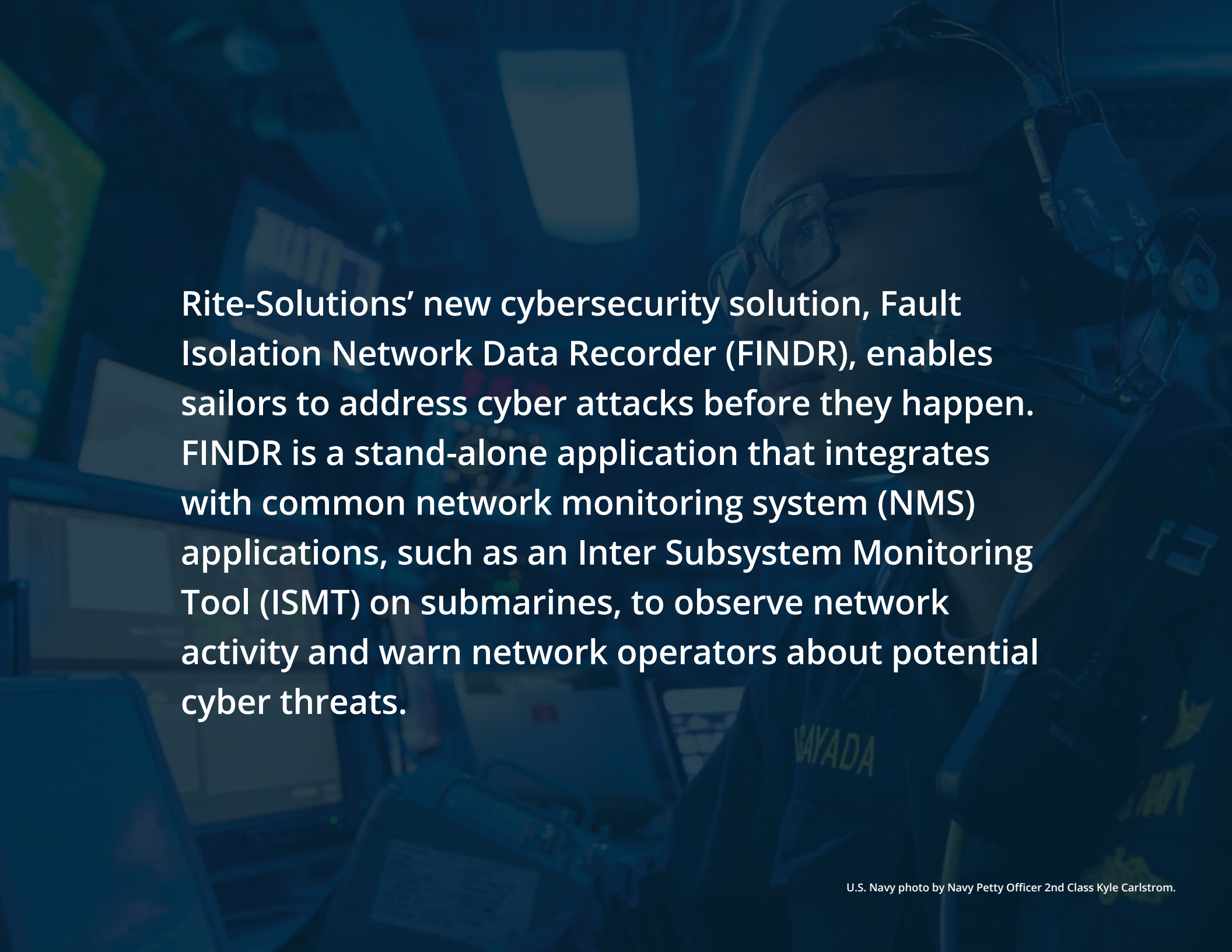
rite SOLUTIONS

FINDR™

Leverage the power of artificial intelligence to proactively prevent cyber attacks.

