carahsoft

NOTHREAT

AI has transformed the attack.

Nothreat is the defense built for it.

Thank you for your interest in exploring this content.

Carahsoft is the **Trusted Government IT Solutions Provider**® supporting a broad portfolio of industry-leading technologies through The Quilt, E&I Carahsoft Cloud Solutions & Services Distributor Contract, TIPS and a wide range of other contract vehicles.

As the **Master Government Aggregator**®, Carahsoft connects government agencies, industry partners, and technology providers to deliver innovative, mission-focused solutions.

In partnership with Nothreat, we provide technology solutions that drive modernization, strengthen operations, and ensure compliance with evolving government standards.

To learn more about how Carahsoft can support your technology needs, please visit carahsoft.com

Explore More Resources:
carah.io/nothreatresources

Join Events & Webinars:
carah.io/nothreatevents

Discover Technology Solutions:
carah.io/nothreat

Learn About Procurement:
carah.io/nothreatcontracts

Connect With Our Team:
Nothreat@carahsoft.com
703-889-9710

NOTHREAT

DECEIVE. DETECT. NEUTRALIZE.

carahsoft

PARTNER BRIEFING

Prepared for Carahsoft · August 2026

AI has transformed the attack.
Nothreat is the defense built for it.

Nothreat is a London-headquartered cybersecurity company providing autonomous threat intelligence and preemptive defense capabilities to government agencies, defense organizations, and commercial enterprises. Our technology autonomously detects and blocks attacks — including zero-days and AI-generated attacks — **before** they reach production systems, working alongside the security tools an organization already owns.

WHY THIS MATTERS NOW

Finding an AI-driven attack is no longer like finding a needle in a haystack — it's a needle in a **needlestack**. AI attacks look identical to legitimate traffic: miss one and you're breached; block the wrong one and you've shut out a real customer. Precision is everything.

Over the past year, attackers gained a new weapon: AI. It has multiplied the **volume** of attacks, the **speed** at which they are launched, and — most importantly — the **number of variations** an attacker can generate. A single attack can now be rewritten thousands of ways, automatically, until one gets through.

Traditional defenses cannot answer this, because they rely on existing firewall rules and signatures based on published vulnerabilities — every one of which requires the attack to have been seen before. Between the moment a new attack begins and the moment a signature or patch exists, most organizations are blind. In the Microsoft SharePoint "ToolShell" case, that window lasted **more than 40 days** — and over 400 organizations were compromised during it.

> Gartner expects preemptive cybersecurity to account for **50% of IT security spending by 2030**, replacing stand-alone detect-and-respond tools as the preferred defense.

WHAT NOTHREAT DOES — THREE CAPABILITIES, FULLY AUTOMATED

1

Deceive

We deploy high-fidelity decoys of the customer's real services — web apps, APIs, portals, IoT devices — inside their environment. No legitimate user ever touches a decoy, so **any interaction is, by definition, an attack.** The result: a clean attack signal, isolated from real traffic, with zero risk to production data.

2

Detect

Our incrementally learning AI classifies the attacker by **how they behave** — not by matching a known pattern. No CVE, no detection rule, no prior knowledge required. This is why Nothreat stops attacks the industry has not yet discovered.

3

Neutralize

Validated intelligence is pushed automatically and in real time to the customer's **existing firewalls** — Cisco, Palo Alto, Fortinet and 20+ other vendors — via one-line configuration. We don't replace their stack; we make it preemptive.

> **Crowd Immunity:** an attack caught at one customer becomes protection for every Nothreat customer within minutes. The network gets stronger with every deployment. Customers opt in to enable this functionality.

THE PROOF — INDEPENDENTLY VERIFIABLE AGAINST PUBLIC RECORDS

40+ days early

Microsoft SharePoint "ToolShell"

Detected and blocked 40+ days before the CVE was published (CVE-2025-53770/71). 235,000+ servers exposed, 400+ organizations breached — Nothreat customers protected throughout.

5 days · hours

Oracle · Windows Server

Oracle attack blocked 5 days before CVE-2025-61884 was published; Windows Server Update Service attack blocked hours before Microsoft's emergency out-of-band fix (CVE-2025-59287).

9.1–11.2×

More attacks blocked

Versus leading next-generation firewalls alone, in recent live $1B+ enterprise deployments, with zero known false positives across the test period.

Springer

Peer-reviewed science

Our incremental-learning approach is published in a Springer research journal — independently reviewed.

