TECHNICAL OVERVIEW

Ridgeback Interactive Defense Platform

Thomas Phillips, CTO
tom@ridgebacknet.com

Reference Links

1. Ponemon Institute, October, 2015
2. RSA Research, March, 2016
3. Ponemon Institute, October, 2015

"Reduce the hostile chiefs by inflicting damage on them; and make trouble for them, and keep them constantly engaged; hold out specious allurements, and make them rush to any given point."

- Sun Tzu

EXECUTIVE SUMMARY

Ponemon Institute reports that the average U.S. company of 1,000 employees spends $15 million a year battling cybercrime, up 20% compared to last year. Despite such high levels of spending ($75B worldwide in 2016), RSA Research indicates that only 24% of firms worldwide are satisfied with their ability to detect and investigate threats, showing dissatisfaction with their capabilities.

Once a data breach occurs, it takes an average of 98 days for financial services companies to detect intrusion on their networks and 197 days in retail (Ponemon Institute report). It gives intruders plenty of time to laterally move across the enterprise (and insider threats can make this worse). For most enterprises, this problem is getting worse due to extremely complex networks, aggressive, automated attacks, and more and more state actors getting involved. The enterprises have realized that perimeters can't be protected, accurate intrusion detection is impossible, static defenses i.e. most of the existing solutions do not work and that the cost of maintenance of security apparatus is becoming cost prohibitive.

New approaches to counter cyber adversaries are overdue and the enterprises are starting to take a serious look at “deception technology” as a viable approach and key element of the overall cybersecurity strategy stack. Most of the current deception vendors are based on HoneyPot and HoneyNet technologies.

This white paper introduces an entirely new approach in deception, fundamentally based on the principles of Sun Tzu's 2000+ year old classic “Art of War”. The security philosophy of Ridgeback Network Defense is that the cost of defense should be minimized while the cost of attack should be maximized making it very difficult to attack and very easy to defend. The paper provides insight in the philosophy and workings of the Ridgeback Interactive Defense Platform.

The security philosophy of Ridgeback Network Defense is that the cost of defense should be minimized while the cost of attack should be maximized making it very difficult to attack and very easy to defend.

TABLE OF CONTENTS

THE PROBLEM

A future where the annual costs of being connected outweigh the benefits is not only possible, it is happening now. According to our project models, annual cybersecurity costs in high-income economies like the U.S. have already begun to outweigh the annual economic benefits arising from global connectivity.

— Atlantic Council, Risk Nexus: Overcome by cyber risks? Economic benefits: and costs of alternate cyber futures

The most prevalent security paradigm, the classification of signals, is an unwinnable arms race. The vast majority of security solutions are designed to detect undesirable endpoint or network behavior, yet it can be proven that accurate and reliable detection is impossible in the general case, and especially so if an adversary has some degree of control over the signals being analyzed.

Organizations have compensated for the underlying problem by increased spending on security solutions. The costs of security continue to increase without bounds. Expenses are spread across:

- New security tool acquisitions and implementations,
- Technology updates and refreshes,
- Additional or more skilled labor, and
- The costs of recovering from security incidents that were not prevented.

Attacks continue unabated, and they are occurring more frequently and with increasing sophistication. Ultimately, the costs of securing IT systems will outweigh the benefits the systems provide.

THE PHILOSOPHY

Reduce the hostile chiefs by inflicting damage on them; and make trouble for them, and keep them constantly engaged; hold out specious allurements, and make them rush to any given point.

— Sun Tzu, The Art of War

Sun Tzu was a Chinese general, military strategist, and philosopher who lived over 2,000 years ago. He wrote a famous book called The Art of War, in which he described strategies to be employed to achieve victory in war. His strategies not only still apply to war today, but they also apply to cyber conflict. Sun Tzu argued that to win a war one should endeavor to cause the enemy to unnecessarily exhaust their resources. He also cautioned that certain mistakes would lead to defeat.

One of the "dangerous faults" that Sun Tzu warned against was "over-solicitude" for one's resources, which exposes one to "worry and trouble." Unfortunately, this fault is the security strategy most commonly employed by organizations. Security tools and professionals spend an inordinate amount of resources trying to monitor and evaluate the security status of every last IT resource, while doing nothing to influence adversary behavior. The end result is an ever-escalatingcost of defense.

Ridgeback Network Defense advocates taking the fight to the enemy and causing the adversary to needlessly exhaust resources. This aggressive strategy results in the cost of attack outweighing the benefits of attack.

INTERACTIVE DEFENSE

Legacy network security products attempt to classify network activity as either good or bad, but the approach fails because adversaries are adept at evading these schemes. Security tools and professionals spend an inordinate amount of resources trying to monitor and evaluate the security status of every last IT resource, while doing nothing to influence adversary behavior. With legacy security products, defending is much more difficult than attacking.

