deep instinct™

CASE STUDY
HEALTHCARE

OneBlood prevents 100% of malware from infiltrating its network to continue its culture of safety

600%
INCREASE IN ATTACKS IN FIRST HALF OF 2021

100%
MALWARE PREVENTED BEFORE IT EXECUTED

2,500+
EMPLOYEES PROTECTED

The Company

More than 250 hospitals across the Southeastern United States rely on OneBlood for safe, available, and affordable blood. OneBlood distributes more than one million blood products annually and operates more than 90 donor centers and 200 of its signature Big Red Buses for blood drives.

Industry: Healthcare

Company size: Mid-Enterprise

Existing Security Solution: Endpoint prevention, detection, and response

The Need: An Ounce of Prevention is Worth a Pound of Cure

Safety is OneBlood's top priority. The nonprofit's mission to enhance the well-being of others through its work with blood and stem cell products and facilitating scientific research requires a fortified cybersecurity posture.

OneBlood must protect its intellectual property and customer data, yet the effectiveness of its endpoint detection solution was waning. The growing and evolving landscape of cyberattacks—in particular ransomware—prompted OneBlood to look for an alternative solution.

"A lot of organizations that have been hit by ransomware pay the money because they haven't been doing their due diligence in business continuity," says John Holder, director of information security and business continuity administrator at OneBlood. "There's no reason to put off information security. Every time criminals get a ransom, they are emboldened."

"Many endpoint security vendors allow first-seen malware examples to get through while sandboxing the threat, and then they will stop the rest. I'm a zero-defect mentality person. I don't want any leakage and that's what Deep Instinct does."

– John Holder, Director of Information Security and Business Continuity Administrator, OneBlood

In Search of Prevention

In early 2020, OneBlood began noticing issues associated with its existing endpoint security solution, which had been put in place six years ago after suffering a ransomware attack.

"Protection started to decline," recalls Holder. "It was time to move toward AI and beyond signature-based detection."

Holder's vision was to move to a modern architecture for endpoint security, and when he came across Deep Instinct's claim that a deep learning approach would prevent 99% of threats pre-execution, he was intrigued.

"We wanted a product that would stop a threat before it executed and found its way inside our network," says Holder. At first, Holder was skeptical that Deep Instinct claims were real, so he says, "We peeled back the onion to see if Deep Instinct is hype or not hype."

The Solution: Peeling Back the Onion

Holder put Deep Instinct to task. He gathered a variety of malware samples, including zero-day threats and trojans that had not been seen in his environment. As an experienced threat hunter, Holder also prepared his own custom malware. His main requirement was that the malware samples could not have been in the wild for more than a week.

A rigorous proof of concept test ensued, using Holder's self-curated and broad set of malware samples. "Deep Instinct found zero-day viruses and trojans and never-before-seen malware that had been in the wild for less than a week," he says.

In OneBlood's proof of concept test, competitive solutions only caught between 70% to 86% of the malware samples. Deep Instinct detected 100%.

Holder didn't stop there. Not convinced what he was seeing was real, he followed up with a second test and received the same results. What was notable was that Holder was testing the malware samples against a Deep Instinct brain that was six months old.

"I was amazed that an engine that was six months old at the time could detect something that had been in the wild for only a week," he says.

Holder put together his findings and recommendations to his team and Deep Instinct was selected. "I was impressed by the Deep Instinct support team and their level of expertise to keep up with me as a threat hunter," he continues. "The commitment to implement our pilot and resolve any issues was refreshing."

Deep Instinct is implemented across OneBlood's endpoints, tablets, laptops, workstations, and servers used by more than 2500 employees at its offices, donor centers, laboratories, manufacturing and distribution sites, workers' homes, as well as in its Big Red Buses used for mobile blood drives.

The Results

Preventing malware before it executes

"My goal is to do everything I can before malware gets to the endpoint," says Holder.

Since implementing Deep Instinct, OneBlood measured a marked increase in attempted attacks of over 600% in the first six months of 2021. "It's eye opening when you see your threat levels increase in such a massive way," he says. "But we haven't had any breaches, data leaks, or exfiltration with Deep Instinct protecting our endpoints."

Improving productivity with a lean team

Deep Instinct allows OneBlood's IT team to run lean—and know where to best focus resources.

"Our other product was a beehive with constant misidentifications or nuisance alerts all day," says Holder. "With Deep Instinct, our frustration level is down significantly," he says.

Because Deep Instinct prevents threats prior to writing to disk, it significantly lowers alerts and false positives.

"Some days I go into the Deep Instinct console and there's no activity at all to take action on," he says. When new systems are deployed or an endpoint comes back online, Deep Instinct is quick to take action, detecting infections and cleaning up as necessary.

Optimizing resources and improving operations

Because Deep Instinct prevents malware and significantly lowers false positives, there are far fewer security events to parse. When events do occur, the security operations center has more resources available to respond to the high fidelity alerts with immediacy.

"Since events are prevented, we know if we see an event flagged we really need to pay attention to it," he says.

When the security team's workload is dramatically reduced, resources are freed up to focus on higher value work like penetration testing and threat hunting as well as basic hygiene. OneBlood counts up savings by avoiding the labor and time associated with remediation and digital forensic investigations. With Deep Instinct, OneBlood also avoids the operational hassle of reinstalling agents and utilities and rebuilding systems after a breach.

In addition, because attacks are prevented and malicious traffic dropped, OneBlood's firewalls and other security defenses can operate at an optimal level.

Prevent first, but don't forget to plan for the worst

Strong business continuity planning and a prevention-first approach provide strong protection against rising cyber-risks, advises Holder.

Deep Instinct's neural network continuously and automatically learns to get smarter on its own, stopping known, unknown, and zero-day threats with better accuracy and speed than other endpoint protection or legacy AV solutions. Deep Instinct automatically prevents malicious files in under 20ms without requiring connectivity to the cloud.

Holder offers advice to security leaders working in healthcare or other sectors. "The ransomware trend is not going away anytime soon. Don't pay the ransom. You need to have sufficient backups and do your due diligence in terms of business continuity planning. By preventing malware from executing first and ensuring sufficient backups to restore your business just in case, you will sleep easier."