lastline®

Why NDR is Now Necessary

Richard Henderson,

Head of Global Threat Intelligence

Synercomm Summit – 12 Sep 2019

Who Am I?

Who Am I?

lastline™

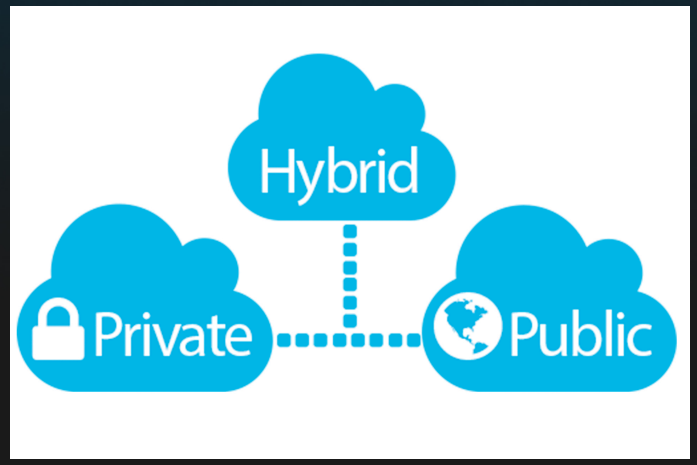
Ayyyy!

lastline™

The Enterprise Security Dilemma

Increasingly Sophisticated Threats

Complex IT Environments



Cyber Security Talent Shortage

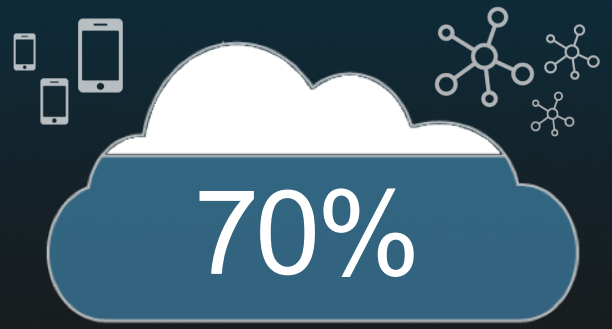
lastline™

Security Challenges

Increasingly Sophisticated Threats

- Nation states and organized crime **use multiple evasion techniques**
- 65% of malware samples are unique

Complex IT Environments



- **By 2020 70% of all IT workloads will run in the cloud**
- IoT is rapidly taking bigger shares of IT budgets
- BYOD is pervasive

Cyber Security Skill Shortage

- By 2021 there will be **3.5 million unfilled security positions**

lastline™

The Challenge of Advanced Malware Protection

- It is difficult for existing security controls to defend against advanced malware
- Perimeter-centric approaches leave organizations exposed
- The gravitational pull of technology advancement will always results in new threat vectors
- Humans are still the weakest link
- Obfuscation of maliciousness has existed since Adam and Eve

lastline™

Asymmetric Warfare 2.0

The supreme act of war is to subdue the enemy without fighting.- Sun Tzu The Art of War.

Raising Awareness

Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States

Report to President Donald J. Trump
by the Interagency Task Force in Fulfillment of
Executive Order 13806

"The central challenge to U.S. prosperity and security is the ***reemergence of long-term, strategic competition*** *by what the National Security Strategy classifies as revisionist powers. It is increasingly clear that China and Russia want to shape a world consistent with their authoritarian model – gaining veto authority over other nations' economic, diplomatic, and security decisions."*[3]

What Keeps CISOs Up At Night

Source: The State of Cybersecurity Priorities and Strategies
Scale Venture Partners

