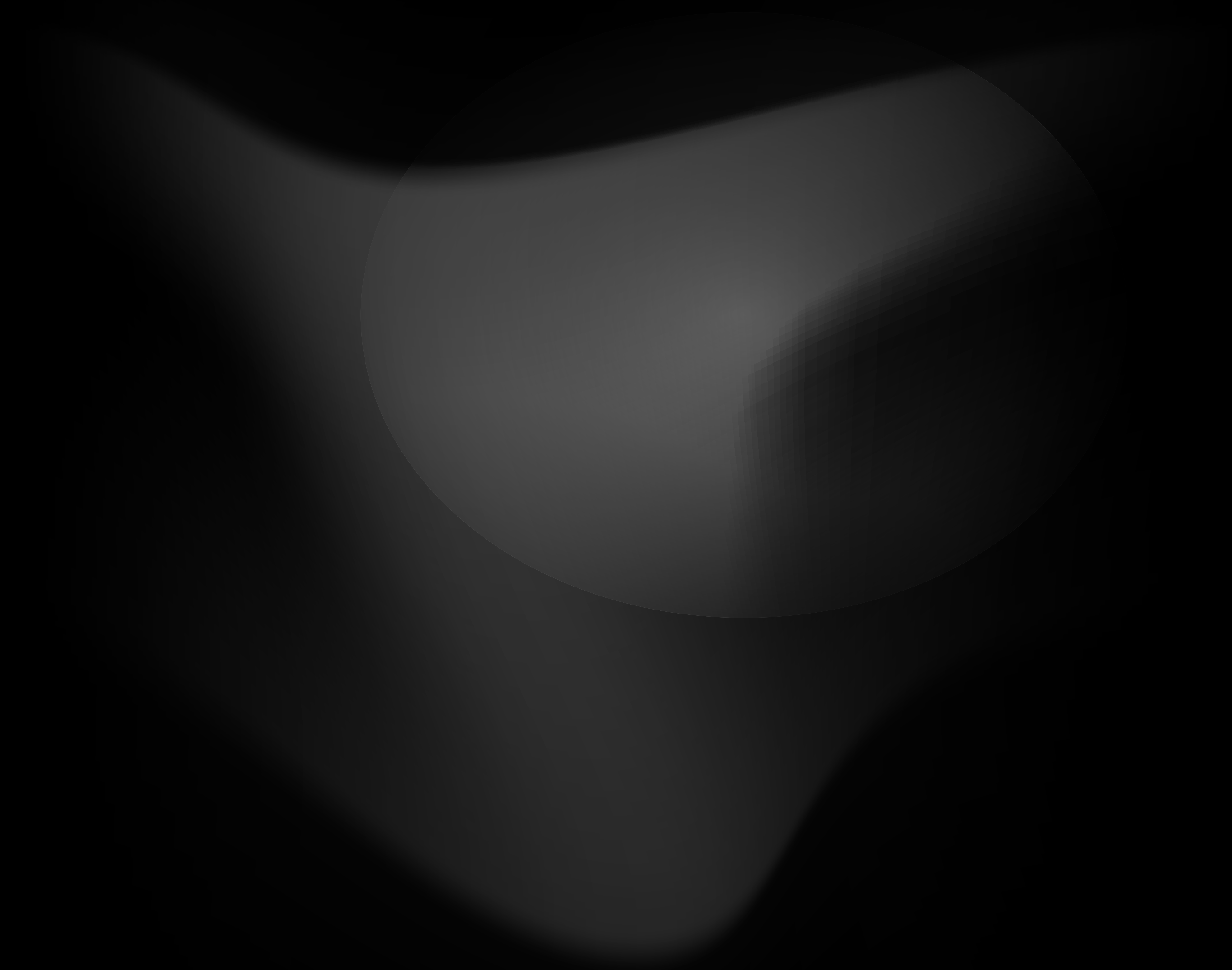
AUGUR



Primary Solution Brief

The Augur Predictive Threat Prevention Platform

AUGUR

The Augur Predictive Threat Prevention Platform

Your Kill Switch for Tomorrow's Threats

Adversaries don't wait. They move at machine speed — acquiring infrastructure, launching zero days, and executing campaigns before most security tools register a signal. Yet most threat intelligence is reactive, built from yesterday's compromises. The result: alert fatigue, wasted cycles, and a race you've already lost.

