Annual IT Security Spend Has Grown From $3bn to $120bn Since 2003, And We're Still Not Secure.

A Brief Guide To Changing The Unsustainable Dynamic In Cyber

10 min eBook

RIDGEBACK

eBook Overview

A New Framework to Win the Cyber Defense Battle

- A runaway problem and its implications
- The single greatest exposure: Lateral Movement
- Traditional defensive approaches are challenged
- Keys to a new kind of response
- Turn the tables on the Adversary by reshaping the battlefield
- Network security as a deterrent
- Security implementations must be easier *and* reduce the burden on the defender
- Tying it all together

Cyber challenges keep compounding

A few key facts about IT make it clear that the dramatic expansion in the utility and availability of computing at every level has helped to create a many-headed issue for security practitioners. The ubiquity and depth of our reliance on IT has grown exponentially based on a few simple facts.

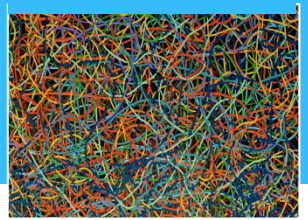
- IT quickly became universally accessible
- Systems are designed to be open and interoperable
- Usage is scalable to millions of myriad stakeholders
- Enterprise networks have become extremely complex
- Security is bolted-on…rather than built in from the start

For cyber Adversaries, these conditions created an opportunity to wreak havoc (with the same advances in resource sophistication at their disposal).

- The universe of threats is absolutely massive and evolving dynamically, minute-by-minute.
- Control over IT assets is binary…you have it or the Adversary does
- Damage and theft can occur in moments

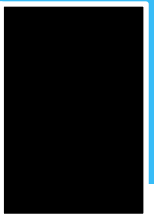
The combination of factors at play has created a never-ending arms race……..without any discernible benefit to the defender.

