



**CROWDSTRIKE**

# NIS2 als Chance – Verteidigung gegen Ransomware- & KI-Angriffe

---

Philip Scheidl, Sales Engineer



# NIS2

## NIS 2 - are you ready?

- Artikel 21, (1): “... geeignete und verhältnismäßige **technische, operative und organisatorische Maßnahmen** ergreifen...”
- Artikel 21, (2), a): “Konzepte in Bezug auf **Risikoanalyse und Sicherheit für Informationssysteme**”
- Artikel 21, (2), b): “Bewältigung von Sicherheitsvorfällen”
- Artikel 21, (2), e): “**Sicherheit der Lieferkette...**”
- Artikel 21, (2), f): “Konzepte und Verfahren zur **Bewertung der Wirksamkeit von Risikomanagementmaßnahmen...**”
- Artikel 21, (3): “Die spezifischen Schwachstellen der **einzelnen unmittelbaren Anbieter und Dienstleister** [...] berücksichtigen”

---

# UNDERSTANDING THE THREAT LANDSCAPE





# Motivations



NATION STATE



CRIME



HACKTIVISM

# Nation State Goals



## CHINA

---

ECONOMIC ESPIONAGE  
INTELLIGENCE COLLECTION



## North Korea

---

CURRENCY GENERATION  
ECONOMIC ESPIONAGE



## IRAN

---

GEOPOLITICAL CAMPAIGNS  
TELECOM FOCUSED



## RUSSIA

---

INFORMATION OPERATIONS  
CRITICAL INFRASTRUCTURE



# Sophisticated & Symbiotic E-Crime Ecosystem



## SERVICES

---

CAPABILITIES ENABLING  
CYBER CRIMINAL ACTIVITY



## DISTRIBUTION

---

VEHICLES LEVERAGED FOR  
DELIVERING TO VICTIMS



## MONETIZATION

---

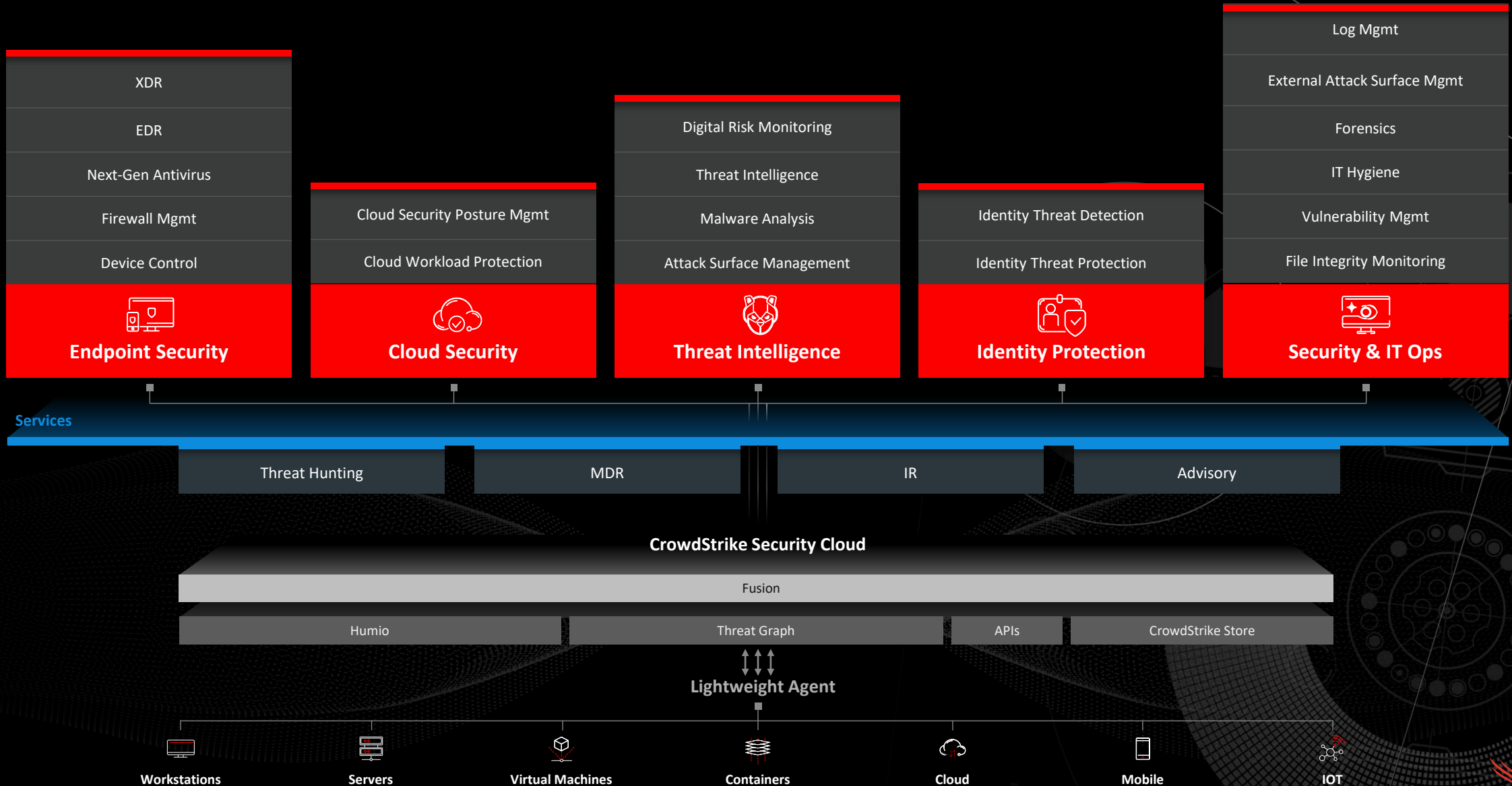
CAPITALIZING ON  
SUCCESSFUL EXECUTION

---

# UNDERSTANDING & DEFEND YOUR ENTERPRISE



# THE FALCON PLATFORM





# DELIVERED VIA ONE AGENT THAT REPLACES DOZENS OF POINT PRODUCTS



**Falcon Agent**

Prevent • Predict • Detect • Respond

✓ **Lightweight**

✓ **Zero reboots**

✓ **Superior user  
experience**

## Endpoints



Workstations



Mobile



Servers



IOT

## Clouds



Data Centers



Workloads



Containers

## Identities



Active Directory



User Accounts



3<sup>rd</sup> Parties



# AUTOMATED HUNTING ENGINE THREAT GRAPH

135 MILLION  
IOA DECISIONS/MIN

1 TRILLION+  
EVENTS/DAY

160+  
ADVERSARIES TRACKED

ENRICHED  
DATA

ANALYZED  
DATA

ACTIONABLE  
INSIGHTS

PREVENT  
THREATS

