THREATDEFEND® DECEPTION AND RESPONSE PLATFORM

WHY CUSTOMERS BUY

- Early in-network threat detection
- Detect malicious actors and insiders
- Attack surface scalability
- Substantiated alerts and forensic reporting
- Easy to deploy and operate
- Attack analysis accelerates response times
- Threat path risk assessment for attack prevention

ALERTS THAT MATTER:

Research shows that deception reduces dwell time by up to 90%, and triage time by up to 12X.

DETECT ANY TYPE OF ATTACK. ANYWHERE IN THE NETWORK.

Real-time detection of known and unknown attackers

SOLUTIONS FOR BUSINESS CHALLENGES

- Active Directory Defense
- Critical Infrastructure Protection
- Endpoint Protection
- External, Insider, and 3rd-Party Threat Detection
- IP Theft Protection
- Remote Worker Risk Reduction
- Secure Cloud Operations

BUILT FOR EVOLVING ATTACK SURFACE

- Endpoints, User Network, Data Center, Cloud, IoT, SCADA, POS, SWIFT, Telecom, Router
**ACCELERATE INCIDENT RESPONSE WITH AUTOMATION.**

Create an active defense with partner integrations and playbooks for automated deployment, blocking, and quarantine.

Augment existing controls to strengthen defenses.

**SIMPLIFIED OPERATIONS**
- Centralized Management
- Machine-Learning Deployment
- Non-Disruptive Deployment and Operations
- Adds Value to Endpoint and SIEM solutions

**VISIBILITY, ANALYSIS, FORENSICS**
- Evidence-Backed Alerts
- Advanced Attack Analysis
- Forensic Collection
- Network Visibility
- Attack Path Predictions
- Time-Lapse Attack Replay
- Company-centric Threat Intelligence

**ACTIVE DEFENSE PARTNERS:** NATIVE INTEGRATIONS FOR INFORMATION SHARING AND AUTOMATED RESPONSE

---

**ANALYSIS & HUNTING**
- FireEye
- ForeScout
- IBM
- LogRhythm
- McAfee
- Micro Focus
- Splunk
- Tanium
- ThreatConnect
- VirusTotal
- Webroot

**NETWORK BLOCKING**
- Check Point
- Cisco
- CrowdStrike
- ForeScout
- GoSecure
- Juniper
- Palo Alto
- McAfee
- Tanium

**ENDPOINT QUARANTINE**
- VMware Carbon Black

**DISTRIBUTION**
- McAfee
- Tanium
- Endpoint management solutions such as SCCM, WMI, Casper, and others

**TICKETING**
- ServiceNow

**CLOUD MONITORING**
- Box
- Google Drive
- Microsoft
- Office 365

**REDIRECTION**
- McAfee

**ORCHESTRATION**
- Demisto
- Splunk
- Resilient

**API INTEGRATORS**

---

**RESPOND QUICKLY WITH EARLY AND ACCURATE ALERTS.**

High-fidelity, substantiated, and actionable alerts reduce triage and response times.