Complex networks, users & unmanaged devices



Massive, evolving threat universe

Control is zero-sum



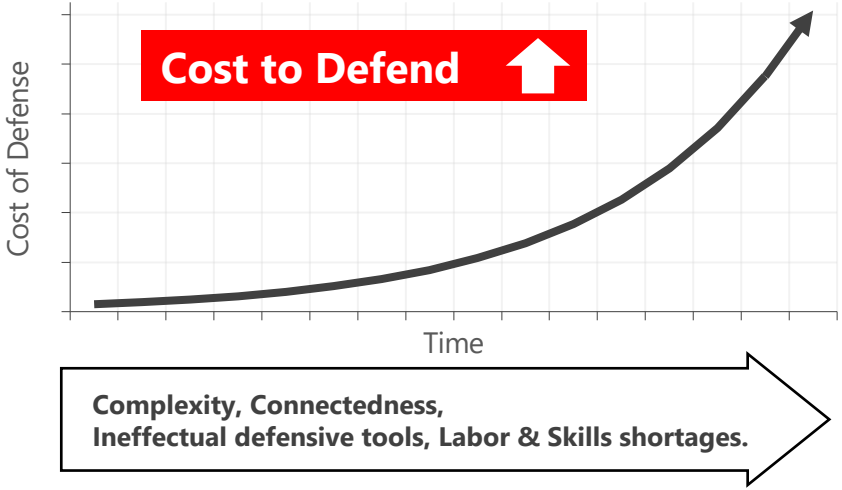
Damage occurs in seconds

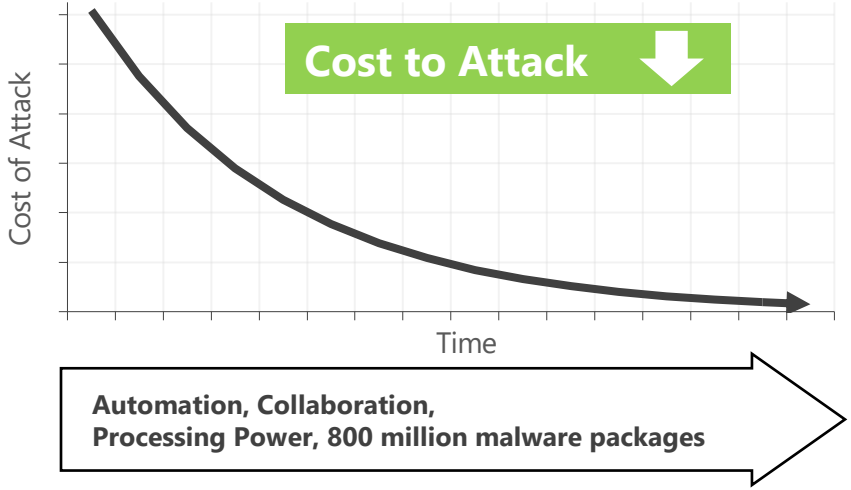
The course we're on is dire

A quick look at the IT spending environment on cyber security gives pause for serious concern.

During the period from 2004 to 2020 *annual* cyber spending globally has increased from $3 billion to over $120 billion. Our complex, interconnected networks are getting harder for put-upon staff to defend; on the other hand, the adversary is in a golden age, enjoying more efficient resources and continually innovating methods to make more frequent, concerted and successful attacks.

As the curves reflecting the growth in spending and the relative ease of attacking continue to separate, our use of Information Technology may logically reach a state in which IT is a greater liability than asset.





The key front in cyberwar is lateral movement

Cyber adversaries need knowledge of your network so they can move through it to expand control over your IT systems, and ultimately grab your valuable data.

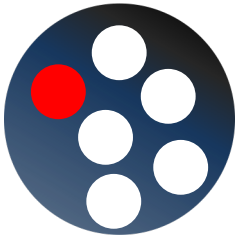
The initial breach is their starting point – but the real damage occurs when an intruder uses *lateral movement* to expand their control over system resources to discover and steal information.

If they can't expand their control over your system resources, they can't find what they're after – they *depend* on lateral movement to achieve their goals.

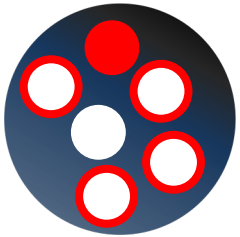
This goes for remotely directed exploits, insider threats, and even malware designed to propagate autonomously.

A single compromised endpoint serves as the launching pad for a deep exploit.

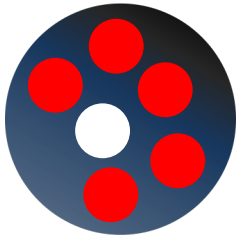
LATERAL MOVEMENT



Compromise an individual endpoint in the network



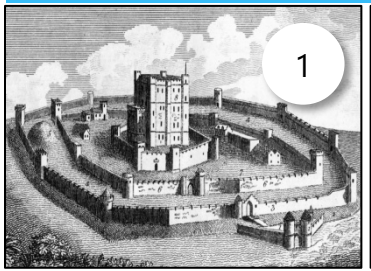
Acquire knowledge of the Network environment

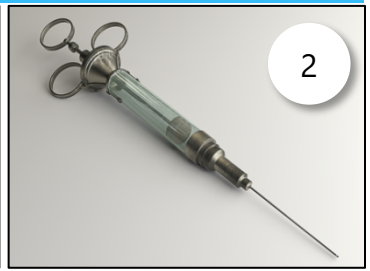


Gain control over resources

Extract Data

Traditional defenses won't ever change the dynamic





1. Perimeter defense
2. Endpoint Defense
3. Behavioral training
4. Intrusion Detection

Keeping the bad guys out has been the top priority. However, with successive generations of interconnected systems, our networks have become extremely complex – so complex that no one can possibly identify every single avenue into the network or protect every endpoint to secure them against intruders. BYOD and IoT add to the challenge.