INVESTIGATE  
FASTER

HUNT  
PROACTIVELY



---

# XDR @ CROWDSTRIKE

ENTERPRISE-WIDE VISIBILITY ACROSS ALL KEY SECURITY  
DOMAINS





---

# XDR

Definition | **Extended Detection Response**

Built on the foundation of EDR, XDR extends **enterprise-wide visibility** across all **key security domains** (native & third-party) to speed and simplify **near real-time** detection, investigation, and response for the most sophisticated attacks



# UNIFY SIGNALS TO FIND THE MOST SOPHISTICATED ATTACKS ACROSS THE ENTERPRISE

## Ingest



Endpoint



Identity



Cloud



Web



CASB



Email



Network



Firewall

## Analyze



Parse



Normalize



Map to Schema



Enrich with  
telemetry &  
threat intel



Advanced  
analytics



Correlate

## Action



**Identify:** Custom & CrowdStrike created detections



**Orient:** Native cross-domain graph explorer



**Hunt:** Unified cross-domain investigations

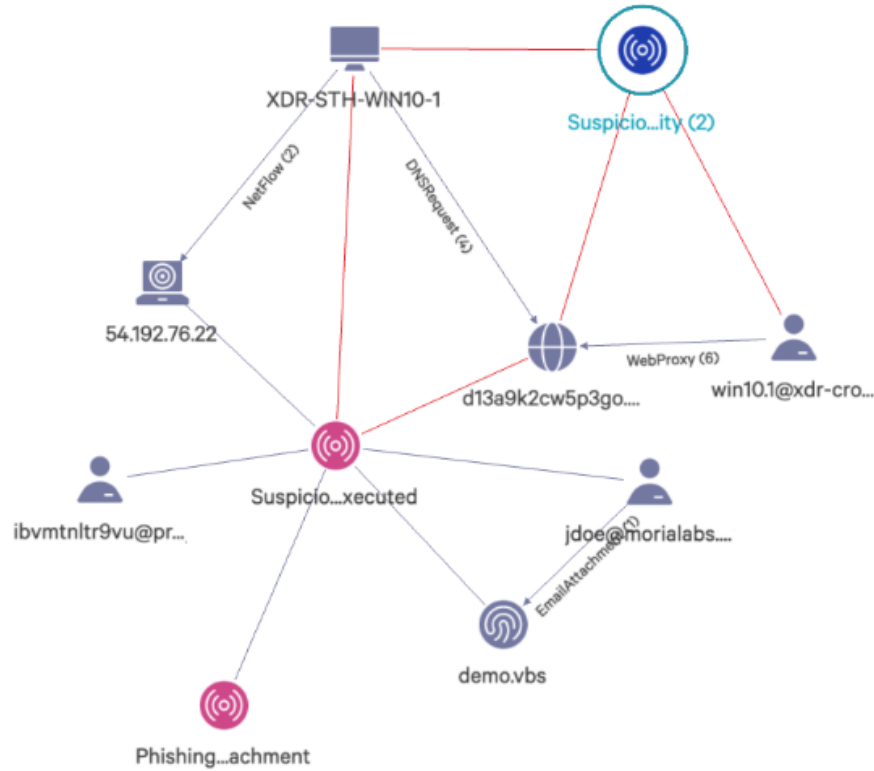


**Respond:** Surgical response for native & third-party tools



**Automate:** Native SOAR automates repetitive tasks





## Suspicious Web Proxy Allowed Activity (2)

### Web indicator

Event time	Log source
Oct. 27, 2022 03:18:51	Zscaler
Tactic & technique	
Command and Control via Application Layer Protocol	
Domain	
Web	
Description	
Suspicious allowed web proxy activity observed.	
Source IP	Destination IP
172.17.0.26	18.65.229.61
Action	ApplicationClass
Allowed	General Browsing
ApplicationName	ContentType
General Browsing	Other
DataDomain	EventID
Web	95
HTTPRequestMethod	HTTPResponseCode
CONNECT	200
MalwareCategory	MalwareClass
None	None
Product	Protocol
XDR	HTTP_PROXY
Reason	RefererURL
Allowed	None
RemoteAddressIP4	RemoteHostname
18.65.229.61	d13a9k2cw5p3go.cloudfront.net







# CROWDSTRIKE FALCON COMPLETE (MDR)

## EXPERTS IN FALCON PLATFORM

Certified analysts, 100% focused on stopping breaches

## EXPERTS IN INCIDENT RESPONSE

Years of DFIR experience, PIONEERED remote remediation as a core competency

## ALWAYS IMPROVING

Every day building countermeasures to respond to the latest threats the moment they emerge

