Cyber adAPT

Network Threat Detection Defined

INSPECT | DETECT | RESPOND

The Threats are Real

Hackers compromise an enterprise's computer network every 39 seconds. Ransomware attacks have nearly doubled in 2019, crippling businesses, health care organizations and government entities. Malware damage has increased, on average, to $2.4 million per attack.

Cybercrime is a $400 billion business, more profitable than the global illegal drug trade. According to Inspired eLearning, 73% of hackers say that traditional firewall and antivirus security is now irrelevant. Most companies' current methods of protection are no longer capable of providing a sufficient level of security.

The best way to protect yourself from modern-day attacks is to detect them when they first appear within your network. At Cyber adAPT, identifying, contextualizing, prioritizing and alerting you to malicious activity before it does harm is what we do.

Technology At-a-Glance

NTD works transparently with other technologies found in a layered security solution, strengthening existing security portfolios.

Additionally, working in conjunction with a cloud-based environment, our solution provides threat intel and machine learning for secondary alarm generation.

These capabilities include:

- Immediate threat detection
- Automated actionable alarm notifications
- Scales to all network sizes and configurations
- Network metadata analysis
- Threat research team
- Custom threat intelligence detection
- Cloud-based AI and Machine Learning
- Investigative services
- Full packet capture (optional feature)

For additional investigative support, Cyber adAPT offers access to our cybersecurity professionals through an optional service agreement.

Contact us today for a comprehensive demonstration: Call at +1 888.666.3001, visit our web site at www.cyberadapt.com, or email at info@cyberadapt.com.

Can you afford not to know?

Cyber adAPT's best in class approach uses patented software to identify the infiltration, scanning and exploitation of an enterprise's network. Cyber adAPT's Network Threat Detection platform (NTD) provides immediate, contextual information that categorizes the risk and urgency of the threat. With comprehensive visibility combined with speed-to-detection, security teams are able to respond immediately to effectively and efficiently remediate attacks before real damage occurs.

Cyber adAPT's NTD passively watches all network traffic activity, 24/7/365, without impacting latency, throughput or performance. Updated hourly with the latest intelligence and logic, NTD keeps watch over all your network traffic – between the perimeter and the end-points and between the end-points themselves.

NTD enhances your cybersecurity posture

NTD enhances your cybersecurity infrastructure, giving you deeper visibility to attacks as they begin. Cyber adAPT's NTD platform seamlessly integrates with SIEMs, firewalls and end-point agents to ensure clear visibility and central management.

Cyber adAPT provides immediate detection upon installation, with no "baselining" required. Saving time and ensuring value from day one. Automated notifications are sent moments after discovery. These notifications provide one-click access to alert-data that prioritizes real threats and offers clear, concise and actionable instructions for incident response 24/7/365. Easy to deploy, use and maintain. Cyber adAPT's NTD automates the most tedious and time-consuming processes.

Cyber adAPT NTD provides complete visibility of and protection from threats that can cost you millions of dollars. Contact Cyber adAPT now to learn more and try NTD in your network.

The scale and costs of breaches are growing exponentially.

Year	People Affected	Company Breached	Cost (USD)
2016	25 Million	Uber	$148 Million
2017	146 Million	Equifax	$1.4 Billion
2018	87 Million	Facebook	$1.63 Billion
2019	104 Million	Capital One	TBD

Cyber adAPT
Network Threat Detection Defined