RIDGEBACK Cyber Protection that Disrupts & Deters Attacks

Ridgeback's patented software dramatically improves the cyber-defense posture of any organization. Ridgeback delivers real-time comprehensive awareness of 'fact of' communications, exposing key issues in network hygiene that are both productivity concerns and security vulnerabilities.

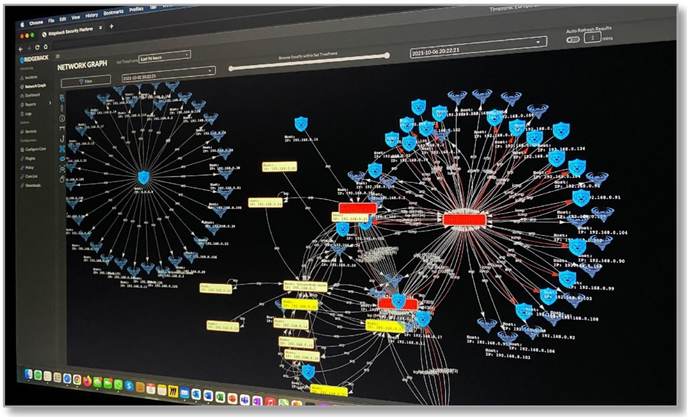
Ridgeback prevents attackers from discovering what is and isn't on the network, while also actively disrupting hacking operations by directly engaging attackers during their reconnaissance and exploitation activities inside the network.

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

THE ONLY PRODUCT THAT AUTOMATICALLY DISRUPTS ATTACKS IN REAL TIME.

AUTOMATES AND SCALES MAN-IN-THE-MIDDLE FOR DEFENSE TO ENGAGE, IMPAIR AND EVICT INTRUDERS AT THE INCEPTION OF THE EXPLOIT.

- Ridgeback is headquartered in Baltimore, MD.
- Founder: USMC Russian linguist, and 25 years US Intelligence Community.
- Solution is based on the strategies of warfare.
- Two issued patents.



Ridgeback applications

With its rich policy engine, Ridgeback delivers a range of high-value applications.

Attack disruption & deterrence – automatically engage malign actors. Inflict costs on attackers to deter current and future intrusions.

ATTACK DISRUPTION & DETERRENCE

Micro-segmentation – define and enforce permissible and impermissible endpoint communications.

MICRO-SEGMENTATION

Network Access Control – enforce limits to network access. Enforce standards for IP & MAC address pairings.

NETWORK ACCESS CONTROL

Network Hygiene – reveal and remediate missing assets and misconfigurations.

NETWORK HYGIENE

System Monitoring – real-time comprehensive situational awareness of communications at Layer 2

SYSTEM MONITORING

Endpoint visibility – Know your active / inactive resources. Track single-point-of-failure nodes.

ENDPOINT VISIBILITY

Red Team – map the live network.

RED TEAM OPERATIONS

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

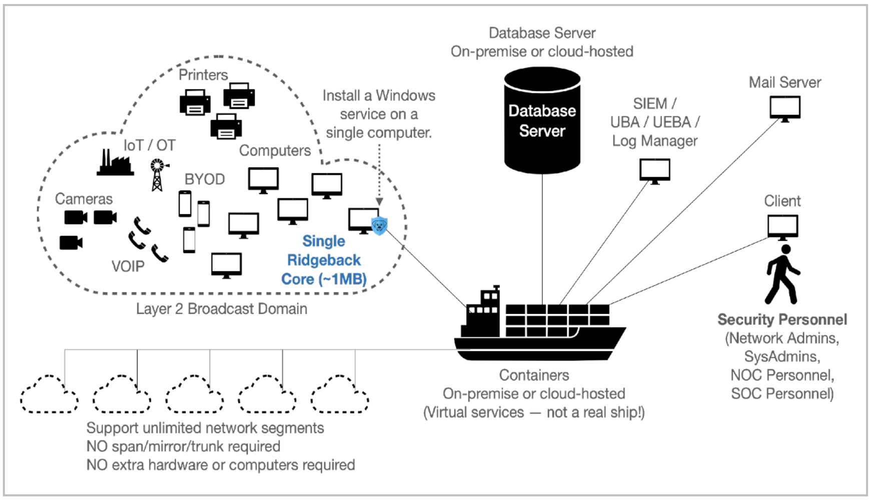
Only one 1MB agent per network segment. Easy deployment; no network modifications. No systems overhead.

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

Unique Deployment Architecture

Ridgeback requires only a single 1MB core installation per network segment. Ridgeback is managed from a central on-premise or cloud-based server.