### **MISSION:**

Manage, monitor, and remediate threats  
24/7/365



# RANSOMWARE & NIS2 – IDENTITIES



---

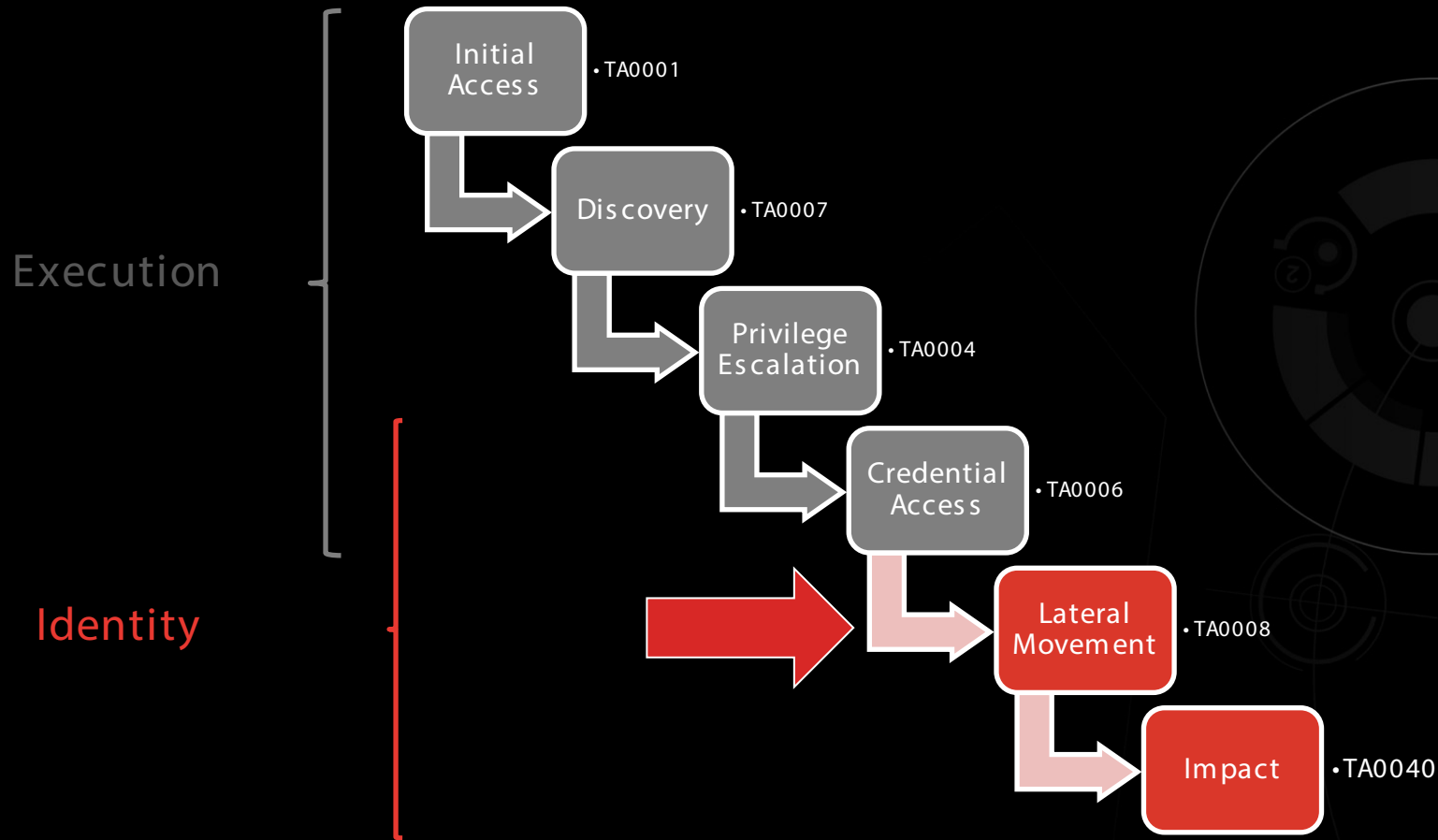
**“80% OF DATA BREACHES HAVE A CONNECTION  
TO COMPROMISED PRIVILEGED CREDENTIALS”**

**- FORRESTER RESEARCH**





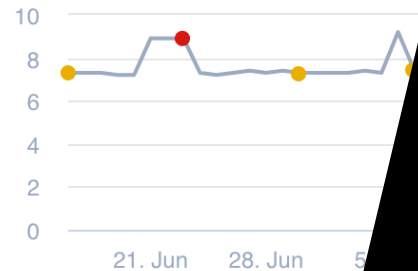
# OFTEN, THEY ARE STARTING HERE



## Risk Score



## Score Trend



## Severity

## Risk



High

Accounts with Privileged SID



Medium

Kerberos Pre-Authentication for TGT is not Required



Medium

Poorly Protected Account with SPN



Medium

SMB Signing Disabled

## FALCON IDENTITY THREAT DETECTION

- Understand what privileged accounts exist
- Understand where privileged accounts are used
- Identify service accounts
- Identify stale accounts
- Assess the risk associated with accounts
- Assess risk associated with account usage
- Identity store stitching and correlation



Rule	Match Count	User Match Count
------	-------------	------------------

Anomalous Authentication	3	2
--------------------------	---	---

3
<a href="#">Identity Verification</a>

## Audit Log

Time ↓	Rule	Trigger	Action
Wed, Jul 14th 2021, 12:07 PM	Anomalous Authentication	Access	Identity Verification
Wed, Jul 14th 2021, 9:12 AM	Anomalous Authentication	Access	Identity Verification
Wed, Jul 14th 2021, 2:53 AM	Anomalous Authentication	Access	Identity Verification

## FALCON IDENTITY THREAT PROTECTION

- Trust..and verify
- Automatically enforce conditional access on anomalous activity
- Create bespoke rules that allow, block, or challenge high-risk identity activity
- Integrate with current identity stores for a zero-friction end-user experience
- Stop adversaries in their tracks



