Archdiocese finds safe haven from cybercrime with Bitdefender MDR

More time on strategic projects, security burden relieved, and overall patch compliance improved

THE CHALLENGE

When an Archdiocese began consolidating IT services across its various agencies and locations, its IT support organization transitioned from supporting several hundred to many thousands of employees.

Senior leadership, with the assistance of outside IT committee members, determined that a managed detection and response solution would help reduce IT operational costs and deliver improved stability across the decentralized organization. After evaluating solutions from various managed security vendors including Bitdefender, Carbon Black and CrowdStrike, IT selected Bitdefender Managed Detection and Response (MDR) Service.

Staffed by experienced security analysts, Bitdefender's MDR Service provides the Archdiocese with 24X7 monitoring of in-depth telemetry to rapidly identify malicious activities, remove threats, reduce investigative time, and limit damage.

The IT Director of the Archdiocese, comments, "We were happy with Bitdefender's GravityZone protecting our parishes for the previous 1 ½ years, so we wanted to give Bitdefender a look as well. We valued Bitdefender's security expertise, advanced software, responsiveness to our questions and with their new service operations center being in built in the U.S, it seemed a good fit."

THE SOLUTION

The MDR Service uses the base of Bitdefender GravityZone Ultra, which provides the Archdiocese with endpoint protection, detection, and response capabilities across more than 5,000 endpoints. The Archdiocese's endpoints include: Windows, Linux and macOS workstations; physical and virtual servers running VMware, Citrix, and an on-premises email solution.

The Archdiocese's MDR Service also incorporates GravityZone HD, which includes Sandbox Analyzer to analyze suspicious files, detonate payloads, and report malicious intent to administrators, and HyperDetect for tunable machine learning, advanced heuristics, and anti-exploit techniques.

The Archdiocese has a Catholic population of roughly half a million people with hundreds of parishes and schools. Employing several thousand employees, the Archdiocese and its agencies provide shelter, hospitalization, addiction services and child services regardless of religion, race or gender.

Industry
Non-Profit

Headquarters
United States

Employees
4,500 (IT staff, 19)

Results

- Delivered 24x7 monitoring of infrastructure endpoints and networks
- Drastically reduced time spent on security operations
- Freed IT staff to spend more time on strategic initiatives
- Increased patch compliance from 75 to nearly 99 percent

Additional MDR Service modules selected by the Archdiocese include GravityZone Patch Management to automate patching and Bitdefender Network Traffic Security Analytics (NTSA) to detect network-based attacks in real time and automate alert triage for incident response.

THE RESULTS

The MDR Service has given the IT team confidence that the outlaying parishes are protected in the face of cyberattacks just as the main campus and local agencies.

"Bitdefender MDR assures me that someone is watching our entire network in real-time, including when my staff and I are not in the office," says the IT Director. "As we've shifted to teleworking with COVID-19, we're able to protect our information assets regardless of where employees are logging in from. MDR is an extension of my team to support the mission of the Archdiocese."

The Senior Infrastructure Engineer adds, "I appreciate the fact that Bitdefender keeps adding valuable features. For example, Bitdefender Endpoint Risk Analytics shows us the current top risks across our organization and gives us remediation list to address those issues. In many cases, after explaining what needs to be done to address the issue, Bitdefender includes a simple 'Fix It' button that will take those remediation steps for us, automatically. In cases where there are many small issues, it can drastically reduce the time we would have to spend addressing those issues."

Bitdefender GravityZone Patch Management has streamlined enterprise-wide updates while eliminating many forced reboots for users.

"Bitdefender Patch Management has been fantastic," states the IT Director. "If a zero-day fix comes out, Bitdefender can update the entire organization with the latest security patch quickly. Patch compliance has gone from 75 to nearly 99 percent. Before, it wasn't uncommon for workstations in remote locations to go years without an update."

The Senior Infrastructure Engineer recalls, "A prime example of this, there have been multiple times when I'm starting my morning out, to discover a critical update was released the night before. I log onto the Bitdefender web panel to get an idea of which systems need to be patched, only to find the patch had already been applied to 98 percent of our endpoints. Before, our help desk team would have spent hundreds of hours calling our locations to help them install the emergency patch."

Because Bitdefender MDR security experts manage alerts, monitor endpoint risks, and maintain security vigilance, the IT team has decreased the amount of time they spend addressing security issues, and can focus more on other projects.

"My team has 19 people and yet we're usually working on 30 to 55 different projects all the time. MDR relieves the security burden on the Help Desk and Operations group and frees us to focus more on strategic projects to support the Archdiocese."

Customer support from the MDR Service has been another asset, explains the Senior Infrastructure Engineer: "MDR promises a one-hour response but we usually hear back within five minutes, which is dramatically better compared to other vendors. With Bitdefender, we contact them and they're immediately on it. We appreciate such fantastic customer support."

"Bitdefender MDR assures me that someone is watching our entire network in real-time, including when my staff and I are not in the office."
- IT Director, Archdiocese

Bitdefender Footprint
Managed Detection and Response Service:
- GravityZone Ultra
- GravityZone Patch Management
- GravityZone HyperDetect
- Bitdefender Network Traffic Security Analytics

IT Environment
- Citrix XenApp
- Citrix XenServer
- Microsoft Exchange
- VMware ESXi

Operating Systems
- Linux
- macOS
- Microsoft Windows

26072020-Bitdefender-CaseStudy-Arch-crea4644-A4-en_EN