A strong second priority is to inoculate every possible endpoint against malicious code. Keeping up with the state of malware, while also ensuring that every machine is reliably up to date is sure to let us down at some point. And this doesn't even cover the proliferation of unmanaged devices in IoT and OT categories.

Training users on standards of behavior is an important contributor to IT best practices, however it is not failsafe…human beings are independent agents whose behavior, even if well intentioned, won't always conform with the needs of security.

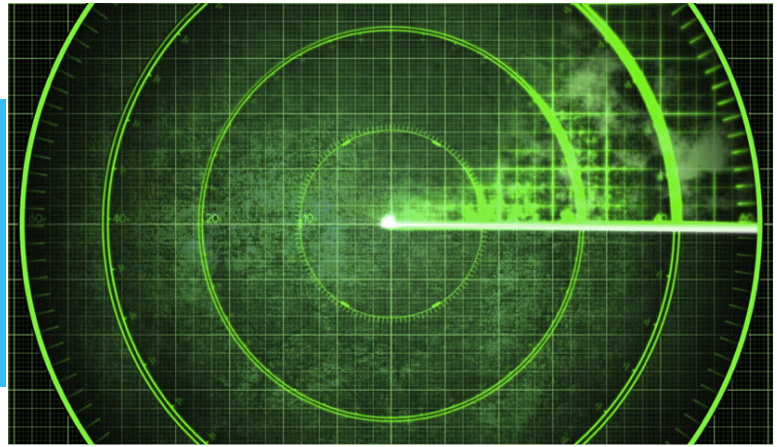
Finally, watching traffic in the network to be sure that efforts to keep intruders out have been successful to discern malicious activity is increasingly critical.

Surveillance cameras are perhaps a funny way to think of Intrusion Detection. But almost all IDS/IPS systems watch network traffic to apply rules or data science to distinguish malicious traffic from normal, benign behavior in the network.

While analytical techniques can alert you to the presence of malicious behavior, they will often alert you that benign behavior appears threatening.

So, now we're dealing with false positives.

Detection systems that cry wolf cost money; real wolves go unnoticed.



False positives result from the fact that large volumes of network traffic generate masses of data, and fine-tuning a detection system in a complex network to be *correct* at distinguishing malicious from benign activity all the time just isn't possible.

You end up either missing bad actors, or being alerted that good actors are bad ones. Most importantly systems that cry wolf mean real wolves are likely to go unnoticed.

Keep in mind that intrusion detection assesses behavior that has *already* occurred, and that each alert needs to be followed up on, creating time-consuming incident response burdens for otherwise busy security teams.

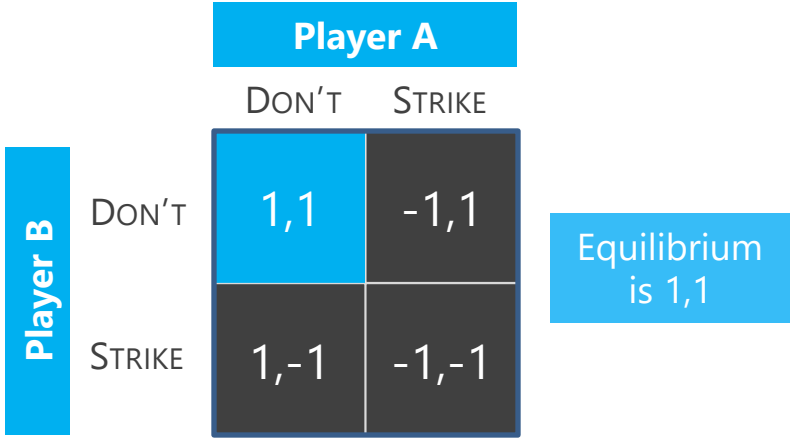
So, intrusion detection is after-the-fact, and ends up consuming wasteful incident response man-hours.

…a day late and a dollar short.