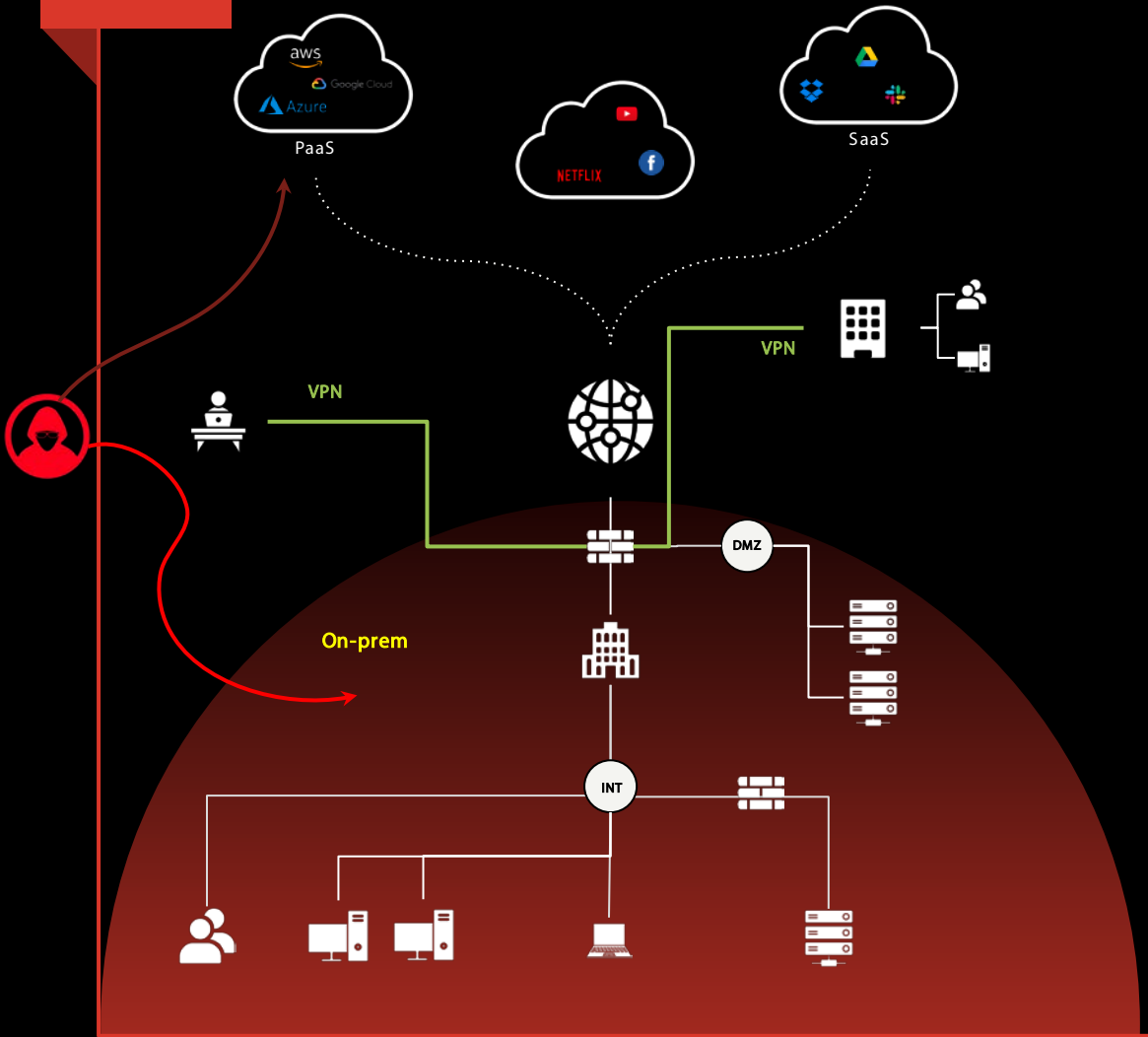
# EASM



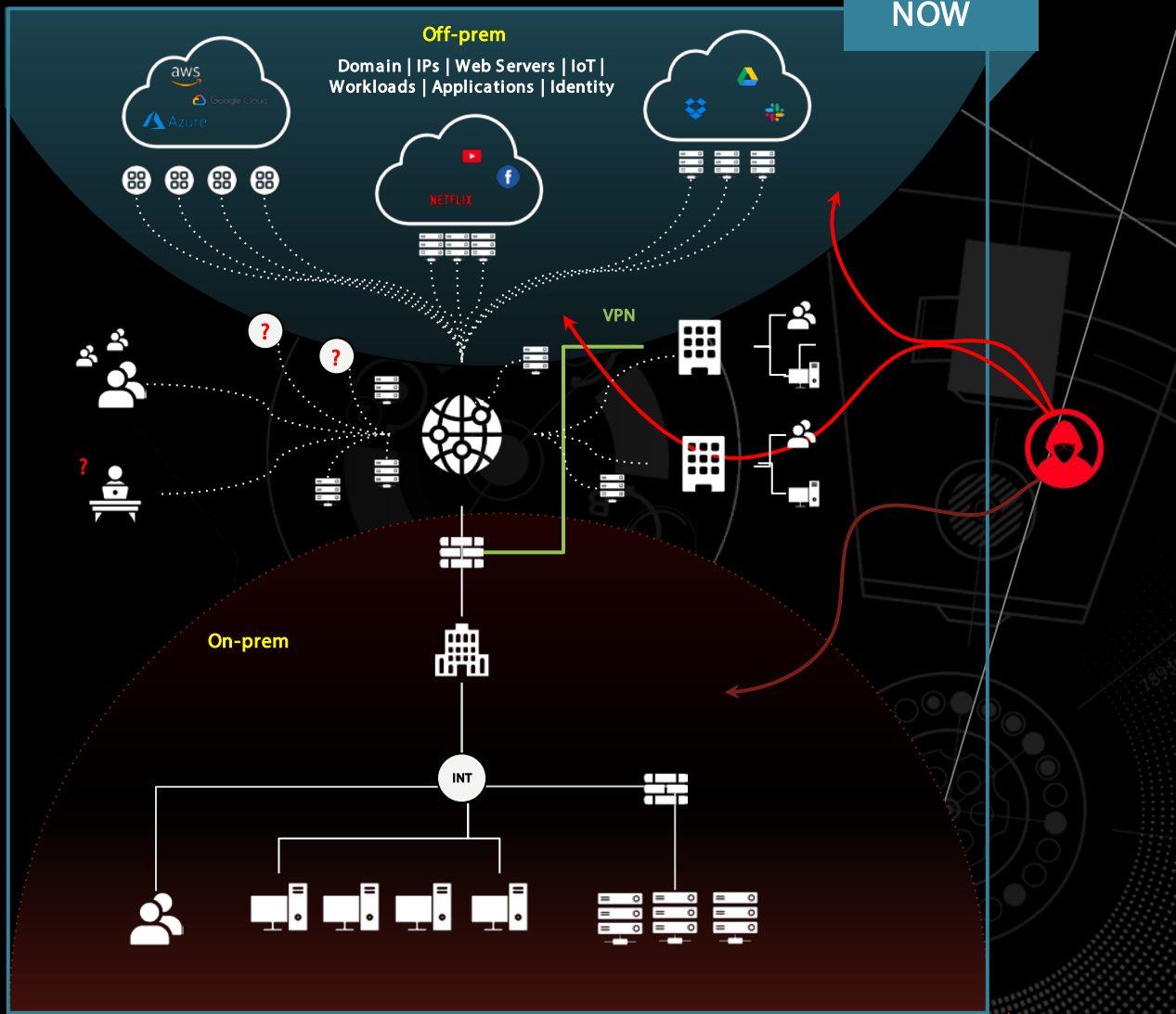