The end result is an ever-escalating cost to defend.

Ridgeback Network Defense takes the fight to the enemy using Interactive Defense and causes the adversary to needlessly exhaust resources. This aggressive strategy results in the cost of attack outweighing the benefits of attack.

What is Interactive Defense?

Interactive Defense is an advanced stealth and deception capability designed to ensnare adversaries in several ways:

- DECEIVE

  Manage billions of decoys in the network that immediately trigger Ridgeback response to the presence of intruders.

- INFLUENCE

  Influence the behavior of intruders so they are easier to detect, shifting the cost of attack back to the attacker.

- ELIMINATE

  Block access to protected network services without revealing the services have been blocked.

Interactive Defense dynamically changes what intruders observe, disguising the network's security posture and creating the circumstances for a victory by the enterprise.

THE OPERATION

Ridgeback is like using weaponized virtual reality (VR) to thwart adversaries.

— Thomas Phillips, CTO Ridgeback Network Defense

Ridgeback is a security platform for injecting, modifying, and dropping Ethernet frames, as needed, with the purpose of influencing adversary behavior. Those familiar with offensive hacking techniques may see the similarity between Ridgeback operation and man-in-the-middle attacks. It is the ability to alter what an adversary observes that allows Ridgeback to influence the adversary's behavior. By influencing adversary behavior, Ridgeback can coerce the adversary into unnecessarily expending resources, and thus dramatically increase the cost of attack.

As soon as Ridgeback is turned on, it begins to actively thwart attacks by giving the illusion of a target-rich network. Although an adversary may believe that connections to the targets are successful, Ridgeback is actually consuming adversary resources, slowing down the adversary's attack platform, and, if desired, automatically disconnecting the adversary from the network.

Ridgeback will automatically report attacks as active threats or possible threats, with both kinds of alerts being actionable. Active threats occur when an adversary attempts to transmit information to or from fake resources using any protocol that can deliver a payload. Possible threats occur when an adversary attempts to scan fake resources using a protocol that does not deliver a payload.

In both cases, the adversary behavior poses an immediate threat to the integrity of the network; the situation should be rectified immediately and without delay. To use the mousetrap metaphor, a mousetrap does not detect mice, but instead, a mouse traps itself within the mousetrap. A trapped mouse should be disposed of immediately.

Ridgeback can be configured to provide any kind of alert or counter measure, as deemed appropriate by the organization's security policies. In addition, Ridgeback's criteria for alert can be adjusted to fit the organization's needs for security or IT management.

HACKER / ADVERSARY EXPERIENCE

You are in a maze of twisty little passages, all alike.

— Will Crowther, Colossal Cave Adventure

Ridgeback is designed to confuse, annoy, frustrate, and slow down adversaries, causing them to waste resources and perform excessive analysis. Confronting Ridgeback is neither enjoyable nor rewarding, and generally feels like a immense amount of wasted effort with no return. By automatically disconnecting an adversary from the network, Ridgeback causes the adversary to reveal any exploitations that can be used to initially breach the network. That is, rather than

generally looking for all possible vulnerabilities, which is an impossible task, Ridgeback forces the adversary to reveal the vulnerabilities that can be exploited.

THE ADVANTAGES

Every great and deep difficulty bears in itself its own solution. It forces us to change our thinking in order to find it.

— Niels Bohr

The key advantages of Ridgeback are:

- Ridgeback influences adversary behavior, dramatically increasing the costs of attack while slashing the costs of defense;
- Ridgeback is quick and easy to deploy;
- Ridgeback can remediate security incidents almost instantly;
- Ridgeback scales easily and affordably;
- Ridgeback is easy and affordable to integrate with other systems; and
- The Ridgeback platform is easy and affordable to extend.

