

The logo for RAPID7, with 'RAPID' in black and '7' in orange.

# Transform Data Into Insights

Clarity, command, and confidence to  
securely move your business forward.

A donut chart with a blue outer ring and an orange inner segment. The text '20%' is prominently displayed in orange, with 'of all assets have critical risk vulnerabilities' in white below it.

20%  
of all assets have  
critical risk vulnerabilities

Haris Pylarinos  
Systems Engineer  
Naftomar

# Products

Accelerating insight for security and IT teams.

## Nexpose

Vulnerability management for today's threat landscape

[Learn More](#)

[Free Trial](#)

## InsightIDR

Complete incident detection and response, SIEM and user behavior analytics

[Learn More](#)

[Watch On-Demand Demo](#)

## AppSpider

Application assessment for the modern world

[Learn More](#)

[Free Trial](#)

## Metasploit

Penetration testing for offensive security teams

[Learn More](#)

[Free Trial](#)

## InsightOps

IT operations and log management for total infrastructure awareness

[Learn More](#)

[Beta Signup](#)

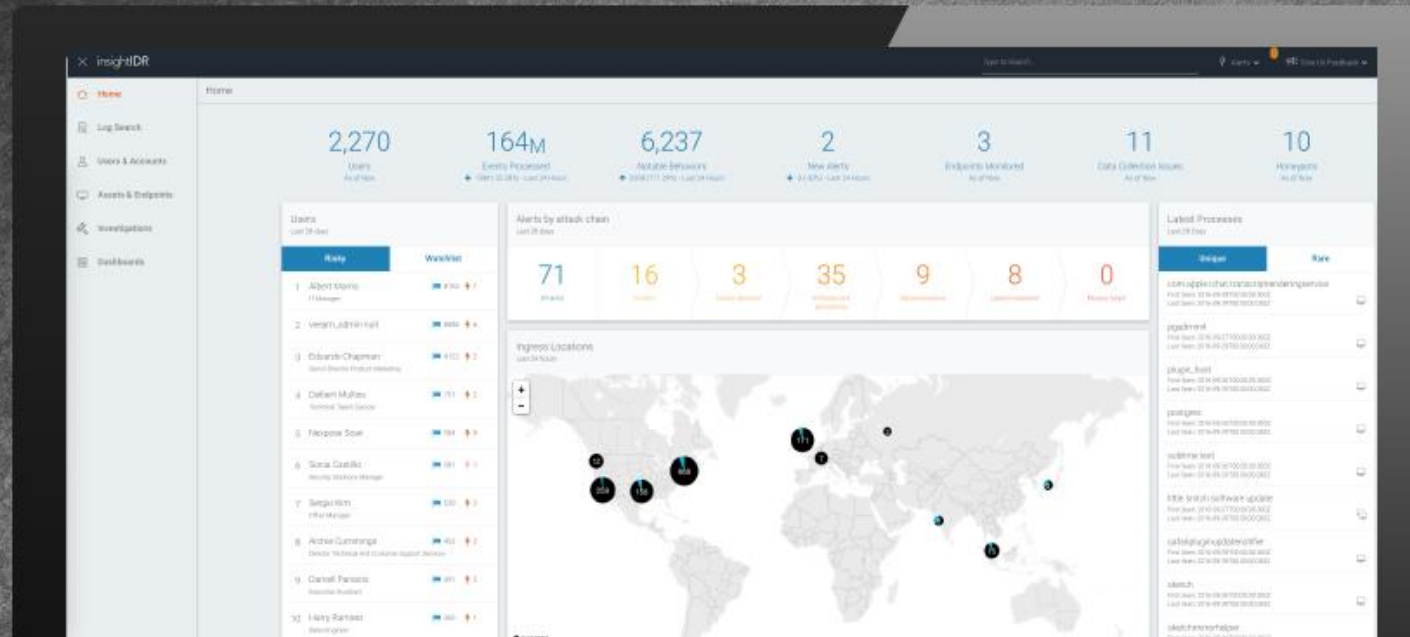
## Looking for services?

From planning and strategy to full-on full service support, our experts have you covered.

[Go to Services](#)

# insightIDR

## Incident Detection & Response



### UNIFY

Combine SIEM, UBA, and EDR to leave attackers with nowhere to hide.

### DETECT

Find unknown threats with User Behavior Analytics and Deception Technology.

### PRIORITIZE

Know exactly where to search with Security Analytics.