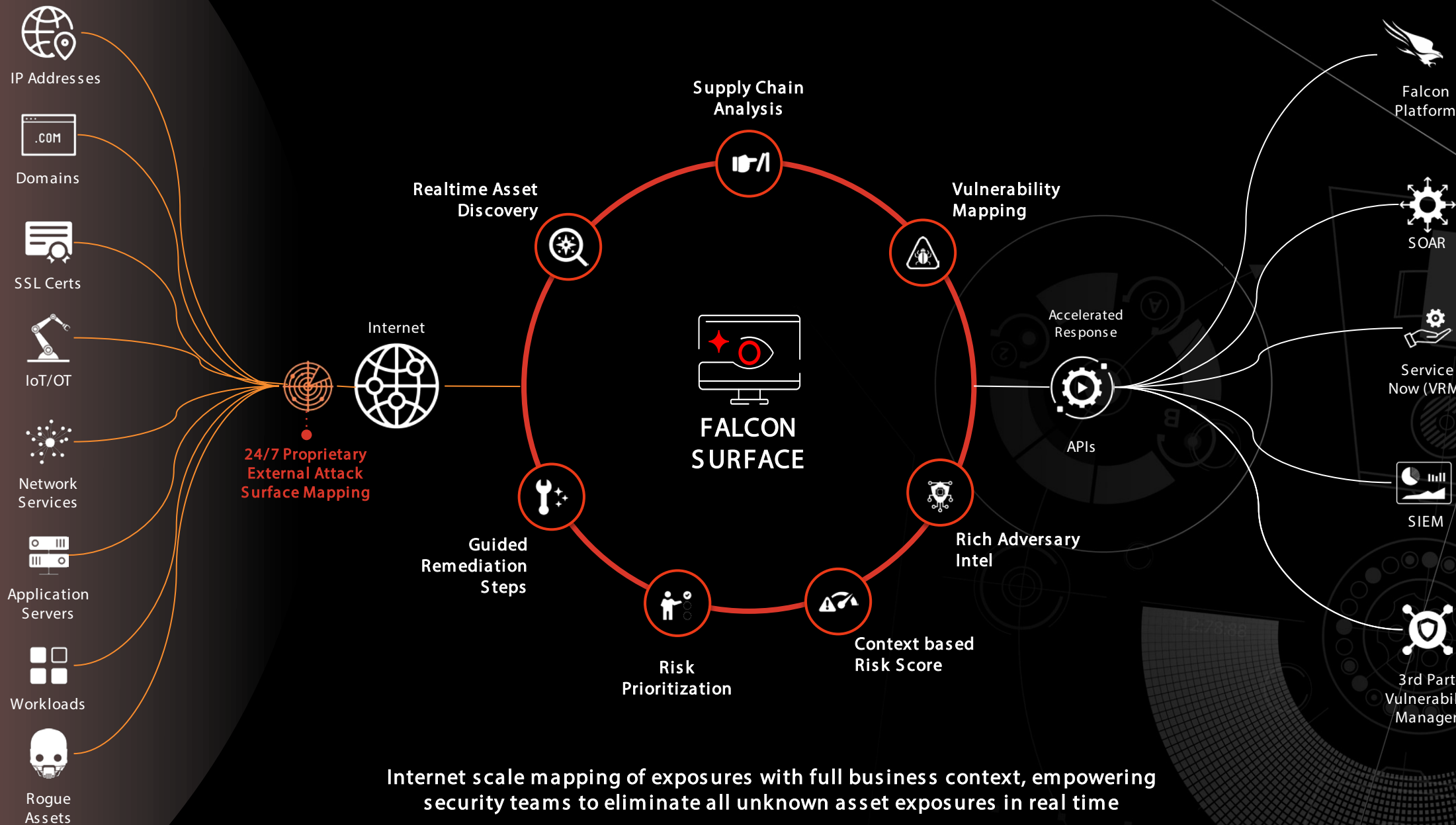
# Your digital footprint is becoming complex