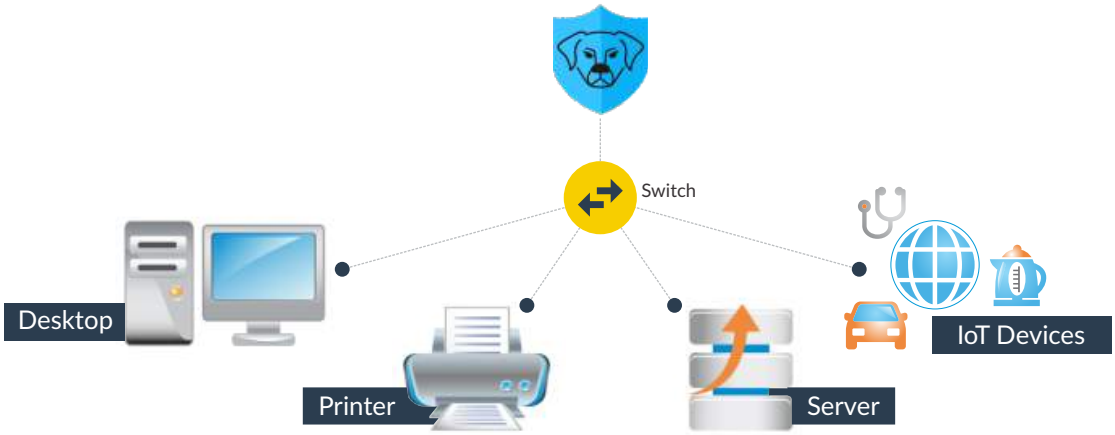
DEPLOYMENT OPTIONS

When I am working on a problem, I never think about beauty but when I have finished, if the solution is not beautiful, I know it is wrong.

— R. Buckminster Fuller

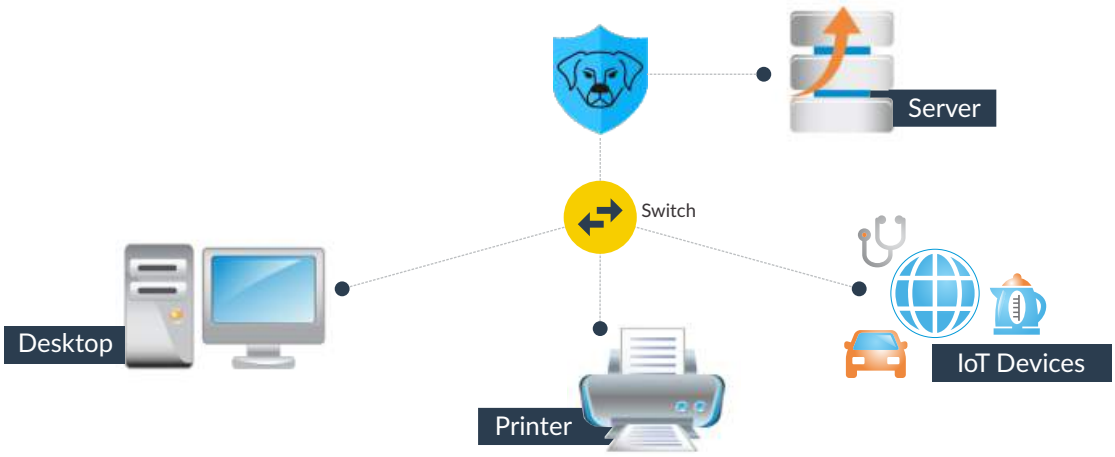
Ridgeback is a standalone software product that can protect an entire subnet using an auxiliary deployment. The auxiliary deployment is the simplest type, requiring little to no configuration of Ridgeback and no configuration for the network being protected.

Auxiliary Configuration



Ridgeback also can be deployed inline to provide additional point defense for a high-value resource.

Inline Configuration

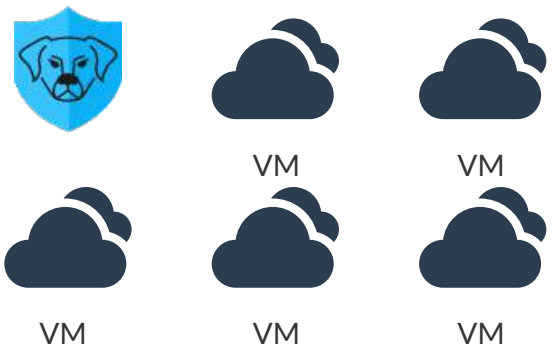


DEPLOYMENT OPTIONS

Ridgeback can operate on a physical network or on a virtual network. The only requirement is that the Ridgeback installation have access to the layer 2 network traffic.

Many possibilities exist for deployment configurations. Some example deployment configurations are illustrated below. Many other possibilities exist for mature organizations that have adopted software defined networking (SDN) or other advanced network technologies.