Game Theory proves we're in trouble if we don't change our approach

Amidst all the runaway spending on traditional, passive defensive methods, and with the pernicious dynamic between Attacker and Defender in mind, zero sum game theory is a helpful theoretical framework we're all familiar with. Zero sum theory is especially applicable to cyber because the defender's loss is the attacker's gain, at the individual resource level, the corporate network level, and writ large across the computing landscape.

According to zero sum game theory, each Player (attacker and defender in this case) chooses a value-maximizing strategy, while giving consideration to the expected response of the Other Player.



Equilibrium is the point at which neither player can improve the outcome for themselves by altering their strategy.

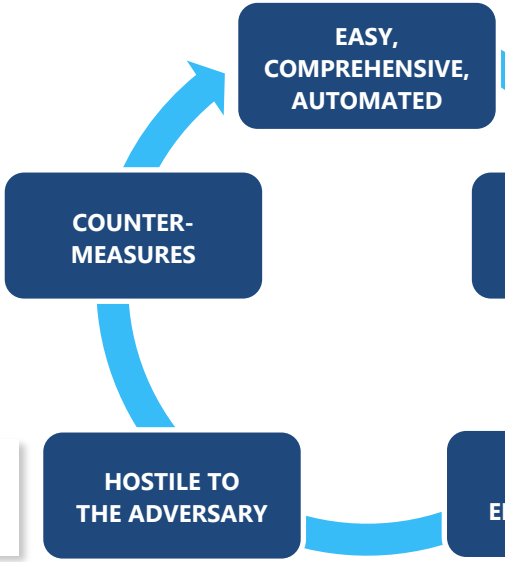
In cyber, our strategy has been to continually augment defensive spending. However, this strategy has exerted no practical effect on the attacker, even as it has dramatically grown the burden on our own operations. In the language of game theory, the equilibrium is really a disequilibrium firmly in favor of the attacker.

The theory suggests that the only possible way to address such a pernicious dynamic is to impose a cost on the attacker that can act as a deterrent to attacks and reset the equilibrium at a point more favorable to the defender.

Keys to a new kind of response

Increase the burden on the Adversary; lighten the load on the defender

There are a few key attributes of a security approach that will render intolerable the Adversary's experience on your network. They will also make make your network security comprehensive, automated, and actually reduce your team's labor burden.



Render security easy to deploy, instantly effective and to reduce incident response manhours. Readily scalable across the enterprise and global network operations.

Know what you need to know about your network's profile from the attacker's point of view, all the time.

Interdict unpermitted communication between any sets of live endpoints without any rigid configuration or hardware requirements (and in real time).

Shape the network to be impossibly hostile to the adversary. Impair them as they attempt lateral movement.

Impair the intruder and neutralize threats so no harm can come to your network or IT resources, and so they but they experience costly burdens.

Turn the Tables on the Adversary

Just like in sports or war if all you do is play defense, you're bound to lose eventually.

Ridgeback plays offense by actively shifting the burden of the exploit back onto the attacker, so you control the outcome.

Ridgeback assumes the perimeter has been breached. It is designed to ensure the breach cannot lead to any further harm by denying the adversary information, arresting the adversary's lateral movement, and counter-engaging threats to extinguish them from your network – all automatically, in real time.

Ridgeback does not use analytics and produces no false positives. it is easy to install, deploy and manage. In fact, there is no burden on the live network or on your compute resources.

As a product, Ridgeback is agnostic to threat types, known or unknown. Its ultimate promise is to generate a comprehensive enterprise security program that is completely adaptive.

