CHƯƠNG 5
NEXT GENERATION IPS

10/2/2021

ThS.Nguyễn Duy
duyn@uit.edu.vn

Content

- Agile Security
- Next Gen IPS?
- How to deploy NG-IPS?

Content

- **Agile Security**
- Next Gen IPS?
- How to deploy NG-IPS?

IT Environments are Changing Rapidly

Devices

Networks

Applications

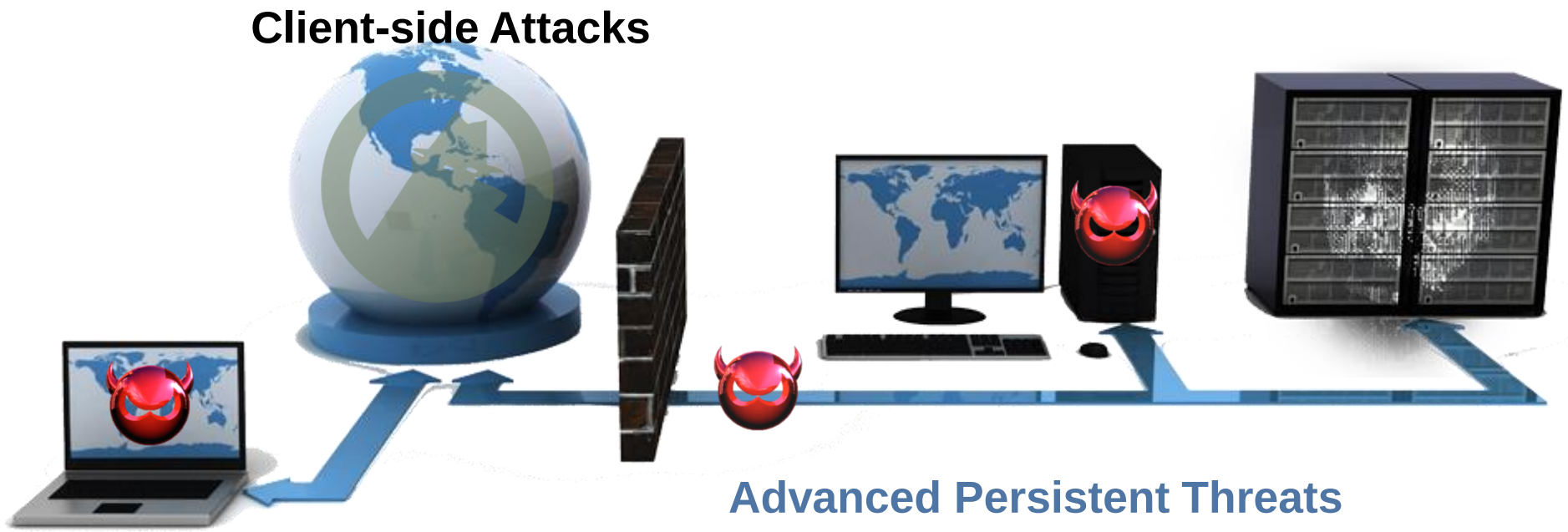
Virtualization

Mobilization

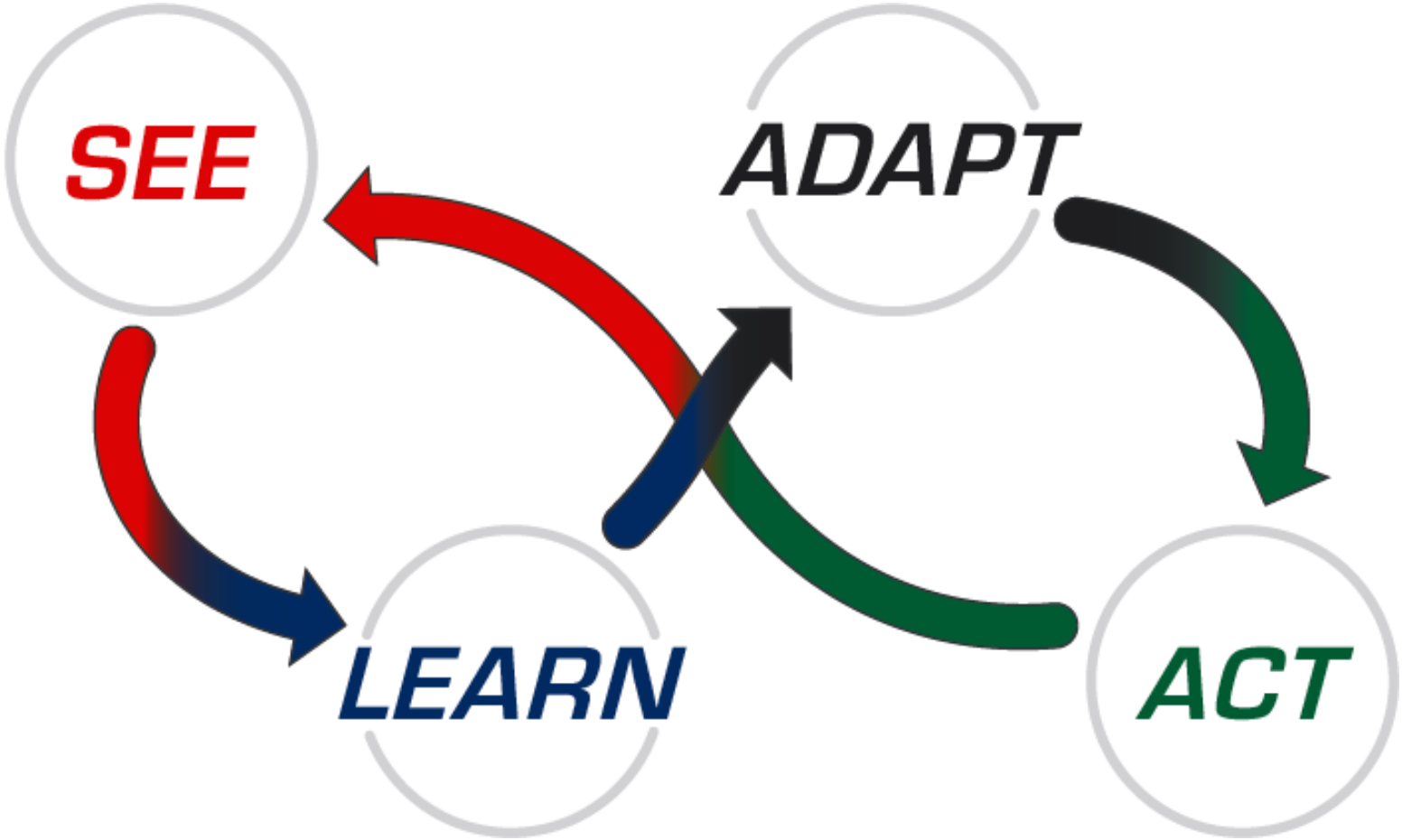
Consumerization

Threats are Increasingly Complex

Targeted | Organized | Relentless | Innovative



Agile Security



…a continuous process to respond to continuous change.