72%

ARE INVESTING THE MOST RESOURCES IN DATA BREACH PROTECTION

40%

DATA BREACHES ARE THE TOP IT SECURITY RISK IN THE ORGANIZATION

46%

DATA BREACHES ARE A TOP 3 THREAT KEEPING THEM UP AT NIGHT

49%

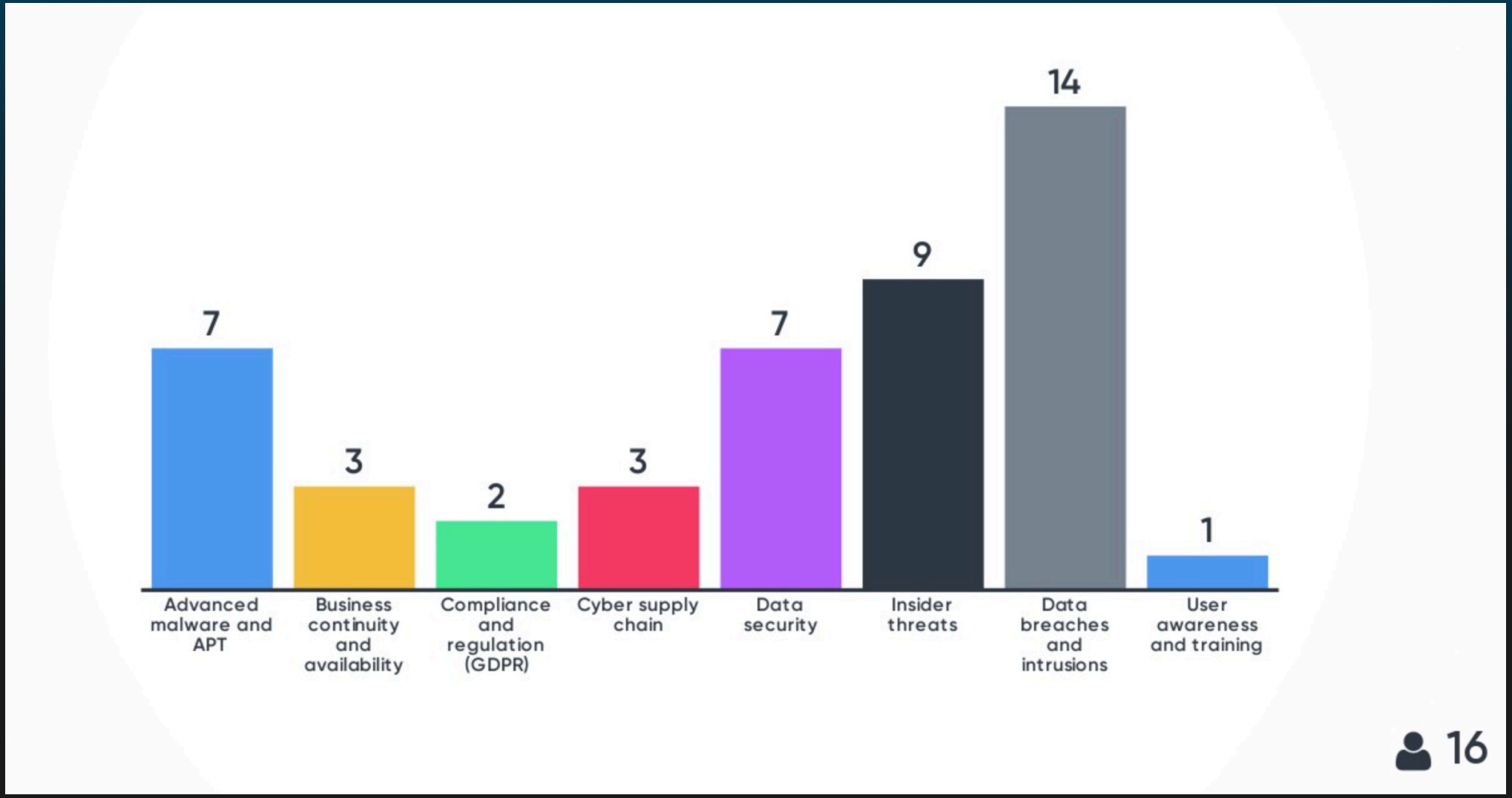
DATA BREACHES ARE THE NO.1 RISK WHERE THEY ARE PLANNING TO DEDICATE MORE RESOURCES IN 2017

