Case Study

todyl | WHITEBOARD IT SOLUTIONS

_How Whiteboard IT Stopped a Ransomware Attack for D'Youville University

Small colleges hold sensitive data but rarely have the staff, budget, or institutional history to build security programs that data requires. Networks grow organically over decades. Vendors get added. Contracts renew without anyone asking whether it all adds up to real protection.

When Joseph Gunnells became CIO at D'Youville University in Buffalo, New York in 2019, he knew exactly what he was looking at. He'd spent his prior role beginning to build a security program from scratch and understood the difference between a technology stack that had been designed and one that had simply accumulated. His first call was to Steve Murphy, CEO of Whiteboard IT Solutions, a local MSP he'd known for years and whose approach to security he respected.

The Ransomware Hit While the Program Was Being Built

Whiteboard's initial review confirmed what Joe suspected. Multiple vendors, multiple products, none fully implemented, and no internal personnel dedicated to security. As existing contracts approached expiration, Whiteboard proposed a structured Todyl rollout timed deliberately to each contract sunset, closing security gaps without paying twice. They started a proof of concept, beginning with Security Information and Event Management (SIEM) and Managed Extended Detection and Response (MXDR).

Fifteen days in, Steve's phone rang at 4 AM. Todyl's MXDR team had detected a compromise in progress. The POC wasn't complete. But Todyl was installed on the exact server that was the path of the compromise, and the platform caught the entire attack chain in real time.

Whiteboard called D'Youville's network administrator directly. Without all the needed tools in place to easily isolate the affected systems, a manual process was quickly implemented to sever the threat actor's connectivity.

Complete Visibility and Coordination Limited the Blast Radius

While the network was being isolated, Joe was managing everything above the technical layer. Faculty had received ransom notifications. The story was spreading on social media before anyone could get ahead of it. Parents were calling. Faculty contract negotiations were ongoing.

Whiteboard quarterbacked the entire response, coordinating with the cyber liability insurance carrier, the incident response team, and the forensics firm, while keeping Joe on track with obligations he hadn't navigated before: engaging a privacy lawyer, filing the FBI incident report, and structuring communications to the university's president's office.

Todyl's MXDR team communicated directly with the threat actors on D'Youville's behalf, gathering intelligence on what had been taken. The answer came back through forensics.

"It was the first time that we had, with [Todyl], logs that showed the entire attack," Steve says. "When we started working with the forensics team, they were blown away."

Zero confirmed exfiltration.

Complete attack chain visibility gave the forensics team what they said they almost never have.

Predictable costs.

D'Youville replaced multiple, partially implemented vendor contracts with a unified Todyl platform at a fraction of prior spend.

90% operational continuity.

When a fiber outage hit campus, Todyl SASE kept the institution running.

What the Incident Built

The ransomware event didn't just validate the platform. It changed the nature of the partnership. Whiteboard expanded from a security engagement into D'Youville's full strategic IT partner. Bi-weekly meetings now cover network architecture, Microsoft 365, hardware procurement, software licensing, telephony, budgeting, project scheduling, and GRC development. When D'Youville sees something in their Todyl environment, all three parties work on it together.

The Secure Access Service Edge (SASE) decision came directly from the incident. The original attack vector ran through D'Youville's remote access infrastructure, inadequate from a security standpoint and cumbersome for pandemic-era remote staff. SASE replaced the VPN entirely. "It's always on, it's always working," Steve says. "We don't have any of the issues we used to have."

When a fiber outage hit campus, Todyl SASE kept D'Youville running at approximately 90% capacity. A security platform had become resilience infrastructure.

Financially, replacing disparate, partially implemented vendor contracts with a single predictable platform has been material. In a higher ed environment where budgets are under constant pressure, predictability carries its own value.

Joe put it simply:

"They make me and my department look good. That's a great feeling, because you don't get partners like that anymore."

Ready to build a security practice like Whiteboard's?

Visit www.todyl.com/contact to talk with our team.

todyl _protect what you build