# UNIFY



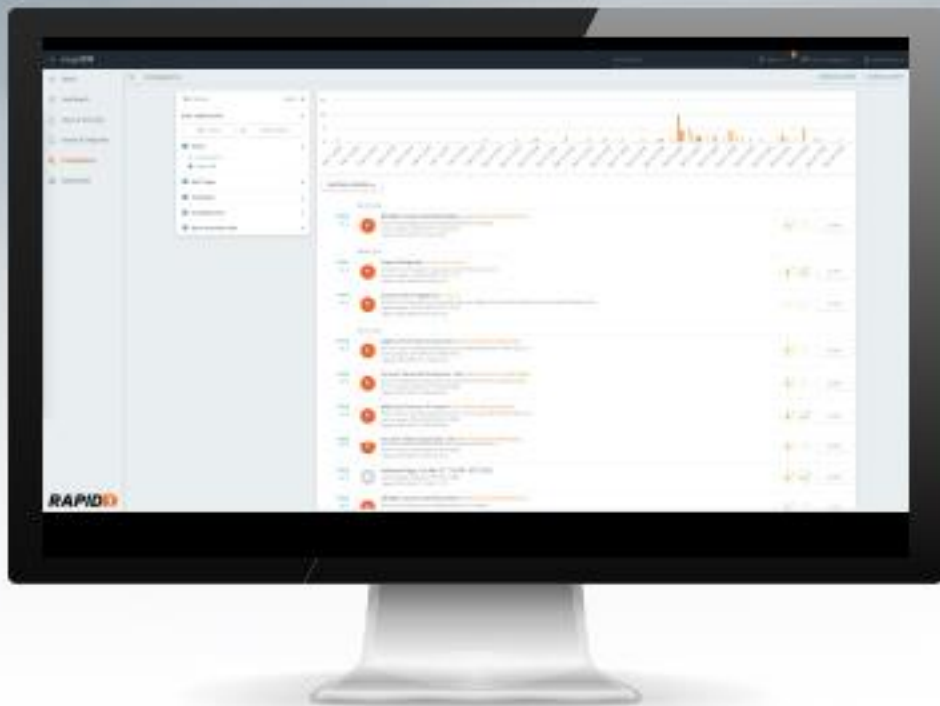
## insightIDR

Through a combination of user behavior analytics (UBA), endpoint detection, and automated intruder traps, InsightIDR unifies and analyzes your data to create high-fidelity, low-volume alerts on actual intruders.

“Even if we had the data, without InsightIDR we would have no way to correlate the separate pieces of information to give us an accurate picture of the event.”

--Russ Swift,  
Information Security  
Manager, BlackLine

# DETECT



## insightIDR

Detect the use of stolen credentials, malware, and phishing, letting you respond before attackers reach critical data.

“InsightIDR gives you that warm feeling inside by catching any suspicious behavior on the network months before you’d otherwise discover it.”

--Tom Brown,  
IT Manager,  
Liberty Wines



# PRIORITIZE



## insightIDR

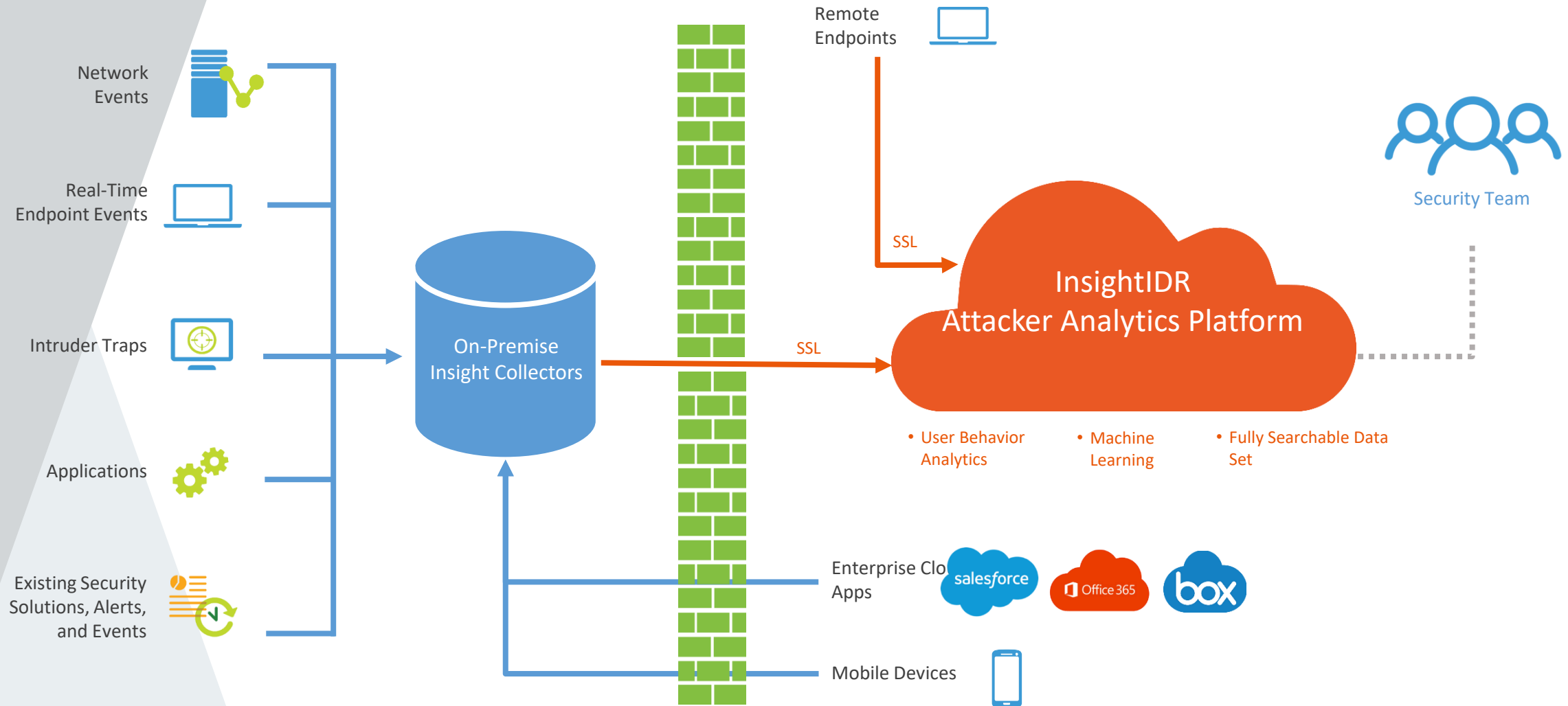
InsightIDR automates the legacy work of log search platforms, providing a visual investigation timeline to speed up investigations by over 20x.

