CASE STUDY

Moffitt Cancer Center

THREAT WARRIOR

THREAT WARRIOR

MOFFITT CANCER CENTER

How ThreatWarrior protects a leading cancer research center and hospital's supply chain from advanced threats

"One day, a security tool began unexpectedly scanning our network. It turned out to be benign — the vendor added this functionality in an auto-update but never informed us. ThreatWarrior detected this anomaly when no other tool did. This gives us the confidence that ThreatWarrior provides a much needed additional layer of protection over our security supply chain."

- Dave Summitt, CISO, Moffitt

ENVIRONMENT

- Top US cancer research center and hospital
- More than 7,000 team members
- Tens of thousands of devices

CHALLENGES

- Growing security supply chain adds complexity and risk to threat surface
- Exponential growth of medical devices on the network
- Proactively hunting threats

SOLUTION

- Deploy ThreatWarrior in the Security Operations Center to:
  - Monitor supply chain and security tooling
  - See all network activity in real time
  - Learn normal behavior of everything connected to the network
  - Act efficiently to stop threats and accelerate response time

RESULTS

- Unprecedented network visibility
- Detected security supply chain anomalies
- Proactive threat hunting capabilities

The Company

Moffitt Cancer Center is a nonprofit cancer research and treatment facility located in Tampa, Florida. It is one of only 51 National Cancer Institute-designated Comprehensive Cancer Centers and is one of the top cancer hospitals in the nation. Since 1999, Moffitt has been recognized as one of the leading care facilities by U.S. News & World Report and, with a team of more than 7,000 members, Moffitt has a $2.4 billion state economic impact.

The Situation

Healthcare providers are up against some of the most difficult cybersecurity challenges. Increasingly complex threat actors have targeted this industry due to the high value of its extremely sensitive data. As such, the impact of a network breach or system compromise on Moffitt could be massively damaging. Regulatory fines, plus the time and associated costs spent on incident management, forensics and recovery would produce unnecessary resource consumption and decreased performance objectives. Responsible for confidential patient data, the organization also faces the threat of losing public trust.

Tasked with improving security measures – a critical priority for Moffitt – IT leadership turned to ThreatWarrior. The organization wanted to adopt a proactive approach to cybersecurity that allowed them to not only detect but hunt threats; an approach that could identify and mitigate cyberattacks before they caused damage.

Additionally, Moffitt needed a solution that could provide network visualization, delivering insights into all network traffic including insider and supply chain activity; a solution powered by real AI that could understand entity behavior to identify emerging threats, internal and external.

The Solution

Immediately upon installation, Moffitt was able to see a 3D visualization of network activity, including all firewalls, endpoints, and IoT devices rendered in real-time. The intuitive, graphical interface allowed Moffitt's team to easily view the threat surface, which helps optimize resource allocation and streamline security efficiencies. ThreatWarrior's 3D Universe also exposes emerging threats in real time.

ThreatWarrior was able to quickly reveal threat events ahead of other tools and technologies. This early detection of suspicious activity allowed security teams to investigate and correct these events.

In one such event, ThreatWarrior identified activity that indicated unusual behavior from one of Moffitt's other cybersecurity tools. The tool had begun performing occasional network scans which was unexpected and unapproved.

Upon investigation, Moffitt discovered that one of their security vendors had actually applied a full version update and feature enhancement to its latest "patch." Because ThreatWarrior is able to identify behavioral anomalies in other security tools, the platform raised an alert to this unwarranted network scanning and Moffitt's team was able to quickly resolve the problem.

While this behavioral change was vendor-initiated and not malicious, it demonstrated to Moffitt ThreatWarrior's ability to detect this type of threat to the supply chain. Should a malicious attack occur — like the SolarWinds breach that was discovered in Dec. 2020 — ThreatWarrior could quickly identify this and prioritize alert delivery to the appropriate team.

THREAT WARRIOR

The Results

ThreatWarrior demonstrated a superior method of network defense against all threat types. The platform's use of deep learning AI is exponentially more powerful than traditional machine-learning solutions, as it builds and refines its own understanding of each network it monitors, free from human bias.

Moffitt's security team is realizing significant benefits by using ThreatWarrior, including:

- An additional, critical layer of security around Moffitt's supply chain
- Faster response to powerful attack vectors, including malware and botnets
- A holistic network view that displays in 3D real-time traffic and information on the current state of the network
- The ability to visually replay threat events and see the paths of communication occurring over time
- Cybersecurity that advances with increasingly complex threats
- Compliance with HIPAA's log auditing and aggregation requirements
- A solution that scales with Moffitt's constantly evolving enterprise

"ThreatWarrior delivered impressive visibility across our entire threat surface. They've provided the additional cyber intelligence we need to move beyond detection and response into advanced threat hunting. We've been able to identify and stop threats more easily with insights from ThreatWarrior."

DAVE SUMMIT
CISO, MOFFITT CANCER CENTER

By deploying ThreatWarrior, Moffitt is achieving its goal of securing its organization against malicious cyber actors while attaining true network visibility and supply chain security. Armed with the most sophisticated cyber defense available, Moffitt has an advanced understanding of its security ecosystem, and knows that as the threat landscape rapidly evolves, ThreatWarrior will evolve with it.

"ThreatWarrior has allowed us to learn about our network and generated great insight into our security posture. We see the benefits of the platform as a potential game changer for security teams."

- Dave Summitt, CISO, Moffitt Cancer Center

About ThreatWarrior
ThreatWarrior is the premier cloud-native network threat intelligence platform that stops both known and unknown cyber threats in real time. The agentless, deep learning platform analyzes network traffic to eliminate blind spots, determine security vulnerabilities, and stop active threats across on-premises, cloud and hybrid environments.

ThreatWarrior is the first solution to combine unsupervised neural networks, continuous deep packet inspection, behavior monitoring, network intelligence and automated response in a single platform. Leading organizations use ThreatWarrior to see everything happening on their network, learn the behavior of everything communicating across their enterprise, and act efficiently to stop threats other solutions miss.

Contact Us

844-463-9440
info@threatwarrior.com
www.threatwarrior.com

11801 Domain Blvd., 3rd Floor
Austin, TX 78758

THREAT WARRIOR