Virtualized or Private Cloud



Example Hypervisors

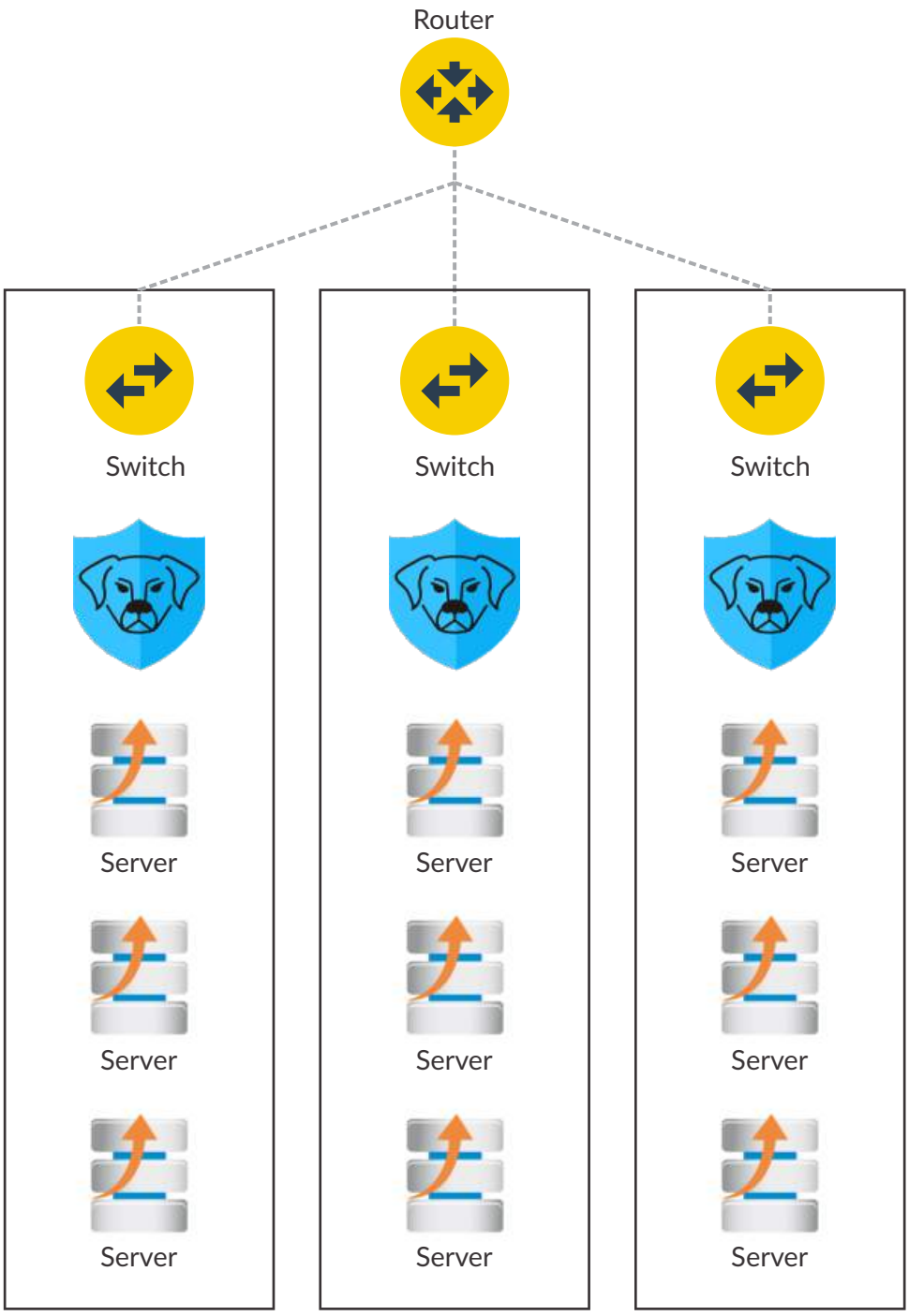
vmware

Xen

Microsoft Hyper-V

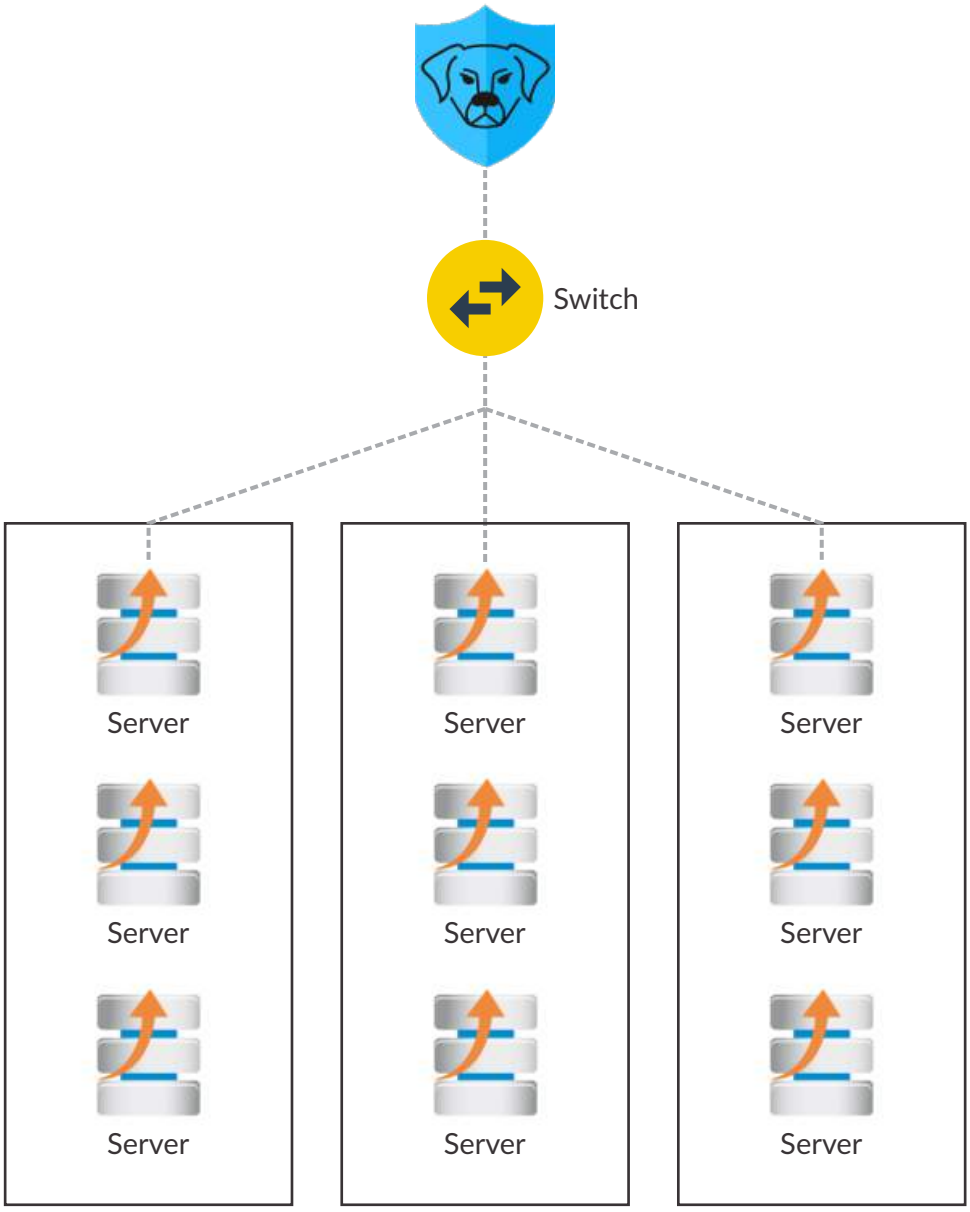
DEPLOYMENT OPTIONS

Top of rack, L2 Broadcast Domain in each rack



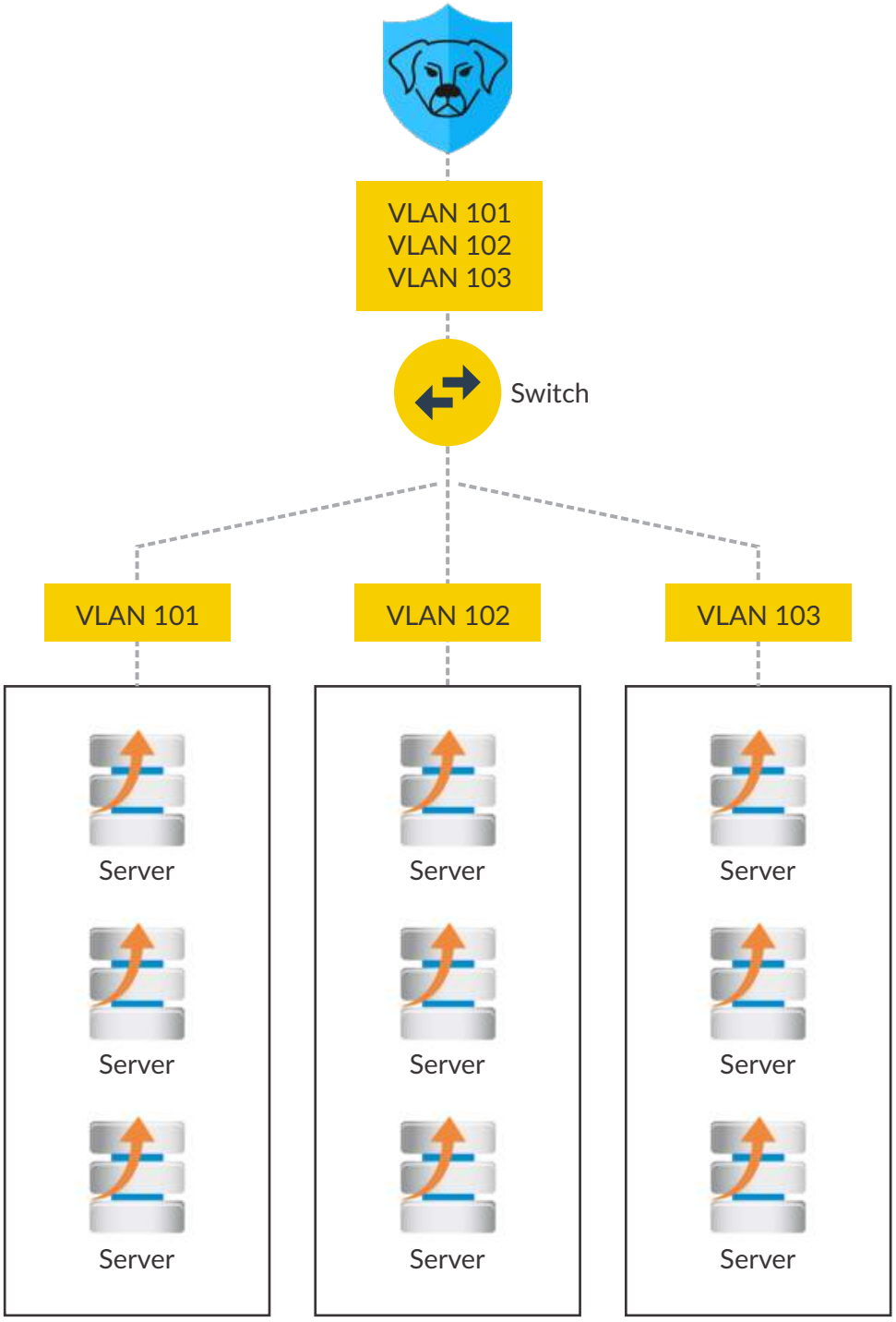
DEPLOYMENT OPTIONS

End of row, L2 Broadcast Domain across all racks



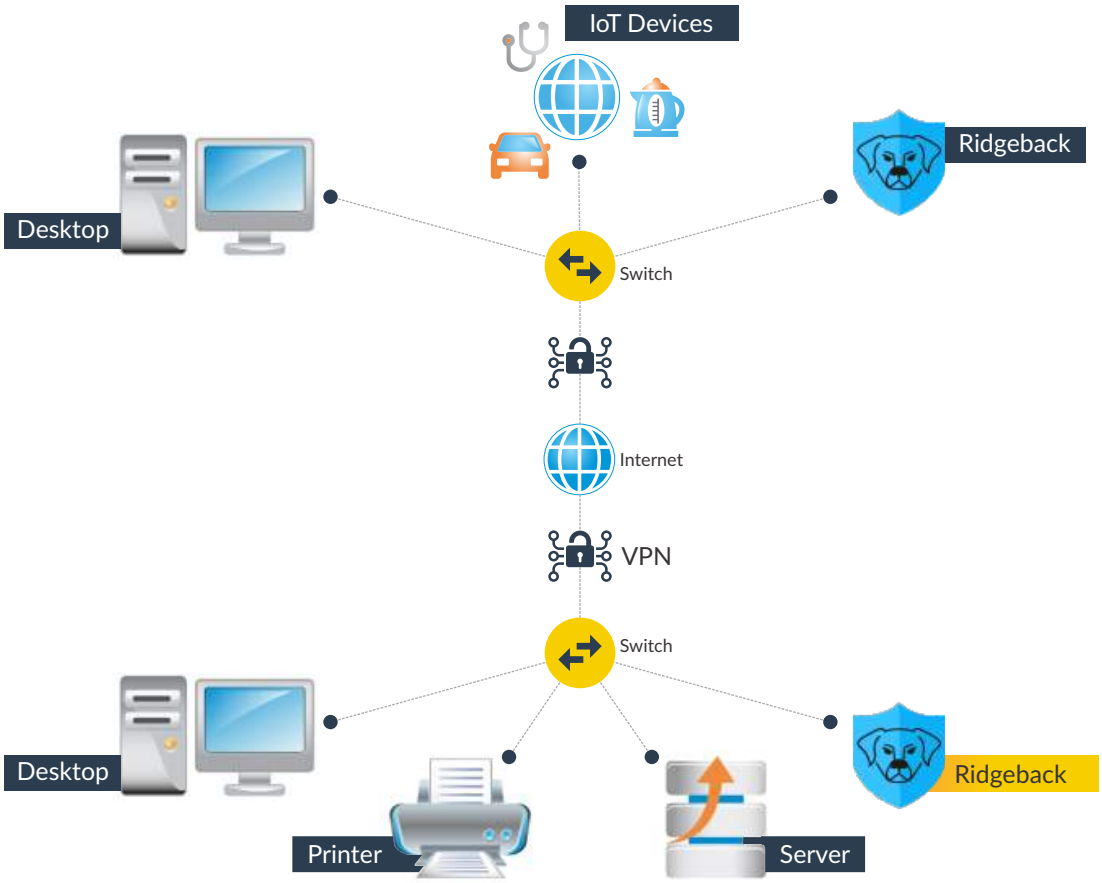
DEPLOYMENT OPTIONS

End of row with VLANs



DEPLOYMENT OPTIONS

Protecting VPN Connections



SCALING & MANAGEMENT

If you are a plumber, you can work on a shed, or you can work on a mansion. It's just scale.

— Martin Freeman

Ridgeback is designed to scale easily and affordably. A single instance of Ridgeback, deployed as software, can protect an arbitrary