U.S. Navy photo by Mass Communication Specialist 3rd Class Ignacio D. Perez.



Rite-Solutions' new cybersecurity solution, Fault Isolation Network Data Recorder (FINDR), enables sailors to address cyber attacks before they happen. FINDR is a stand-alone application that integrates with common network monitoring system (NMS) applications, such as an Inter Subsystem Monitoring Tool (ISMT) on submarines, to observe network activity and warn network operators about potential cyber threats.

U.S. Navy photo by Navy Petty Officer 2nd Class Kyle Carlstrom.

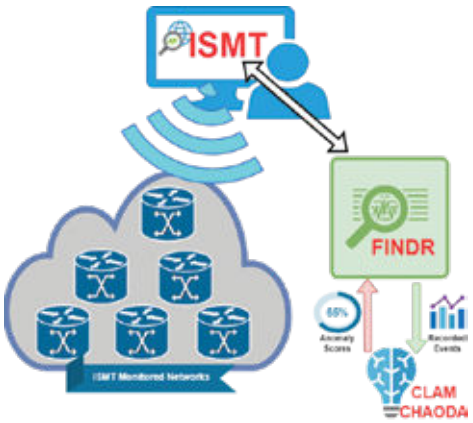
FINDR™

Network Monitoring Cannot Prevent Cyber Threats

The Navy's networks are constantly under attack. A 2022 Forbes article states the government/military faces the second-highest number of average weekly cyber attacks, up 47% from 2021. Current NMS tools alert operators to network events in real-time. Some events could be cyber attacks. However, a reactive approach to cyber threats could be too late. Systems could be compromised, communications interrupted, missions jeopardized, and sailors put in harm's way.

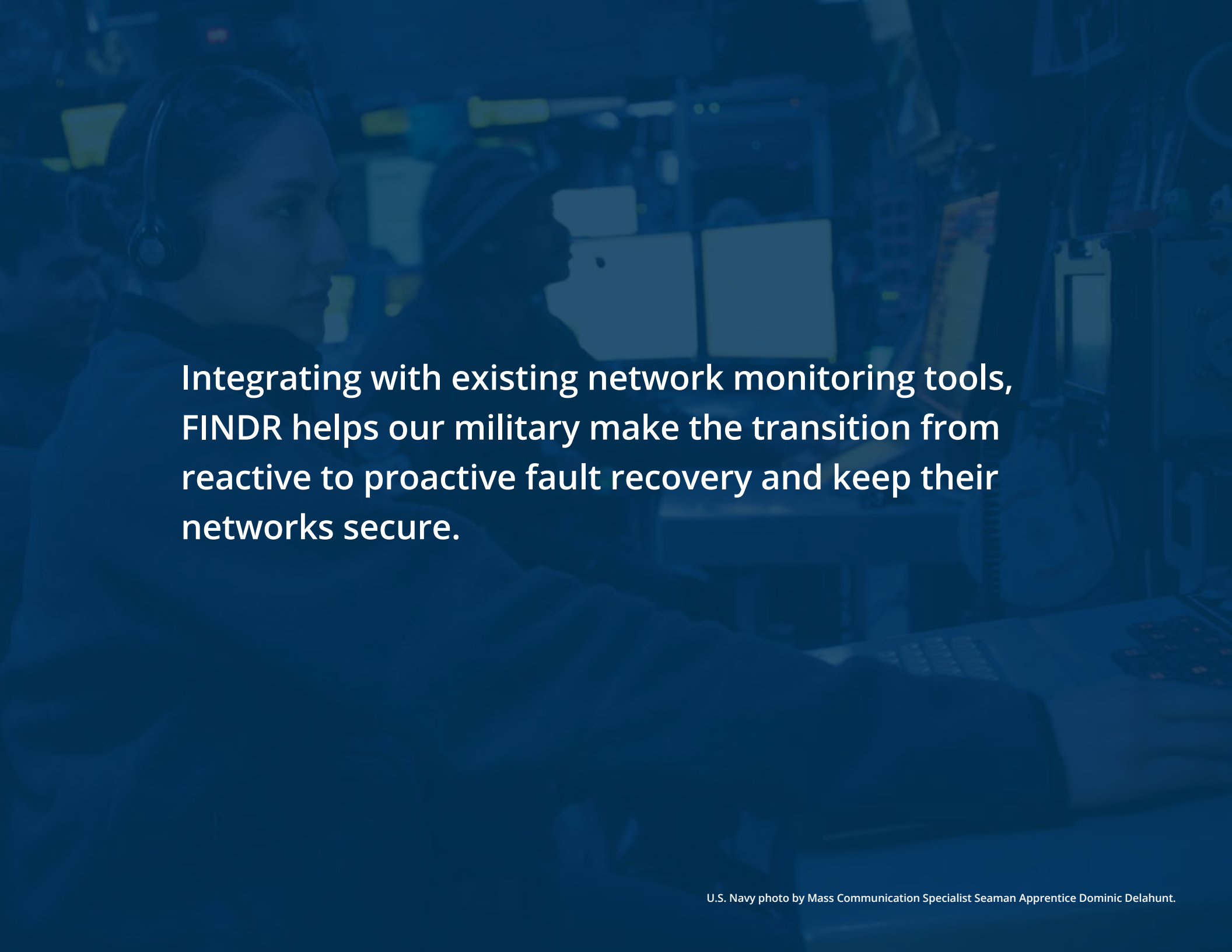
FINDR Takes a Proactive Approach to Cybersecurity

