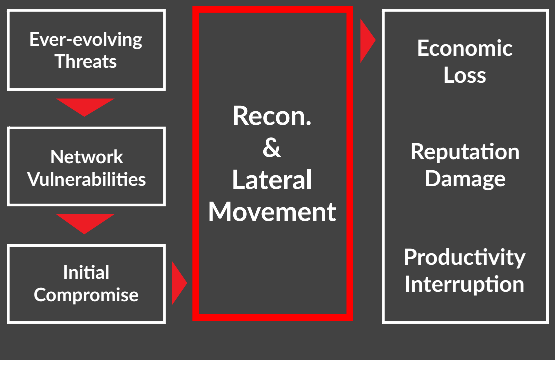


- Threats evolve continuously and unpredictably, while complex company networks are impossible to defend at the perimeter. Breaches occur routinely.
- **Lateral Movement,** the expansion of control over network resources by the Adversary after the initial breach, is what permits cyber damage. A network with 1,000 endpoints presents more than 700 million internal attack vectors for and Adversary to use to expand their control over assets.
- Solutions to address lateral movement are passive, analytical or after-the-fact. They generate 50%+ false positive alerts.
- The attacker continues to have the upper hand over the defender. Ridgeback inverts that dynamic.

RIDGEBACK

Adaptive Security System

Stops Lateral Movement | **Evicts Intruders Before Harm Occurs** | **No Human Intervention Needed**

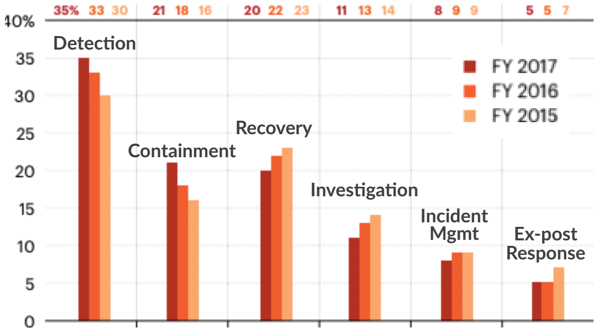
PRODUCT ADVANTAGES

Ridgeback's theory of defense – reshape the network battlefield so enterprises can win – is adaptive to any threat type, on any network. Ridgeback impairs the attacker, not the defender by disrupting the attack like no other product. Networks with Ridgeback will never be an Adversary's target of opportunity.

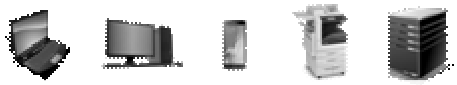
- **Sees the attack vectors** attackers use to do harm in your network.
- **Poisons the network data** attackers need to expand their control over network assets.
- **Enforces communications policies between live endpoints.**
- **Makes your network hostile to the attacker** with millions of landmines that evict attackers in real time.
- Data poisoning, policy enforcement and phantom resources create **an impossible challenge** that repels and evicts attackers.
- **Ridgeback software deploys easily** on one server or VM, it is agent-less on endpoints. There is no bandwidth overhead. Easy to manage – applicable to enterprises large and small.

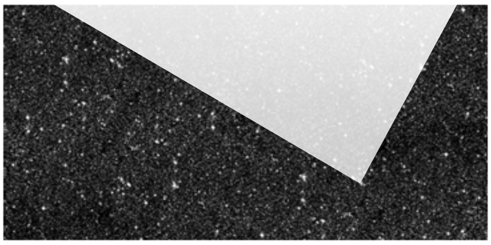
Companies spend most on Detection

Percent of Internal Budget by Category



Corporate cybersecurity spending trends reflect concern about identifying threats and containing damage. Despite this spending, cyber damage continues to escalate. Ridgeback resolves detection and reduces the need for recovery spending. (Source: Accenture Ponemon 2017)





Ridgeback poisons the information needed to move laterally, while live resources in the network are plunged into a galaxy of millions of phantom resources and fake data 'manufactured' by Ridgeback. Adversary contact with Ridgeback phantoms triggers automatic countermeasures that prevent damage before it can occur.

Ridgeback Operates on Layers 2,3,4 delivering...

1 Visibility

- Comprehensive, real-time visualization of the network
- Visibility into live assets and all network communication
- Continuous attack surface scanning and risk assessment
- Continuous, real-time, 24X7 monitoring

2 A Hostile Network

- Network hostile at every stage of the exploit.
- Poison data. Deny the Adversary any useful knowledge.
- Automated countermeasures.
- Compromised host isolation.

3 Policy Enforcement & Adaptation

- Fine-grained security policies.
- Software-only approach.
- Automated countermeasures.
- Reporting integration / compliance.

For further information

info@ridgebacknet.com