Hostility to the Adversary

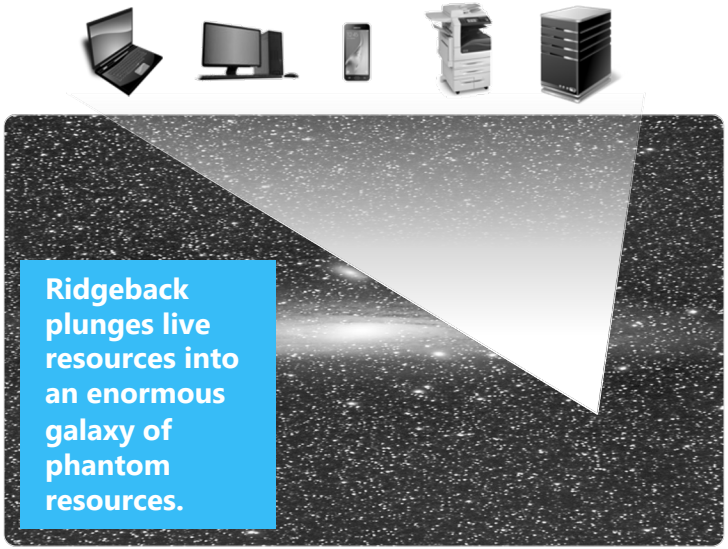
Policy Enforcement

Countermeasures

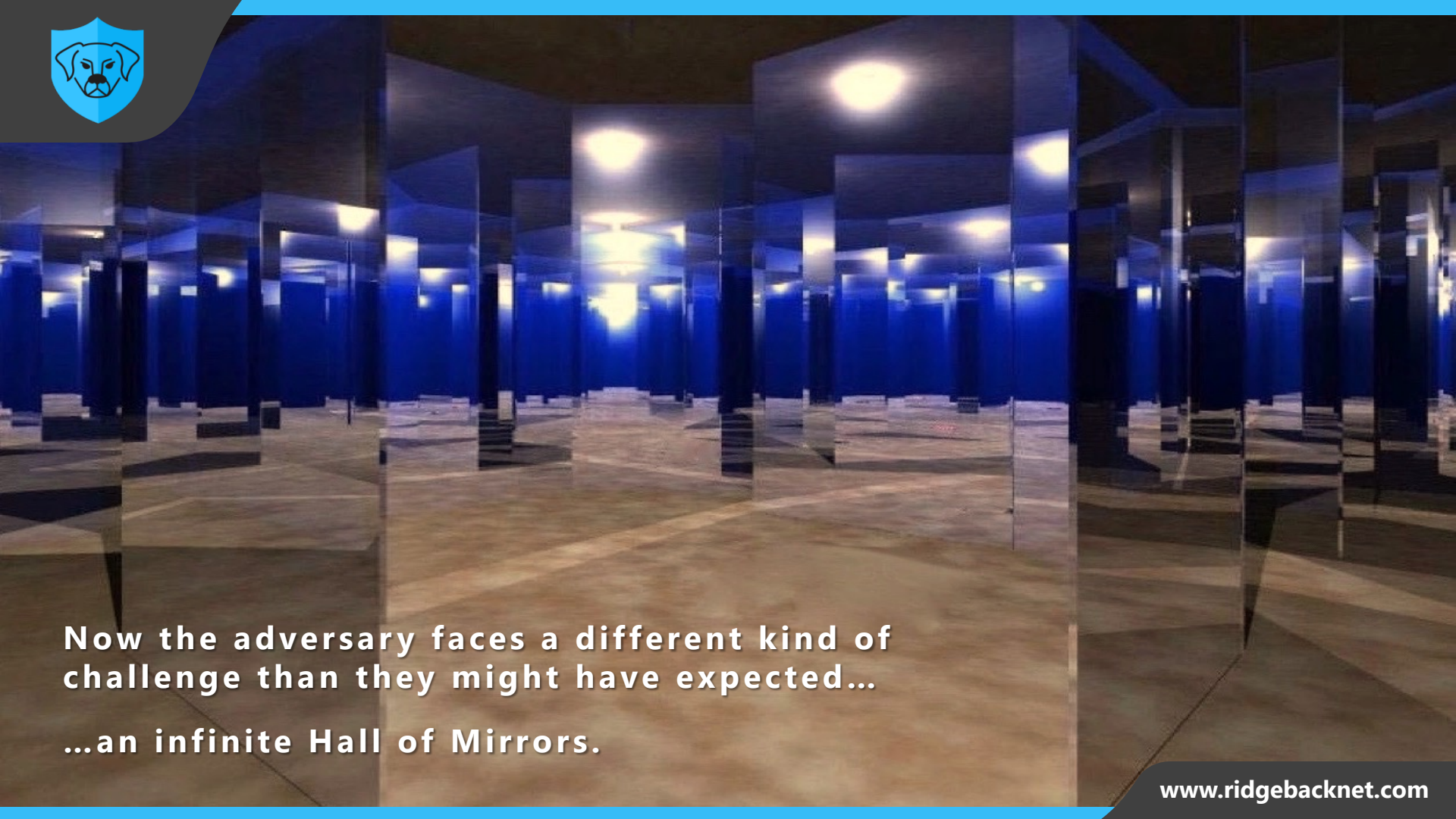
Continuous Visibility

Easy. Comprehensive. Automated.

How? Reshape the Battlefield



- First, Ridgeback actively observes *ALL* internal network communications between live resources to provide real time insight into what's there…as well as what's not there, e.g. decommissioned servers that other endpoints continue to see as a trusted connection. Not only do you see a continuous live picture of the network, anomalies in configuration hygiene are surfaced for remediation.
- Second, Ridgeback presents an inordinately large and confusing network environment in which the data needed by intruders to move laterally is poisoned and useless for network reconnaissance. Ridgeback also comingles all the live resources on your network with what appear to be *millions or billions* of 'available' IT resources – hardware, services, etc. – but are in fact all illusions created by Ridgeback.
- When a communication policy is violated or any compromised host on your network (a resource that has fallen under the control of an adversary) attempts to map the network, to move laterally or to propagate malicious code, contact with a Ridgeback phantom is a sure thing.
- To use military jargon, the attack surface has been altered, expanded billions-fold, to make the attacker's job impossible.


Now the adversary faces a different kind of challenge than they might have expected…
…an infinite Hall of Mirrors.

Now Fight Back

Changing the attack surface is just the first effect Ridgeback creates.