FINDR helps network operators get ahead of the curve and take a proactive approach to cybersecurity. By detecting anomalies in network event data, FINDR prompts operators to check the network and take preventative measures before a cyber attack occurs, allowing our warfighters to continue their mission safely.



FINDR integrates with monitoring systems, like an ISMT, to send network event data to an AI model that detects network anomalies and potential cyber attacks. FINDR sends proactive alerts back to the ISMT.

U.S. Navy photo by Mass Communication Specialist 2nd Class Justin Stack.



Integrating with existing network monitoring tools, FINDR helps our military make the transition from reactive to proactive fault recovery and keep their networks secure.

U.S. Navy photo by Mass Communication Specialist Seaman Apprentice Dominic Delahunt.

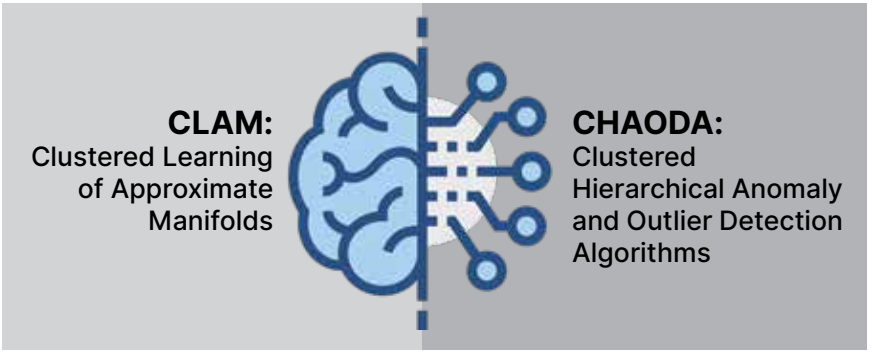
FINDR™

FINDR's AI-Powered Model Identifies Network Anomalies to Prevent Cyber Attacks

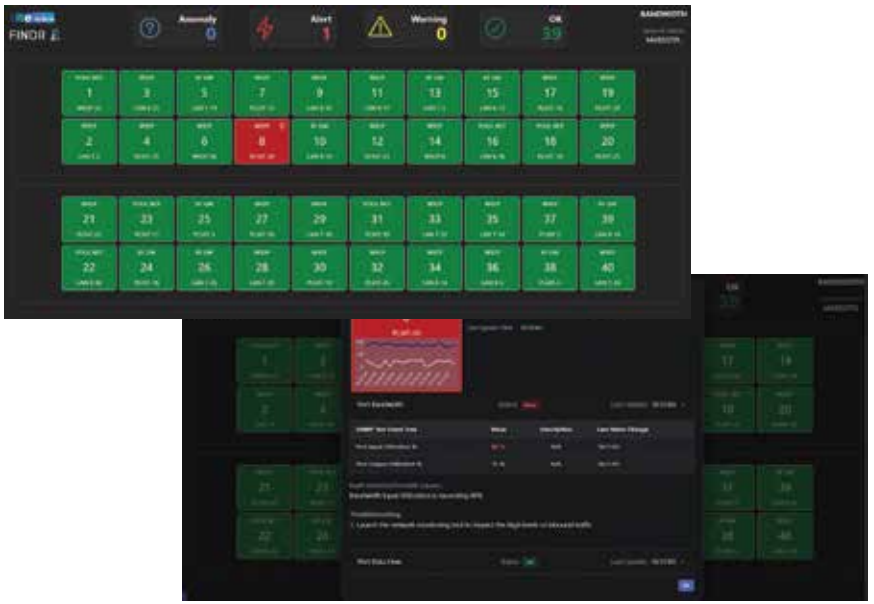
