CASE STUDY

WEBROOT®
Smarter Cybersecurity

and

Arkansas Hospice

> I've recommended this product to people in both my personal and professional life and everyone who has tried it has loved it.
>
> **Steven Bryant, IT Manager at Arkansas Hospice, Inc.**

At a Glance

Vertical
Healthcare

Year Founded
1992

IT Manager
Steven Bryant

Endpoints Managed
250

Website
arkansashospice.org

Key Findings

Time Savings
140 hours per year

Efficacy
100% decrease in infections

Efficiency
Endpoint scans dropped from 35 minutes to 2 minutes.

Server scans dropped from 2 hours to 3 minutes

Arkansas Hospice Ensures HIPAA Compliance with Webroot

Background

The mission of Arkansas Hospice, Inc. is to enhance the quality of life for those facing serious illness and loss by surrounding them with love and embracing them with the best in physical, emotional and spiritual care. They bring people and organizations together who share a common desire – to make certain that comfort, dignity, and peace at the end-of-life is possible for everyone – and foster these partnerships so that their impact is meaningful to patients and their loved ones, as well as for the donor, the Arkansas Hospice team, and everyone in between.

The Challenge

Working in healthcare presents special challenges to IT managers and network security professionals. Not only are they faced with the plethora of challenges that day-to-day security operations present, from network uptime to server maintenance to unexpected hardware challenges, but they're constantly aware that – at any given moment – an uninformed user could be responsible for introducing information-stealing malware that could jeopardize the organization's HIPAA compliance.

According to Steven Bryant, "As the IT manager and HIPAA officer of our organization it is my job to make sure our network is secure and no patient data is leaking to the outside world. I am always trying to stay ahead of the next 'big threat.' Currently, it's ransomware, but in the past it's been everything from Sasser/Blaster to Polip.a. Each new type of malware that comes out is the underworlds' reaction to new security techniques, patches, or just an attempt to exploit a new infection vector or action. When your network contains patient information or banking information or whatever specific confidential data your company is trying to protect, it's so important that you stay ahead of the wave."

Bryant realized they had a looming problem. With the mission-critical task of protecting patients' private information and healthcare data, his network was "seeing zero-day malware and new variant viruses getting past our antivirus software. My IT team was completely reactive: pulling machines off the network, recovering data, sanitizing (often meaning re-imaging) to try to keep threats from spreading. Daily and weekly workstation cleanup was just a part of our routine." It wasn't working, and the efforts were beginning to feel futile. "We were using simple definition-based protection and found ourselves in a constant battle against zero-day threats and even some older threats that, for whatever reason, our previous product didn't protect us against."

The Solution

Bryant set out to find a better solution to zero-day attacks and malware that can propagate through a network in seconds. According to Bryant, "I took this task as an opportunity to search for a more complete, effective, and comprehensive solution and researched available products for several months, testing most of them to see who had the best." After a thorough search, Bryant heard about Webroot and decided to give it a try, "I have to admit that the first time I ran a full scan on a machine with this software I was dubious about its effectiveness – it only took a few seconds, and the 'best' software on the market was taking 20 minutes to perform the same scan. But results don't lie."

Bryant was almost immediately convinced, "As soon as I started using Webroot, I knew this product was different. It wasn't just hashing against a database, which doesn't protect you against zero-day threats and malware variants being produced by the assorted 'malware kits' being sold on the web. Webroot was doing those things, but it was also looking at behaviors and using heuristics to decide if applications were performing threatening actions. It was doing it all through a cloud-based 'web' of clients that respond to threats in real time and instantly warn other clients of newly discovered threats. By leveraging this client feedback it is able to keep the entire Webroot client base much more secure."

Not only did Bryant find Webroot SecureAnywhere® Business Endpoint Protection effective at stopping the latest threats in real time, he was also impressed with how lightweight and quickly deployed the agent is. Bryant says, "It has an amazingly small footprint and scans incredibly fast." With an installation file that's less than a megabyte, the client begins protecting endpoints in a matter of seconds.

Results

Bryant and his team couldn't be happier with Webroot. One of their biggest pain points before deploying Webroot – putting out constant fires from new malware infections – has been all but removed from his teams' day to day operations. According to Bryant, "Webroot was a game changer. Instead of reacting to compromised machines, it has kept the new stuff out in the first place, allowing my team to focus more on training staff, user safety, and some of the aspects of security that software can't protect you from – the people factor. Since deployment, the only infections we've found on any machines in production were rooted prior to installation, which really shows how ineffective our last solution was." On top of finding more time for his team to focus on strategic objectives, Bryant has also been pleased when he's needed to reach out to Webroot support, "I've only had to speak to Webroot support a few times. In each case I got a technician very quickly and they knew exactly how to solve my problem. I'd say the support team is extremely knowledgeable and friendly."

In fact, Bryant has become extremely enthusiastic about Webroot, "The end result is spectacular. We've seen a dramatic reduction in infections on our network and when we do get an alert these days it's always just Webroot telling us it detected a threat, isolated it, and disabled it before it could spread. I've recommended this product to people in both my personal and professional life and everyone who has tried it has loved it, especially the other IT professionals I've turned on to this."

About Webroot

Webroot delivers next-generation network and endpoint security and threat intelligence services to protect businesses and individuals around the globe. Our smarter approach harnesses the power of cloud-based collective threat intelligence derived from millions of real-world devices to stop threats in real time and help secure the connected world. Our award-winning SecureAnywhere® endpoint solutions and BrightCloud® Threat Intelligence Services protect millions of devices across businesses, home users, and the Internet of Things. Trusted and integrated by market-leading companies, including Cisco, Citrix, F5 Networks, Aruba, Palo Alto Networks, A10 Networks, and more, Webroot is headquartered in Colorado and operates globally across North America, Europe, and Asia. Discover Smarter Cybersecurity™ solutions at webroot.com.

World Headquarters
385 Interlocken Crescent
Suite 800
Broomfield, Colorado 80021 USA
+1 800 772 9383

Webroot EMEA
6th floor, Block A
1 George's Quay Plaza
George's Quay, Dublin 2, Ireland
+44 (0) 870 1417 070

Webroot APAC
Suite 1402, Level 14, Tower A
821 Pacific Highway
Chatswood, NSW 2067, Australia
+61 (0) 2 8071 1900