Case Study

ThreatDown™
Powered by Malwarebytes

ThreatDown on a Mission to Protect the Next Leaders of the Church

Founded in 1957, and located in Kansas City, Missouri, the "heart of America", Midwestern Baptist Theological Seminary and Spurgeon College is on a mission to equip students to be the next leaders of the church.

The tech-savvy seminary consists of an undergraduate college, a graduate school, and a school of doctoral programs, and offers residential, hybrid and online courses.

Its small IT team is responsible for keeping the lights blinking on 209 workstations (including 28 Macs), and 24 servers. With no Security Operations Centre (SOC) and limited time to devote to security, the team is highly selective about the software it uses, requiring tools that are "autonomous" and "informative.”

When Director of Information Technology, Steve Stone, was challenged by seminary leadership to overhaul IT and security with the question "what's the best way to do this?", he turned to ThreatDown Vulnerability Assessment, Patch Management and Managed Detection & Response (MDR) solutions.

> “Whenever there was an infected computer, it might have a competitor's product on there, but if it wasn't working, I'd throw Malwarebytes free scanner on there and do a quick clean. The scanner has been tried and true with my peers and with myself in removing stuff that other things don't remove.”
>
> **Steve Stone, Director of Information Technology**
> **Midwestern Baptist Theological Seminary and Spurgeon College**

Partner-at-a-glance

Customer - Midwestern Baptist Theological Seminary and Spurgeon College

Industry - Education

Country - United States

Displaced Solution - Kaspersky

ThreatDown Solutions

ThreatDown Vulnerability Assessment
ThreatDown Patch Management
ThreatDown MDR
(Managed Detection & Response)

Pain Points

- No Security Operations Centre (SOC)
- Limited time to devote to security
- Small IT team is highly selective about the software it uses

An Unusual Procurement

The seminary's switch to ThreatDown was swift, but unusual. Stone describes the previous endpoint security solution as “just a mess.” The centralized management console was unable to find the endpoints it was supposed to be managing, and scans would regularly take several hours, leading to complaints from users that computers were inoperable. Prior to Stone's arrival, the organization had even suffered a ransomware attack that ran through its entire server stack.

The final straw came for the incumbent security vendor in March 2022, after it was put on the FCC's national security list, following Russia's invasion of Ukraine. Unwilling to persevere with a product branded an "unacceptable risk" to the United States' national security, the seminary wrote off the remainder of its multi-year license and began an urgent acquisition process for a successor.

For Stone, the decision was an easy one. “I already had a quote in my back pocket,” he told us. Like many people who work in IT, he had come to trust the Malwarebytes scanning technology that powers ThreatDown. “I’ve been using the free Malwarebytes scanner for years, I’m an IT guy, I knew it was good.”

Results

- **Peace of Mind:**
  Confidence knowing that ThreatDown provides strong protection against endpoint threats
- **Comprehensive Visibility:**
  A view into the security status of student machines—whether the machines are on or off campus
- **Ease of Use:**
  A simple solution that provides a great user experience for the IT Team, as well as the students

GLBA Compliance

Alongside providing comprehensive threat detection and response capabilities, the newly installed ThreatDown also took a huge bite out of the seminary's GLBA compliance obligations.

As a provider of federal financial aid to students, Midwestern Baptist Theological Seminary is classed as a financial institution by the FTC, which is responsible for enforcing the Gramm-Leach-Bliley Act (GLBA). Changes to the way the act was enforced left higher education institutions facing a much more stringent and specific definition of what it means to be secure in 2023.

And the auditors weren't the only ones raising eyebrows at the new software's capabilities. "When we were talking with our consultants they said, 'we know you can't do any sort of managed system'", Stone told us. His reply, "actually, we do have a managed system, it's called MDR.”

> "The fact that we had the ThreatDown suite, the MDR and all that in place, ticked off a good two thirds of the requirements for GLBA in and of itself."
>
> **Steve Stone, Director of Information Technology**
> **Midwestern Baptist Theological Seminary and Spurgeon College**

IT 2.0

“My boss calls it IT 2.0 for Midwestern,” says Stone, describing the overhauled IT and security apparatus that underpins the seminary’s activities.

When Stone arrived to take up his position as Director of Information Technology, the institution was on the up, thanks to a turnaround masterminded by Midwestern’s fifth president, Dr. Jason K. Allen. Stone was given license to not just solve problems, but to think about solving them in the best way.

What followed was a root and branch rethink of IT. Servers were migrated to a hosted private cloud, and the network architecture and infrastructure completely updated. The seminary’s single subnet has given way to a segmented network of almost 100 subnets, a measure straight out of the effective ransomware defence playbook.

The seminary’s applications are kept up to date by ThreatDown’s vulnerability assessment and patch management software. “It's been very helpful to just highlight things and say ‘run this update’," says Stone, who also told us that “some update schedules just happen automatically.”

And when Stone and his staff go home at night, Midwestern’s IT 2.0 is watched over by the 24/7 security experts of ThreatDown’s Managed Detection & Response (MDR) team.

ThreatDown™ Powered by Malwarebytes

threatdown.com

corporate-sales@malwarebytes.com

☎ 1.800.520.2796