- Extremely lightweight and invisible to normal network operations.
- Ridgeback is infrastructure agnostic. All hardware, all operating systems, transient devices and frequently-changing networks are protected.
- Ridgeback works instantly, no calibration or 'learning' required.
- Portable: Ridgeback can also be provisioned on a single laptop for rapid network assessments.


Database Server
On-premise or cloud-hosted
Printers
Install a Windows service on a single computer.
Database Server
SIEM / UBA / UEBA / Log Manager
Mail Server
IoT / OT
Computers
BYOD
Cameras
Client
VOIP
Single Ridgeback Core (~1MB)
Layer 2 Broadcast Domain
Security Personnel
(Network Admins, SysAdmins, NOC Personnel, SOC Personnel)
Containers
On-premise or cloud-hosted
(Virtual services — not a real ship!)
Support unlimited network segments
NO span/mirror/trunk required
NO extra hardware or computers required

Network Situational Awareness

Real time picture of the network map including details about IPs, OUIs, MACs, Ports, Services and patterns of Communication across geographies.

Visibility into Threat Landscape

Real time details of threats with and without payloads, open ports, LLMNR traffic, Missing assets, unauthorized scans, device discovery etc.

24 X 7 Network Monitoring

Means to monitor organization's security posture in real-time. Instant Identification + Elimination of Threats. 24X7 continuous, automatic and autonomous network VA and hygiene management.

Comprehensive Active Response

Any policy violation or contact with non-existent resources is instantly and automatically addressed across the entire organization.

Enterprise-ready solutions

No false positives, alert fatigue or analytical latency. No dependency on, nor requirement for, additional personnel. Focus on stopping the attack at the reconnaissance stage. Readily integrated into existing SOC operations.

.

Portable: on a laptop

Network-wide: one Ridgeback core per network segment

Rapid Assessments

Why?
Actual network behavior is opaque. See concerns instantly.

- Cyber risk audits.
- Regulatory compliance.
- M&A due diligence.
- IT services assessments.
- Cyber risk underwriting.
- Network forensics.
- VAPT.

Situational Awareness

Why?
Hygiene problems are productivity & security issues.

- Monitoring of network hygiene & configuration issues
- Compliance
- IT Management
- Security

Attack Disruption & Deterrence

Why?
Making the exploit painful defeats and deters attackers.

- Monitoring of network hygiene & configuration.
- Countermeasures to disrupt & deter attacks.
- Compliance, IT management
- Active defense

Unique Operating Profile

RIDGEBACK

Deployment	• One Ridgeback core (1MB) per network segment. • One central manager, one database. Multi-tenancy for IT services providers.
Operations (OSI Layers 2, 3, 4)	• 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	• Ridgeback injects frames to respond to communication attempts in the dark space. • Offending machine OS engaged in the kernel.
Policy framework	• Instantly triggers actions and countermeasures when defined conditions are observed, live-to-live or live-to-dark.
Countermeasures	• Automatically address out-of-spec and malign activity. • Lock processes and connections, isolate offending hosts.

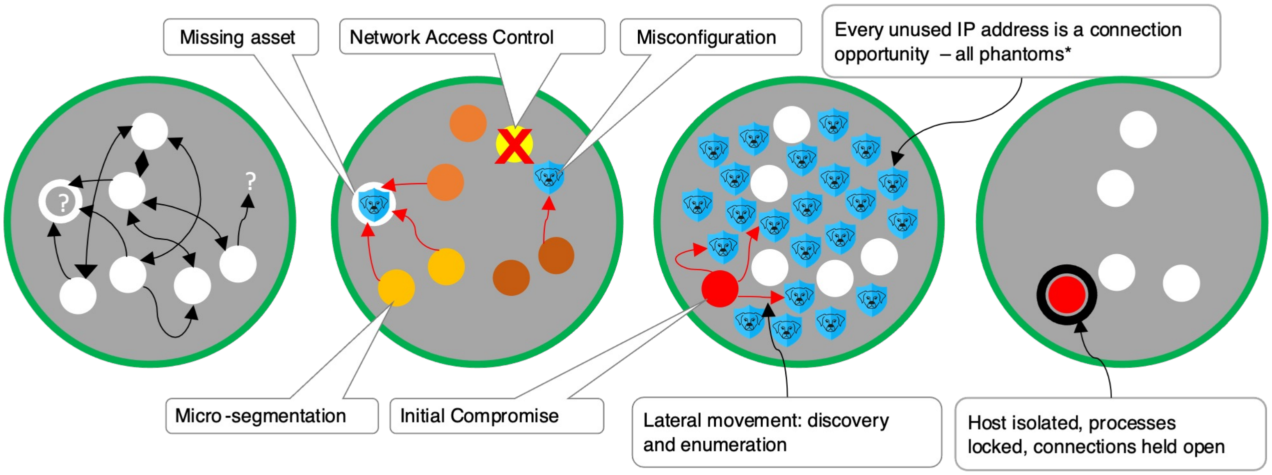
Know your assets | **See how they are communicating** | **Define acceptable-use** | **Auto enforce acceptable-use** | **Auto impair, evict intruders**