Lenovo

OEM validation

Piloted inside Lenovo ThinkEdge SE10 edge devices, running on 2MB RAM and under 2% CPU. Showcased at Lenovo Day and COP29.

National scale

Government-proven

Protecting government and critical infrastructure — creating national threat intelligence.

WHERE NOTHREAT IS DEPLOYED TODAY

Public sector

- **Transportation** — a national flag-carrier airline
- **Public safety** — a national Ministry of Emergency Situations
- **Healthcare** — a national Ministry of Health
- **Critical infrastructure** — a national water supplier

Private sector

- **Financial services** — commercial banks, incl. a leading bank in a Central Asian market
- **Telecommunications** — an incumbent telecom group with multiple mobile operators in several countries
- **Sport** — a top-tier national football club

WHAT CUSTOMERS AND PARTNERS SAY

"Nothreat's solution represents a significant leap forward in IoT security.

Rasim Bakhshi
Director, Lenovo Global Technology

"Collaborating with Nothreat enables us to strengthen our infrastructure's protection against potential cyber threats.

Dovlat Dovlatov
Deputy CEO, Azerconnect Group

WHY NOTHREAT IS STRAIGHTFORWARD TO SELL

- **No rip and replace** — we enhance the customer's existing firewalls and security stack rather than competing with it, removing the biggest objection in most security deals.
- **Fast time to value** — decoys are cloned and live in minutes, not days, with no changes to existing infrastructure.
- **Deployable on-premise or in a sovereign cloud** — data stays where it must stay; built for government, defense and regulated industries.
- **Vendor-agnostic and modular** — works with what the customer already runs; sold as a full platform or as individual modules.
- **A clear demo moment** — a live, undetectable clone of a real service, shown in a single session; it lands with technical and non-technical audiences alike.

WHAT MAKES NOTHREAT DIFFERENT

Nothreat is the only platform that combines **three capabilities competitors sell separately** — deception that captures a clean attack signal, **signature-free AI detection**, and automated protection pushed into the customer's **existing firewalls, EDRs or XDRs** — in one autonomous system. Point solutions do one of these; **no one else does all three together.** And because every deployment feeds **Crowd Immunity**, an attack caught at any customer becomes protection for all of them — a defence that compounds with scale, which a stand-alone tool cannot replicate.

WHERE NOTHREAT SITS VERSUS THE MARKET

SIGNATURE-INDEPENDENT ↑

Darktrace · Vectra behaviour-based, but reactive — they detect after the attacker is inside	**NOTHREAT** autonomous · signature-free · preemptive **on-premise — unlike cloud-only competitors**
CrowdStrike · Palo Alto · Fortinet powerful platforms, engineered to detect and respond once the attack is underway	**Morphisec · Acalvio · CounterCraft** preemptive point tools — each covers one piece of the chain

REACTIVE → PREEMPTIVE →

What this means for a sales conversation:

- Against **Darktrace / Vectra**: they alert once the attacker is already inside; Nothreat intercepts during reconnaissance — before the breach.
- Against **firewall vendors**: we are not a rip-and-replace competitor — we make the firewall the customer already owns preemptive.
- Against **deception point tools**: decoys are only our data source — detection, blocking and crowd-wide distribution are automated on top.

THE PLATFORM AT A GLANCE — ONE CORE, MODULAR PRODUCTS

Nothreat Platform THE CORE	The incrementally learning AI brain — continuous threat exposure management (CTEM): generates the customer's own threat intelligence, orchestrates detection, analysis and response across all modules, and distributes Crowd Immunity protection. Deployable on cloud or on premise.
Nothreat CyberEcho DECEIVE	US-patented deception: high-fidelity, undetectable clones of the customer's real services placed in the attacker's path. Any interaction is a confirmed threat — clean signal, zero risk to production.
Nothreat ThreatShield NEUTRALIZE	Real-time threat-intelligence feeds pushed into Cisco, Palo Alto, Fortinet and 20+ other firewalls with one line of configuration — turning the customer's existing perimeter into a preemptive one.
Nothreat AIoT Defender EDGE & IOT	An ultra-light AI firewall embedded directly in IoT, IIoT and edge devices — 2MB RAM, under 2% CPU, no extra hardware. OEM-ready; piloted inside Lenovo edge devices.
Nothreat AI Analyzer REPORT	An on-premise AI agent that turns raw attack data into short, plain-language reports for leadership and SOC teams — with guaranteed accuracy of the statistics, unlike general-purpose LLMs.

Sold as a full platform or as individual modules — so a partner can lead with the piece that fits the customer's budget and expand from there.