BEFORE



NOW

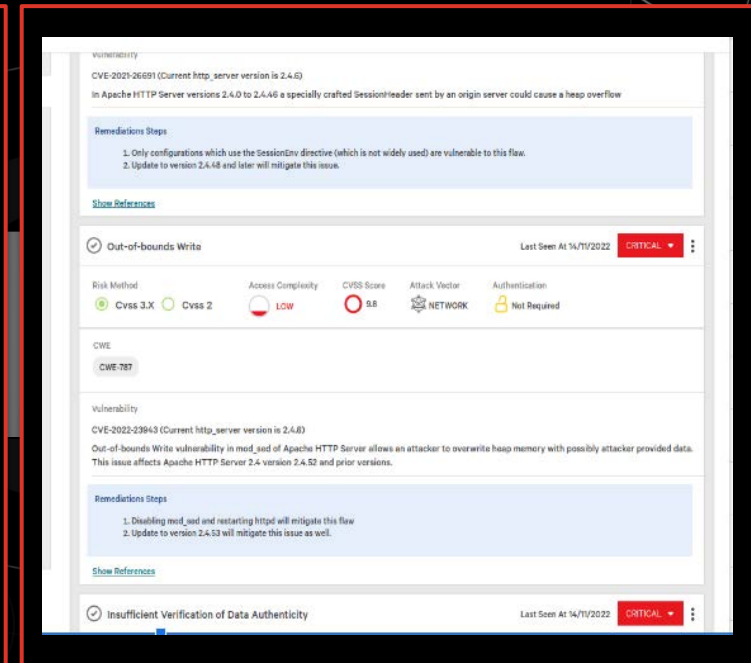
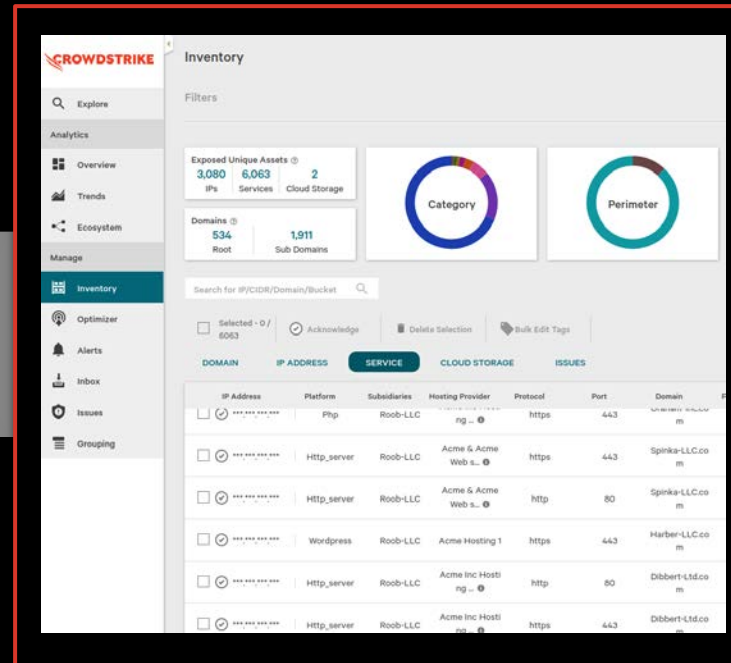
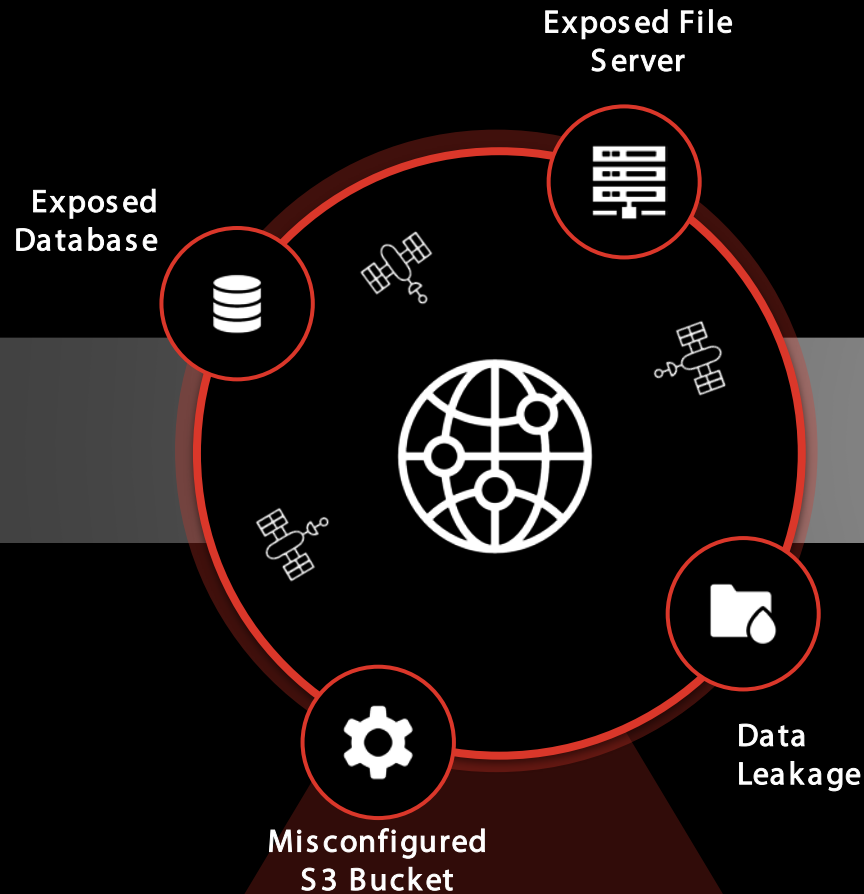




