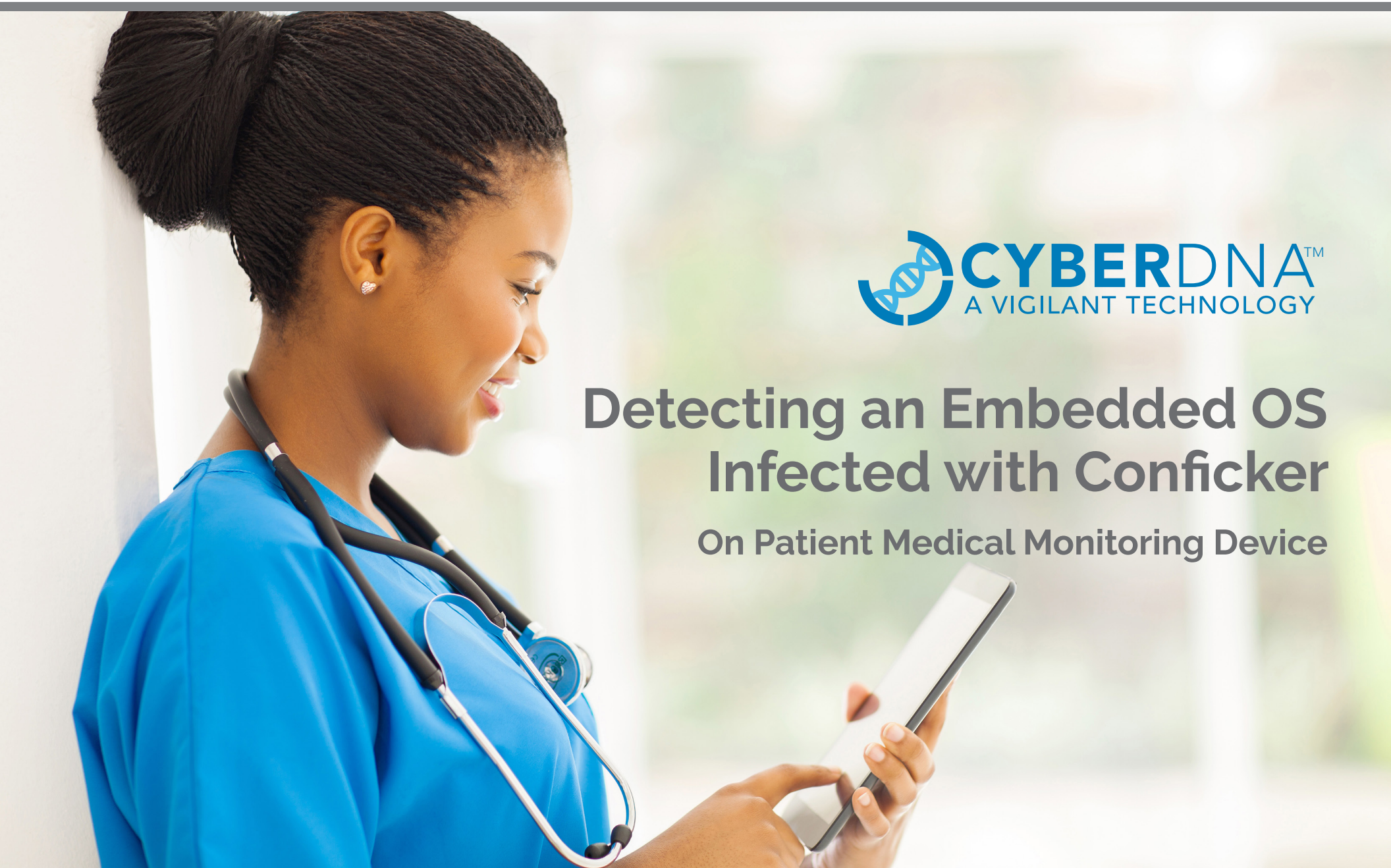
Case Study

LANTELLIGENCE
We make the NETwork!



