

Insurance provider fortifies defenses against cyberattacks

Bitdefender beats back advanced threats, provides increased infrastructure visibility, and delivers cost and time savings



Government Employees Health Association (GEHA) is a self-insured, not-for-profit association providing medical and dental plans to federal employees and retirees and their families through the Federal Employees Health Benefits Program (FEHBP) and the Federal Employees Dental and Vision Insurance Program (FEDVIP).

Industry
Insurance

Headquarters
Lee's Summit, Missouri, USA

Employees
1,500 (IT staff, 18)

- Results**
- Achieved 100 percent success rate in blocking malware
 - Reduced security administration resources from one FTE to one-quarter FTE
 - Consolidated 41 virtual appliances to four central scanning servers, reducing server costs
 - Gained centralized visibility of protection status across entire infrastructure
 - Complied with regulatory requirements for device control

THE CHALLENGE

We don't have to look far for news about high-profile data breaches. Almost weekly, governments, companies, political organizations and other entities are compromised in cyberattacks. As a provider of health insurance to federal government employees, GEHA must be vigilant about safeguarding protected health information (PHI) under United States law. Cybercriminals work hard to steal personal data about federal employees, particularly those with security clearances. Theft of such data could result in significant financial penalties and reputation harm for the company.

Prior to Bitdefender, GEHA used Microsoft System Center Endpoint Protection (SCEP) and Trend Micro Deep Security. As attack vectors became more sophisticated, ransomware and other threats began bypassing the solutions. In fact, one attack locked out 80 percent of employees from accessing their files for 13 hours.

To address growing security concerns, the IT team evaluated Cylance, Trend Micro OfficeScan, and Bitdefender GravityZone. In addition to reviewing industry security research studies from Gartner Group, AV-TEST, AV-Comparatives, and NSS Labs, IT tested how the security solutions detected and stopped hundreds of malware samples that mimicked zero-day signature-less threats.

GEHA's Security Team Lead Josh Gilliland explains, "Bitdefender GravityZone was far and above the best at detecting and blocking malware. In our tests, GravityZone blocked 100 percent of 500 malware samples we threw at it while other vendors could only keep out 50 to 60 percent. We also were impressed with GravityZone's layered security and next-gen feature set from device control to machine learning to content filtering. Bitdefender was the clear choice."

GEHA recently upgraded to GravityZone Elite after successfully using GravityZone Enterprise Security for 12 months. GravityZone Elite incorporates Sandbox Analyzer, an endpoint-integrated sandbox to analyze suspicious files, detonate payloads, and report malicious intent to administrators, and HyperDetect, a next-generation security layer that provides tunable machine learning with advanced heuristics and advanced anti-exploit techniques.

THE SOLUTION

GravityZone Elite protects GEHA's 1,900 virtual and physical servers, workstations, and virtual desktops across two data centers. The environment comprises primarily Microsoft Windows and VMware, and smaller Citrix XenDesktop, Linux, Apple, and Nutanix environments. GEHA is rolling out Microsoft Azure infrastructure as a service (IaaS), which also is protected by GravityZone.

Bitdefender Professional Services assisted the insurance provider with setting up the GravityZone server and policies. GEHA also uses Bitdefender Gold Support.

"Our experience with Bitdefender Professional Services and customer support has been excellent," says Gilliland. "The deployment was smooth, straightforward and simple. Every person we've worked with at Bitdefender has been responsive and pleasant."

THE RESULTS

Security management has been a breeze with GravityZone. One advantage is seamless integration between GravityZone and VMware vCenter server management software.

Gilliland states, "We now see everything from a protection status at a glance via one console. Our staff has found GravityZone much easier to manage than other vendors' security solutions."

"Before, we had to assign a Trend Micro virtual appliance to each host, which made management more time consuming. With GravityZone, we consolidated 41 virtual appliances to two central scanning servers in each data center, which saved us in server costs."

In fact, GEHA reduced security administration staffing from one full-time equivalent (FTE) to one-quarter FTE since adopting Bitdefender.

GravityZone also has proven exceptional at keeping out threats. One feature is that GravityZone complies with NIST 800-53 regulatory requirements for device control, which prevents employees from infecting workstations with external devices.

"GravityZone has remarkable efficacy in blocking malware," notes Gilliland. "It's had a 100 percent success rate. HyperDetect will help close the gap in addressing file-less malware, which is a fast-growing category. Sandbox Analyzer also will provide us with strong defenses against zero-day threats."

GEHA greatly values Bitdefender's strong customer commitment.

Gilliland reflects, "Bitdefender views this as a two-way relationship as opposed to just making a sale and disappearing, which we've seen from other vendors. The sales and technical teams go above and beyond in soliciting our feedback on the products."

"We now see everything from a protection status at a glance via one console. Our staff has found GravityZone much easier to manage than other vendors' security solutions."

— Josh Gilliland, Security Team Lead, GEHA

Bitdefender Footprint

- GravityZone Elite Security
- GravityZone On-Premises Management Console

IT Environment

- Citrix XenDesktop
- Microsoft Azure
- Nutanix
- VMware vCenter Server
- VMware vSphere

IT Environment

- Apple (Mac)
- Linux
- Microsoft Windows