

MAO, MEDICAL ADVOCACY AND OUTREACH, TAKES A GIANT STEP FORWARD IN SECURITY AND DATA PRIVACY

Check Point solutions deliver the most innovative and effective security including protecting endpoints, delivering deep threat visibility, and helping ensure compliance at a glance.



Customer Profile

MAO provides educational, medical, and social services to those affected by HIV and related illnesses.

Challenge

- Upgrade the clinic's security posture to defend against threats and support growth
- Meet compliance requirements
- Stop malware and ransomware infections

Solution

- Check Point Harmony Endpoint
- Check Point Quantum Maestro
- Check Point R80

Benefits

- Prevented ransomware infections
- Ensured cyber protection and privacy of client data
- Gained at-a-glance visibility of systems' compliance status
- Improved efficiency and served more patients through secure innovative remote services

“Check Point gives me full confidence in our ability to grow and effectively maintain security and privacy. I've worked with most of the other products out there, and Check Point gives me the most peace of mind.”

— Benjamin Urquhart, Division Manager of Information Technology, MAO

Overview

MAO

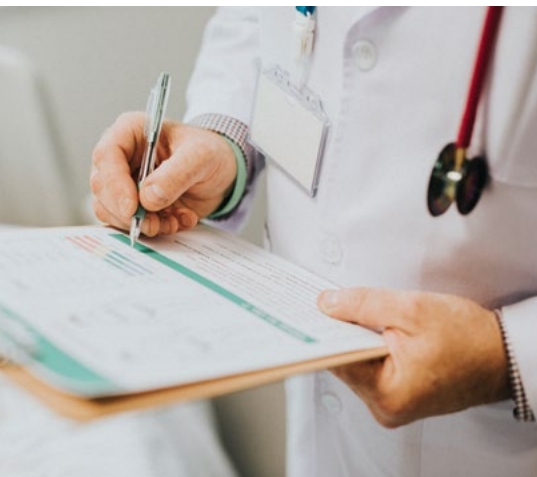
Based in Montgomery, Alabama, Medical Advocacy & Outreach (MAO) is a nonprofit medical institute providing HIV, Hepatitis C, and diabetic care. MAO began in 1987 as a volunteer organization. Today, its services span 28 Alabama counties. In 2011, MAO launched the Alabama e-Health Telemedicine Initiative, delivering HIV-specific care, pharmacy consultations, mental health counseling, and social services, a pharmacy and dental clinic opened in 2017. The organization continues to look for ways to improve Healthcare options in their coverage areas.

Business Challenges

Starting With a Clean Slate

When Benjamin Urquhart joined MAO as Division Manager of Information Technology, he found that the network and security infrastructure was not able to support the organization's rapid growth. For several years, MAO had relied on third parties for network management and security services. An anti-malware product installed on the endpoints was not enough to meet compliance requirements, and other security measures were not current.

“As a medical provider, HIPAA compliance and data privacy concerns are critical, especially when working with HIV cases, which have stricter regulations,” said Urquhart. “We decided to bring our network and security management in house for more control and better protection. It was time for a clean slate.”



“Check Point Compliance also has been a massive help to us, We can easily see which units are compliant, which aren't, and then we can immediately address those. The visualization is fantastic.”

— Benjamin Urquhart,
Division Manager of Information
Technology, MAO

Urquhart had experience with Check Point solutions in the past. Before he approached MAO senior management and the Board of Directors to explain why the organization needed enterprise-level security and technology, he launched a small proof of concept deployment of Check Point Security Appliances and R80 Cyber Security Management.

Solution

Crystal-clear Visibility

The Check Point security logs with analysis and reporting found thousands of botnet connections, malware, and other malicious threats coming in and going out of the network. With SmartEvent providing crystal-clear visibility into cyber attacks, it was easy to see how serious the threats were.

“I expected to see these kinds of threats, but even I was surprised at the volumes,” said Urquhart. “The Check Point solutions gave me hard data about how much visibility we lacked and where we were at risk.”

The data was also compelling to the Board and senior managers, who approved a significant security and technology initiative to not only support the organization's growth, but also provide compliance ready security. Urquhart deployed the Check Point Security Appliances over one weekend to secure the clinics as quickly as possible. Check Point SandBlast Agent with Threat Emulation and anti-ransomware now defends end-user systems against zero-day threats, bot communications with command-and control servers, and other advanced attacks.

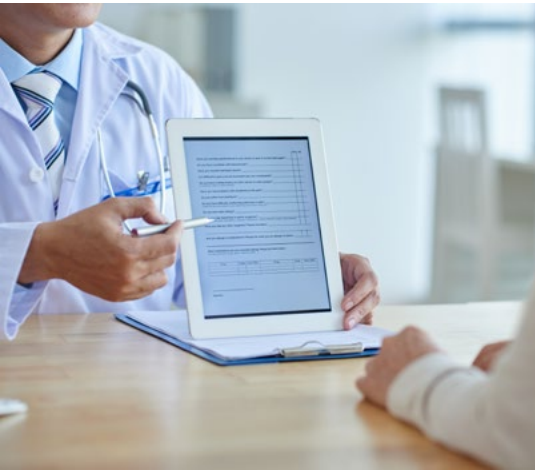
Check Point Anti-Malware efficiently detects malware with a single scan, while Check Point Compliance continuously monitors security infrastructure, gateways, technologies, policies and configuration settings all in real time to ensure compliance requirements.

Results

Stopped Ransomware

Check Point SandBlast Agent Threat Emulation has detected and sandboxed numerous malicious downloads and attachments, protecting endpoints from infection. When ransomware attacked a user's browser, Check Point stopped it instantly, preventing it from encrypting MAO fileshares.

Users no longer see popups, odd windows, or redirects on their computers. Check Point has virtually eliminated endpoint security-related calls from users, freeing technicians for more strategic projects. Urquhart further reduced risk of cyber threats by blocking endpoint access to non-work-related websites and social media outlets.



“Check Point Compliance also has been a massive help to us,” said Urquhart. “We can easily see which units are compliant, which aren’t, and then we can immediately address those. The visualization is fantastic.” Check Point Compliance translates thousands of complex regulatory requirements into actionable security best practices.

Secured Innovative Services

MAO serves a large rural population, many of whom live far from a MAO location. Tablets and laptops are utilized to provide direct Telehealth needs and these devices are secured with Check Point SandBlast Agent, these devices connect to the MAO Polycom Bridge system for real-time communication. All calls are encrypted to ensure privacy and compliance, and they are managed from the same Check Point Cyber Security Management console.

Enabling innovative remote telehealth services also eases the burden on the MAO transportation department. Instead of having to pick up remote clients weekly, MAO transportation picks them up when they need to physically see a physician or caregiver. Shifting much of client-caregiver communication to secure tablets greatly reduces the number of trips needed and increases efficiency.

Delivered Deep Visibility

“The Check Point Cyber Security Management console, R80 makes a massive difference in visibility,” said Urquhart. “I can see everything in a true single pane with all events correlated within SmartEvent. We plan to dive deeper into SmartEvent and the SandBlast Agent forensics capabilities when our infrastructure upgrade is complete.”

Urquhart recounts that shortly after he joined MAO, an auditor visited and asked about encryption on the telemedicine units, endpoint security, and other security measures. The clinic had none of those measures in place, resulting in a number of red findings.

“The auditor returned recently and what we can do now is vastly better,” he said. “We’re doing everything from encryption for telemedicine, implementing endpoint protection, enabling VPN for

For more information, visit: <https://www.checkpoint.com/products/>