“I don’t have a team available to set things up and monitor it all day. I need the analytics to bring to light what’s important and what’s not.”

----Chad Klierer, ISO,  
Pioneer Telephone

# InsightIDR Solution Architecture

insightIDR



# Disrupting the Attack Chain

## Infiltration and Persistence


- Phish users
- Use leaked credentials
- Connect to network
  - Anonymize access
  - Deploy backdoors

## Infiltration and Persistence

- Detect phishing attempts
- Identify malware
- Alert on leaked credentials
- Monitor inbound connections



# Disrupting the Attack Chain



## Reconnaissance

- Get user list
- Scout targets
- Find vulnerabilities

## Reconnaissance

- Detect network scans

# Disrupting the Attack Chain

## Lateral Movement

- Access machines with credentials
- Collect more passwords
  - Increase privileges

## Lateral Movement

- Detect intruders switching identities
- Detect unusual authentications
- Identify privilege escalation
  - Detect password guessing attempts & pass-the-hash



# Disrupting the Attack Chain

## Mission Target

- Access critical data
- Upload data to external location

## Mission Target

- Detect suspicious access to critical data
- Monitor data traffic and cloud usage

# Deception Technology: Finding Attacks Beyond Logs

## Honey Pots



**What:** Virtual machine that appears as legitimate assets. Will alert on malicious behavior, such as network scans to identify network architecture.

**Why:** Valuable to identify early attacker reconnaissance before lateral movement occurs.

## Honey Users and Credentials



**What:** Create fake accounts to lure attackers to authenticate. Since not tied to a real user, attempts to authenticate are reliably malicious.

**Why:** Attackers frequently enumerate AD/LDAP to find next targets.

## Honey Files



**What:** Create fake files along with legitimate critical data and be alerted any time the files are accessed or modified.

**Why:** Attackers can read or extract critical data. Also ransomware can encrypt company data and provide the decryption mechanism for a fee.

# Raw Logs and Custom Alerts

- Parse any log as raw data and use later in analysis
- Create customized alerts based on log queries
- Create custom dashboards and reports





The background is a dark-themed dashboard with several data visualizations. At the top left, a line graph shows an upward trend from February to September 2015. To its right, a card displays the text 'of all assets have SSL Certificates that are set to expire in the next 30 days' with an 'Expand Card' button. Below the line graph, a circular gauge chart shows '20% of all assets have critical risk vulnerabilities'. At the bottom right, a scatter plot titled 'ASSETS BY RISK AND VULNERABILITIES' shows a positive correlation between asset value (x-axis, 0 to 1,250k) and the number of vulnerabilities (y-axis, 0 to 5,000).

# Thank you!

[hpylarinos@outlook.com](mailto:hpylarinos@outlook.com)

[www.linkedin.com/in/hpylarinos](https://www.linkedin.com/in/hpylarinos)

Haris Pylarinos  
Systems Engineer  
Naftomar