Internet scale mapping of exposures with full business context, empowering security teams to eliminate all unknown asset exposures in real time



# FALCON SURFACE MAPS THE WORLD'S INTERNET EXPOSURES IN REAL-TIME

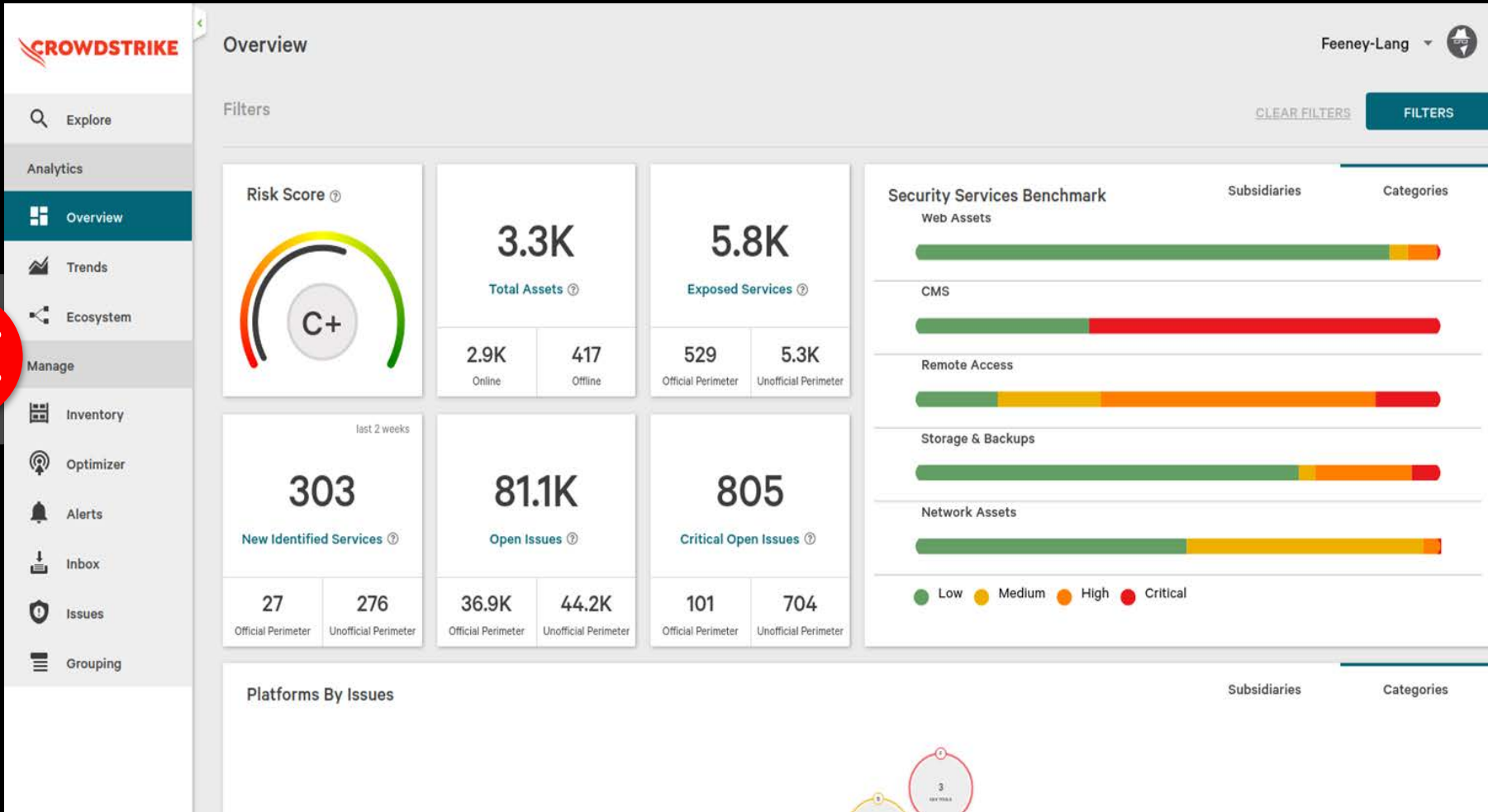


**1** Scan the entire internet for exposed assets

**2** Create exposed asset inventory and analyze security posture

**3** Prioritize risk and generate