GARLAND TECHNOLOGY
See every bit, byte, and packet®

+ NEXTRAY

Network TAPs and Network Detection & Response

Security Operation Center (SOC) teams successfully hunt, investigate, and remediate threats.

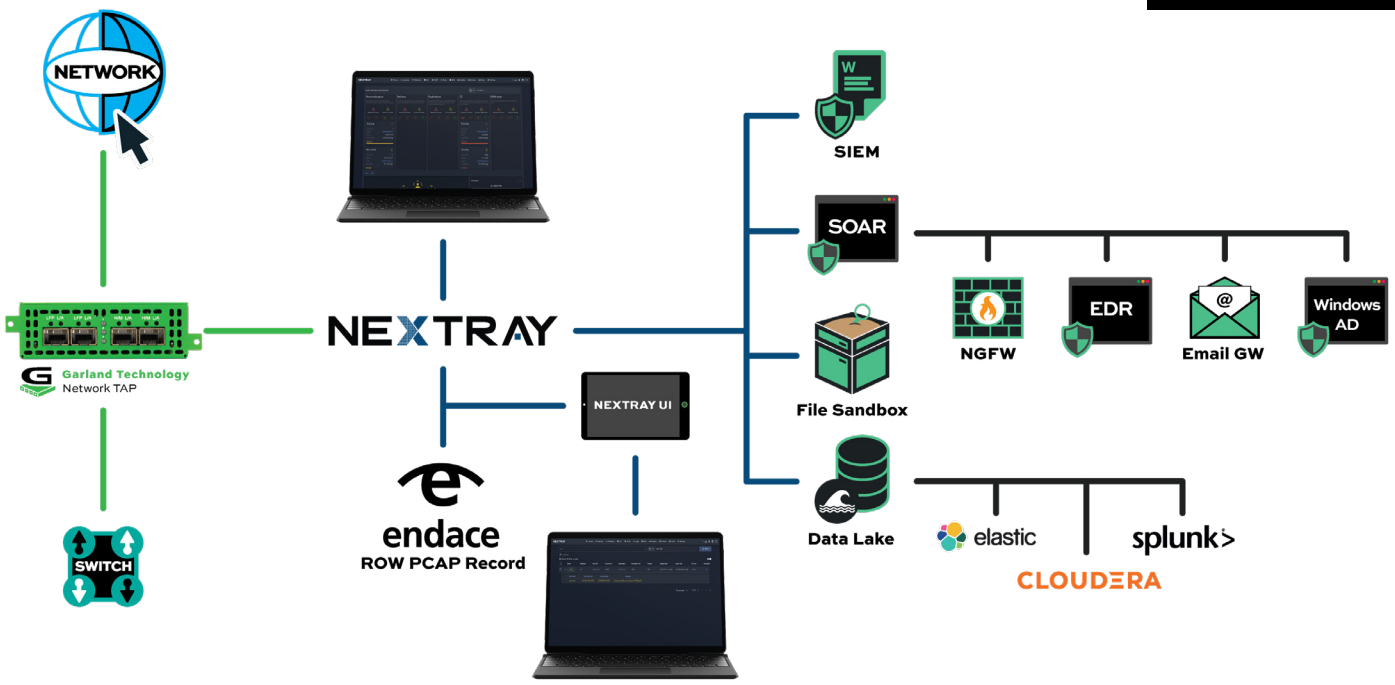
PROBLEM #1

Command & Control encompasses a variety of techniques employed by attackers to connect to targeted network systems under their control. To evade discovery, enemies frequently attempt to mimic routine, expected communications. Depending on the structure and defenses of the victim's network, an adversary may employ a variety of covert techniques to establish command and control. For example, as of early 2023 the MITRE ATT&CK architecture enumerates sixteen separate command and control methods, each having a number of sub-techniques that have been used in past hacks.

SOLUTION #1

Connecting NextRay AI Network Detection & Response (NDR) systems to networks, clouds, endpoints, and applications using a Garland Technology Network TAP ensures NextRay AI NDR delivers on its promise of early stage threat detection and advanced response capabilities. NextRay AI NDR allows security personnel to:

- Identify freshly created network connections sent or received by untrusted hosts.
- Analyze traffic patterns and inspect packets associated with protocols that deviate from the expected.
- Monitor network data streams for anomalies and identify suspicious behavior that generally utilizes a network.
- Capture difficult to-detect beacon behavior using Artificial Intelligence.



PROBLEM #2

Exfiltration refers to the methods adversaries may employ to take information from a network. Once adversaries have obtained data, they frequently package it to prevent detection while discarding it. Compression and encryption may be included. Typically, techniques for extracting data from a target network involve transferring it across their command and control channel or an alternate channel, and may also involve imposing transmission size restrictions.

When a data breach leads to identity theft or the violation of government or industry compliance standards, the offending organization may face fines, lawsuits, reputational harm, and even the revocation of its business license.

SOLUTION #2

Using a Garland Network TAP, NextRay AI systems passively collect network communications and deliver it to a unified detection and response platform so it's easier to take focused and strategic action; often with one-click resolution. NextRay AI NDR allows security personnel to:

- Recognize an adversary's behavior in which data is divided into fixed-size chunks rather than full files, or in which packet sizes are restricted below specific thresholds.
- Identity the pathways attackers can steal data by revealing leaking data over an existing command and control channel.
- Identify freshly created network connections sent or received by untrusted hosts.
- Make attackers' behavior visible particularly when attackers schedule data theft to occur only at specific times or intervals.

HOW IT WORKS

1. Installed between two network devices network TAPs from Garland Technology are connected to the IT network.
2. The NextRay AI NDR connects to the network TAPs as an out-of-band security tool.
3. Network TAPs copy full-duplex traffic and send copies to the NextRay AI NDR.
4. NextRay AI NDR's multi-method, automated threat detection capabilities detect threats before they become destructive with speed and efficiency. The sensor provides powerful, continuous, and autonomous analytics and is centralized with AI Engine.
5. NextRay AI NDR's comprehensive and speedy integration of SOAR and SIEM standardizes your SecOps procedures, enabling collaboration and automation, expediting investigations, and decreasing reaction times.
6. High-fidelity alerts from the NextRay AI NDR help prioritize the severity of incidents and built-in orchestration automates routine tasks so teams can focus on more critical initiatives.

About NextRAY AI

NextRay AI provides the most robust artificial intelligence solutions for cyber security analyst and IT professionals, empowering them to comprehend intricate network patterns to identify, prevent, and counter cyber threats. NextRay AI developed its pioneer solution incorporating advanced AI and machine learning algorithms, a comprehensive and highly-efficient open-source framework that delivers a broad, real-time understanding of network data traffic. Visit nextray.ai for more information.

About Garland Technology

Garland Technology is a US based manufacturer of network TAPs, Network Packet Brokers, and Inline Bypass solutions. We engineer, manufacture, and support our hardware solutions in Richardson, TX. Since 2011, we've been helping companies' network monitoring and security tools deliver on their promise of performance and protection because we reliably deliver all of the data the tools need to shine. For help with projects large and small, including installations, upgrades, and streamlines, or to learn more about the inventor of the first bypass technology, visit GarlandTechnology.com or @garland-technology-llc

Have Questions?
sales@garlandtechnology.com | +1 716.242.8500
GarlandTechnology.com/nextray

See every bit, byte, and packet®

06.19.23