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

DECEIVE. EVEN THE MOST SOPHISTICATEDattaCKER.

Lures and decoys misdirect and reveal in-network threats

EARLY AND EFFICIENT ATTACK DETECTION

- External, insider, and 3rd party threats
- Early reconnaissance/credential theft
- Threat lateral movement
- Not reliant on signatures or pattern matching

DESIGNED FOR AN EVOLVING ATTACK SURFACE

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

VISIBILITY, ANALYSIS, FORENSICS

- Substantiated alerts and forensics
- Advanced attack analysis
- Attack path predictions
- Time lapse attack replay

AUTHENTIC DECEPTION: ATTACKERS ARE UNABLE TO TELL REAL FROM DECEPTION

- Endpoint, server, network, application, data, and deceptions
- Real OS/image, services, and application customization
- Machine learning for authenticity and easy deployment
- Agentless endpoint deception incorporates with Active Directory for authenticity
DETECT. ANY TYPE OF ATTACK. ANYWHERE IN THE NETWORK.
Real-time detection of known and unknown attackers

ACCURATE DETECTION
• Ever-changing attack vectors
• Credential, lateral, polymorphic
• Evolving attack surface
• Engagement-based and actionable
• Easy deployment and operations

DEFEND.
ACCELERATE INCIDENT RESPONSE WITH AUTOMATION.
Create an active defense with partner integrations and playbooks for automated deployment, blocking, and quarantine

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

INVESTIGATION / ANALYSIS & HUNTING
Carbon Black.
IBM
IBM Radar
McAfee
Micro Focus
Splunk
ThreatConnect

CONTAIN / NETWORK BLOCKING
Check Point
Cisco
Fortinet
Juniper Networks
Palo Alto Networks
Symantec
Virus Total

CONTAIN / ENDPOINT QUARANTINE
Carbon Black.
Cisco
CounterTack
ForeScout
McAfee

DISTRIBUTION
Endpoint agents such as SCOM, WMI, Casper...

TICKETING
ServiceNow

CLOUD MONITORING
Box
Google Drive
Salesforce

TRAFFIC REDIRECTION
McAfee