one of the top industries of attack.

To effectively defend data against these new and advanced threat vectors, data protection must be reimagined with proactive capabilities that secure data, anticipate risks, and deliver trusted recoverability in the face of any threat.

NEW DATA MOTIVES AND FLAWED THINKING

While *conventional* ransomware encrypts data and holds it hostage for a lofty payout, today's threats anchor on the double and triple extortion of your data. Want proof?

83% 83% of cyberattacks involve some form of data leakage, exfiltration, theft, or damage.[1]

In other words, the primary aim of most attacks is not simply to deny access to your data, but to use it in malicious and harmful ways.

While traditional data protection solutions can play a pivotal role in recovering post-attack, they are often reactionary, narrowly focused, and insufficient to keep pace with evolving threats and motives. As cyber risks evolve, data estates grow, and IT resources shrink, today's institutions and organizations need a more proactive way of identifying risks and defending data sooner. One that doesn't sit idle in the background, bracing for impact, but delivers progressive data protection capabilities that meet threats head-on, insulate student and faculty data and its exposure, and picks up where conventional security tools leave off.

A NEW ERA OF DATA PROTECTION

Data protection has long been described as a last line of defense, only coming into play after damage occurs. Commvault shifts this paradigm by uniquely delivering proactive and innovative protection and security capabilities proven to minimize damage, reduce risk, and eliminate downtime — uniformly across your institute's data estate (on-prem, in the cloud, and across SaaS environments). Commvault's multilayered data protection intelligently secures data to rapidly uncover risk, minimize cyberthreats, continuously control data and its access, and drive more informed recovery outcomes, wherever data lives.

Source 1: https://www.computerweekly.com/news/252513735/Backups-no-longer-effective-for-stopping-ransomware-attacks

NEXT-GENERATION DATA PROTECTION FROM COMMVAULT

Only Commvault provides layered protection that actively defends data and its recoverability across the industry's broadest workloads.

Secure

Hardened, zero-trust architecture with built-in immutability and security protocols to secure data, prevent unwanted access, and drive compliance in the face of evolving cyberthreats.

Defend

Patented early warning and in-depth monitoring to surface and neutralize zero-day and insider threats before they cause harm, containing breaches, limiting exposure windows, and flagging malicious activity sooner to reduce recoveries.

Recover

Proactive and reliable recoverability across on-prem, cloud, and SaaS apps that's proven to reduce downtime, thwart data loss, and accelerate response times for unrivaled business continuity.

COMMVAULT BENEFITS

- **Business continuity:** Ensure trusted recoverability and compliance. Eliminate downtime, maintain operations, and exceed SLAs broadly across data estates.
- **End-to-end observability:** Gain unrivaled visibility and telemetry. Leverage end-to-end insights to eliminate blind spots, monitor activities, and anticipate risk before, during, and after an attack.
- **Damage prevention:** Reduce and prevent data damage. Surface zero-day threats in production environments, divert direct attacks on backup infrastructure, and prevent infection of backups.
- **Data integrity:** Employ in-depth detection and forensics. Spot anomalous behavior and latent threats, prevent sensitive data from exposure and exfiltration, and isolate data for clean recoverability.
- **Intelligent outcomes:** Use advanced automation and AI to automate workflows and classify data and its sensitivity, monitor file activities, and roll back to pre-infectious states while reducing cognitive load.
- **Cost savings:** Safeguard data with speed, precision, and confidence. Avoid financial loss, minimize interruptions, and adhere to stringent compliance and industry regulations.

To learn more, visit **commvault.com >**