

IntraHealth International **boosts ransomware immunity**

Malwarebytes scales defenses and increases responsiveness

Business profile

IntraHealth was originally founded in 1979 at the University of North Carolina at Chapel Hill School of Medicine. Today the nonprofit organization works globally, helping countries ensure that their health workers are trained, supported, and equipped. More than 500 employees work in 37 countries, creating a challenging endpoint security environment. That's why IntraHealth chose Malwarebytes.

Business challenge

The aftermath of ransomware

Based in Chapel Hill, North Carolina, IntraHealth engages with healthcare policy teams and agencies across Africa, the Americas, and Asia. Employees travel extensively to assist clients with digital health initiatives, education, leadership development, measurement and analytics, and healthcare advocacy programs. Jeffrey Brown, Global Help Desk Supervisor for IntraHealth, and his team support more than 800 endpoints.

Many remote offices are small, without local IT support. Brown's team or a local IT professional supports them if needed. Offices with more than 20 employees have a full-time help desk person or local consultant to handle issues. Prior to deploying Malwarebytes, laptops would become infected with localized viruses or malware, which varied between countries. A help desk team member could quickly recover systems from backup. When advanced global threats began to emerge, IntraHealth adopted cyber insurance to protect against a worst-case scenario.

In April 2018 a ransomware attack disabled the organization's BitDefender antivirus software and encrypted systems. The cyber insurance company sent a forensic team to manage the attack, cleanup, and remediation.

OVERVIEW

INDUSTRY

Nonprofit

BUSINESS CHALLENGE

Increase protection against advanced threats while simplifying endpoint security

IT ENVIRONMENT

Firewalls, layered security, cyber insurance

SOLUTION

Malwarebytes Endpoint Protection

RESULTS

Prevented ransomware encryption from re-occurring

Enabled "live" proactive defense

Streamlined response to incidents

Simplified updates for systems in remote areas with limited bandwidth



MALWAREBYTES ENDPOINT PROTECTION IS FABULOUS. WE CAN SEE THREATS IN OUR ENVIRONMENT WHEN THEY APPEAR—BEFORE THEY CAN BECOME A PROBLEM.

JEFFREY BROWN, GLOBAL HELP DESK SUPERVISOR, INTRAHEALTH INTERNATIONAL

The solution

Malwarebytes Endpoint Protection

Brown and his team often used the Malwarebytes remediation tool to clean up infections that the antivirus product missed. During ransomware remediation, the forensic team also suggested using Malwarebytes to ensure that systems were truly clean.

“We always came back to Malwarebytes,” said Brown. “If we used Malwarebytes to clean up systems, why not use it to protect them? The ransomware attack and the forensic team’s recommendation convinced our executive team.”

Brown and his team conducted a 30-day trial of Malwarebytes Endpoint Protection. They quickly became familiar with the console, planned the deployment, and configured policy. As soon as the purchase was complete, they replaced BitDefender and rolled out Malwarebytes across the organization.

“We used group policy to deploy Malwarebytes for systems on our global WAN,” said Brown. “It was installed on remote mobile devices when users returned to the office. Malwarebytes now protects everything—laptops, desktops, and servers.”

“Live” protection enables proactive defense

“Malwarebytes Endpoint Protection is fabulous,” said Brown. “We see threats in our environment when they appear—before they can become a problem. Visibility from a ‘live’ reporting environment enables us to avoid compromises.”

In the past, antivirus “after the fact” reports only showed what had happened during previous weeks and months. Malwarebytes provides at-a-glance status of systems and detections as they occur and over the previous few days. Brown can quickly identify trends and take proactive measures to prevent infection. IntraHealth also coordinates Malwarebytes data with its Cisco Meraki firewalls.

“We can immediately ban any infected machine from the network,” said Brown, “and we contact the local IT person to check it. In the past, local staff members were often too busy to check the system right away. Without network access for the user, it becomes a priority.”

Streamlined tool kit simplifies everything

Malwarebytes streamlined the team’s processes while increasing organization-wide protection. Proactive defense and remediation in a single platform reduced the number of different products used to manage endpoint security. If a threat evades outer defenses, help desk staff don’t have to look for a specialized tool or download another product. They simply run a complete Malwarebytes scan, and if the system requires rebooting, Malwarebytes tells them.

“Systems download Malwarebytes updates directly,” said Brown. “It’s much more efficient and doesn’t disrupt the network. Updates are naturally staggered over time because users begin work at different times.”

Next Steps

IntraHealth is working with a training partner to help staff in remote offices learn more about cyberthreats and how to avoid them. Brown’s team also is evaluating other tools that can deliver exhaustive endpoint system details to complement Malwarebytes protection.

“Malwarebytes simultaneously boosted our defenses and improved our responsiveness,” said Brown. “We’re more confident in our ability to protect our users as they work to protect healthcare providers around the world.”



malwarebytes.com/business



corporate-sales@malwarebytes.com



1.800.520.2796

Malwarebytes proactively protects people and businesses against dangerous threats such as malware, ransomware and exploits that escape detection by traditional antivirus solutions. Malwarebytes completely replaces antivirus with artificial intelligence-powered technology that stops cyberattacks before they can compromise home computers and business endpoints. Learn more at www.malwarebytes.com.