Next, if one endpoint is trying to scan, connect with or engage resources that exist only as Ridgeback inventions, or live resources attempt communication in violation established policy…Ridgeback acts back, instantly, with countermeasures.

Unlike detection systems that assess traffic to produce an alert of what *might* be malicious behavior, Ridgeback makes no judgments – and generates no false positives.

Ridgeback creates an infinite minefield that an adversary cannot avoid. When a mine is tripped, the offending host is taken offline., and the intruder is impaired.

The battle is won before the attack can spread.

1

Ridgeback transmits a wholly inaccurate, useless picture of a network loaded with poisoned data resources and rife with connection opportunities – but are Ridgeback phantoms.

2

Every Ridgeback phantom acts like a landmine.

When a phantom is contacted, or a predetermined policy is violated…

3

…the compromised resource interacting with a Ridgeback phantom or violating policy is taken offline automatically, arresting its ability to move laterally so it *can't do any harm.*

4

In order to tie the Intruder up in knots, every connection with a Ridgeback phantom or in violation of policy – and the process making the connection – is held open and cannot be closed.

Security needs to be easy

Ok. Here's how Ridgeback's infinite minefield makes security easy.

Ridgeback is software that runs in containers for scalability and high availability.

A central management interface controls Ridgeback operations across the entire network.

Each individual remote core (<1MB) can serve an entire network segment, anywhere globally.