60%

BUILT AN IN-HOUSE SOLUTION DUE TO A LACK OF COMMERCIAL ALTERNATIVES

lastline™

What (Actually) Keeps CISOs Up At Night



lastline™

Network Security – Traditional Markets

Perimeter Focused
PaloAlto Networks, CheckPoint

Web Application – Vulnerability, Threat, DDoS
Imperva, F5

Signature-based Detection
Cisco, Trend Micro, McAfee

Network-based Threat Behavior (Sandbox)
FireEye

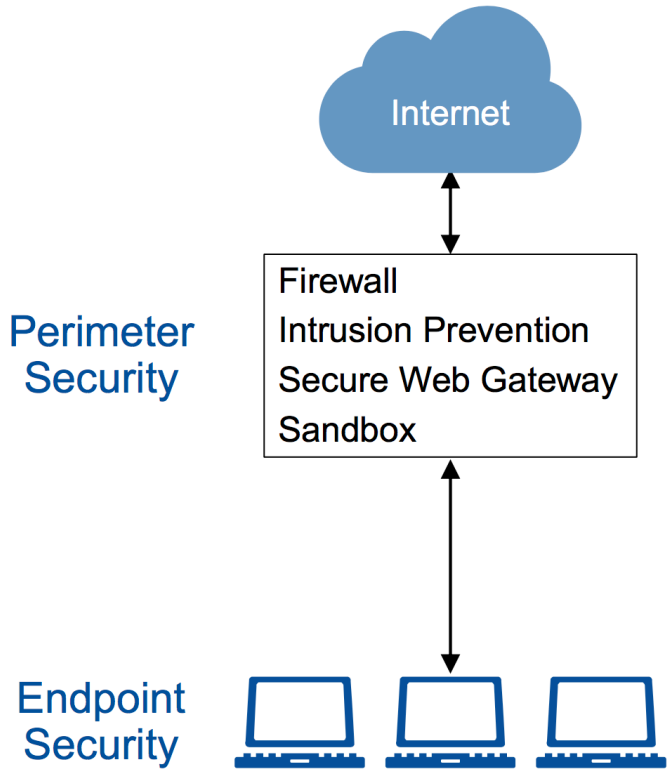
Email Application – Spam + Threat Detection
Proofpoint, Ironport

Web Traffic – Policy, URL Filtering and Threats
Symantec, McAfee, Websense

lastline™

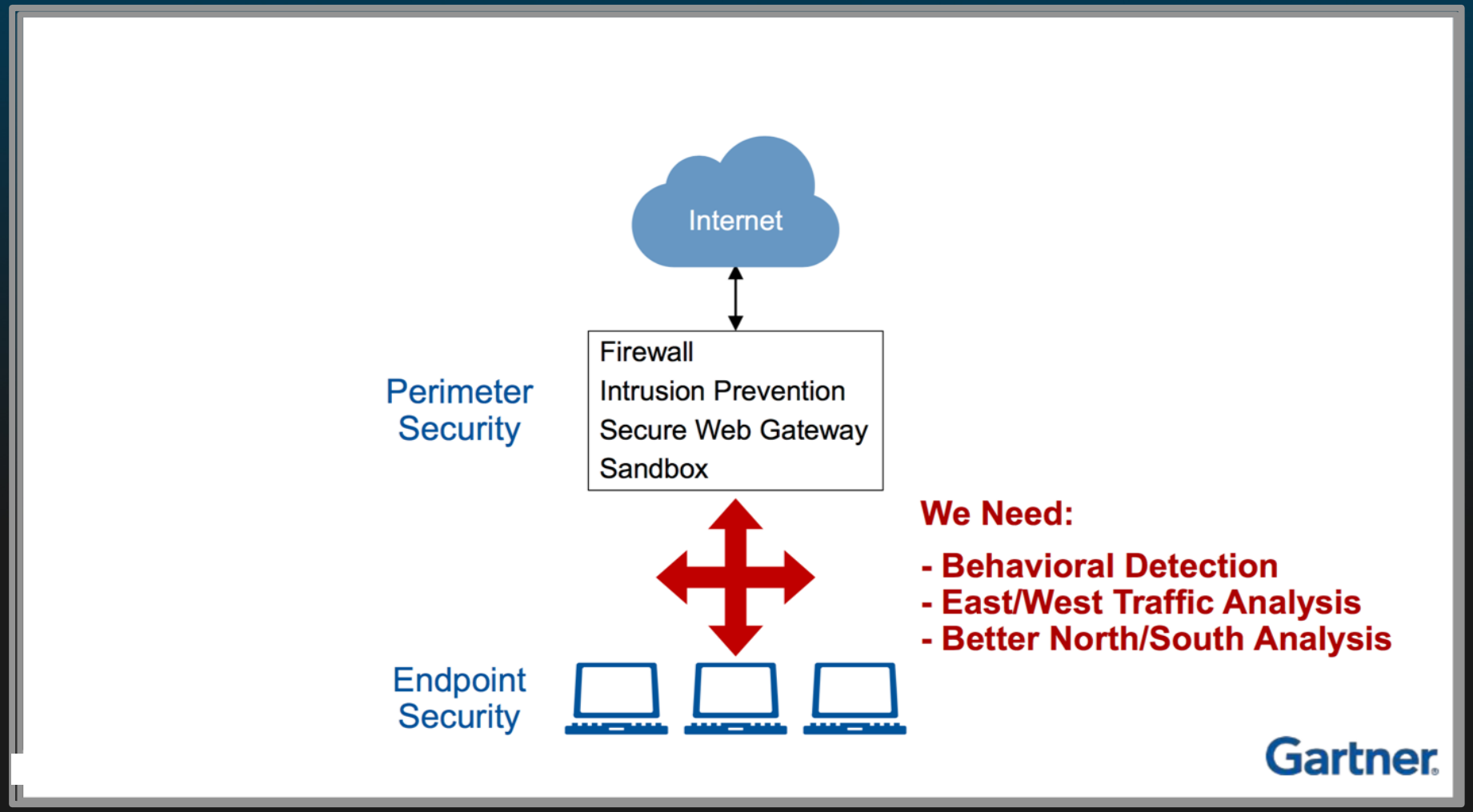
The Missing Piece?

