SHARDSECURE

Solution Brief

Neutralize Ransomware in Higher Education

Ransomware is on the rise across organizations, industries, and nations. In 2022 alone, there has been a 24% global increase in ransomware, with one in 53 organizations now affected.[1]

Attacks are also increasing in a surprising place: universities. A 2022 Sophos survey[2] of more than 700 schools revealed that 64% of higher ed institutions were hit by ransomware in the last year. Additionally, attackers' encryption success has been significantly higher than average in universities, with 74% of attacks successful in higher ed compared to the global rate of 65%.

These attacks have had a considerable impact. Colleges and universities, some with tens of thousands of students, have had to cancel classes, replace devices, and pay steep ransoms and recovery costs. The Sophos report notes that 98% of colleges universities hit by ransomware were able to get *some* of their encrypted data back — but only 2% got all of their data back. One college in the American Midwest was even forced to close permanently due to enrollment shortfalls and fundraising problems that resulted from the loss of their data.[3]

ShardSecure's Microshard technology™ neutralizes the impact of ransomware for colleges and universities. Our solution makes use of data desensitization, self-healing data, automatic data migration, and other features to ensure that cyberattackers don't interfere with so much as a single seminar.

Reconstruct data that's been compromised by ransomware

We perform multiple data integrity checks during our microsharding and reassembly processes. If any storage location fails the check, our self-healing data feature will reconstruct the affected data, automatically and transparently returning it to its original state. This applies to ransomware attacks and to any other attack that tampers with, deletes, or otherwise interferes with your data integrity. Unauthorized deletions, as in the case of attackers who destroy data that they are unable to encrypt or steal, are simply reversed — even if an entire storage location is unavailable.

Our solution can also be configured to share alerts with your institution's security team or IT department to initiate your incident response and investigation procedures.

97% of higher education respondents hit by ransomware said the attack impacted their ability to operate.

Higher education respondents paid an average of $1.42 million to remediate ransomware attacks, more than the global average.

9% of higher ed respondents reported a recovery period of 3-6 months for their institution (more than double the global average of 4%), and 40% took over a month to recover (double the global average of 20%).[2]

[1] A third of companies hit with ransomware didn't have to pay… Here's how they did it. (2022, June 9). CyberTalk. Retrieved October 14, 2022, from https://www.cybertalk.org/2022/05/18/a-third-of-companies-hit-with-ransomware-didnt-have-to-pay-heres-how-they-did-it/

[2] The State of Ransomware in Education 2022. (2022, July). Sophos. Retrieved October 14, 2022, from https://assets.sophos.com/X24WTUEQ/at/pgvqxjrfq4kf7njrncc7b9jp/sophos-state-of-ransomware-education-2022-wp.pdf

[3] Ransomware attack shutters 157-year-old Lincoln College. (2022, May 10). CBS News. Retrieved October 14, 2022, from https://www.cbsnews.com/news/lincoln-college-closes-ransomware-hackers-illinois/

Protect against double extortion ransomware

Most colleges and universities store significant amounts of confidential data. Grades, disciplinary records, medical files, and financial information like tuition and payroll details are just some of the types of sensitive material that institutions must protect.

With ShardSecure, confidential material that is exfiltrated in a ransomware attack becomes unusable to attackers who seek to extort your college or university. Even if a storage location is compromised, attackers will have access to only an unintelligible fraction of the complete data set. We also remove metadata and other identifying information so that attackers have no way to reassemble your confidential material.

Integrated defense-in-depth

While attackers who access encrypted data can eventually decrypt that data with enough time and compute power, they cannot do the same with microsharded data. Microshard technology does not rely on any concept of a key, so there is nothing to unscramble or decrypt.

For colleges and universities that already use encryption, ShardSecure can add an extra layer of data protection. Specifically, encrypted data can be microsharded and distributed to multiple customer-owned storage locations. Even if a storage location is breached, attackers will only have access to an unintelligible fraction of the institution's encrypted data, foiling any decryption attempts.

Learn More

Visit us at https://shardsecure.com for more information and to schedule a demo.

@ShardSecure
@ShardSecure
@ShardSecure

101 Avenue of the Americas
9th Floor, New York, NY 10013
United States of America

info@shardsecure.com

SHARD SECURE