You Can't Protect What You Can't See

Breadth: who, what, where, when

Depth: as much detail as you need

Real-time data

See everything in one place


Threats

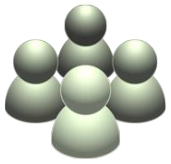

Devices

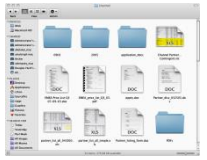
Applications


Network


Vulnerabilities

OS


Users


Files

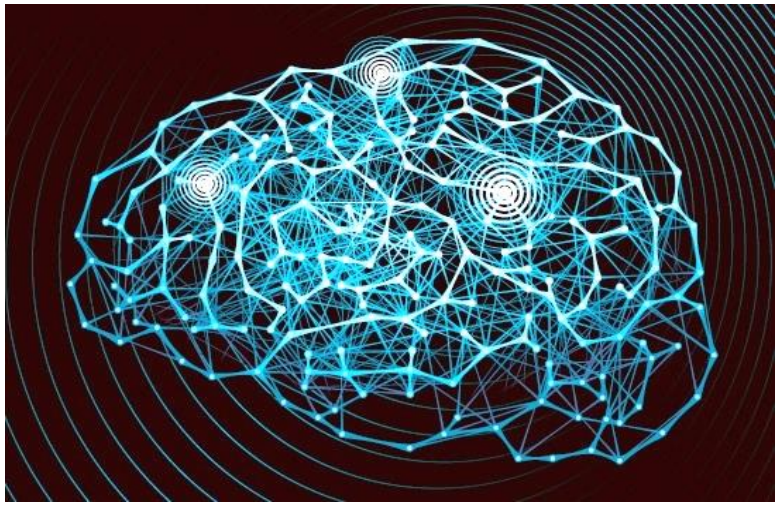
Sourcefire provides information superiority

Leverage Awareness For Knowledge

Gain insight into the reality of your IT and security posture

Get smarter by applying intelligence

Correlate, prioritize, decide



Collective intelligence elevates overall defense

Change is Constant

Automatically optimize defenses

Lock down your network to policy

Leverage open architecture

Configure custom fit security

Sourcefire invented customized security & self-tuning

Act Decisively & Efficiently

Block, alert, log, modify, quarantine, remediate

Respond via automation

Reduce the 'noise'

Superior protection through intelligence & automation

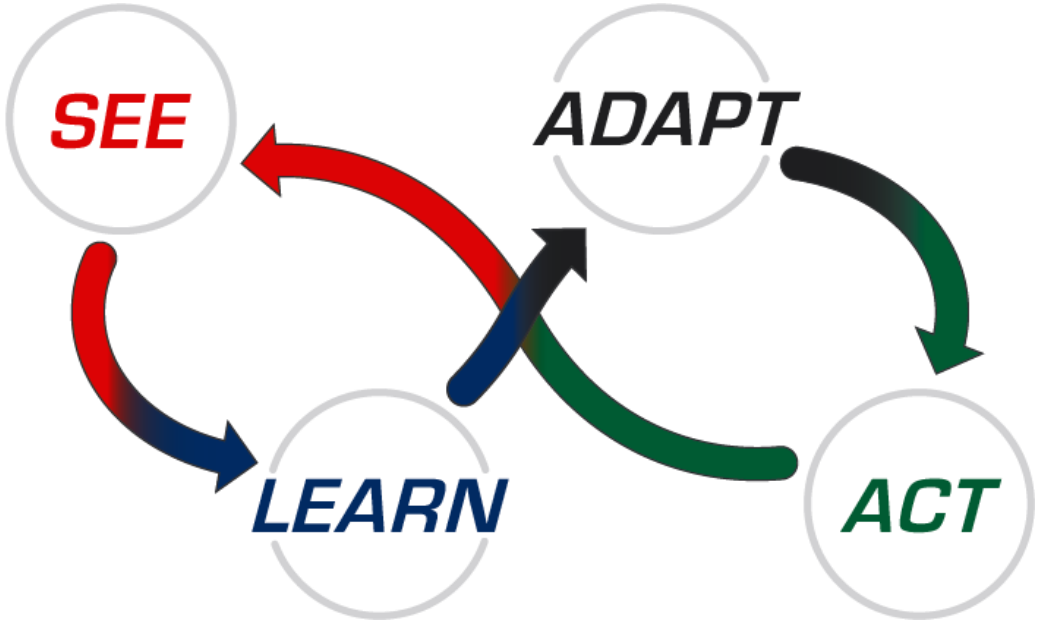
Content

- Agile Security
- **Next Gen IPS?**
- How to deploy NG-IPS?

Next Generation IPS

Next-Gen IPS (NGIPS)

- Standard first-gen IPS
- Application awareness
- Content awareness
- Full-stack visibility
- Context awareness