What's Missing From This Picture?



Gartner

Network Detection and Response (NDR)



lastline™

Traditional Malware Scanning Tools Lack Visibility

Legacy Sandboxes

- Can only guess to the nature of the file
- Malware must be executed to be effectively analyzed
- Analysis environment is learned when malware executed
- Malware adapts to evade the sandbox in the future

Deep Content Inspection

- ✧ Complete kernel-level visibility
- ✧ IDENTIFIES and BYPASSES malware's evasive techniques
- ✧ **Manipulate**s & **interacts** with artifacts to elicit behaviors
- ✧ Version-less detection alleviates expense of sandbox "gold images"
- ✧ Dormant Code Analysis identifies latent code blocks awaiting activation

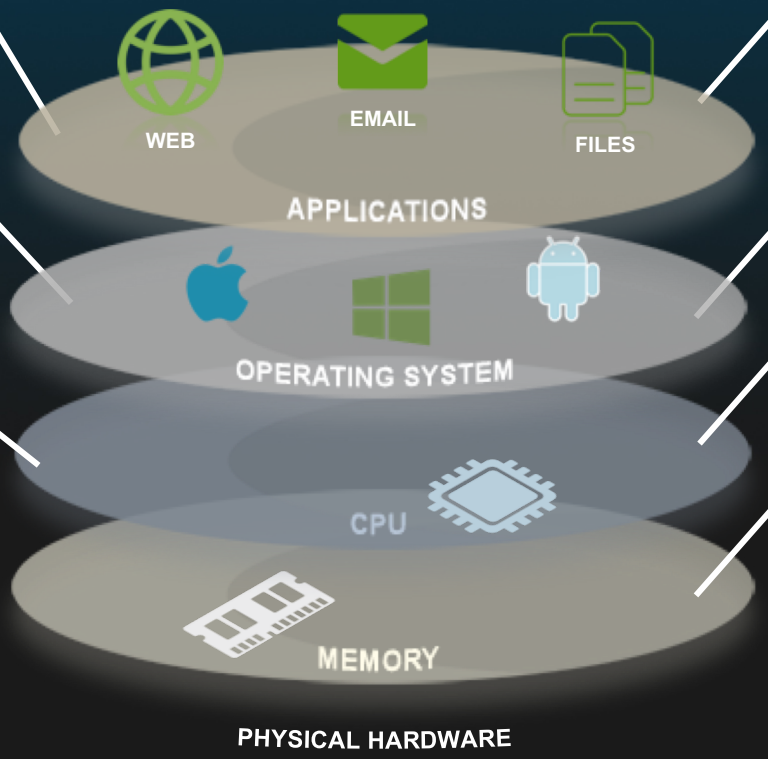
lastline™

The Deep Content Inspection Difference

Version-less inspection and analysis does not require gold images

Dormant code analysis
Exploit symptom diagnosis

Dynamic code analysis elicits malicious behaviors



Identification of malicious document macros

True Kernel visibility

Evasion detection & TLS fingerprinting

Inspection of malware memory including encrypted strings

lastline™

How I learned to stop worrying…
…and love AI-powered NDR.

