



Keys to network security

Ridgeback is comprehensive and easy. It also deters attackers.


Know your assets	See them communicate	Define acceptable-use	Auto enforce acceptable-use	Auto disrupt, evict intruders
-------------------------	-----------------------------	------------------------------	------------------------------------	--------------------------------------

Ridgeback’s patented software dramatically improves the cyber-defense posture of any organization with a number of high-value capabilities. Ridgeback prevents attackers from discovering what is and isn't on the network, while also actively disrupting hacking operations by directly engaging attackers during their reconnaissance and exploitation activities inside the network. Ridgeback delivers real-time system monitoring that exposes key factors in network hygiene that are both productivity concerns and security vulnerabilities.


When any impermissible communications are observed, Ridgeback implements man-in-the-middle techniques automatically, at scale to disrupt the adversary without imposing any impact on authorized users and network activity. Ridgeback is the only product available that deters attackers by making their hacking operations painful.

Limit Complexity. It is increasingly evident that layering numerous solutions to address specific exposures can dramatically increase management complexity. When complexity grows the probability that security systems aren't properly configured, integrated and managed climbs dangerously, and security levels drop.


Ridgeback delivers value

- 


ENDPOINT VISIBILITY

You can't protect assets you don't know you have. It is imperative to be aware – all the time – what assets should or shouldn't be on the network.
- 


SYSTEM MONITORING

Real-time situational awareness arises from knowing you can see which endpoints are communicating and when. When System Monitoring is combined with Endpoint Visibility, you have the data to shape and enforce policies.
- 

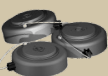
NETWORK HYGIENE

Misconfigurations, missing assets and other IT problems cause productivity issues, but they are also vulnerabilities. Intruders can hide amongst the noise and exploit systems if there is a high rate of out-of-spec behavior.
- 

NETWORK ACCESS CONTROL

Your network should never accommodate unknown devices. Make sure no unauthorized endpoint can successfully join the network. When combined with Endpoint Visibility, policies limiting network access are a huge step towards secure operations.
- 

MICRO-SEGMENTATION

Some devices should never communicate with others. For example, a bank teller's terminal shouldn't contact a payroll server. Enforce rules that define unacceptable communication by combining System Monitoring, Endpoint Visibility and acceptable use policies.
- 

ATTACK DISRUPTION & DETERRENCE

Traditional defenses are passive. Attackers consider these measures puzzles to solve or locks to be picked. Engaging the attacker to disrupt them imposes a cost on them. Halt the attack in its tracks and make it so attackers don't want to come in the first place.



Powerful and Easy

Easy Deployment and Operation Across Global Network Segments or Portable on a Laptop

Only one 1MB agent per network segment. Easy deployment; no network modifications. No systems overhead.

Instant-on: delivers value immediately. Easy integration with security ecosystem. Real-time, automatic and autonomous.

Easy

Only one single <1 MB core per network segment. No endpoint agents. No special training.

Deterrent

The only cyber deterrent: automatically engage, disrupt and impair the adversary.

Deterministic

No false positives. Exposes hostile behavior and configuration/hygiene problems deterministically.

Fundamental

Operates on Layer 2, beneath all other layers.

Comprehensive

Observes live-to-live and live-to-dark space communications. Protects IT and OT alike.

Lightweight

No network or endpoint overhead. No endpoint agents.

Immediate

Works instantly. No special re-configurations required.

Portable

The entire solution can be deployed on a single laptop.

Deployment	<ul style="list-style-type: none"> One Ridgeback core (1MB) per network segment. One central manager, one database. Multi-tenancy for IT services providers.
Operations (OSI Layers 2, 3, 4)	<ul style="list-style-type: none"> Comprehensive, real-time inventory of live assets on the network Observes layer 2 traffic between live assets Observes communications attempts between live assets and every dark IP
Phantoms	<ul style="list-style-type: none"> Ridgeback injects frames to respond to communication attempts in the dark space. Offending machine OS engaged in the kernel.
Policy framework	<ul style="list-style-type: none"> Instantly triggers actions and countermeasures when defined conditions are observed, live-to-live or live-to-dark.
Countermeasures	<ul style="list-style-type: none"> Address out-of-spec and malign activity. Lock processes and connections, isolate offending hosts.

Real-time live assets & 'Fact of' communications

Reveal hygiene issues
Instantly enforce policies

Millions of landmines
disrupt exploitation

Hacking operations are
painful for the Attacker