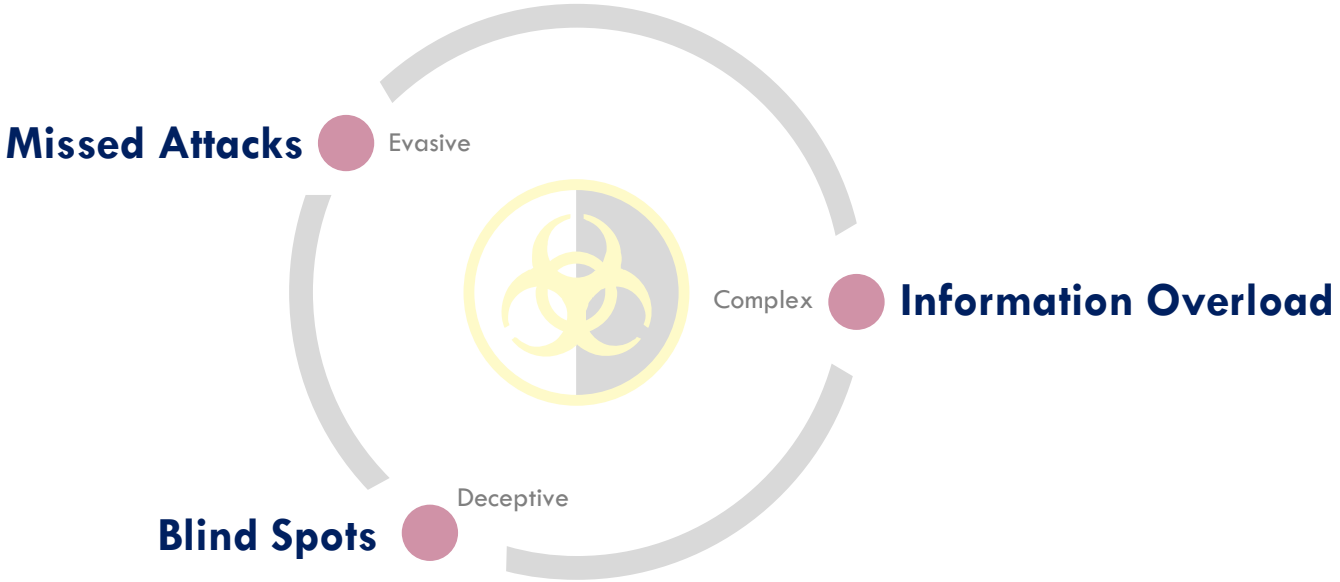


Gartner®

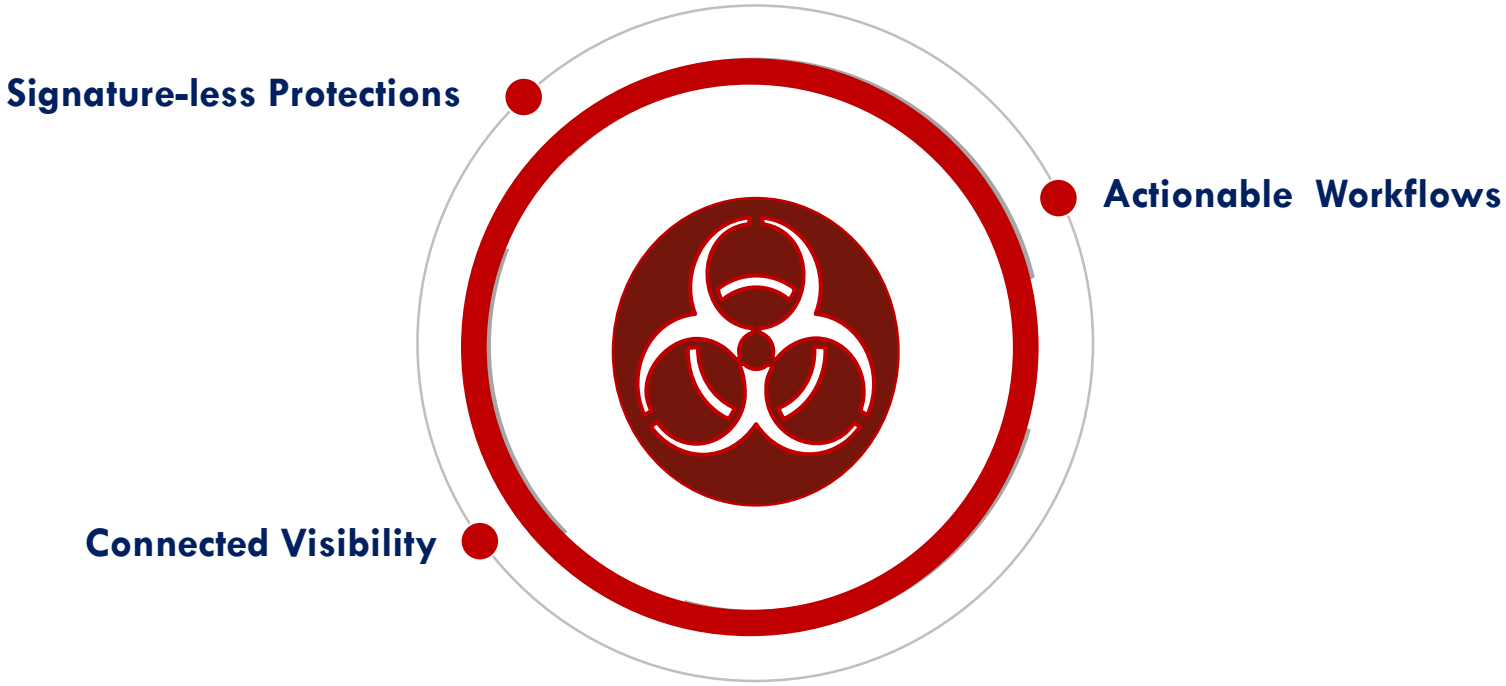
"Next-generation network IPS will be incorporated within a next-generation firewall, but most next-generation firewall products currently include first-generation IPS capabilities."

Source: "Defining Next-Generation Network Intrusion Prevention," Gartner, October 7, 2011.
"Defining the Next-Generation Firewall," Gartner, October 12, 2009

