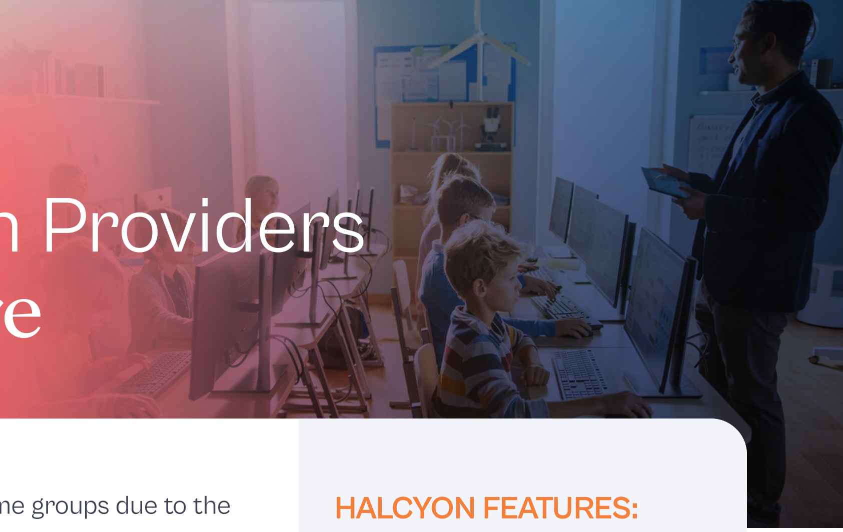
halcyon

Protecting Education Providers Against Ransomware



K – 12 schools and colleges are a lucrative target for cybercrime groups due to the large attack surface, relaxed BYOD policies, and lack of investment in cybersecurity resources. Educational institutions collect and store a treasure trove of personally identifiable (PII) information, have financial information for tuition, and can serve as a jumping-off point for other sophisticated cyberattacks. They additionally have high visibility when things go wrong as parents, elected officials, and news media can put immense pressure on the school's administration when things go wrong.

Unfortunately, most education institutions have very limited budgets for modernizing IT departments and even less to invest in cybersecurity innovation and qualified staffing. This combination has proven to be a breed ground for ransomware attacks. In 2021 the downtime for US schools due to ransomware incidents is estimated to have cost **$3.56B and impacted close to 1,000,000 students (about the population of Delaware)**.

The July 2022 ransomware attack against the Los Angeles Unified School District (LAUSD) highlights the fact that existing security tools are unable to effectively detect and prevent ransomware showing that a new approach to building resilient infrastructure is needed.

The Challenges

Ransomware poses several challenges to any education provider:

People & Process – Most ransomware events start with a human entry point. Whether it's social engineering, phishing, accidental misconfiguration, or a rogue insider – people and processes are what cybercriminals use to gain access to a system. Legacy technical debt, underfunded programs, and non-investment in skilled resources leave openings throughout the IT stack for attackers to leverage.

Motivations – Ransomware groups are organized, competent, and motivated by profit. They quickly adapt to changing conditions and only must be right once – defenders need to be right every time.

Downtime – From when it is first detected to when recovery is complete, an organization needs 7 – 21 days to restore normal operating conditions from a ransomware attack. That is weeks of degraded services to students and families, possibly impacting the entire school year.

HALCYON FEATURES:

- Four layers of ransomware prevention and protection:
  - Pre-Execution
  - Exploitation
  - Behavioral
  - Resiliency
- Exceptionally low system resource consumption
- Supports Windows 10 & 11, Windows Server: 2012 R2, 2016, 2019, 2022
- Simple deployment with no reboots required

THE HALCYON STORY

Based in Austin, TX, Halcyon was founded in 2021 by a team of cyber industry veterans after battling the scourge of ransomware and advanced threats for over a decade at some of the most innovative and disruptive security vendors of our day, including leaders from Cylance (now Blackberry), Accuvant (now Optiv), and ISS X-Force (now IBM). Halcyon is focused on building products and solutions for mid-market and enterprise customers that give organizations the edge against ransomware and other advanced threats.

Ransomware Stats in Education

In 2021, ransomware attacks cost U.S. Schools $3.65B in downtime and recovery

In 2020, 1,681 schools, colleges and universities were ransomed

Cyber insurance premiums have spiked in 2021 (as high as 334%)

157-year-old Lincoln College closed its doors due to a ransomware attack in 2021

Building Resilience

The new model of building resilient organizations requires:

- **Defense Resilience –** Existing EPP, EDR, and XDR is not built to stop ransomware. Halcyon's AI is trained on millions of real-world ransomware incidents to plug detection and prevention gaps left by traditional security tools.
  - **Bypass and Evasion Prevention –** Modern attackers target popular security tools and leverage bypass techniques to disable and render them useless. Halcyon's unique architecture allows our platform to augment and armor all other security tools running on an endpoint and prevent them from being unhooked.
- **Operational Resilience –** Every minute a system is down from a ransomware attack it costs hard dollars. Halcyon has two key features that reduce the recovery time from ransomware from weeks down to minutes.
  - **Full Encryption Key Capture –** Our intelligent agent captures the encryption event, shuttles the keys into a secure enclave and, after the malicious process is blocked, automatically decrypts any impacted files on the endpoint. This eliminates the need to pay a ransom.
  - **Data Exfiltration (Q3 2023) –** Ransomware operators hide their data exfiltration extremely well and handily fool common data loss products. Halcyon's data exfiltration module extends the core capabilities to shut down attackers attempting to remove data to hold for ransom on a leak site.

Ransomware is one of the biggest threats facing organizations today. Modern endpoint protection products are losing the battle against ransomware as evidenced by the daily headlines announcing yet another breach. Halcyon is designed to work alongside existing endpoint security products and can be deployed into environments that have previously been compromised to prevent ransomware from executing.

For more information on how Halcyon efficiently and effectively defeats ransomware attacks, contact our Sales Team at sales@halcyon.ai or visit halcyon.ai to request a free ransomware readiness report today.