

## CASE STUDY

# MARTIN'S POINT HEALTH CARE REPLACES LEGACY AV WITH ENDGAME

## SUMMARY

Martin's Point Health Care (MPHC) is a not-for-profit primary healthcare provider as well as a health insurance provider. Headquartered in Portland, Maine, the company employs 800 full-time staff, and has 18 locations in multiple states. MPHC leadership needed to better understand their risk posture and be able to securely share patient information across their organization to deliver high-quality patient care. Endgame provided full-stack protection coupled with ease of use to provide a comprehensive solution to address cyber threats and provide reporting to determine the health of their enterprise.

## THE CHALLENGE

MPHC has a small and nimble enterprise security team tasked with protecting critical patient health records and ensuring their heavy regulatory footprint of compliance with HIPAA (Health Insurance Portability and Accountability Act) and PCI DSS are met. This means the ability to keep pace with targeted attacks that are a constant for MPHC. The MPHC board needed to know their risk posture and the health of the enterprise. Their current anti-virus solution from Symantec failed to give their leadership the level of visibility and the protection to safeguard critical patient information and ensure compliance with regulatory requirements

The IT team needed a solution that would address three primary challenges:

- Block targeted attacks including and beyond malware.
- Monitor 24x7 device activity, even when offline.
- Provide the MPHC Board and leadership a status of the health of their enterprise network.

### INDUSTRY

HEALTHCARE

### COMPANY

- HEAVY REGULATORY FOOTPRINT
- NIMBLE SOC TEAM
- HIGHLY SEGMENTED NETWORK FOR PCI DSS AND HIPAA COMPLIANCE

## SOLUTION

Martin's Point Health Care performed an extensive evaluation of endpoint security options, including cloud-based next-gen AV solutions to replace Symantec's anti-virus solution. They chose Endgame because it was the only solution that provided the comprehensive visibility with full-stack protection across the breadth and depth of the MITRE ATT&CK™ matrix. Other next generation-AV solutions were too complex for junior analysts to use and too slow to stop unknown threats. The MPHHC team found Endgame's distributed architecture and robust two-way API seamlessly integrating with other existing network tools and operational processes within their environment.

## RESULTS

Endgame provided full-stack protection that stopped targeted attacks before they started, stopped ongoing attacks before any damage or loss occurred, and minimized the time IT spent trying to detect and contain threats.

Another benefit the healthcare company team realized over other solutions was Endgame's ability to eliminate multiple host agents with one single agent platform. Endgame replaces existing AV, endpoint detection and response, and incident response agents, drastically reducing the cost and time required to stop emerging threats. The platform provides comprehensive protection and detailed reporting to help their leadership understand their risk posture.

### WHY ENDGAME

- FULL-STACK PREVENTION, ACCELERATED DETECTION AND RESPONSE, AND AUTOMATED THREAT HUNTING ACROSS THE BREADTH AND DEPTH OF THE MITRE ATT&CK™ MATRIX.
- UNPRECEDENTED SPEED TO STOP THREATS IN REAL-TIME AT SCALE IN A HIGHLY REGULATED ENVIRONMENT, WITH MINIMAL PERFORMANCE IMPACT.
- EASY TO USE AND AUTOMATED INTERFACE ENABLED JUNIOR SOC ANALYSTS TO RAPIDLY TRIAGE, INVESTIGATE, AND RESPOND TO ALERTS.



"VISIBILITY AND FAST RESPONSE ACROSS OUR NETWORK ARE CRITICAL TO PROTECTING OUR INFRASTRUCTURE. ENDGAME'S ABILITY TO PROVIDE FULL-STACK PROTECTION GAVE US THE CONFIDENCE TO REPLACE OUR TRADITIONAL-AV SOLUTION AND GIVE COMPREHENSIVE PROTECTION AT THE EARLIEST STAGES OF THE ATTACK LIFECYCLE."

MATTHEW WITTEN, CISO,  
MARTIN'S POINT HEALTH CARE



**ENDGAME.**

ENDGAME.COM

Schedule a demo now with [endgame.com/demo](https://endgame.com/demo)



@EndgameInc



Endgame