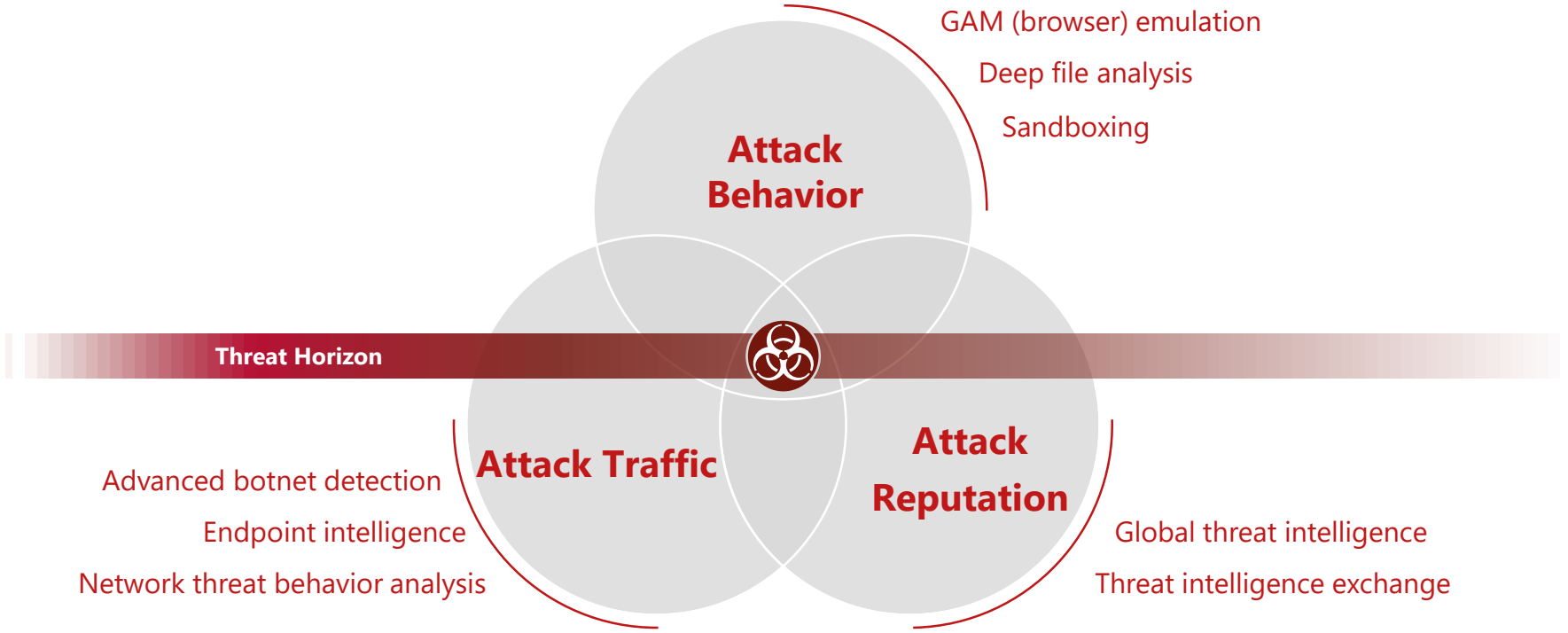
Traditional Threat Inspection



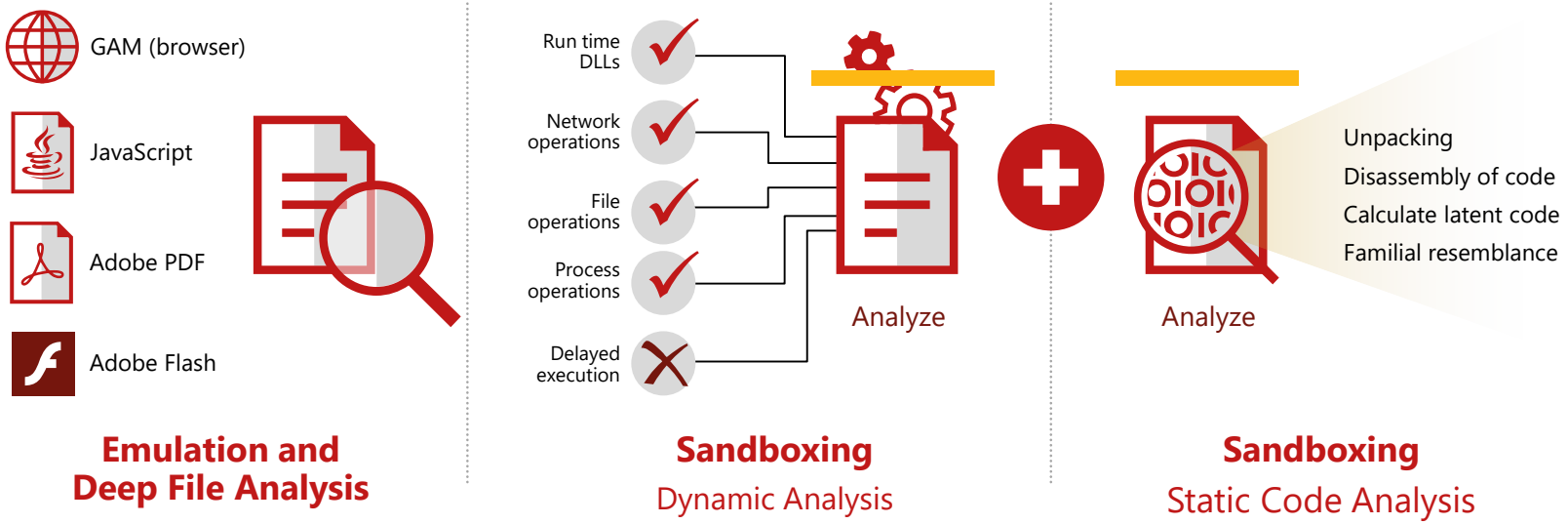
Advanced Targeted Attack Prevention



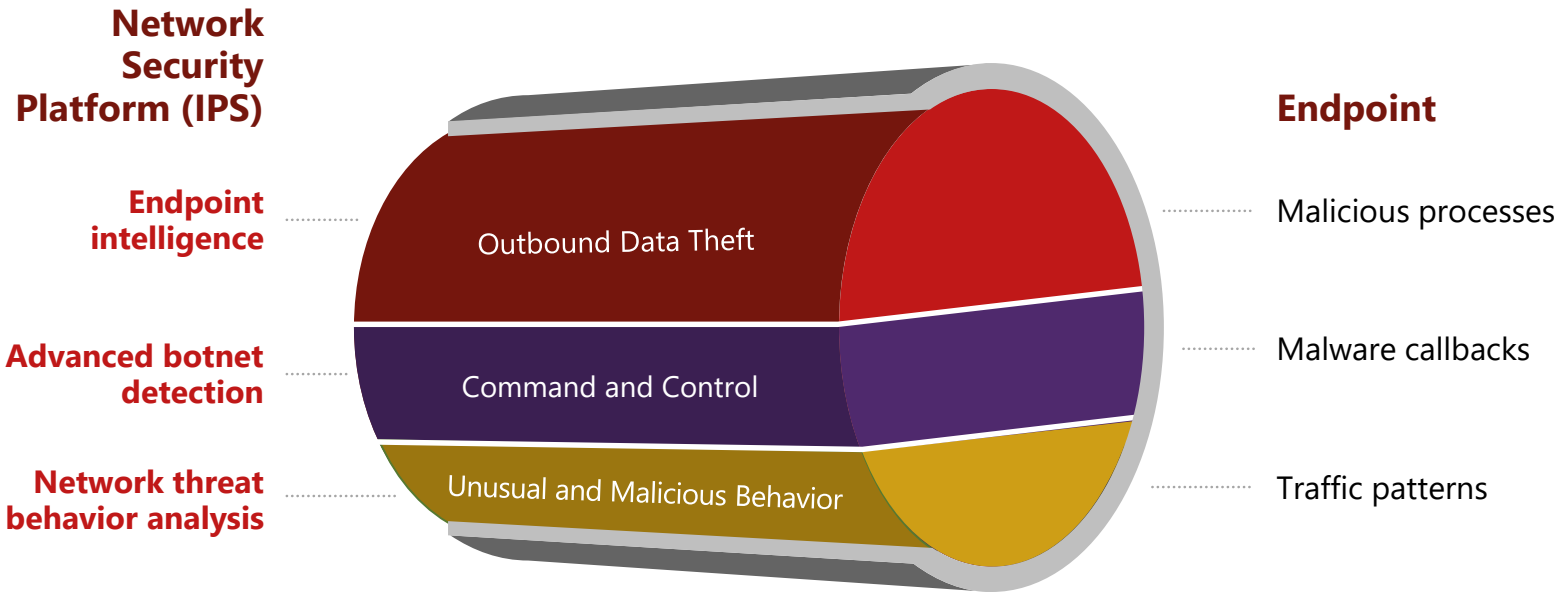
Approach to Signature-less Inspection



Understand Attack Behavior

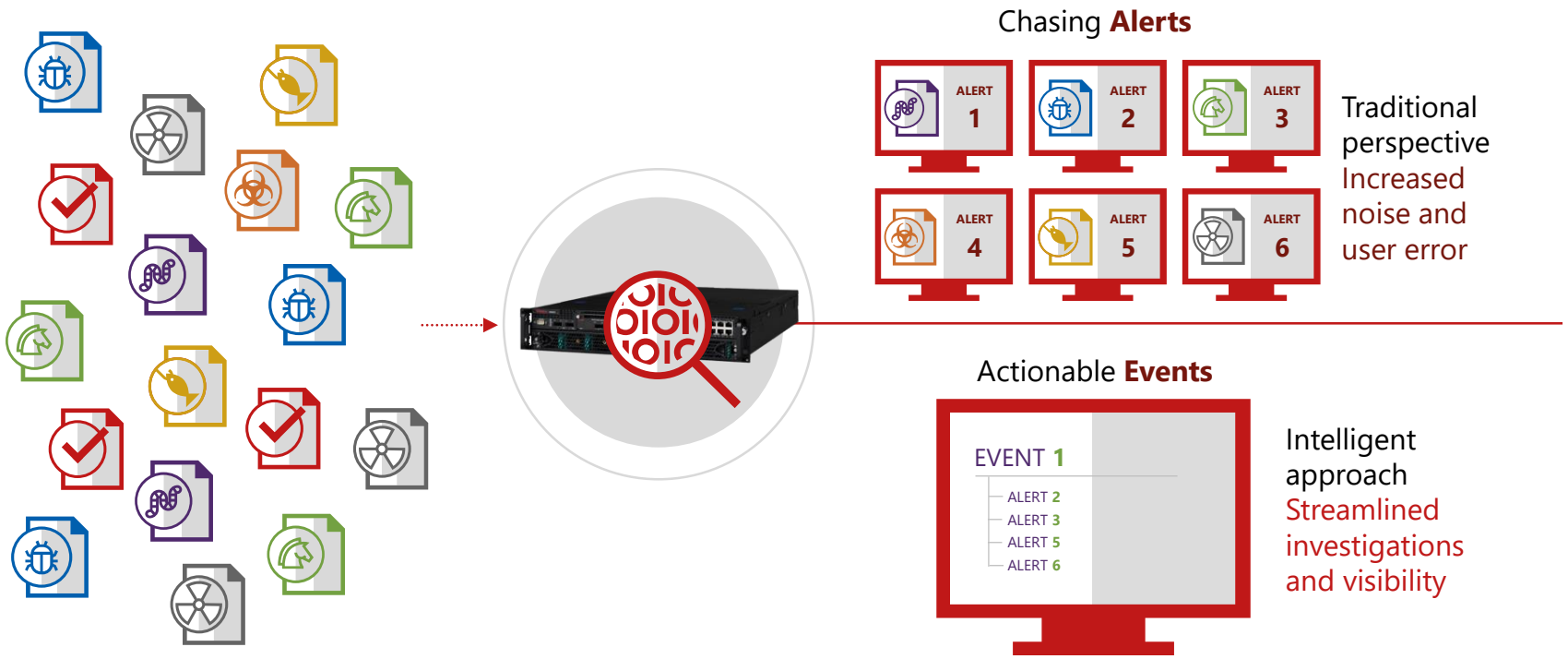


Find Stealthy Attack Traffic

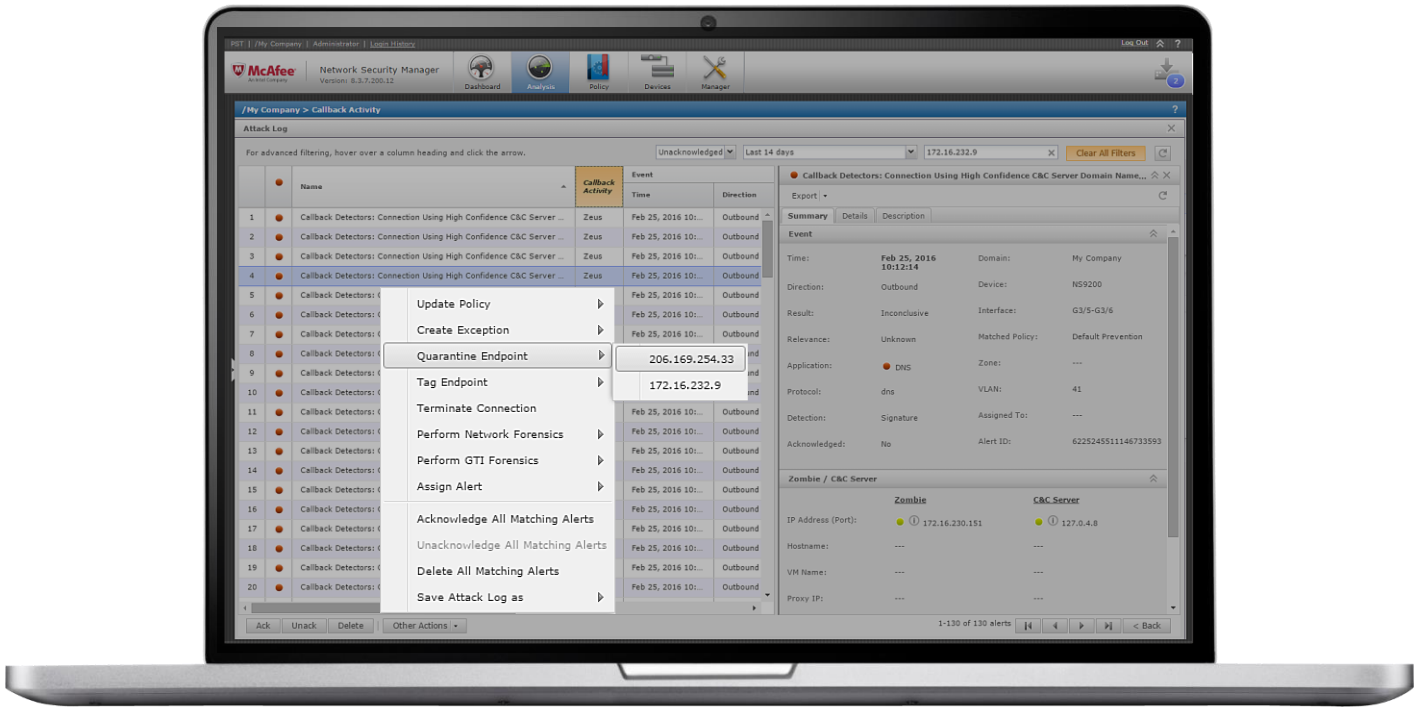


Approach to Actionable Workflows

Discover Breaches Faster



Stop Malware Callback Activity



Identify
top callback activity

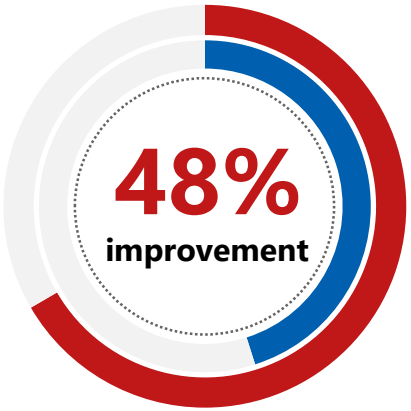
Drill down
on infected systems

Understand
impact of infection

Take action
to quarantine endpoints

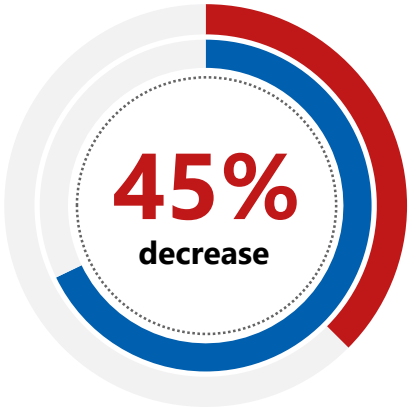