The existing strategies are failing…

$3M-$4M cost per breach

($150 per record compromised)

4 million stolen records per day,
4,000 ransomware attacks per day
200,000 new malware discoveries per month
50% of all internet traffic today is bots

Dwell time of an average attack is ~200 days

lastline™

The Concept Behind NDR

lastline™

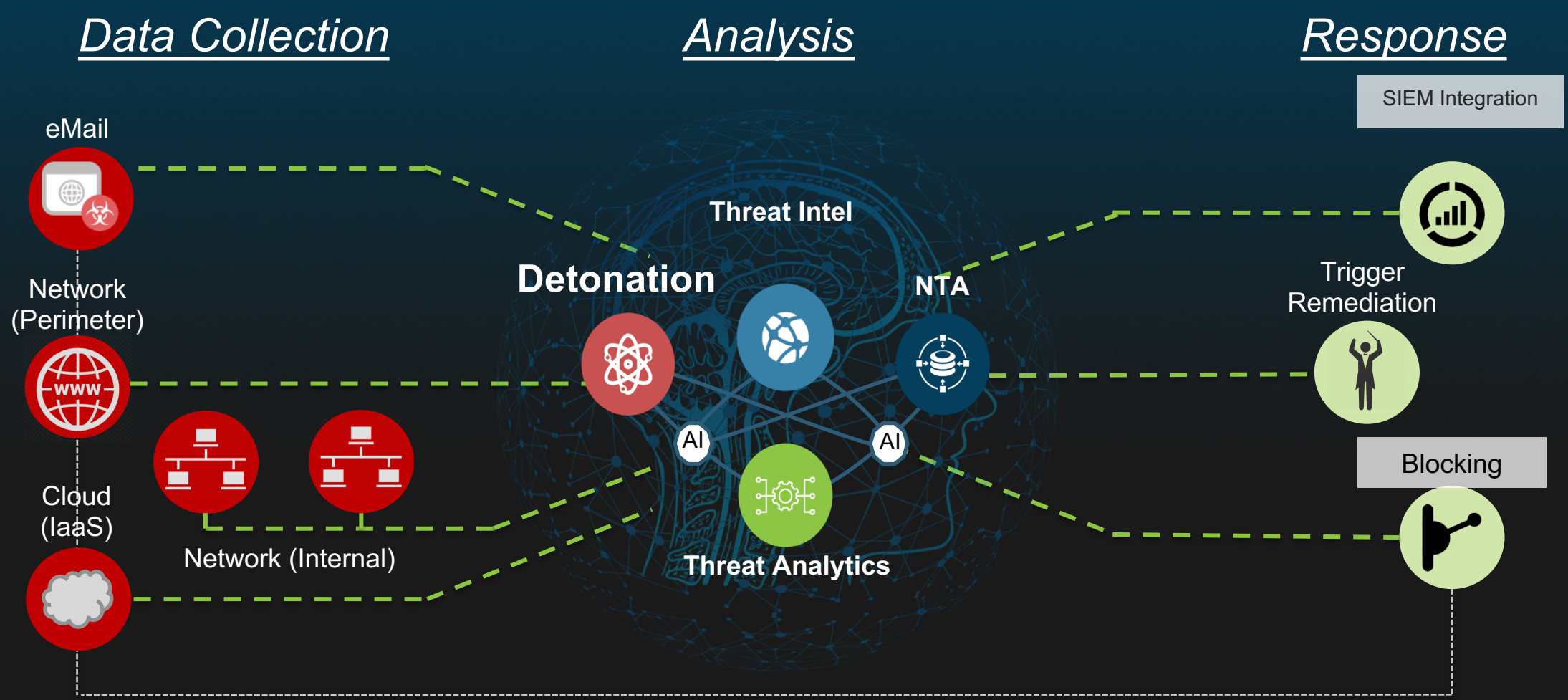
The Concept Behind NDR

"Reality is one, though wise men speak of it variously."