FINDR augments existing network applications that sailors are already familiar with, which reduces the training burden on our military. Operators continue working in the environment in which they are trained and versed. FINDR Takes a Proactive Approach to Cybersecurity.

Behind the scenes, FINDR records network events and incidents from an NMS and streams the data to a state-of-the-art network anomaly detection model called CLAM-CHAODA. The AI model uses a multi-algorithmic approach to compute the probability of anomalies within the transmitted data.

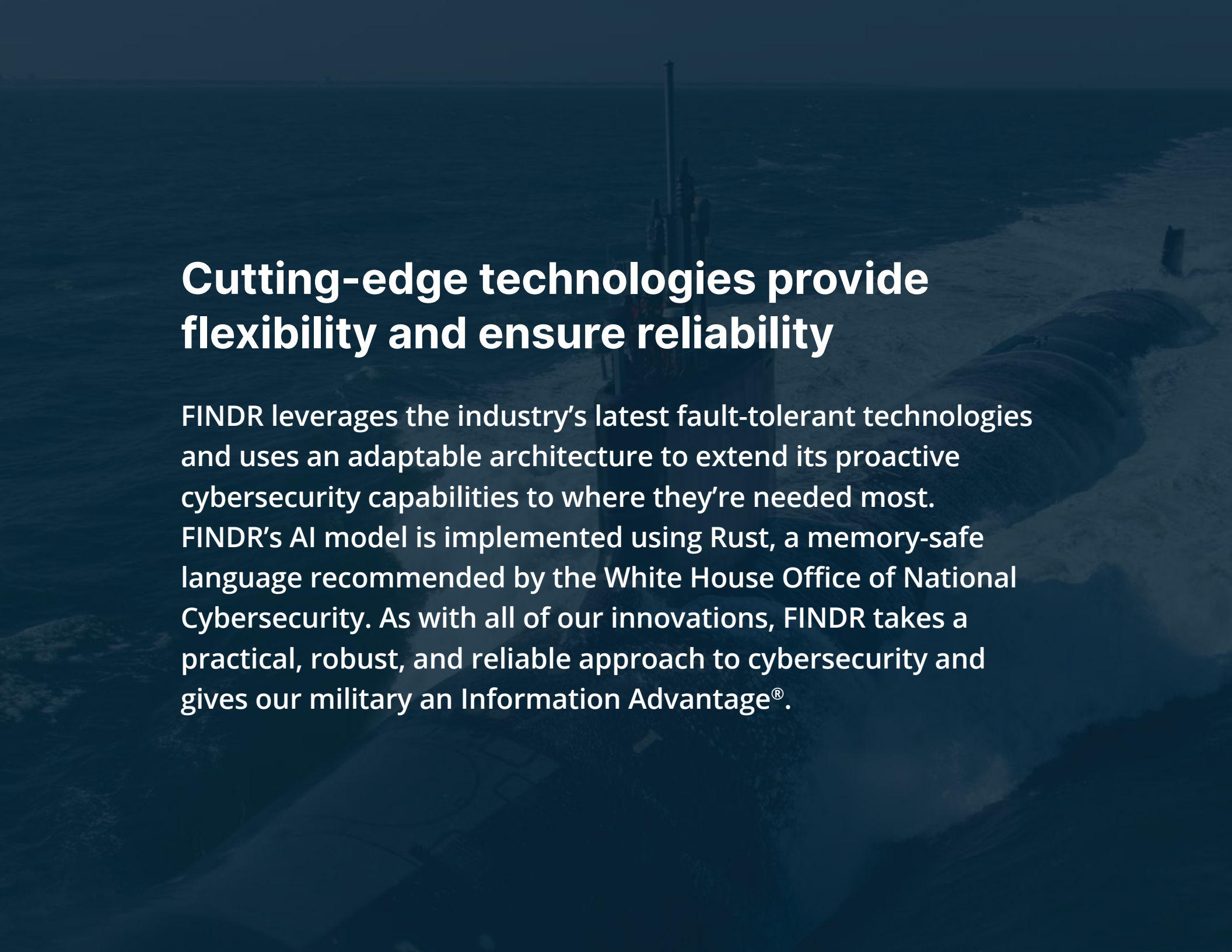
When anomalies are detected, FINDR relays proactive network fault alerts to the operator through the NMS so they can take preventative action to protect the network's security. For example, the NMS may flag a specific switch port, prompting the operator to tighten access control, or determine if the network has changed from what is expected, such as the addition of a new unrecognized device.