The Right Data at the Right Time

Threat Visibility



in identifying threats
before they become events

Incident Response



in user-impacting breaches
and malware incidents

McAfee Non McAfee

"We can identify threats before they become events with McAfee NSP…we're probably at about

98%

proactive identification

now, versus 78% before."

IDC Business Value of Network IPS, Feb 2015

Problems We Want to Solve for the Cloud

Visibility

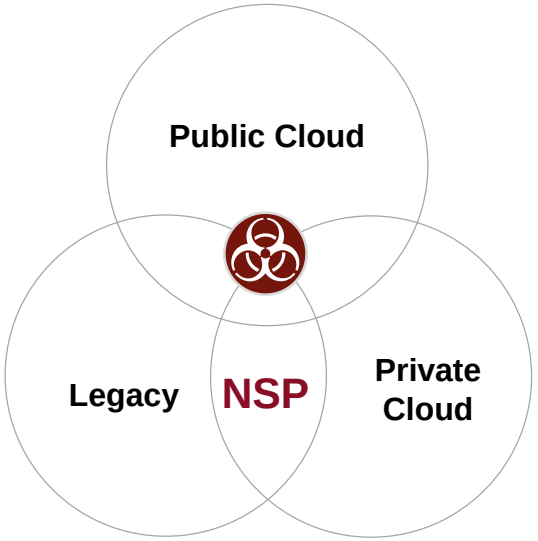
"Shadow IT makes it difficult to track systems, leaving them vulnerable to breaches."

Cloud Scale

"Are my security controls at cloud scale or a choke point?"

"Security comes with cost of performance?"