Augur flips the script. It's not about reacting faster. It's about acting first.

Prediction is Power, and Augur Wields it First

Augur is the first AI-powered threat prevention platform that identifies attack infrastructure before it's weaponized — an average of 51 days before anyone else sees it. Built on a decade of machine learning and behavioral science, the platform continuously analyzes global internet activity, profiles malicious infrastructure in its earliest stages, and automatically blocks threats before they ever touch your environment.

This isn't detection. It's foresight in action.

Built for Action

- **Predictive threat prevention:** blocks infrastructure before it's used
- **Autonomous enforcement:** no manual triage or analyst review required
- **AI behavioral modeling:** learns, adapts, and predicts with near-zero false positives
- **Seamless integration:** works with your existing stack — SIEM, SOAR, EDR, firewall
- **Threat attribution:** maps infrastructure to known adversaries and campaigns

Built for Defenders

- **CISOs and security leaders** seeking to demonstrate measurable risk reduction
- **SOC and intel teams** looking for earlier signals and better prioritization
- **Security architects and engineers** wanting to automate threat prevention without adding noise

How Augur Sees Threats Before They Exist

Security shouldn't start at impact. Most tools alert you after damage is done. Augur works differently: it identifies threats during the setup phase — before payloads, before exploitation, before anything hits your environment. **Here's how it works:**

01 **Ingest and analyze:** Augur monitors global IP space in real time, tracking domain registrations, DNS shifts, and IP acquisitions that reveal early signs of attacker setup.

02 **Predict and prioritize:** AI-powered behavioral models flag likely threats and surface only high-confidence pre-indicators of compromise (PreIOCs) — early signals no one else sees.

03 **Correlate and confirm:** Predictions are validated against internal telemetry. If internal traffic hits predicted infrastructure, Augur confirms targeting and blocks it automatically.

04 **Automate and enforce:** Blocklists and intelligence are pushed directly to your SIEM, SOAR, firewall, or EDR — no triage, no waiting, just threats stopped cold.

What makes Augur different?

Augur Delivers	Why It Matters
PreIOCs, not IOCs	Detects threats before they're operational, not after damage begins
<0.01% false positives	No alert storms, no handholding — just clean, trusted intel
51-day predictive lead time	The earliest warning system in cyber defense
Real automation	Predicts, correlates, and enforces — without analyst overhead
AI that acts, not just alerts	Built for autonomous action, not dashboards

Augur Saw It Coming — and Blocked It

Customers like ADP, Cisco Talos, and Greenhill & Co. trust the Augur platform to stay ahead of the threat curve automatically. Our platform has a documented track record of predicting major cyberattacks long before they became known incidents. **These attacks weren't just detected, they were prevented.**

Attack	Augur lead time
solarwinds	Six months early
LOG4J	Three months early
COLONIAL PIPELINE CO.	13 months early
Progress MOVEit	14 months early

You Can't Fight What You Can't See — Augur Can

If you're tired of chasing alerts and reacting late, maybe it's time to stop playing defense and start owning the fight. **Augur isn't another feed. It's your cybersecurity kill switch** — a real-time, autonomous system that shuts down adversaries before they strike.

▶ Download our white paper or book a strategy session to explore predictive threat prevention in your environment.

About Augur

Augur is the cybersecurity kill switch that stops threats before they are launched. Trusted by leading financial institutions, global energy providers, and critical infrastructure operators, the Augur Predictive Threat Prevention Platform uses AI and behavioral modeling to identify malicious infrastructure before it's weaponized — an average of 51 days before anyone else sees it. With cutting-edge behavioral modeling and a near-zero false positive rate, Augur delivers high-confidence threat predictions that enable security teams to act early, automate enforcement, and avoid disruptions, damages, and costly remediation.

▶ Learn more at www.augursecurity.com