- the *Rigveda*, dated to have been composed between 1500 and 1200 BC

lastline™

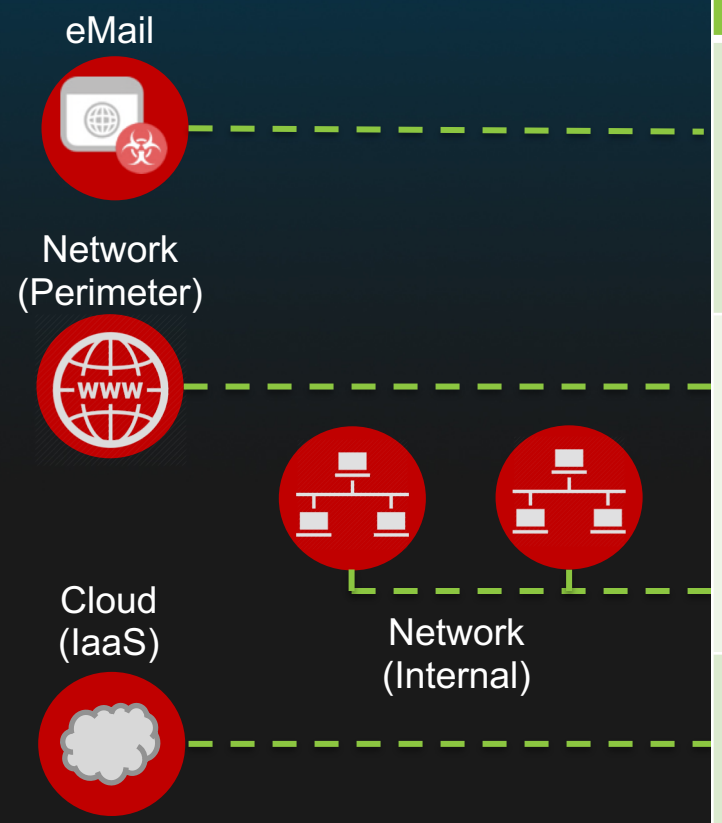
Solution Architecture



lastline™

Solution Architecture

Data Collection



Sensor Type	Data Collected	Considerations
eMail	Headers, Content, URLs, Attachments	On-premise, O365, G-Suite, blocking or monitor mode
Perimeter (North/South)	Deep Packet Inspection (DPI), App Protocol: HTTP, TLS, DNS, SMB, etc. Metadata, Netflow, ICAP, Files	Appliance or Software, Any Ingress/Egress point
Internal (East/West)	DPI, HTTP, TLS, DNS, SMB, etc. Metadata, Netflow, ICAP, Files	Appliance or virtual appliance