Single Pane of Glass



Virtual Network Security Platform (vNSP)

Built for the Cloud

- Inline IPS/IDS
- Security group
- AutoScale
- CloudTrail/VPC logs

Built in Security

- Delivered with CloudFormation Template
- Ansible/Chef/Puppet

Load Balanced

- Automatic client based load balancer
- Integrated with AutoScale

Virtual Overlay Network

- Micro-segmentation across heterogeneous cloud
- App fencing

Low OpEx/CapEX

- Ready for orchestration
- Live update of sensors & agents
- Flexible license

Single Console

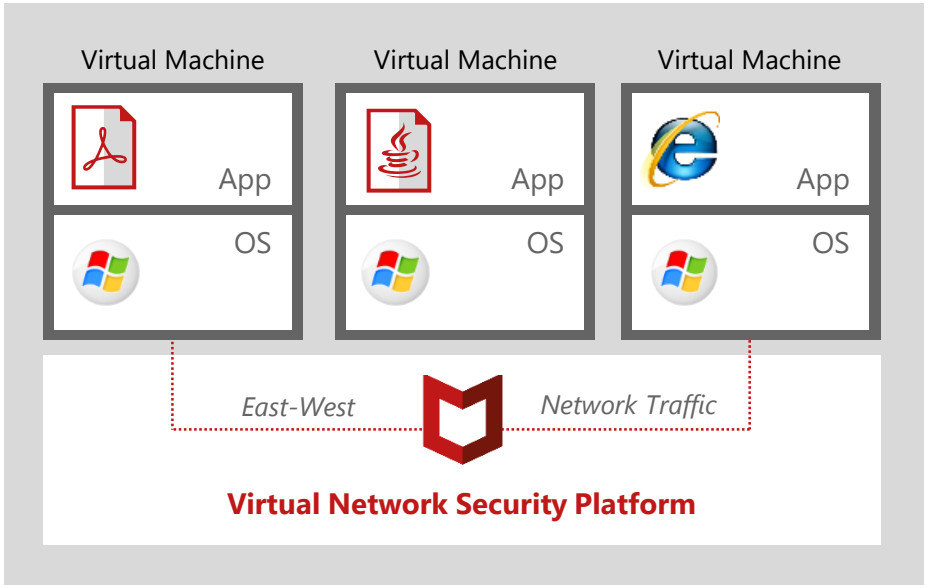
- Single NSM to manage appliance, OpenStack, VMware & AWS
- Manage from AWS or on-prem
- Monitor user access across cloud

Scale Security into the Virtual Data Center

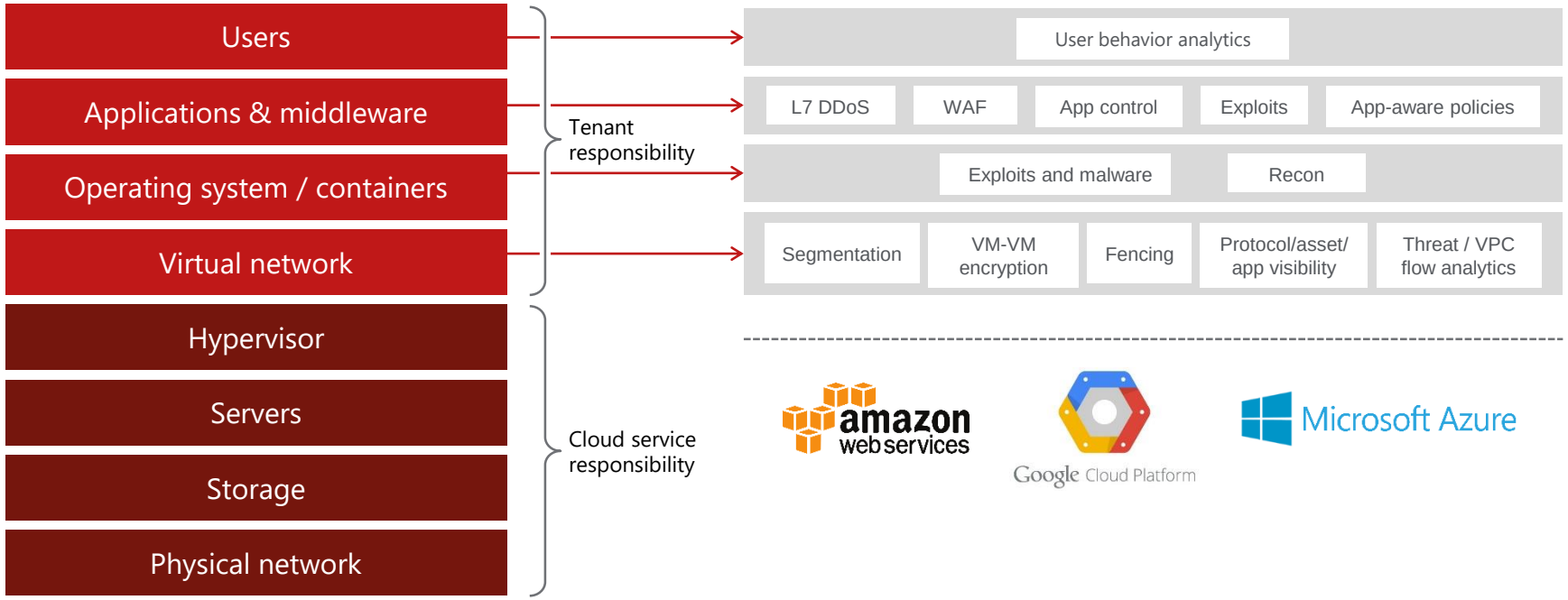
Industry Proven IPS inspection
Gartner Leader and NSS recommended

Next Generation Features
Application control, DDoS, callback detection, ATD, endpoint and threat intelligence

Multiple Deployment Modes
Support for SDN Controller (NSX) or dedicated installations.