CYBERDNA™
A VIGILANT TECHNOLOGY

Detecting an Embedded OS Infected with Conficker

On Patient Medical Monitoring Device

Executive Summary

Vigilant was engaged by a Healthcare Provider who was experiencing an extreme drop in bandwidth availability within their infrastructure. Their IT staff had been working the problem for two weeks without any detection or artifacts of the problem visible in their existing IDS/IPS or logs.

Upon starting the engagement, we placed CyberDNA sensors into locations that would give us the best collection ability of all traffic traversing their network. We place our collection devices very carefully as an attacker that is working remotely has to travel across the network at some point on their way out to the Internet. This allows for an interesting vantage point as no matter what way the attacker tries to change the way they look they still have to travel the network and are detectable if you are able to look at the data the right way. Vigilant's approach gives immediate visibility and can inform a customer in near-real-time of what is happening in the deepest parts of their network. It's like turning the lights on late at night to see if there is a monster in the room, although you hope there isn't one. Whether there is one or not you at least know and can take the appropriate action.

Within minutes of turning on Vigilant's CyberDNA service our analyst team was able to detect in an agent-less way that multiple heart monitor devices at a remote hospital location were running an embedded operating system infected with a botnet known as Conficker. They may never have known what was going on or that they were on heart monitors hooked up to patient however the attackers were using these devices to attack other locations on the Internet and brought down the hospitals network in the cross fire.

There were two problems here:

- Conficker was bringing their network down and
- The devices were running out of compliance operating systems and were connected to patients.

The Hospital had the devices removed and cleaned up the network, they also contacted their vendor as the embedded OS running on the Heart Monitor was not compliant. When you use third party software or devices like POS Systems, medical devices, etc., you are as the mercy of the levels of security the vendors have built into them.

This botnet attack was carried out by tactics that Vigilant detects every day. Without the visibility that Vigilant can bring it would have likely gone undetected in this victimized organization because their detection tools simply didn't see it.

"Vigilant CyberDNA can give you visibility into remote devices without needing to have any agents installed on them.

By doing this we can show you all software and operating systems running on your network.

We keep your vendors honest about security and reduce your risk and we do it 24/7."

Detection Of Embedded Operating Systems

When a system is placed into your environment that you do not have control over it becomes a potential risk. This is due to the fact that you can't control or see what the OS on a copier, a postage machine, medical devices etc. unless you have the ability to have full visibility into your network flow traffic and multiple data sources. Ultimately you need real time alerting from the Customer site including full packet capture, Heuristic, Anomaly, Signature and Intelligence based detections are analyzed at the customer site. Relevant event data is then sent to the CyberDNA Intel Center where Vigilant CyberDNA analysts review and classify alerts responding to the incident. CyberDNA Analysts will notify customers of Realized Threats as it pertains to escalation policy with specific remediation guidance.

The threat is resolved.

New Malicious traffic is sent to our correlation engine and sandbox for analysis.

Notifications are shared through Vigilant's Customer Portal where they are presented to the right point of contact in your organization.

New intelligence is sent directly to remote sensors across all CyberDNA customers for increased detection capability.

How It Was Resolved In This Case:

- The patient medical devices running embedded Windows 98 were first infected with Conficker behind the hospital firewall and were brought active as part of a firewall.
- The effects of the infected devices caused a large bandwidth draw on the Hospital network resulting in applications being rendered unusable.
- All IDS/IPS and detection methods available within the hospital network did not detect the Windows 98 OS nor the Conficker infection.
- CyberDNA was placed within the environment and immediately, in an agentless way, detected both the non-compliant OS running on the devices and that Conficker was the source of the Bandwidth draw.
- Vigilant's Analyst team notified the customer of the infected systems. The customer removed the systems from the patients, cleaned them and notified the manufacturer of the vulnerability.

About Vigilant

Vigilant Technology Solutions is a Cyber Security Firm based out of Cincinnati, Ohio providing Security Solutions and its Patent Pending CyberDNA Network Security Monitoring Solution to Customers in the Financial, Healthcare, Automotive, Manufacturing and Construction industries.

Vigilant has been operating since 2009, is privately held (and will remain that way) with no outside investment funding.