number of network subnets. Ridgeback modifies network traffic to influence adversary behavior. This eliminates three key bottlenecks often found in other security solutions:

- Ridgeback does not have the problem of exceptionally complex and time-consuming analysis of very large data sets.
- Ridgeback does not have the problem of maintaining lists of all known vulnerabilities.
- Ridgeback does not have the problem of deploying and managing new IT assets in response to threats.

Compared to other security solutions, Ridgeback just works. Connect a physical or virtual computer to a network, turn it on, and Ridgeback immediately starts protecting the networks it can see.

Central management and integration can be achieved under a single pane of glass by using Ridgeback Central. Local management and integration with Ridgeback can be performed with each Ridgeback having its own web-based interface and structured data store. Both models offer great flexibility and easy scaling without limits or bottlenecks.

INTEGRATION

Systems thinking is a discipline for seeing wholes. It is a framework for seeing interrelationships rather than things, for seeing patterns of change rather than static "snapshots."

— Peter Senge, The Fifth Discipline

It is very straightforward to integrate Ridgeback with other systems and products.

The Ridgeback Log Adapter (RLA) stores event and action records in an easily accessible SQLite database. Documentation and sample database queries can be found in the Ridgeback Github open source repository:
https://github.com/ridgebacknet/ridgeback-hunter-db
For example, data may be pulled from the RLA database and sent to the SIEM used by the organization.

Ridgeback can also be integrated with ticket or incident response systems. The watchdog script included with the ridgeback-ui package can be used to automatically open tickets whenever a security incident occurs. The watchdog can also be configured to launch vulnerability scanners or implement desired countermeasures.

The Ridgeback UI server can be accessed via HTTPS and RESTful commands so that the interface can be operated programatically.

Finally, a number of convenience scripts come with the ridgeback-core and ridgeback-ui packages.

