



OVERVIEW

NexThreat LLC is a certified 8(a), SDVOSB, and HUBZone small business founded in 2016 and headquartered in Alexandria, Virginia, delivering IT, data, cybersecurity, and AI services across the Department of Defense, federal civilian agencies, and the Intelligence Community. We span the full mission stack — offensive and defensive cyber operations (OCO/DCO), Continuous Diagnostics and Mitigation (CDM/ISCM) and RMF/ATO compliance, enterprise data architecture and SIEM engineering, Zero Trust at enterprise scale, and the security of frontier AI systems. We serve as SETA and engineering lead on the Army's Rapid Cyber Development Network (RCDN) supporting U.S. Cyber Command, integrated data across nine agencies on the DHS/CISA CDM DEFEND E program for up to 45% gains in asset awareness, and secure the Department of Energy's AI-enabled Genesis Mission research platform. Backed by a TS/SCI (Q)-cleared workforce with NATO Facility Clearance since 2018 and commercial innovation proven for Fortune 500 clients such as Visa, Morgan Stanley, and Koch Industries, NexThreat helps government customers build efficient, resilient, and cost-effective mission and security postures.

CORE COMPETENCIES

- **Cybersecurity Operations** — OCO/DCO, SOC, SIEM (Splunk/ELK/ArcSight), incident response, insider threat, and Zero Trust
- **Cyber Risk & Compliance** — RMF/ATO, FISMA and NIST 800-53, continuous monitoring (CDM/ISCM), and CMMC
- **Data Engineering & Analytics** — enterprise data architecture, ETL, data quality, and dashboards
- **AI & Intelligent Automation** — AI/ML and agentic-AI security, AI-driven automation, and proven RPA and CI/CD
- **IT Systems & Software Engineering** — systems/software engineering, DevSecOps, CI/CD, cloud, and modernization
- **Advisory & Program Support (SETA)** — technical advisory, program/project management, and acquisition support

COMPANY DATA

UEI
P9LJP16X9MH3

CAGE CODE
7L3P4

FOUNDED
2016

BUSINESS SIZE
Small Business

SET-ASIDES
8(a) · SDVOSB · HUBZone · SDB

NAICS
541330, 541511, 541512, 541513, 541519, 541611, 541690, 541715

PSC
DJ01, DJ10, DA01, R425

GSA SCHEDULE
47QTCA22D0060 · 8(a) Sole Source Pool

HACS SINS
All (HVA · RVA · Cyber Hunt · IR · Pen Test)

CERTIFICATIONS

ISO 9001:2015 CMMC Level 2

FACILITY CLEARANCE

TS/SCI (Q); NATO since 2018

CERTIFICATIONS · SET-ASIDES · CONTRACT VEHICLE



DIFFERENTIATORS

- **TS/SCI (Q)-cleared workforce and NATO Facility Clearance held since 2018**
- **Supports the only Title 10/Title 40 cyber program of its kind in the DoD (CYBERCOM JDE / Army RCDN)**
- **Securing frontier and agentic AI in production** — DOE's AI-enabled Genesis Mission research platform
- **Quantified delivery across domains** — an estimated \$5M saved at the VA, up to 45% asset-awareness gains at CISA, and 75,000 endpoints secured at DLA
- **Proven commercial innovation** — Fortune 500 clients including Visa, Morgan Stanley, and Koch Industries
- **8(a) / SDVOSB / HUBZone / SDB on GSA HACS (47QTCA22D0060)** — direct set-aside and sole-source paths

PAST PERFORMANCE

U.S. Cyber Command & U.S. Army — RCDN / Shadow's Edge

Subcontract — DCI Solutions · 2025–2028

Chief Engineer and senior systems/software engineering lead for USCYBERCOM's Rapid Cyber Development Network and the 90th COS Shadow's Edge programs; reduced requirements rework 20%+, cut deployment friction ~15% via containerized (Docker/Kubernetes) parity, and reduced manual regression effort ~25% through CI/CD automation.

DHS / CISA — CDM DEFEND E

Subcontract — ManTech · 2018–2024

Chief Data Architect and SIEM SME across nine federal agencies; integrated agency data on Splunk and Elastic (ELK) for up to 45% gains in asset awareness, 40%+ data-quality improvement (75%+ fewer duplicates and false positives), and ATO support across ten federal boundaries.

U.S. Dept. of Energy IN-20/IN-27 — Genesis Mission AI Platform

Subcontract — Deck Prism (REDVAT) · 2025–2029

Securing every phase of DOE's AI-enabled Genesis Mission research platform — from secure storage and AI-based evaluation of proposals to agentic AI directing physical test equipment under an accredited architecture — and delivering independent audits and SME direction to strengthen the DOE insider-threat (UAM) program.

DEPARTMENT OF WAR



FEDERAL CIVILIAN



COMMERCIAL

