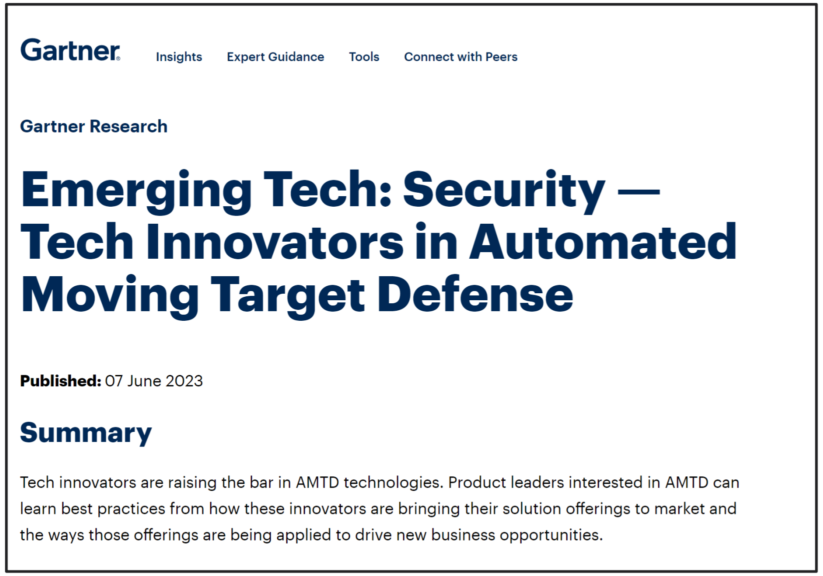
Zero Trust, Future-Proof, Application Networking Protected by an AMTD

DISA TEM
June 11, 2025

Tom McNamara
tom@hopr.co

Hopr.co Company Overview

- ❑ Who is Hopr.co?
  - A cybersecurity innovator focused on proactive defense.
  - Mission: To fundamentally change the cybersecurity paradigm from reactive detection to proactive disruption.
  - Specializing in Automated Moving Target Defense (AMTD) and advanced Zero Trust application networking.
- ❑ Why AMTD?
  - Traditional defenses (firewalls, EDR, even static Zero Trust) struggle against sophisticated, persistent adversaries.
  - The "static nature of the enterprise network" is a recognized vulnerability (DISA's problem statement).
  - AMTD introduces unpredictability, making the adversary's job exponentially harder and more costly.
- ❑ Our Core Philosophy:
  - Continuous change as a defensive weapon.
  - Decentralized access control managed by trusted workloads.
  - Simplifying complex security challenges for critical infrastructure and multi-cloud.
- ❑ *Key Differentiator: Preemptive, automated disruption at the workload level. "**Zero Trust by the Transaction**".*
  - *Analogy: Think of our approach like constantly changing the locks and moving the doors to enter a high value building, making it impossible for an intruder to know how to get inside.*



Gartner Research

Emerging Tech: Security — Tech Innovators in Automated Moving Target Defense

Published: 07 June 2023

Summary

Tech innovators are raising the bar in AMTD technologies. Product leaders interested in AMTD can learn best practices from how these innovators are bringing their solution offerings to market and the ways those offerings are being applied to drive new business opportunities.

Problem

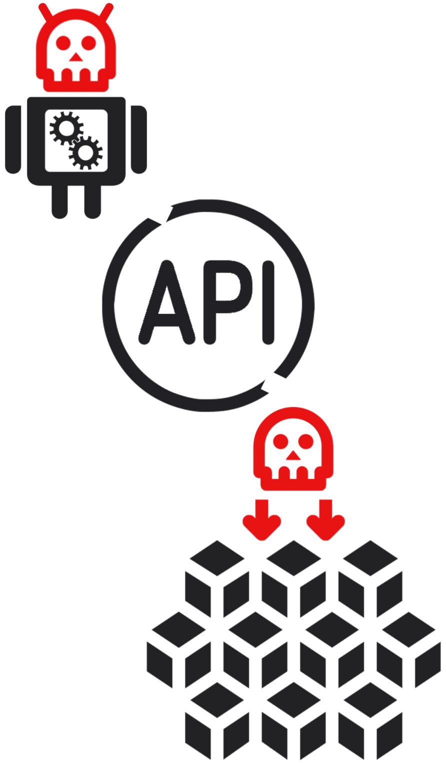
□ Addressing the Static Enterprise Network

- DISA's Challenge:

"DISA is looking for solutions to address the static nature of the enterprise network. How can DISA detect bad actors and bots and utilize deception technology to impose a cost on the adversary through interacting with false targets, providing time and space for operators to remediate the revealed or discovered vulnerability?"