Cloud (IaaS)	Metadata, Netflow, ICAP, Files	Visibility varies from cloud to

lastline™

Solution Architecture

Analysis

On-premise
Hosted
Public Cloud

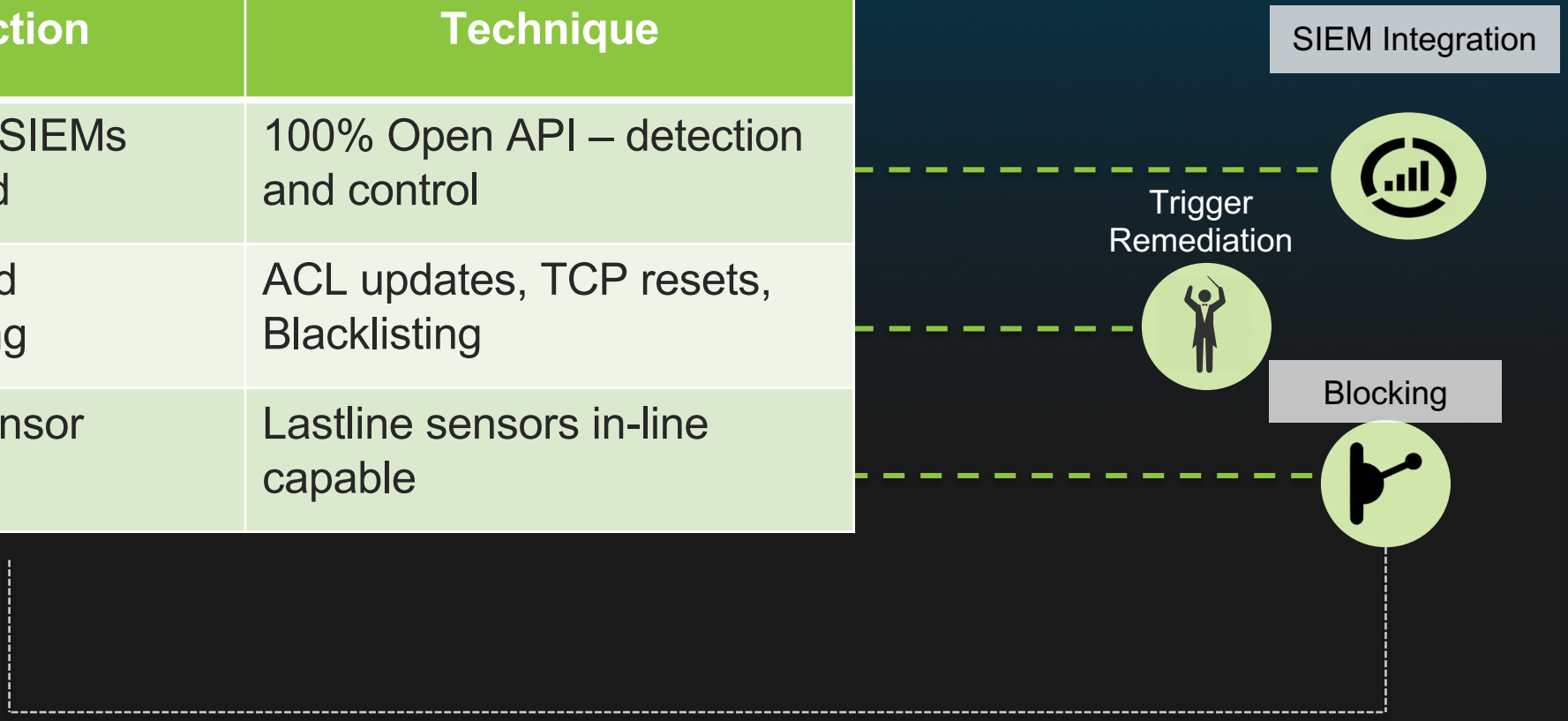
Detection	Techniques	Advantages
Signatures and Reputation	DPI, Threat Intelligence	Automated (AI-based) signature generation
Threat Behaviors	Full System Emulation, AI-based Static File Classification	Visibility into every single instruction and OS kernel
Network Behaviors and Anomalies	Supervised and Unsupervised AI, Heuristics	AI trained on more data sources and richer inputs deep ML expertise