guided remediation steps

# Do you know your external attack surface?



FALCON SURFACE

BOOK YOUR DEMO TODAY





# A PROVEN SECURITY LEADER

Leader In

Gartner • FORRESTER® • IDC

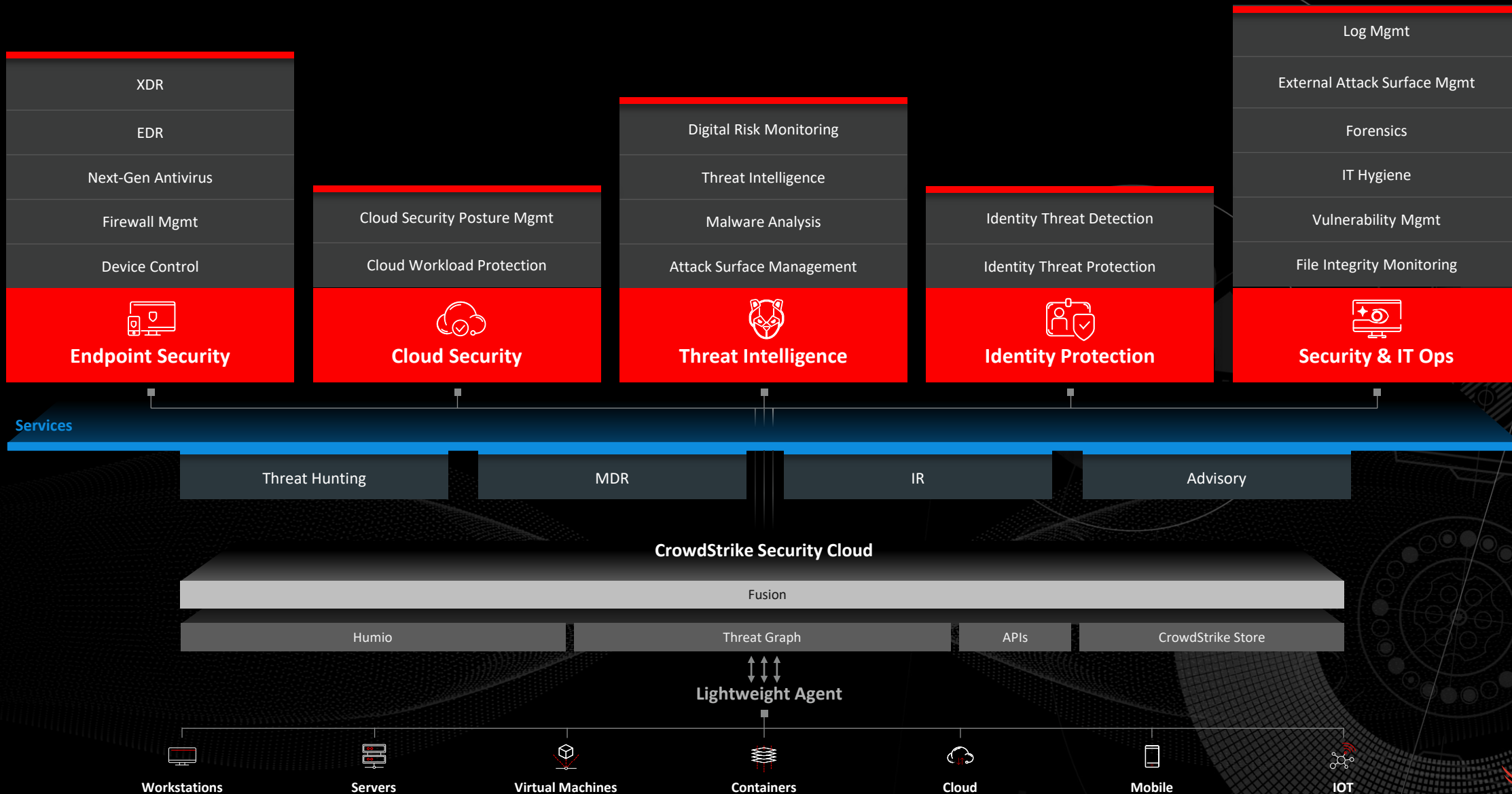
Validated

MITRE • AV comparatives • SE Labs

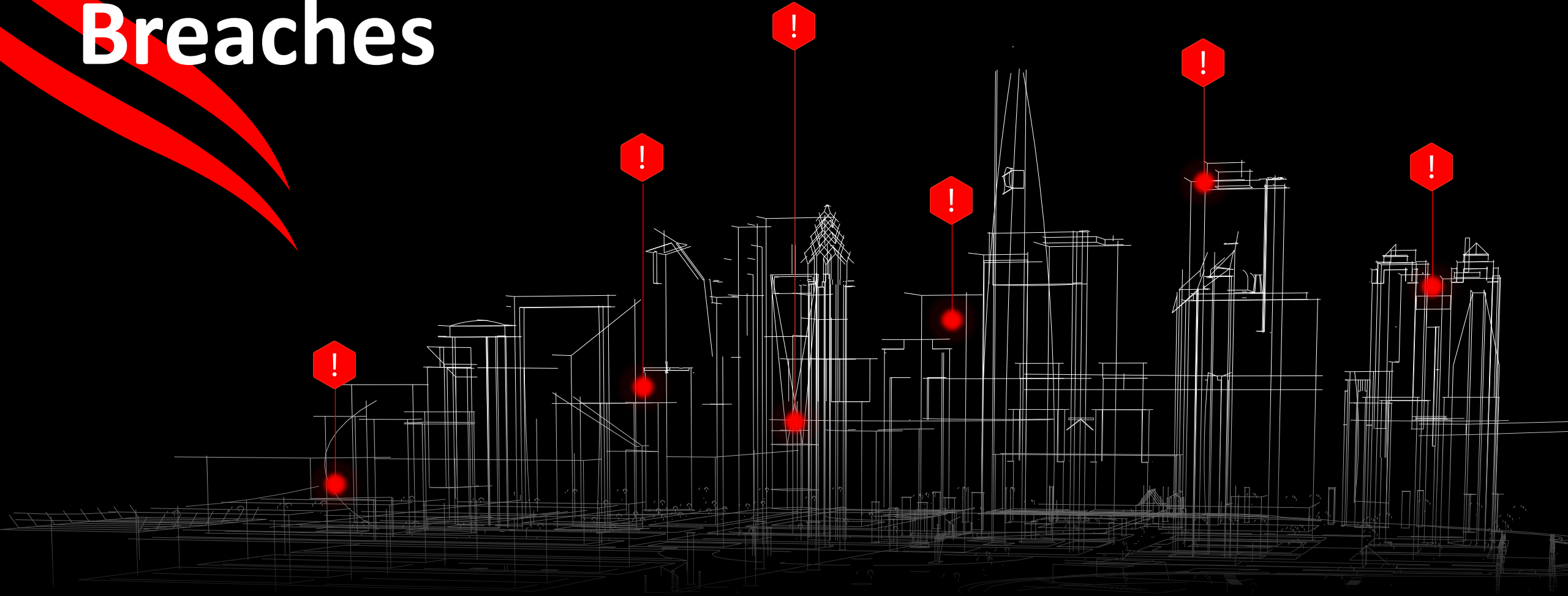
## Compliance & Certifications



# THE FALCON PLATFORM



# We Stop Breaches



---

# THANK YOU