□ Our Answer

- Hopr.co's AMTD directly solves this by turning static targets into dynamic, moving ones, leveraging deception at the identity and access layer.



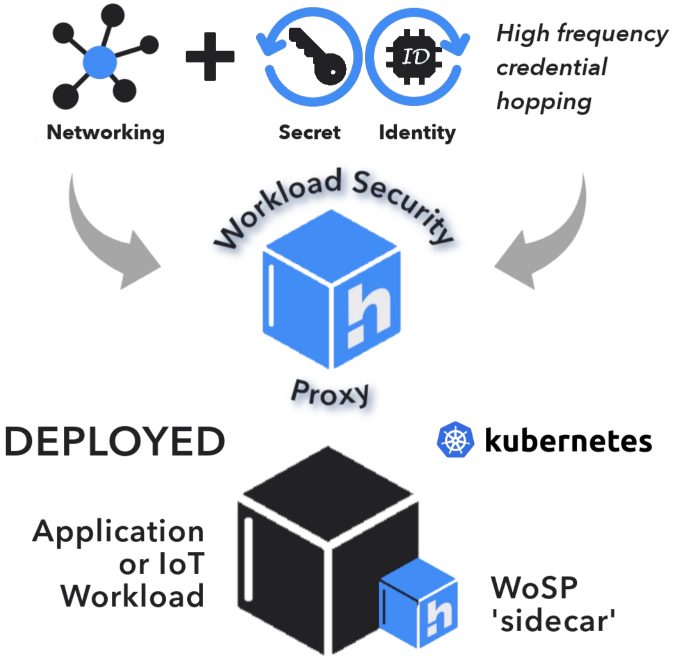
Think of this as being similar to Layer 2 "frequency hopping"

What is an Automated Moving Target Defense (AMTD)

- Making the target unpredictable: AMTD continually changes the attack surface to disrupt adversary operations.
- Shifts from detection-and-response to preemptive disruption.
- Imposes significant computational and cognitive cost on the adversary.

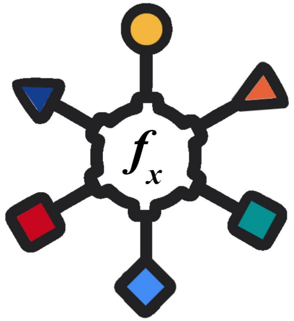
❑ Hopr.co’s Cloud Native AMTD solves DISA’s Problem

- Mechanism: Our Workload Security Proxy (WoSP) automates the rotation of workload access credentials at a high frequency
- Detection & Deception: Any attempt by a bad actor or bot to use a stolen, outdated credential immediately fails. Realtime detection of attempted unauthorized access.
- Imposing Cost: Adversaries cannot establish persistent footholds or perform lateral movement because valid credentials are constantly changing. Their reconnaissance, C2, and exploitation efforts are continuously invalidated and require constant, costly re-adaptation.



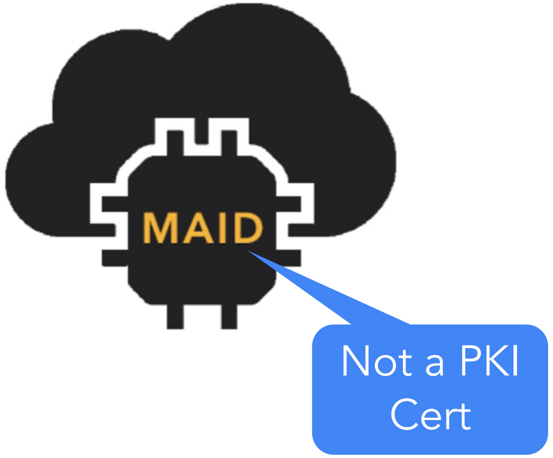
Three Hopr Innovations Create the AMTD

Codes Hidden In Plain Sight (CHIPS™) uses algorithms to generate identical secrets at two workloads