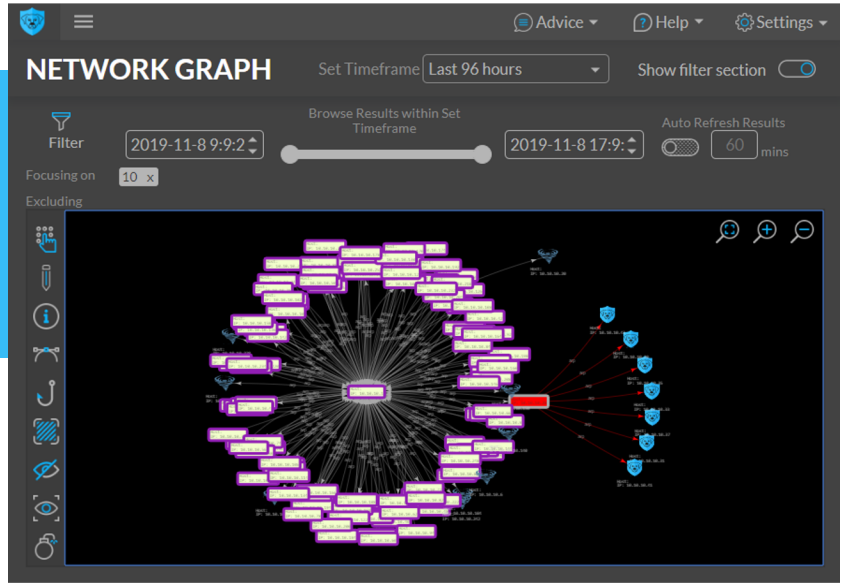
Every asset or resource within each network segment served by a single Core falls instantly into the protective envelope of Ridgeback.

It takes about an hour to have Ridgeback up and running. There's also nothing to change on the live network, and no agents to install on each local device.

Ridgeback is designed to be managed using our interface, or easily integrated with other tools.

Ridgeback is instant-on, starting its work immediately at launch

1 Download 2 Install 3 Connect 4 Launch

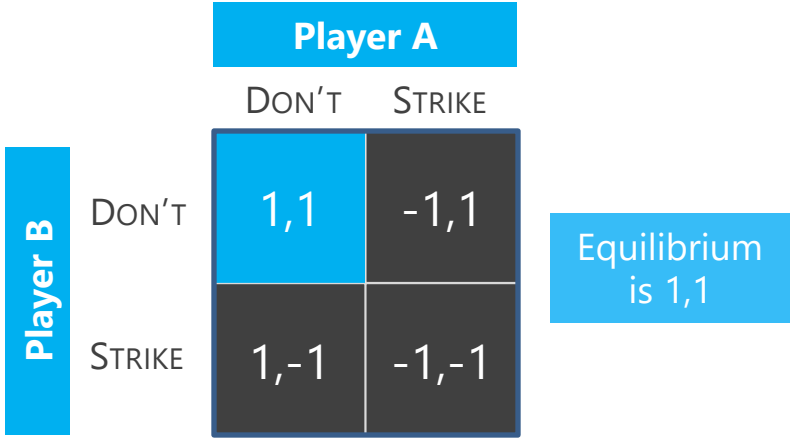


Ridgeback's fit with Game Theory

Ridgeback substantially lightens the burden of security on the enterprise, and puts the cost of an Attack squarely back on the Adversary in a couple of important ways.

1. A network that instantly presents an obviously inhospitable environment to the Intruder creates an incentive to abandon the attack and go elsewhere.
2. If the Intruder moves forward with the exploit, interaction with Ridgeback ties the effort up in knots…by keeping the connections and processes used by the Intruder open at the kernel level, and by isolating the compromised resource from contact with any other live resource.

An intruder's experience, in addition to being fruitless, will be profoundly confusing, frustrating and wasteful…acting as a deterrent to their malign intent. Unlike traditional, passive defenses, the burden is squarely placed back on the Intruder.



Watch or Fight back?

Here's a quick quiz to draw the distinction between Active Engagement and Intrusion Detection systems.

"Your kitchen is exposed to frequent mouse infestations.