Improving Fidelity and Reduced False Positives

lastline™

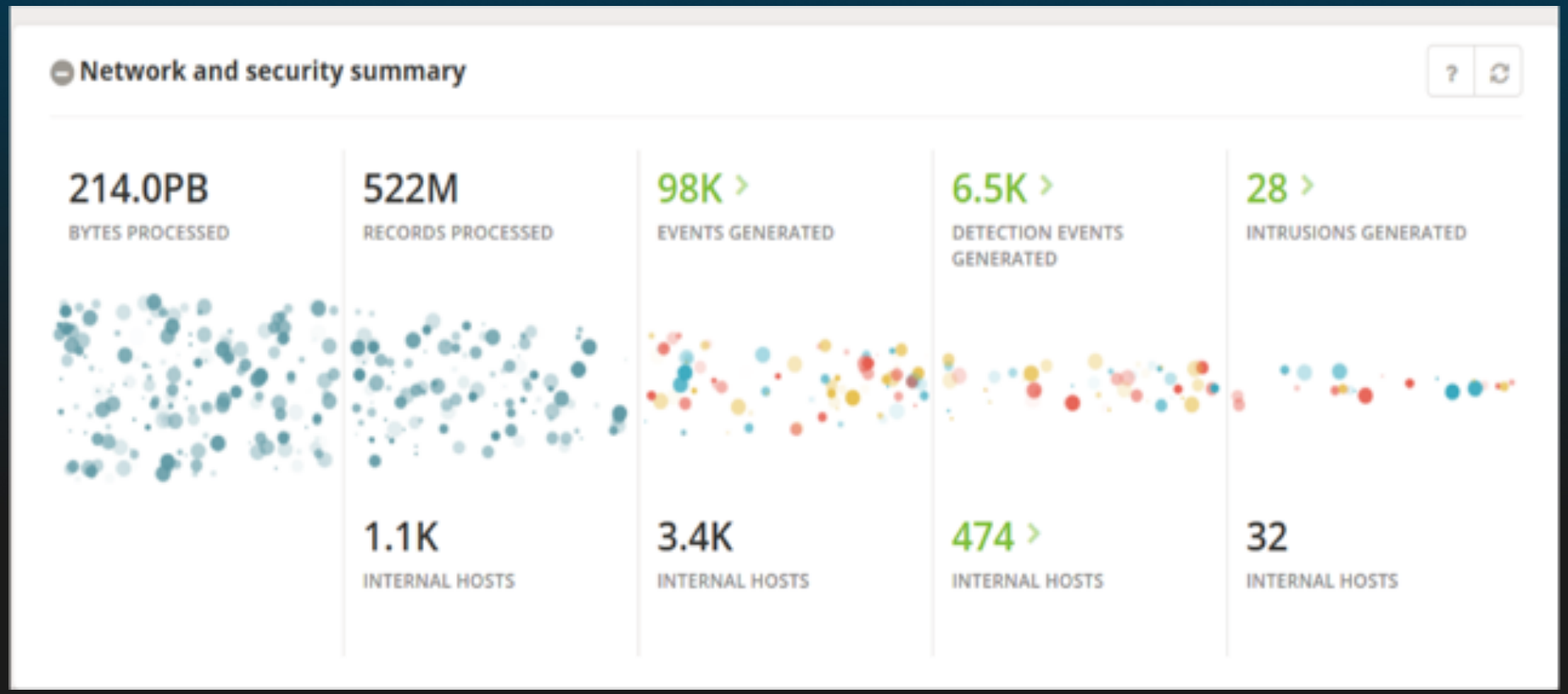
Solution Architecture

Action	Technique
All major SIEMs supported	100% Open API – detection and control
Command Messaging	ACL updates, TCP resets, Blacklisting
Native sensor blocking	Lastline sensors in-line capable



lastline™

How Effective Can it Be?



lastline™

Places to Monitor on the Network

Traffic going outside the organization

Internet ←→ Inside
- Most common inspection for Web, E-mail, file xfer
- Key for detecting malware C&C traffic

Partner/Extranet ←→ Inside

Possible contamination from external network

Partner may not know they are infected

Traffic inside the organization

Inside → Inside

Lateral propagation of malware

Monitoring traffic to/from file servers, intranet web

Within a virtual machine network

Virtualization very popular, some traffic never seen on network

lastline™

Superior Analysis Advanced Threat Detection

			Lastline/NDR	Traditional NTA	Advanced Malware	Next-Gen Firewalls
Perimeter	URL in email that points to an unknown phishing site		✓	✗	✓	✗
	PDF doc that includes a URL that links to malware	Emotet	✓	✗	●	✗
	Malicious advertising	Coinhive	✓	✗	✓	●
	Exploit against web server in the cloud	Drupalgeddon	✓	✗	✗	✓
	Infected IoT devices	Reaper	✓	●	✗	✓
Network Activity	Obfuscated command & control and beacon	Cold River	✓	✓	●	✗
	Active directory attacks	Kerberos Golden Ticket	✓	✓	✗	✗
	Ransomware spreads laterally	WannaCry, EternalBlue	✓	✓	✗	✗
	Distinguish a benign from a malicious RDP connection		✓	✗	✗	✗
	Exfiltrate data via DNS tunneling	FrameworkPOS	✓	●	●	●

lastline™

The Most Valuable Intel is in Your Network

lastline™

Negative Value of External Feeds

Lots of overlap, right?

1	2	3	4	5	6	7	8	10	11	12	15	16	18	19	20	21	24	25	27	29	30
-	1%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	1%	0%
49%	-	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%

/www.first.org/resources/papers/conf2016/FIRST-2016-63.pdf

Types of data: **"blacklists"**

/www.first.org/resources/papers/conf2016/FIRST-2016-63.pdf

Key results:

- More than **96%** of domain names are unique to one list
- IP addresses are unique to one list **82%-95%** of the time

122M IPs, **31M** domains (2nd year)

- Internal threat data is gaining traction
- Unempowered/overworked junior staff
- Irrelevant IoCs

- Too Voluminous
- Triage Blindness
- Lack of Context

lastline™

External Threat Metrics for CISO Metrics

- Threat Actors employed over 40 payload types to attack enterprises
- 1 in 500 threats infiltrate enterprise security deployments
- You are Patient0 in 65% of threat encounters
- 1in12 threats displayed advanced capabilities
- 90% of detections are generic and are remediated in the same way

lastline™

Interested in Learning More?

Get a free threat assessment or an easy-to-deploy Proof of Value demo of Lastline Defender and see how it can dramatically increase the quality of your alerts

Deploy a sensor in as little as 30 minutes

Turn low fidelity alerts or false positives into high fidelity alerts

lastline™

Did We Make it on Time?

Questions?
rhenderson@lastline.com
LinkedIn
@richsentme – Tweet Tweet

lastline™

Thank You!