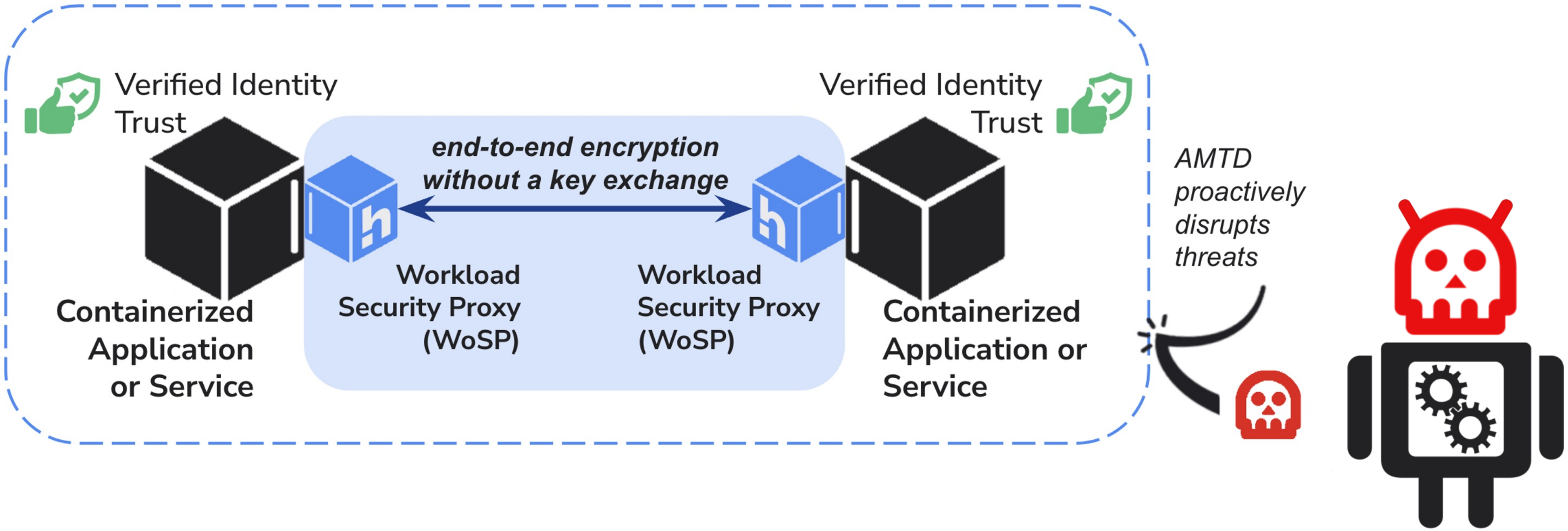
Synchronous Ephemeral Encryption (SEE™) Protocol
(Zero Trust & Future-Proof Encryption)

Machine Alias ID (MAID™)
Dynamic Workload Identity Verification (Enhanced Zero Trust)



Not a PKI Cert

Hopr's Cloud Native AMTD Shrinks the Attack Surface


Verified Identity Trust
Containerized Application or Service
end-to-end encryption without a key exchange
Workload Security Proxy (WoSP)
Workload Security Proxy (WoSP)
Verified Identity Trust
Containerized Application or Service
AMTD proactively disrupts threats

Full application layer protection with a new AMTD at every communication session.

