Attivo NETWORKS

DECEPTION FOR ACTIVE DEFENSE

AT-A-GLANCE

# 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

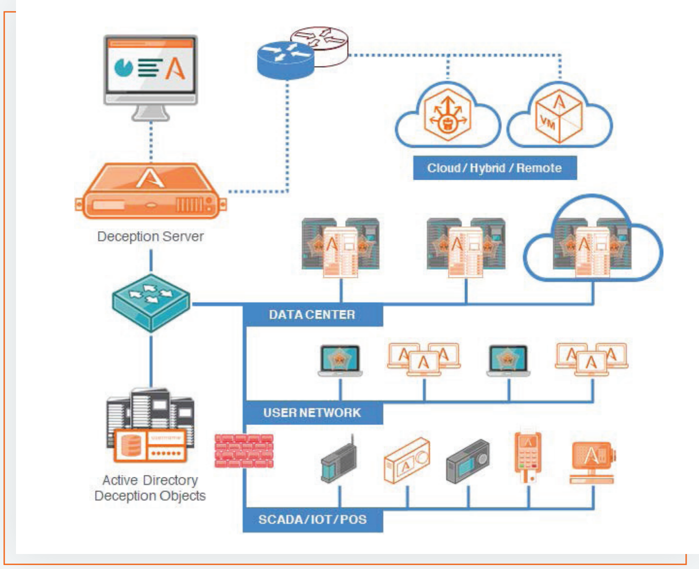
RANSOMWARE

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

In-Network Threat Detection

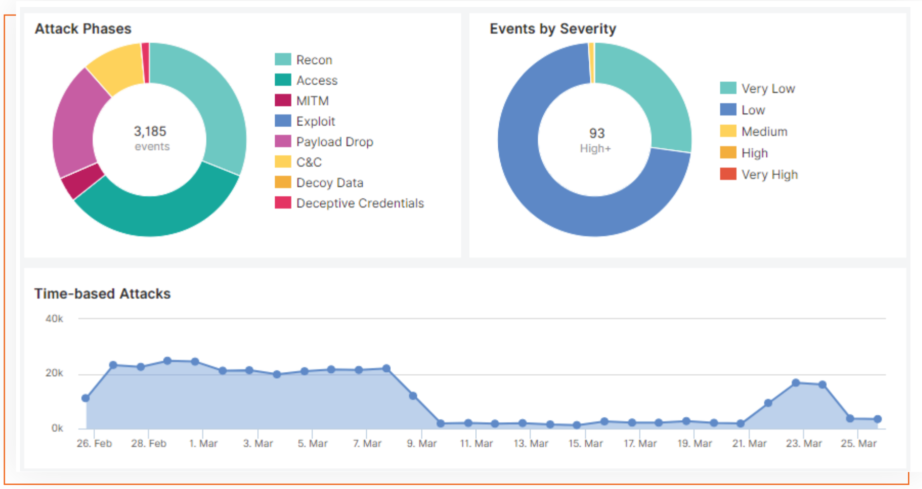


### BUILT FOR EVOLVING ATTACK SURFACE

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

# **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

FIREEYE, FORESCOUT, IBM QRadar, LogRhythm, McAfee, MICRO FOCUS, REVERSING LABS, splunk>, TANIUM, ThreatConnect, VirusTotal, WEBROOT an opentext company

### NETWORK BLOCKING

Check Point SOFTWARE TECHNOLOGIES LTD., CISCO, FORTINET, JUNIPER NETWORKS, paloalto NETWORKS, BROADCOM

### ENDPOINT QUARANTINE

aruba a Hewlett Packard Enterprise company, CISCO, CROWDSTRIKE, FIREEYE, FORESCOUT, GOSECURE POWERED BY COUNTERTACK, McAfee, SentinelOne, TANIUM, vmware Carbon Black.

### DISTRIBUTION

CROWDSTRIKE, McAfee, TANIUM

Endpoint management solutions such as SCCM, WMI, Casper, and others

### TICKETING

servicenow

### CLOUD MONITORING

box, Google Drive, Office 365, salesforce

### REDIRECTION

McAfee

### ORCHESTRATION

CORTEX XSOAR BY PALO ALTO NETWORKS, Resilient an IBM Company, splunk> phantom, SWIMLANE

### API INTEGRATORS

DIGITAL DEFENSE INCORPORATED, Quantea