Mindcore Technologies: Canvas Ransomware Attack Exposes Preventable Security Gaps

Mindcore Technologies urges Texas businesses to review vendor security and access controls after the Canvas ransomware attack disrupted Baylor.

BOCA RATON, FL, UNITED STATES, May 15, 2026 /EINPresswire.com/ -- Mindcore Technologies, a national managed IT and cybersecurity services provider, today issued commentary on the ransomware incident targeting the Canvas learning platform, which disrupted thousands of colleges and universities across the United States in early May 2026, including Baylor University in Waco, Texas. The ransomware group ShinyHunters claimed responsibility for the attack, which the group used as leverage by allegedly threatening to release personal data unless ransoms were paid.

> “Almost every single breach that we deal with, somebody either clicked on an email that had a link in it. As soon as you do that, you're giving people a key to the front door.”
>
> *Matt Rosenthal, CEO of Mindcore Technologies*

Matt Rosenthal, CEO of Mindcore Technologies, said the scale of the incident reflects baseline cybersecurity failures rather than a sophisticated novel attack. According to industry estimates cited in news coverage of the incident, the Canvas platform serves approximately 9,000 schools and as many as 275 million students, teachers, and staff worldwide.

"Almost every single breach that we deal with, and we deal with them every single day, somebody either clicked on an email that had a link in it, or they actually clicked on it, opened it and entered some information," Rosenthal said. "As soon as you do that, you're giving people a key to the front door."

Rosenthal stated that the dominant attack vector behind incidents of this scale remains credential theft through phishing, and that multi-factor authentication, when properly enforced across every access point, sharply reduces the value of stolen credentials.

"You've got to turn that on for every single account," Rosenthal said. "It should be your email, the banks, the credit cards. If you don't have that turned on, you're literally asking for a problem."

Mindcore Technologies stated that the Canvas incident should be treated by Texas businesses as a prompt to review three layers of cybersecurity posture: platform vendor selection, organizational access controls, and individual credential hygiene.

At the platform layer, Mindcore noted that any vendor holding data at scale carries an obligation to deploy phishing-resistant authentication on administrative accounts, continuous monitoring of authentication patterns, network segmentation that prevents lateral movement, and encryption that limits the commercial value of exfiltrated data. Rosenthal said these are operational baseline requirements rather than advanced controls.

At the organizational layer, Mindcore advised businesses across Texas, including Waco, Dallas, Houston, Austin, San Antonio, and Fort Worth, to apply data minimization, identity federation, and segmentation between vendor environments and core operational systems. Mindcore stated that these mechanisms determine whether a third-party platform breach becomes a contained event or a multi-week operational disruption.

At the individual layer, Rosenthal recommended unique passwords for each account, multi-factor authentication on every account that matters, and skepticism toward unexpected emails and links. He noted that individual behavior should be treated as the last layer of defense, not the first, and that organizations relying on perfect end-user decisions will fail.

Mindcore Technologies stated that businesses across Texas operating on third-party platforms for customer records, case files, financial data, or operational control systems face the same exposure pattern demonstrated by the Canvas incident. Industries cited by Mindcore as having heightened exposure include healthcare, legal services, financial services, and manufacturing.

The company stated that vendor procurement practices in many organizations continue to over-weight features and price while under-weighting security posture, breach history, and incident response transparency.

About Mindcore Technologies
Mindcore Technologies is a national Technology Service Provider headquartered in Boca Raton, Florida, with service coverage across Texas including Waco, Dallas, Houston, Austin, San Antonio, and Fort Worth. Mindcore provides managed IT services, cybersecurity, cloud infrastructure, compliance IT, and NetSuite services to businesses operating in regulated industries. More information is available at https://mind-core.com.

Matt Rosenthal
Mindcore
+1 561-404-8411
email us here
Visit us on social media:
LinkedIn

YouTube