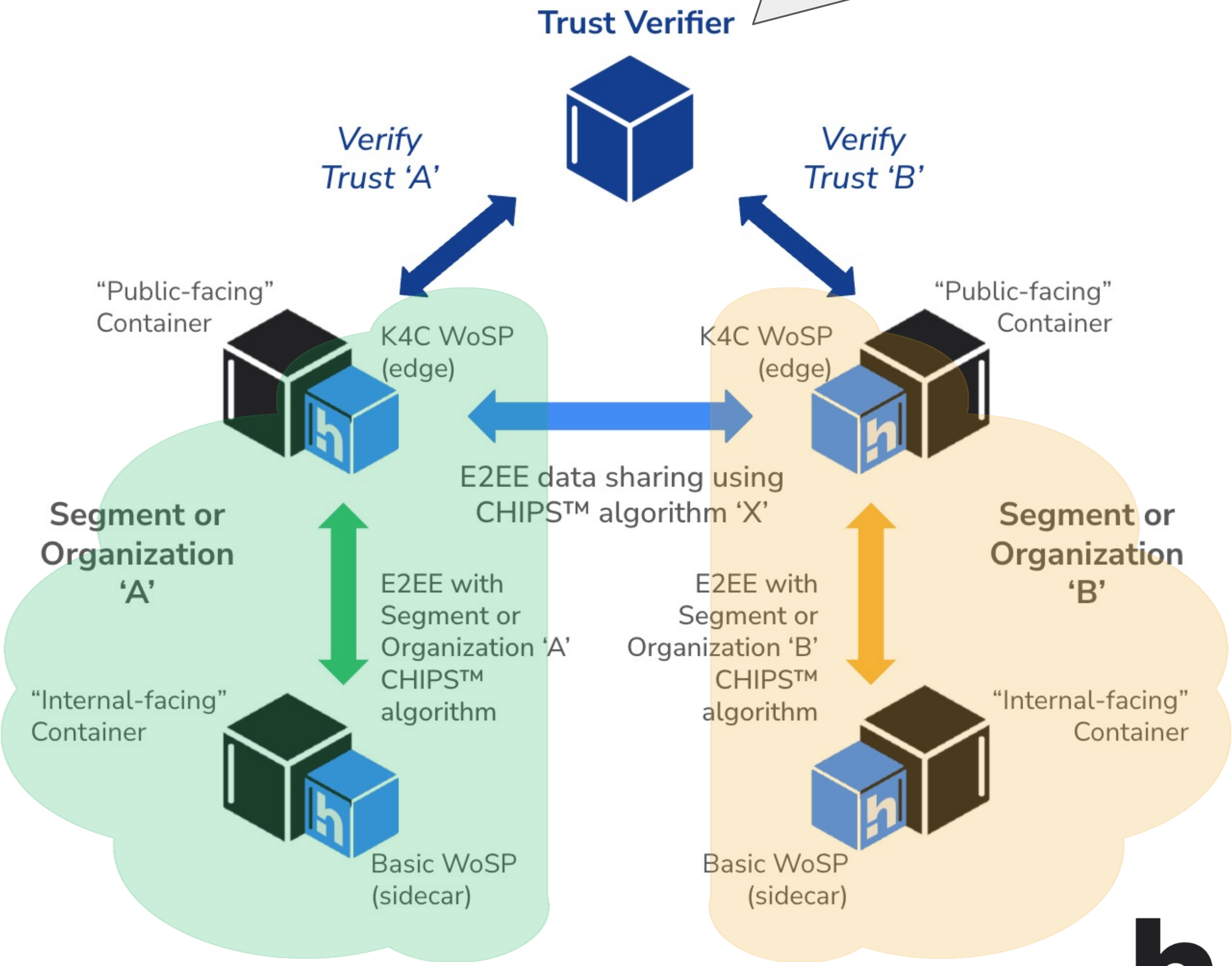
Only trusted application workloads with verified identities can access each other and exchange data