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


Missing asset
Network Access Control
Misconfiguration
Every unused IP address is a connection opportunity – all phantoms*
?
?
Micro-segmentation
Initial Compromise
Lateral movement: discovery and enumeration
Host isolated, processes locked, connections held open

* Phantom – something apparently seen, heard, or sensed, but having no physical reality.

Applicable to small, mid-sized and large organizations

Ridgeback allows businesses to implement capabilities across any network type, from offices to factories to hospitals to global, distributed computing environments that would otherwise require multiple products from different vendors.

Smaller businesses
Managed by a very small IT team.
No dedicated security budget.

Mid-sized companies
Managed by an IT department,
and maybe a small security team.

Larger enterprises
Dedicated security team managing
a suite of interlocking security tools.

Attack Disruption + **Network Monitoring** + **NAC Micro-segmentation** + **Red Team Operations** + **Integrations with other tools**

Less sophisticated — SECURITY STRATEGY — More sophisticated

Schedule a follow up discussion now: **info@p2sc.net**

Advantages

1 **Comprehensive monitoring**. Builds comprehensive, real-time inventory of live assets on the network, both IT &OT (any hardware, any OS). Observes and logs all traffic between live assets at Layer 2 as it occurs. Observes and logs connection attempts between live assets and every unused port on every unused IP

2 **Live-to-live policy enforcement**. User-defined policies enforce acceptable use for live-to-live communications. Ridgeback invokes countermeasures – including host isolation – when policies are violated. Out-of-spec events are instantly and automatically addressed.

3 **No dark space for attackers to hide**. Ridgeback injects custom ethernet frames on-the-fly, to create phantom endpoints that respond to ARPs, ICMP and TCP/IP payloads in the dark space. 100% of the IP address space appears to be addressable.

4 **Deterministic: no false positives.** Actual connection attempts to phantoms expose and disrupt reconnaissance and exploitation. Phantoms also reveal previously unidentifiable hygiene and configuration issues, e.g., missing assets, misconfigured systems.

5 **Painful for the Adversary**. Connection to any Ridgeback phantom results in the process being locked in the operating system kernel. Locked connections are immediately visible to the defender. Offending hosts can be automatically taken offline.

Policies & Reporting

Policy Framework – condition real-time intervention according to *any* observed conditions.

Examples of policy triggers

- Assets connected, disconnected
- Live-to-live communications observed
- Phantoms injected (live-to-dark communications)
- Port scan states
- Time of day, week, month
- Any non-Ridgeback data trigger
- Any multi-factor combination of data
- Chained policies, in sequence

Examples of Actions

- Notifications & Syslogs
- Isolate threat endpoint
- Isolate high value endpoint
- Trigger actions by other tools

Reporting – real-time status of your network and potential vulnerabilities.

Examples of reporting tools

- Live Incident report
- Network Graph: Live-to-live communications observed
- Network Graph: Phantoms triggered (live-to-dark)
- Threat Summary
- LLMNR Misconfigurations
- Attack Surface Summary: Current Vulnerabilities
- Attack Surface Matrix: vulnerabilities overview
- Asset Inventory: List all active nodes on network
- Raw Logs (Also available in database
- Analytics: Charts
- Policies Active, Policies Available

Reporting: real-time and historical insights into network behavior

Manage incidents – automatically engage malign actors. Inflict costs to deter intrusions, review ongoing and historical incidents and take action.	Incidents
Dynamic network visualization – Your network will make sense, and you will see who is talking to what, and all the attempts to discover assets.	Network Graph
At-a-glance – see immediately what has happened and what is happening, both reconnaissance activity and active threats.	Threat Summary
Hygiene – See the most common and easily addressable vulnerability.	LLMNR Summary
Know your risk – see what is available to attackers on your network.	Attack Surface
Asset Management – Know your active / inactive resources.	Asset Inventory
All Data Available – Search and segment - unlimited possibilities.	Forensics (Logs)

Schedule a follow up discussion now: **info@p2sc.net**