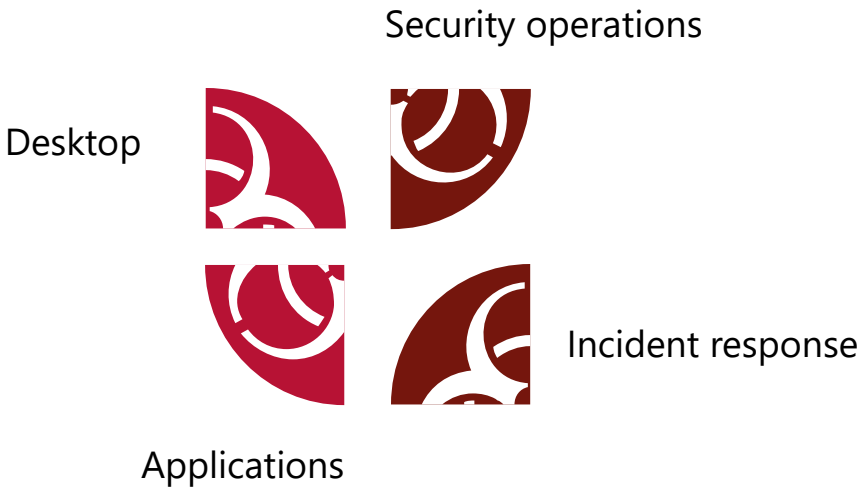


Security in the Public Cloud



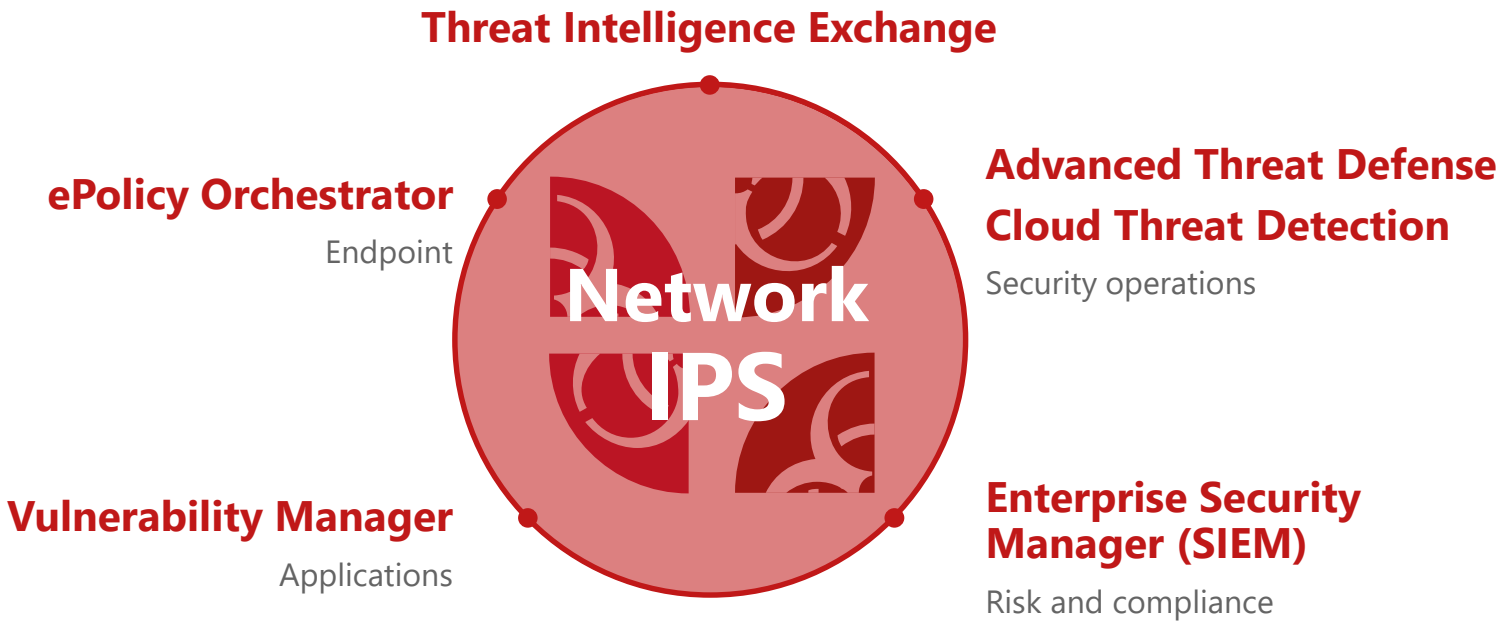
Approach to Connected Visibility

Fragmented Visibility



Connected Visibility

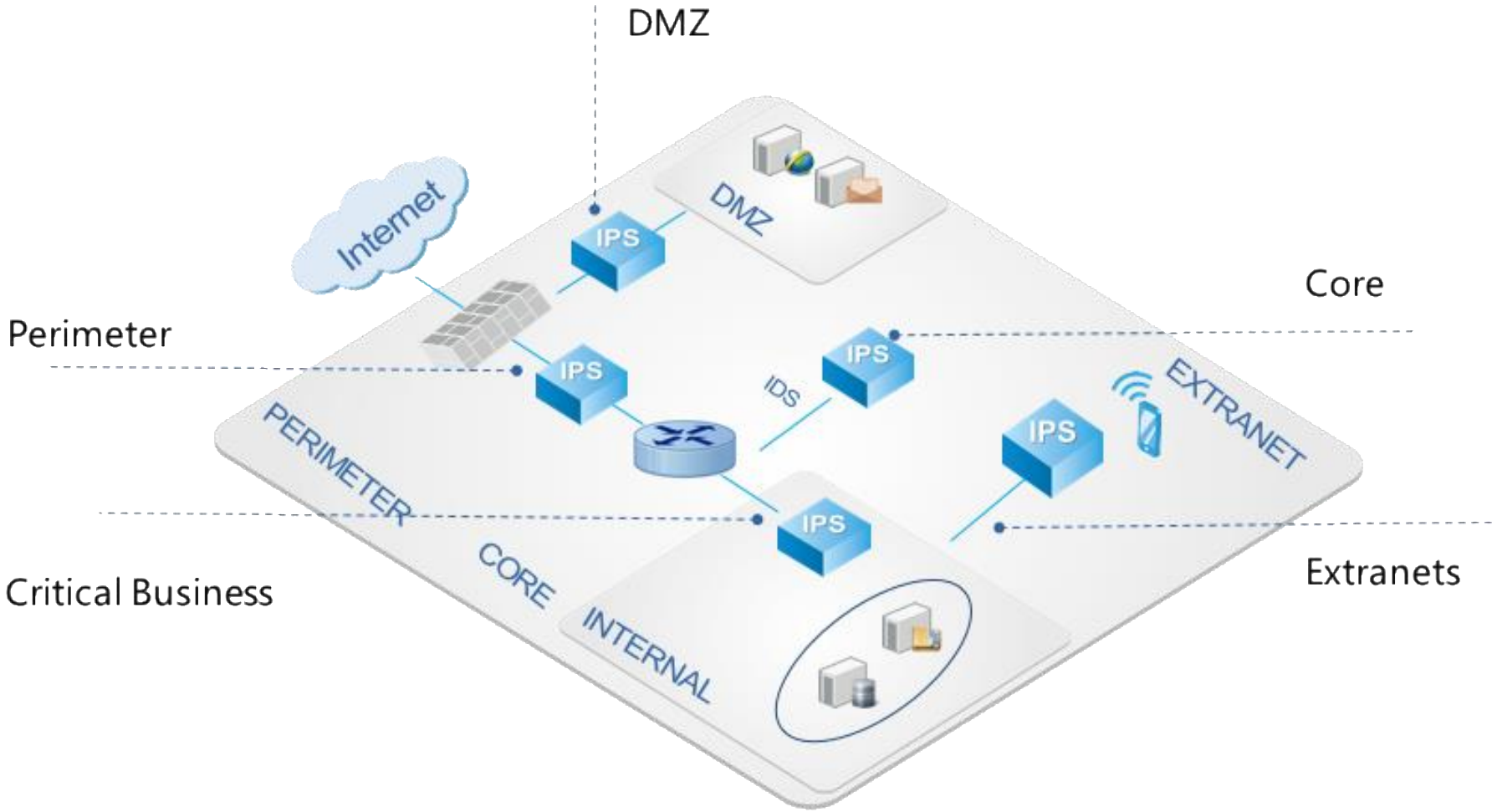
Break down data silos



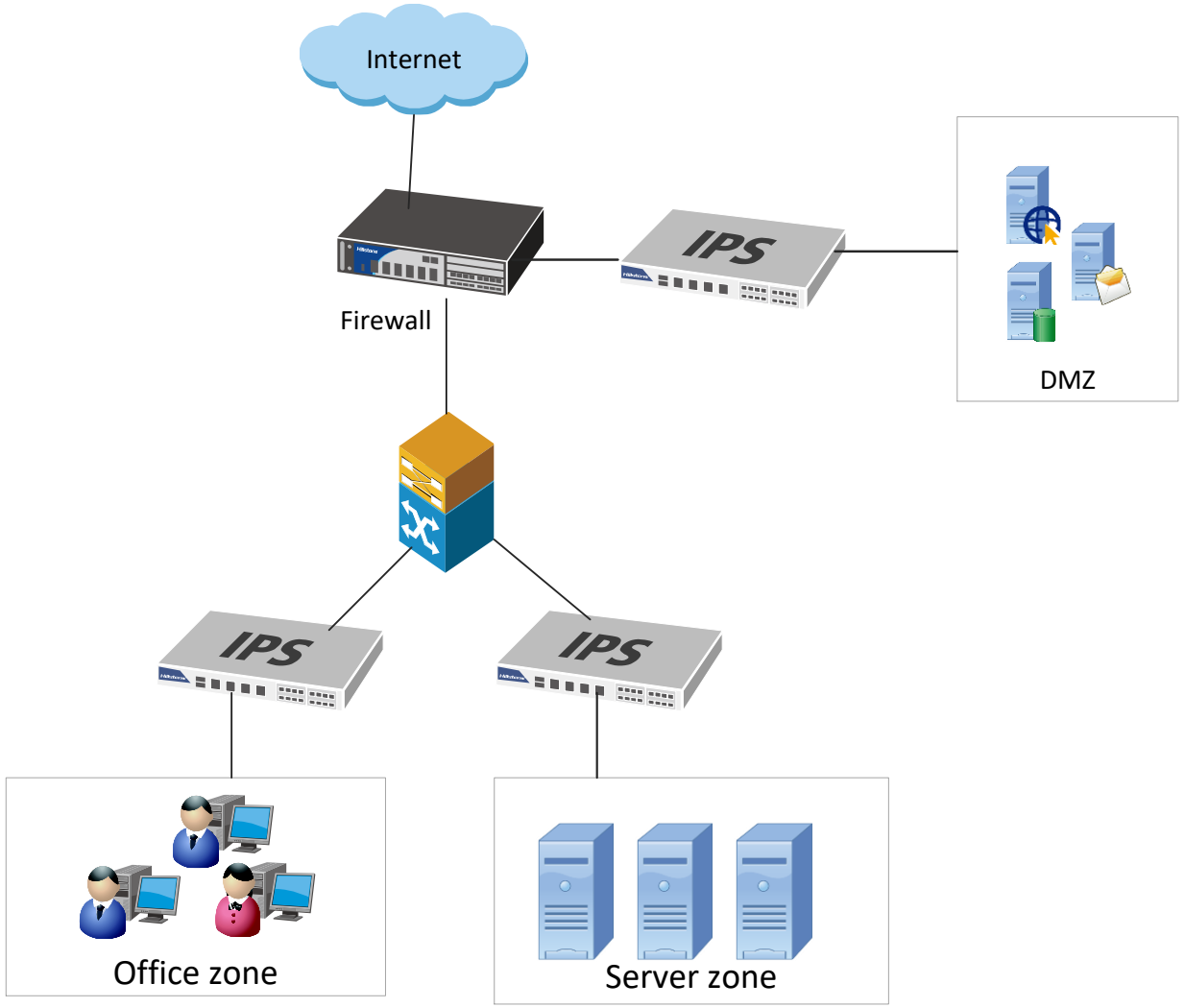
Content

- Agile Security
- Next Gen IPS?
- **How to deploy NG-IPS?**

Deployment Scenarios



Deployment in Enterprises



Requirements

- ❑ Protection against sophisticated attacks
- ❑ Insight into network environment

Solutions

- ❑ Strong defensive capabilities
