“We’re able to do things other MSPs can’t because we have Todyl.”

Justin Smith
President, Midshore Technology Services

Stopping BEC and building client trust with a security-first mindset

When a dual-entity construction company needed to consolidate its IT program, it consulted Midshore Technology Services for help. At first, the company was wary of the value of managed services. After learning what managed IT could offer from Midshore President Justin Smith, however, the company signed on as a client. That’s when things got interesting.

How Midshore stopped ongoing business email compromise with MDXR

Midshore rolled out Todyl to protect the company’s systems and collect data. Previously, Midshore had only used Todyl’s SASE and SIEM modules but decided to roll out MXDR as well to onboard the new client.

The Todyl MXDR team and SIEM almost instantly flagged exploited remote access software on the client’s endpoints as a potential threat. Smith and his team quickly uninstalled and patched the software. Three days later, however, the client contacted Smith regarding a rise in phishing attempts on employees.

Smith dug in immediately, noting that the emails had no sender address and likely originated from within the company. Smith ingested the company’s Microsoft 365 (M365) data into Todyl. In less than 20 minutes, MXDR detected and fully investigated anomalous access to M365 from multiple geographically dispersed IP addresses, alerting Midshore over Teams. Cross-referencing backend data, Smith confirmed that two M365 accounts were compromised, acting swiftly to deactivate them.

Since then, the client has not experienced any further BEC thanks to Smith’s quick work and collaboration with Todyl MXDR. MXDR detected the signs of compromise with just three days of user behavior data and still alerted on them faster than several other existing security solutions within Midshore’s tech stack.

<20 mins
time it took to uncover M365 indicators of compromise

3 days
data needed to act accordingly

Zero
BEC after Midshore and MXDR saved the day

Security first: Midshore’s competitive differentiator

This security-first mindset not only protected Midshore’s client from further compromise: it’s helping Midshore expand as well. Beginning his career as a security practitioner, Smith founded Midshore to provide security first in a world where other MSPs still focus on break-fix IT services.

MIDSHORE
TECHNOLOGY SERVICES

todyl

“We’ve outcompeted the smaller MSPs in our area, so our competitors now are 2-3x our size,” Smith says. “We’ve found that our security bench, in terms of tools and staff, has put us leaps and bounds ahead of the competition. And a big part of that tool belt is Todyl.

“With Todyl, we’ve consolidated multiple networking and other tools into one platform. It works well, we get a lot of data and a lot of visibility. We’re able to control the network in ways that other MSPs can’t. We’re able to do things other MSPs can’t because we have Todyl... Todyl is my favorite partnership right now.”

How Midshore saved their clients from BEC and insider phishing

Midshore onboards client and rolls out Todyl MXDR

Although originally skeptical of MSPs, the dual-entity construction client asked Midshore to be their IT partner. Smith and his team implemented Todyl across their IT environment including the 24x7 coverage of Todyl MXDR.

MXDR flags compromised software usage

Right away, MXDR and SIEM identified abused vulnerable remote access software on the company’s devices. Smith and the Midshore team acted quickly to remove the software and patch it to the latest version.

Client reaches out about ongoing phishing

After some time, the client contact complained about ongoing phishing attempts on their employees. With a security-first mindset, Smith began investigating immediately.

Midshore ingests M365 data into Todyl

Smith noticed that the emails were coming from within the organization. To get a better understanding, he began collecting the company’s M365 data to get a better understanding.

Midshore collaborates with MXDR to identify and stop BEC

Correlating MXDR’s findings on the M365 data with his own investigations, Smith confirmed two compromised M365 accounts within the company were responsible for the phishing. The Midshore team deactivated the accounts and prevented further compromise.

About Midshore Technology Services

Maryland-based Midshore Technology Services provides professional IT support and technology services for your business, performing proactive maintenance, monitoring, and backups. Built with security in mind from day one, they help companies of all sizes stay safe from cyberattacks.