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

RECONNAISSANCE

STOLEN CREDENTIALS

MAN-IN-THE-MIDDLE

RANSOMWARE

ACTIVE DIRECTORY

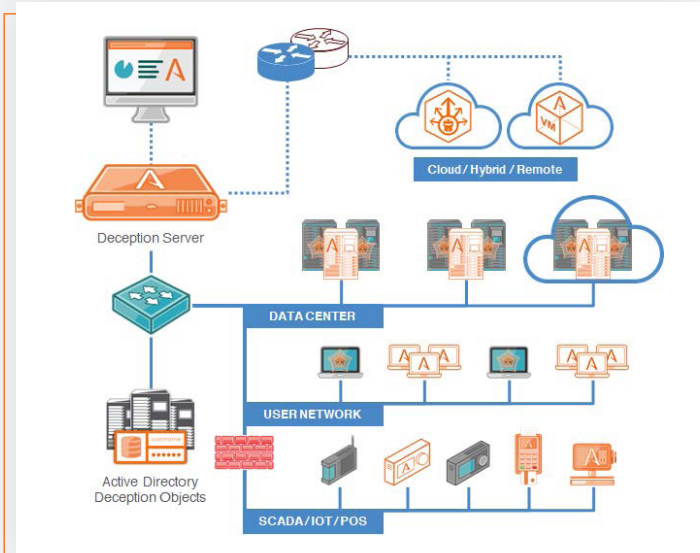
SOLUTIONS FOR BUSINESS CHALLENGES

- 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

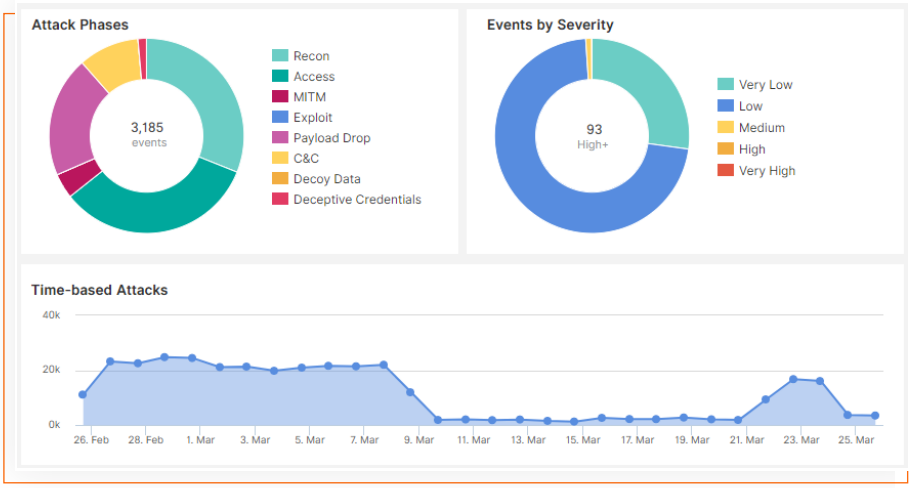
- Endpoints, User Network, Data Center, Cloud, IoT, SCADA, POS, SWIFT, Telecom, Router

In-Network Threat Detection



RESPOND QUICKLY WITH EARLY AND ACCURATE ALERTS.

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



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

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.

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

ANALYSIS & HUNTING	NETWORK BLOCKING	ENDPOINT QUARANTINE
FIREEYE, FORESCOUT, IBM Radar, LogRhythm, McAfee, MICRO FOCUS, REVERSING LABS, splunk>, TANIUM, ThreatConnect, VirusTotal, WEBROOT	Check Point, CISCO, FORTINET, JUNIPER NETWORKS, paloalto NETWORKS, Symantec + BLUE COAT	aruba, CISCO, CROWDSTRIKE, FIREEYE, FORESCOUT, GoSECURE, McAfee, TANIUM, vmware Carbon Black.

DISTRIBUTION	TICKETING
McAfee, TANIUM. Endpoint management solutions such as SCCM, WMI, Casper, and others	servicenow

CLOUD MONITORING	REDIRECTION
box, Google Drive, salesforce, Office 365	McAfee

ORCHESTRATION	API INTEGRATORS
DEMISTO, splunk> phantom, Resilient an IBM Company	DIGITAL DEFENSE INCORPORATED