

THREATDEFEND™ DECEPTION AND RESPONSE PLATFORM

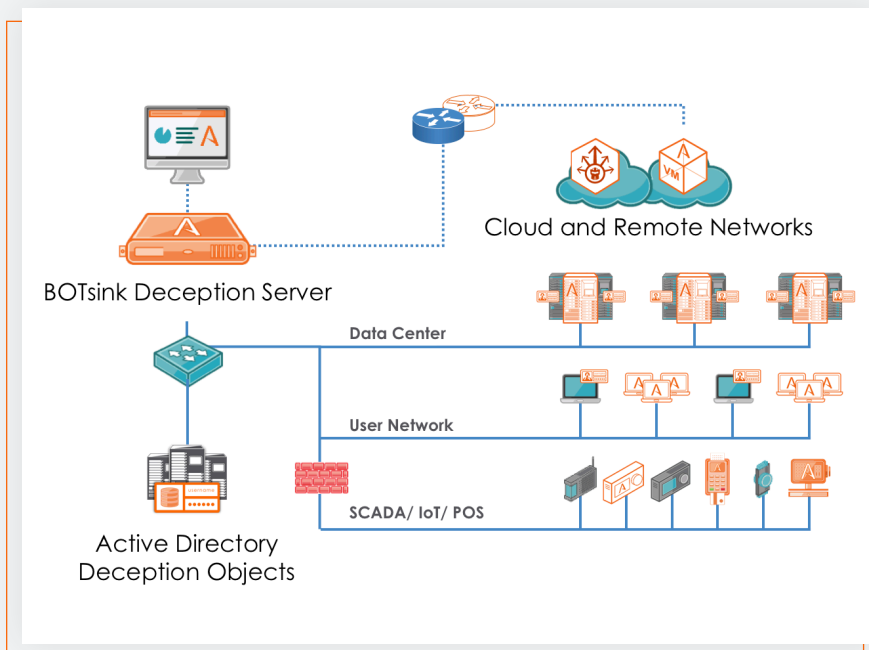
WHY CUSTOMERS BUY

- 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 SOPHISTICATED ATTACKER.

Lures and decoys misdirect and reveal in-network threats



DECEIVE AND MISDIRECT ATTACKS

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

BUILT FOR 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

- Dynamic endpoint, server, network, application, and data deceptions
- Real OS, customizable services and applications
- Machine learning authenticity and QuickDeploy
- 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



RECONNAISSANCE



STOLEN CREDENTIALS



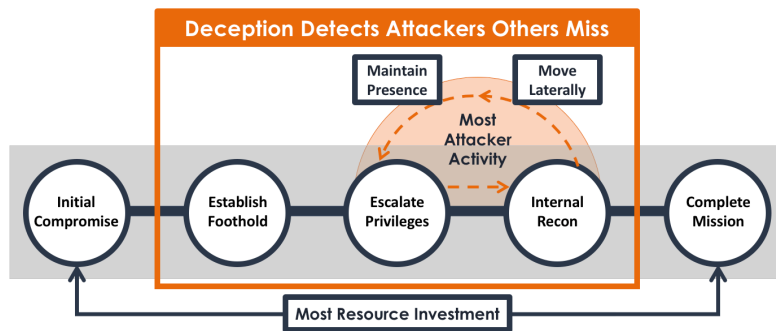
MAN-IN-THE-MIDDLE



RANSOMWARE



ACTIVE DIRECTORY



Most investment is at the perimeter. Most attacker activity is internal.

ACCURATE DETECTION

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

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

| | | |
|--|--|--|
| <p>INVESTIGATION / ANALYSIS & HUNTING</p> <p>Carbon Black, ForeScout</p> <p>IBM Radar, LogRhythm</p> <p>McAfee, MICRO FOCUS</p> <p>splunk, TANIUM</p> <p>THREATCONNECT, virus total</p> | <p>CONTAIN / NETWORK BLOCKING</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>CONTAIN / ENDPOINT QUARANTINE</p> <p>aruba a Hewlett Packard Enterprise company</p> <p>Carbon Black.</p> <p>CISCO</p> <p>CounterTack</p> <p>ForeScout</p> <p>McAfee</p> <p>TANIUM.</p> |
| <p>DISTRIBUTION</p> <p>McAfee, TANIUM. Endpoint mgmt solutions such as SCCM, WMI, Casper...</p> | <p>TICKETING</p> <p>servicenow</p> | |
| <p>CLOUD MONITORING</p> <p>box, Google Drive, salesforce</p> | <p>TRAFFIC REDIRECTION</p> <p>McAfee</p> | |
| <p>ORCHESTRATION</p> <p>DEMISTO</p> | | |

DEFEND. ACCELERATE INCIDENT RESPONSE WITH AUTOMATION.

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