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 nearly doubled in 2019, crippling businesses, health care organizations and government entities. Malware damage has increased, on average, to $2.4 million per attack. According to Inspired eLearning, 73% of hackers say that traditional firewall and antivirus security alone do not provide a sufficient level of protection. As such, most companies' current methods of protection are no longer capable of providing adequate security in line with today's growing threats.

The best way to protect against modern-day attacks is to detect them when they first appear within the network. At Cyber adAPT, identifying, contextualizing, prioritizing and alerting an enterprise 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, Cyber adAPT's solution provides threat intel and machine learning for secondary alarm generation.

NTD capabilities include:

- Immediate threat detection
- Automated actionable alarm notifications
- Ease of installation
- Scalability to all network sizes and configurations
- Network metadata analysis
- Custom threat intelligence detection
- Unique sources of threat intel
- Cloud-based AI and Machine Learning
- Full packet capture (optional feature)

For additional investigative support, Cyber adAPT offers access to a team of 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.

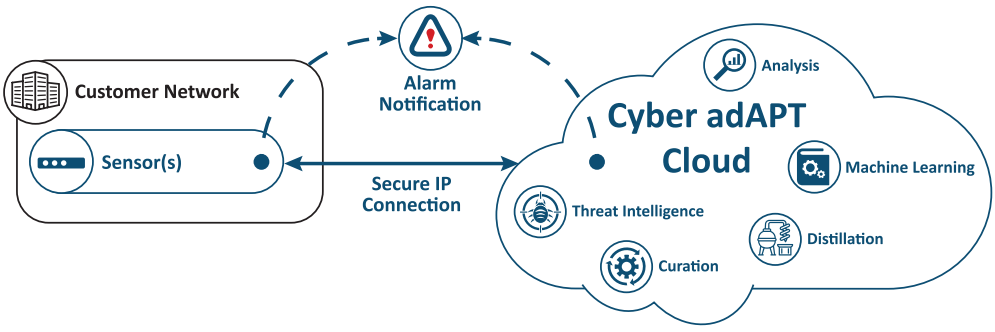
Cyber adAPT's NTD passively watches all network traffic activity, 24/7/365, without impacting latency, throughput or performance. Automatically updated hourly with the latest threat intelligence and logic, NTD keeps watch over all network traffic – between the perimeter and the end-points and between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

NTD enhances cybersecurity posture

NTD enhances cybersecurity defenses, giving 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, thus 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 an enterprise millions of dollars. Contact Cyber adAPT now to learn more and try Cyber adAPT's network threat detection today.



Cyber adAPT

Network Threat Detection Defined