EXTENSIBILITY

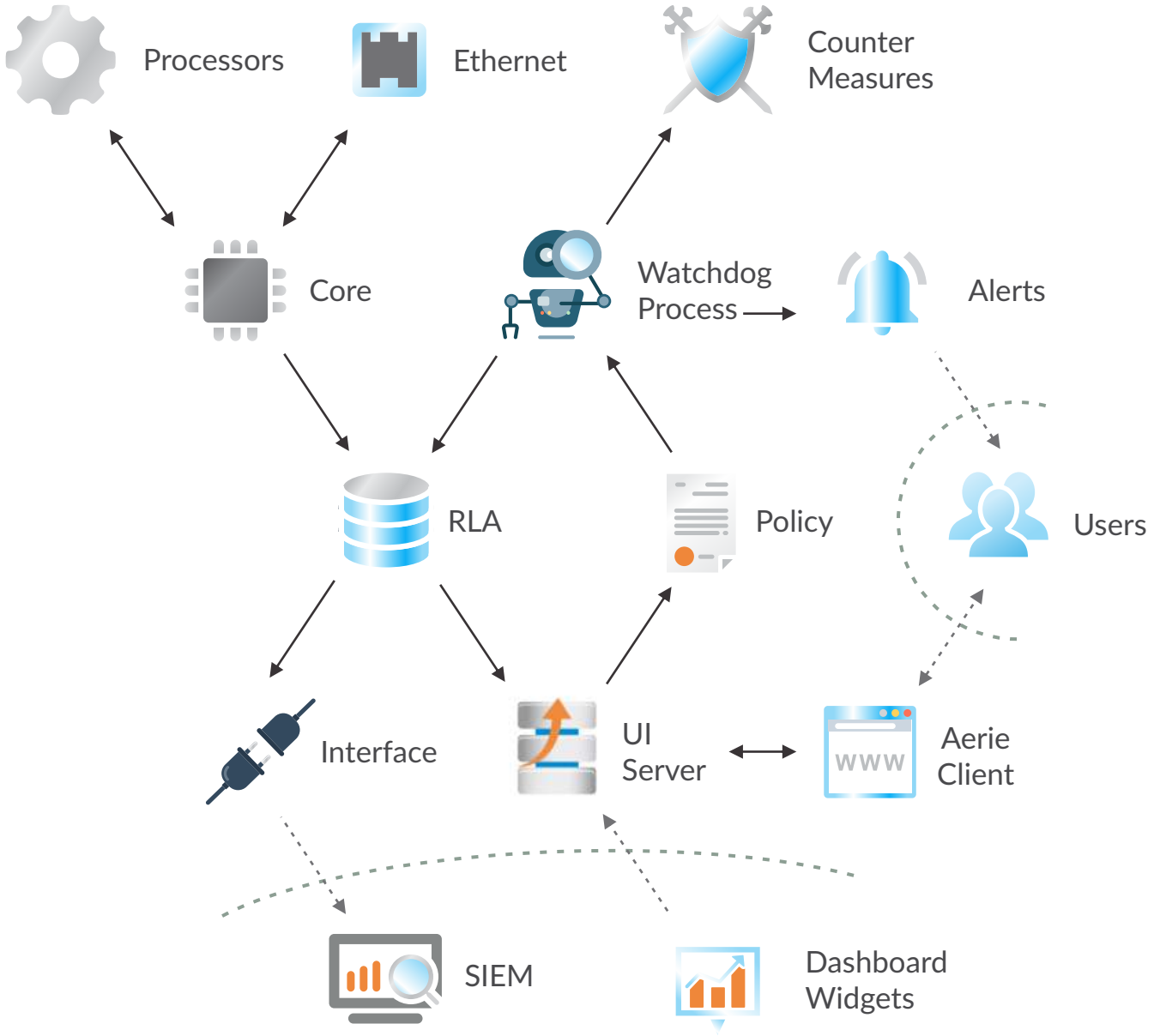
Ridgeback is a platform that is easy to extend. The base functionality of Ridgeback can be extended by adding new dashboard widgets, new watchdog processes, or new protocol processors.

A web developer familiar with JQuery can create a new dashboard widget in 60-90 lines of Javascript code. Sample widgets are available in the Ridgeback Github open source repository: https://github.com/ridgebacknet/ridgeback-hunter-widgets

New watchdog processes can be created by users that are knowledgable in shell scripting and SQL. The processes can be security-focused, or be designed for general IT management, such as sending reports on IT asset inventories and configurations.

An advanced developer can create new protocol processors. The developer should be experienced in writing C code and be very knowledgeable in network protocol processing.

ARCHITECTURE



- **Core** - The core of the Ridgeback system, which processes network data. The core can insert, modify, or delete network traffic.
- **RLA** - Ridgeback Log Adapter, used to adapt Ridgeback output to other systems.
- **DB** - Ridgeback Hunter maintains an easily accessible state in a convenient Sqlite database.
- **Policy** - Security policies are stored in a standard JSON file.
- **Watchdog** - Monitor system status and initiate alerts or countermeasures when required.
- **Alert** - A notice sent to users.
- **Countermeasure** - An action taken to remove a threat from the network.
- **UI Server** - Provides an HTTPS management interface to a Ridgeback installation.
- **Aerie Client** - A web-based interface to manage a Ridgeback installation.

CONCLUSION

The battle field of cybersecurity is ever changing and is currently difficult to win. Today's cyber adversaries breach or circumvent perimeter defenses like a sponge and the real battle is in preventing the east west proliferation with insiders threats and lateral movements. The existing security solutions have proven without a doubt that the most prevalent security paradigm, the classification of signals, is an unwinnable arms race.

What can an enterprise do about it? The Ridgeback Interactive Defense Platform, fundamentally based on the principles of Sun Tzu's 2000+ year old classic “Art of War” is a genuine alternative. The security philosophy of Ridgeback Network Defense is that the cost of defense should be minimized while the cost of attack should be maximized making it very difficult to attack and very easy to defend. With Interactive defense, Ridgeback takes the fight to the enemy using Interactive Defense and causes the adversary to needlessly exhaust resources. This aggressive strategy results in the cost of attack outweighing the benefits of attack and in the process eliminates the attackers.

With Ridgeback you can turn the tables on Cyber criminals to protect your network and win the Cyber war!

To know more about Ridgeback's Interactive Defense Platform or to download and experience it's cyber security protection first-hand, please visit our website at:

www.ridgebacknet.com.