Kerberos for the Cloud - The K4C WoSP

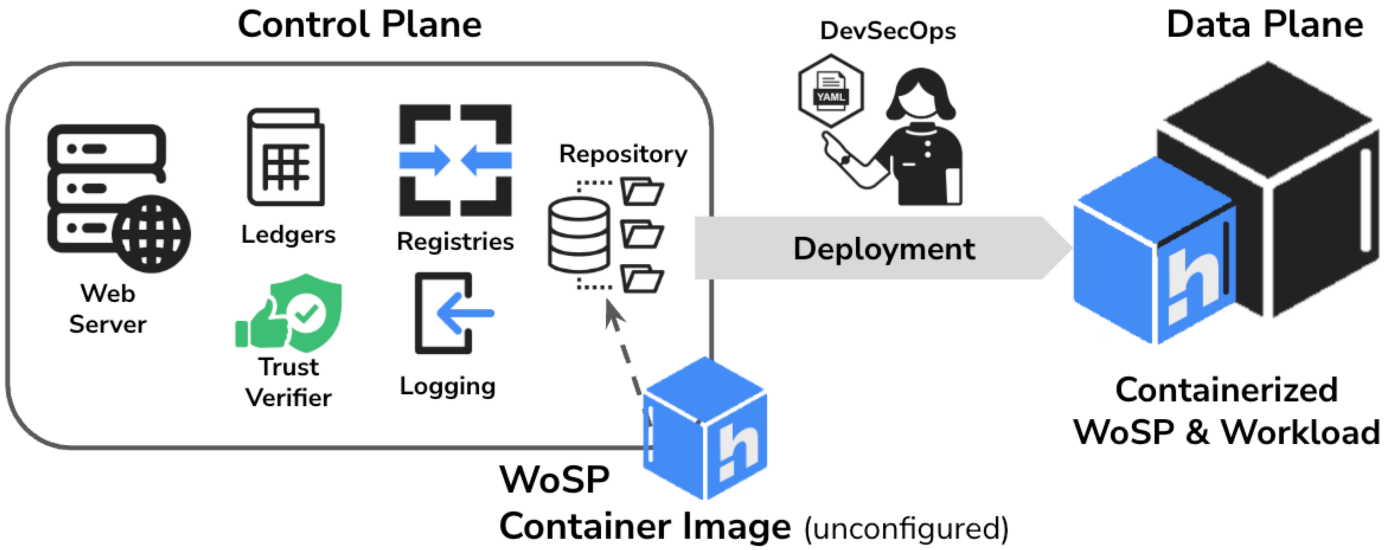
A WoSP with additional capabilities to establish trust before connecting with third party workloads.

- Organizations with public facing workloads, such as in an ecosystem, would configure WoSPs differently.
- Hopr, as identity provider is the trust verifier for each organization.
- In the K4C protocol, Hopr separately verifies trust of each third-party workload.
- If trusted, Hopr issues each workload a one-time CHIPS™ Algorithm ID for their direct session.

Verifier provides each WoSP a one-time CHIPS™ Algorithm when trust is verified


Trust Verifier
Verify Trust 'A'
Verify Trust 'B'
"Public-facing" Container
K4C WoSP (edge)
K4C WoSP (edge)
"Public-facing" Container
E2EE data sharing using CHIPS™ algorithm 'X'
Segment or Organization 'A'
Segment or Organization 'B'
E2EE with Segment or Organization 'A' CHIPS™ algorithm
E2EE with Segment or Organization 'B' CHIPS™ algorithm
"Internal-facing" Container
"Internal-facing" Container
Basic WoSP (sidecar)
Basic WoSP (sidecar)

Operational Efficiency



Cloud-Native & Cloud agnostic Deployment

- Mechanism: Deploys as an overlay (WoSP) without requiring any changes to existing application code, APIs, or infrastructure.
- Benefit: Rapid deployment across diverse environments (on-prem, hybrid cloud, multi-cloud, tactical edge) – crucial for DISA's global footprint and modernization efforts.
- Time & Space: Quick deployment means immediate imposition of cost on adversaries, buying time for remediation.

Simpler and faster to implement than Workload Identity Federation

Direct Application to DISA's Missions

□ National Leader Command Capabilities (NLCC) & Nuclear C3 (NC3):

Challenge: Protecting the most critical, often legacy, C2 systems from sophisticated nation-state attacks.

Hopr.co Impact: Dramatic increase in resilience, assured integrity and confidentiality even under active attack. Prevents attackers from gaining access to these highly sensitive systems.

