

# 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

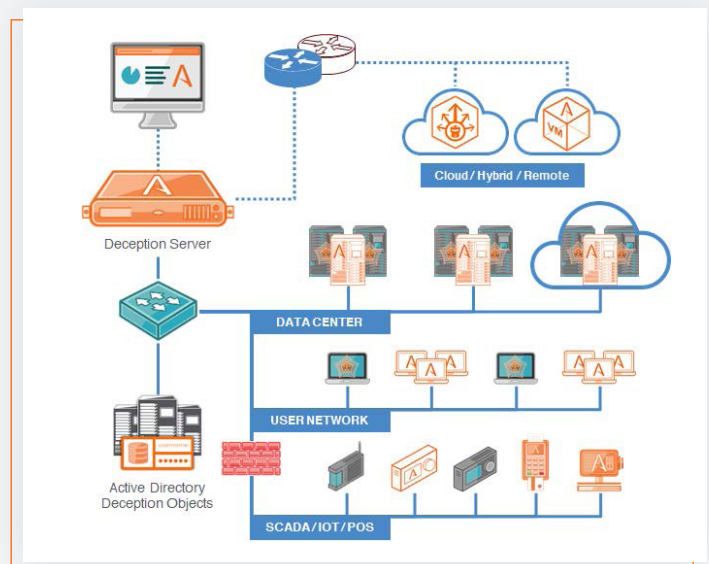
## SOLUTIONS FOR BUSINESS CHALLENGES

- 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

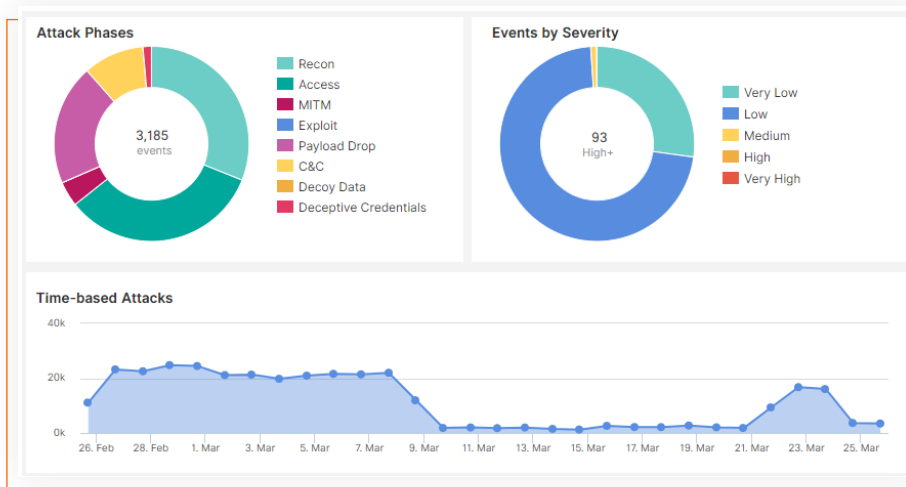
- Endpoints, User Network, Data Center, Cloud, IoT, SCADA, POS, SWIFT, Telecom, Router

### 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

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

# 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.

<p><b>ANALYSIS &amp; HUNTING</b></p> <p>FIREEYE &lt; FORESCOUT</p> <p>IBM Radar :: LogRhythm</p> <p>McAfee MICRO FOCUS</p> <p>REVERSING LABS splunk &gt;</p> <p>TANIUM ThreatConnect</p> <p>VirusTotal WEBROOT an opennet company</p>	<p><b>NETWORK BLOCKING</b></p> <p>Check Point SOFTWARE TECHNOLOGIES LTD.</p> <p>CISCO</p> <p>FORTINET.</p> <p>JUNIPER NETWORKS</p> <p>paloalto NETWORKS</p> <p>Symantec. + BLUE COAT</p>	<p><b>ENDPOINT QUARANTINE</b></p> <p>aruba a Hewlett Packard Enterprise company CISCO</p> <p>CROWDSTRIKE FIREEYE</p> <p>FORESCOUT. GOSECURE POWERED BY COUNTERBOX</p> <p>McAfee TANIUM</p> <p>vmware Carbon Black.</p>
<p><b>DISTRIBUTION</b></p> <p>McAfee TANIUM</p> <p>Endpoint management solutions such as SCCM, WMI, Casper, and others</p>	<p><b>TICKETING</b></p> <p>servicenow.</p>	
<p><b>CLOUD MONITORING</b></p> <p>box Google Drive salesforce Office 365</p>	<p><b>REDIRECTION</b></p> <p>McAfee</p>	
<p><b>ORCHESTRATION</b></p> <p>DEMISTO splunk phantom resilient an IBM Company</p>	<p><b>API INTEGRATORS</b></p> <p>DIGITAL DEFENSE INCORPORATED</p>	