- ❑ Deep visibility from L2 – L7
- ❑ Unknown threat detection
- ❑ Automated analysis and

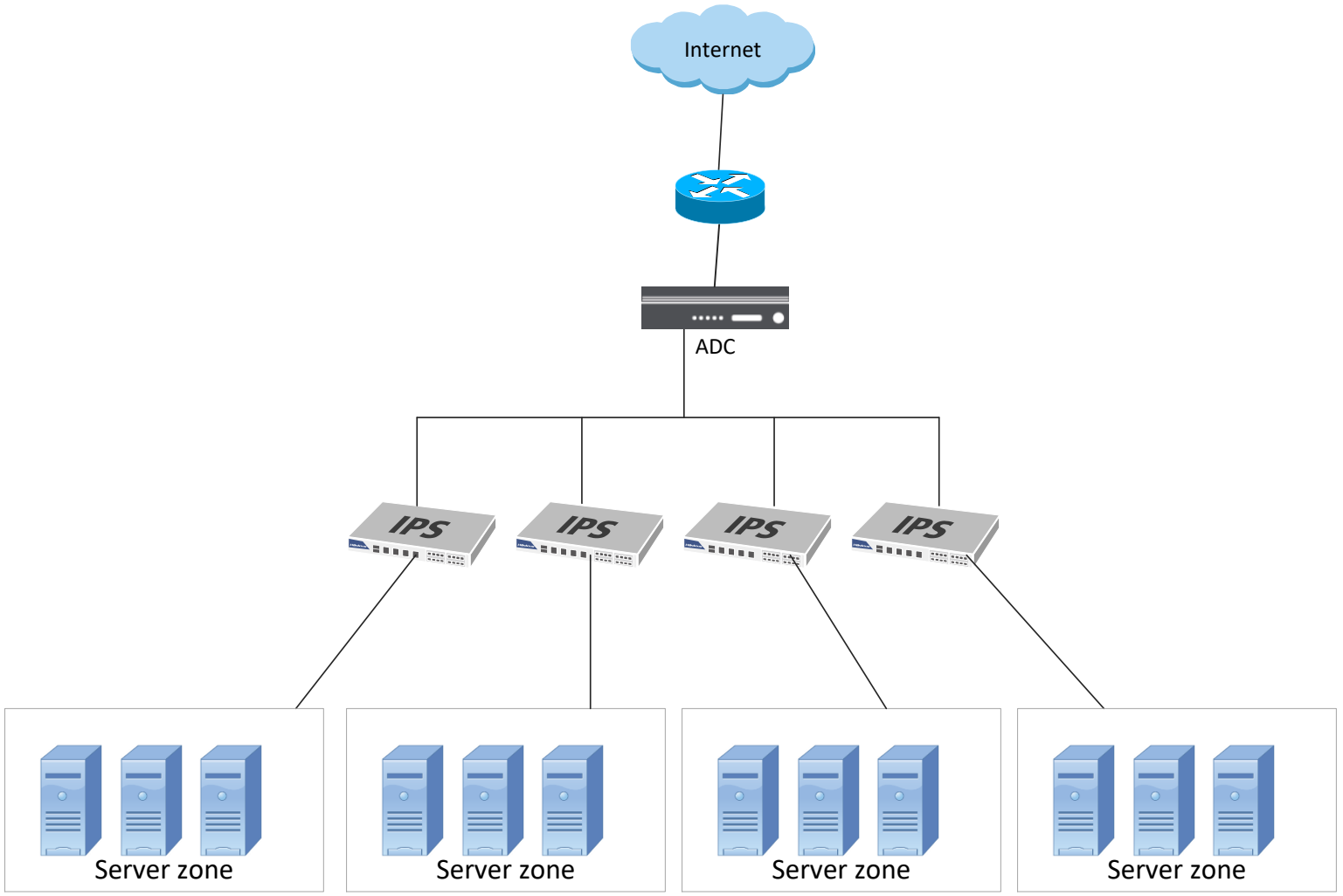
Products

- ❑ S Series

Market

- ❑ Education
- ❑ Enterprises
- ❑ Government

Deployment in Service Provider/Data



Requirements

- ❑ Protection against sophisticated attacks
- ❑ High performance

Solutions

- ❑ Integrate with ADC
- ❑ Strong defensive capabilities
- ❑ Deep visibility from L2 – L7
- ❑ Unknown threat detection
- ❑ Automated analysis and

Products

- ❑ S-Series

Market

- ❑ Service Provider
- ❑ Data Center

Question ???