□ AI Attack Prevention & AI Security:

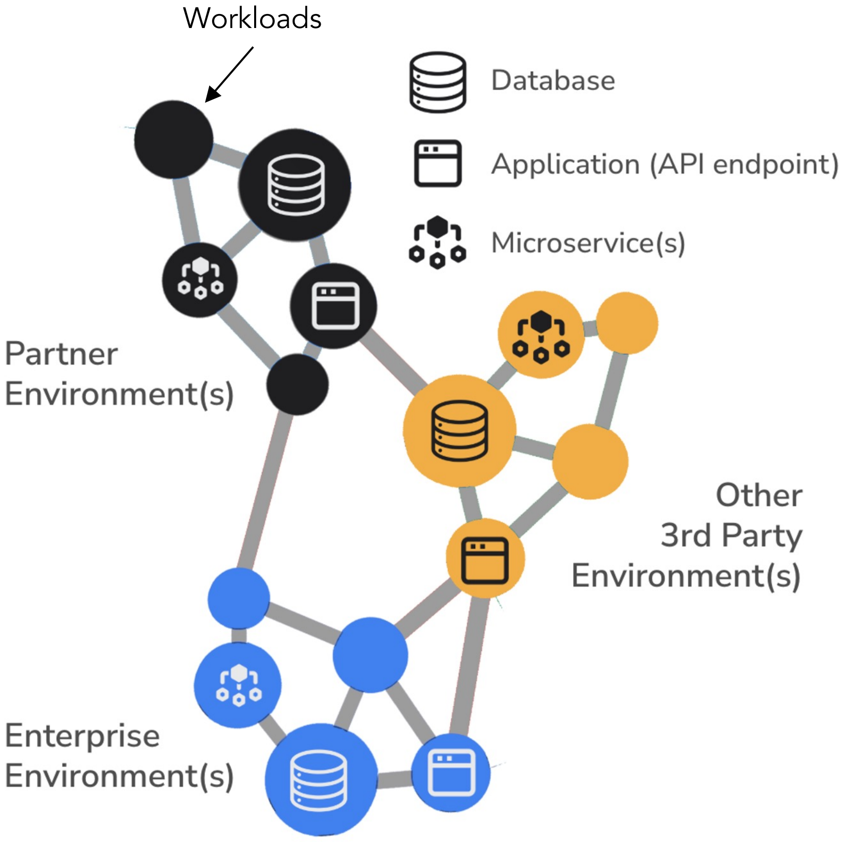
Challenge: Countering AI-powered reconnaissance, exploitation, and securing DISA's own AI/ML models.

Hopr.co Impact: Disrupts AI-driven attacks. Secures the data and runtime environments for DISA's AI/ML initiatives, protecting against data poisoning and model manipulation.

□ Multi-Organizational Context (US & Partner Nations):

Challenge: Securing communications and data sharing across disparate networks with varying security postures.

Hopr.co Impact: Provides a consistent, dynamic, Zero Trust security layer that enables seamless coalition app networking without requiring a complete overhaul of partner systems. Enables secure timely C2 for CJADC2.


Workloads
Database
Application (API endpoint)
Microservice(s)
Partner Environment(s)
Other 3rd Party Environment(s)
Enterprise Environment(s)

Multi-cluster, Multi-cloud, Multi-domain C2 Application Networking at Layer 7

Summary of Benefits for DISA

□ Proactive Disruption: Forcing the adversary to continuously adapt and re-recon, consuming their resources and preventing persistent footholds.

□ Real-time Detection: Immediate identification of unauthorized access attempts via failed credential usage.

□ Reduced Adversary Dwell Time: By invalidating stolen credentials and preventing lateral movement, we shrink the window for successful exploitation.

□ Buying Time: The constant change and disruption provide operators with critical time and access rejection provides actionable intelligence to remediate discovered vulnerabilities before significant damage occurs.

□ Enhanced Resilience: Greater assurance of mission continuity for critical systems even in a contested environment.

Demo Introduction

A recorded demo of two Workload Security Proxies protecting data and rejecting untrusted access

Hopr WoSPs in Operation

Questions

Tom McNamara
tom@hopr.co

Thank You

Tom McNamara
tom@hopr.co