CHAODA is a set of algorithms used by CLAM to examine real-time NMS data streamed by FINDR. The CLAM-CHAODA model identifies issues and outliers in the data and assigns an anomaly score. FINDR sends the anomaly score to the NMS to proactively alert operators about network issues that could potentially be cyber attacks.



An NMS displays the overall status of a network switch (above image). Selecting a warning or alert will provide additional information and a recommendation to correct the issue (below image).



Cutting-edge technologies provide flexibility and ensure reliability

FINDR leverages the industry's latest fault-tolerant technologies and uses an adaptable architecture to extend its proactive cybersecurity capabilities to where they're needed most. FINDR's AI model is implemented using Rust, a memory-safe language recommended by the White House Office of National Cybersecurity. As with all of our innovations, FINDR takes a practical, robust, and reliable approach to cybersecurity and gives our military an Information Advantage®.

Proven, Through Partnerships and Peer-Reviews

FINDR is the result of a collaborative effort with the University of Rhode Island (URI), sponsored by the Office of Naval Research (ONR), whose mission is to partner with academia and industry to deliver critical, cutting-edge capabilities for our sailors.

FINDR's roots can be found in two Innovation Vouchers awarded by the Rhode Island Commerce Corporation, which supported AI research on anomaly detection at URI. That work became the foundation of an ONR grant that successfully demonstrated that our approach is not only as good as other detection algorithms but also faster and does not require expensive AI-specific hardware. The results were shared at the IEEE Big Data Conference in 2021 and have since been peer-reviewed and published in academic circles.

U.S. Navy photo by Mass Communication Specialist 1st Class Mark D. Faram.

rite SOLUTIONS

Corporate Headquarters
One Corporate Place
2nd Floor
Middletown, RI 02842
401.847.3399

185 South Broad Street, Suite 303
Pawcatuck, CT 06379

1220 12th Street SE
Washington, DC 20003

16156 Dahlgren Road, Suite 102
Dahlgren VA 222485

Scan to learn more.

rite-solutions.com