Question: Do you…"

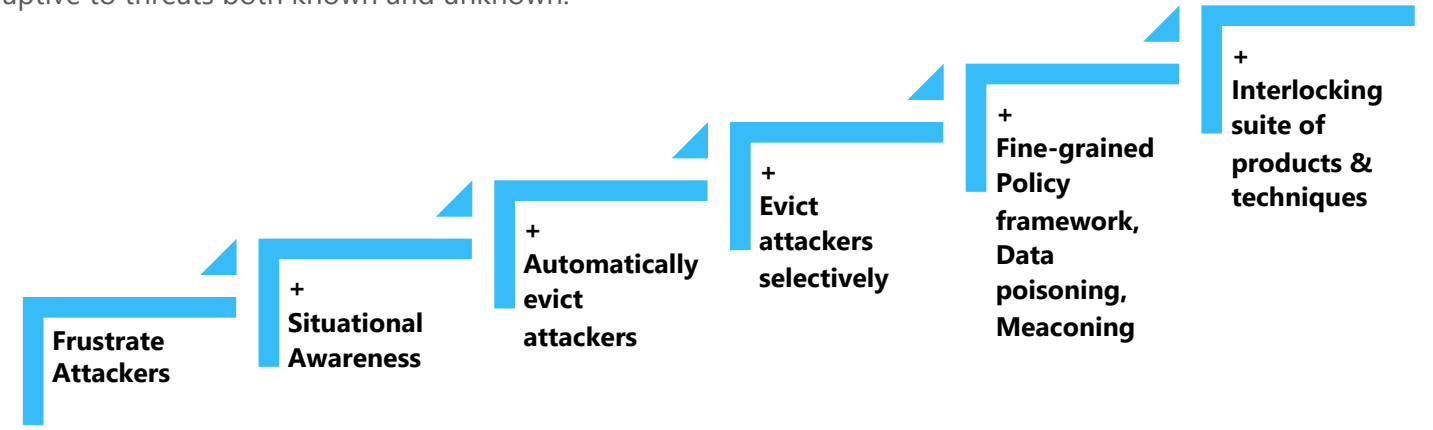
A. Set up a network of cameras and motion detectors that track mouse activity?

B. Set billions of unavoidable mousetraps that eliminate mice when tripped?

Intrusion detection systems only do A.
Ridgeback does A. and B.

Comprehensive adaptive security, Irrespective of the scale or sophistication of your IT operations

Ridgeback fills a critical hole in security, whether you're managing a suite of interlocking techniques to protect a highly sensitive global network, or you just want an easy way to make your network dramatically less attractive to an Intruder than other networks in the neighborhood. It will also assure you that your network is completely adaptive to threats both known and unknown.



Smaller business environments with limited number of IT personnel

Multi-location mid-sized companies, managed by an IT department

Large global enterprises with a dedicated strategy/security team.

RIDGEBACK

A Comprehensive Security Strategy Must Address Lateral Movement

- Traditional, passive defenses get breached too often, and they continue to drive up our costs.
- Adversaries us Lateral movement techniques to expand control over your systems.
- Control over more system resources allows an Intruder to steal your data and inflict damage.
- Intrusion detection is after-the-fact. False positives create more wasteful incident response work.
- Control is a zero-sum game. Either you have it or the Adversary does.
- It's getting easier to attack, harder to defend in spite of our heavy investments in people, process and product.

Ridgeback is Comprehensive, Easy and Defeats Lateral Movement

- Ridgeback reshapes the battlefield in ways that make it impossible for the Adversary, easy for you.
- The hall of mirrors / infinite minefield gets threats off the network immediately.
- Ridgeback is real time. No false positives.
- Ridgeback provides situational awareness of both benign and malicious behavior, and allows easy policy enforcement
- Ridgeback is easy to install, deploy and manage for any enterprise type or size.
- Security is comprehensive, easier and adaptive.
- You can test Ridgeback on your network to see its value demonstrated in hours.

If you'd like discuss comprehensive, easy security that changes the unsustainable dynamic in cyber, reach us at

info@ridgebacknet.com