VIGILANT TECHNOLOGY SOLUTIONS

CyberDNA Solution Overview

Vigilant's CyberDNA Managed Network Security Monitoring Service leverages a distributed network of passive network security sensors and takes a different approach to monitoring customer infrastructure.

CyberDNA is a fully managed service with certified information security analysts pro-actively hunting for compromises and security risks in your organization. We serve as an extension to your existing team, notifying you in record time about the security events that matter, while providing clear and easy to understand recommended courses of action, so you can address the issue and get back to running your business.

CyberDNA is a fast and affordable Enterprise Security Monitoring Solution. After a 15-minute installation, you can have a detection capability that rivals many of the leading security conscious organizations. We know because our team has experience protecting some of the largest Fortune-500 global enterprises in the world.

CyberDNA will:

- Give your IT Staff more time: CyberDNA will give them specific, timely information that reduces the amount of time they need to search for issues and helps them fix the problem fast.
- Minimize your incident costs by finding attacks when they happen, not the industry average of 205-240 days after the fact.
- Give you access to a Cyber Security team at a fraction of the cost.

CyberDNA offers:

- US Based Analysts – Fully Vetted
- Unlimited Incident Response (Unique to Vigilant)
- 24x7 Full Forensic Analysis, Network DVR (PCAP) and Detection
- Full Logging and Distributed Sensors
- Elite Analyst team with White Glove Approach with full Threat Hunting
- Invisible and Undetectable protection
- 4 Free Quarterly Assessments
- No hardware to purchase
- A sentry making sure that all your defenses are working.

Vigilant Analysts

Many of our analysts are GIAC certified and carry multiple industry certifications. Our backgrounds range from small business to global Fortune-10 and span numerous industries including Finance, Healthcare, Automotive, Manufacturing, Aerospace & Defense, and Telecommunications.

Our analysts are all US Citizens, many of which hold Secret or TOP Secret US Department of Defense security clearances, and undergo extensive background, reference, and drug screen checks.

Managed Endpoint:

Vigilant's Managed Endpoint brings direct containment and remediation to your endpoints.

Features:

- Uses a broad suite of McAfee Products
- Agent points to Vigilant for added threat intelligence beyond McAfee default
- Integrates with CyberDNA for Host Verification
- Managed Host Based Firewall
- Dynamic Application Containment
- Machine Learning with Dynamic File Analysis
- Global File Reputation Checking
- Managed Client Web Control
- Endpoint Detection & Response (EDR) Capability
- Remotely investigate & respond by our Analysts
- Active Response and Remediation
- Supports all cloud environments
- Virtualization friendly, supports all major hypervisors
- Cross platform - supports all major Operating Systems

Combined with CyberDNA, Managed Endpoint provides the ability to determine the trusted nature of devices on your infrastructure 24x7 with a localized containment strategy.

Assessment Scope and Approach

The CyberDNA trial is an opportunity for customers to try our service for free to make sure they absolutely love it before they buy it. Our engineers first meet with your team to decide on the best location to install our sensor into your network. The sensor is then provisioned and sent to your site. After installation our Analysts immediately go to work inspecting your traffic for threats. If we find any active threats, we'll contact you immediately. Otherwise, on the 5th day of the trial we compile a report, which encapsulates our most noteworthy findings.

It's truly amazing the level of visibility and insights one can obtain over their network by passive monitoring. This is why we also make a significant amount of information from your sensor(s) available to you in real time on our Customer Portal.

The portal is a great place to see what versions of software are running in your environment, and which ones are out of date. You can know without a doubt when your company policies and regulatory requirements are not being met. You can even track your organization's true bandwidth usage, and explicit content usage. The customer portal is your one stop shop for managing tickets and incidents, and keeps you on the pulse of your overall security posture.

Deciding to retain our services beyond the trial is as simple as "Yes". We simply convert your existing sensor to a permanent one and immediately go to work fine-tuning it to your specific network environment and organizational monitoring needs. There's no time wasted on deploying replacement equipment, or additional software licenses to hassle with.

Contact LANtelligence team to learn how to get your 5-day free CyberDNA trial

866-510-8547

contactme@lantelligence.com