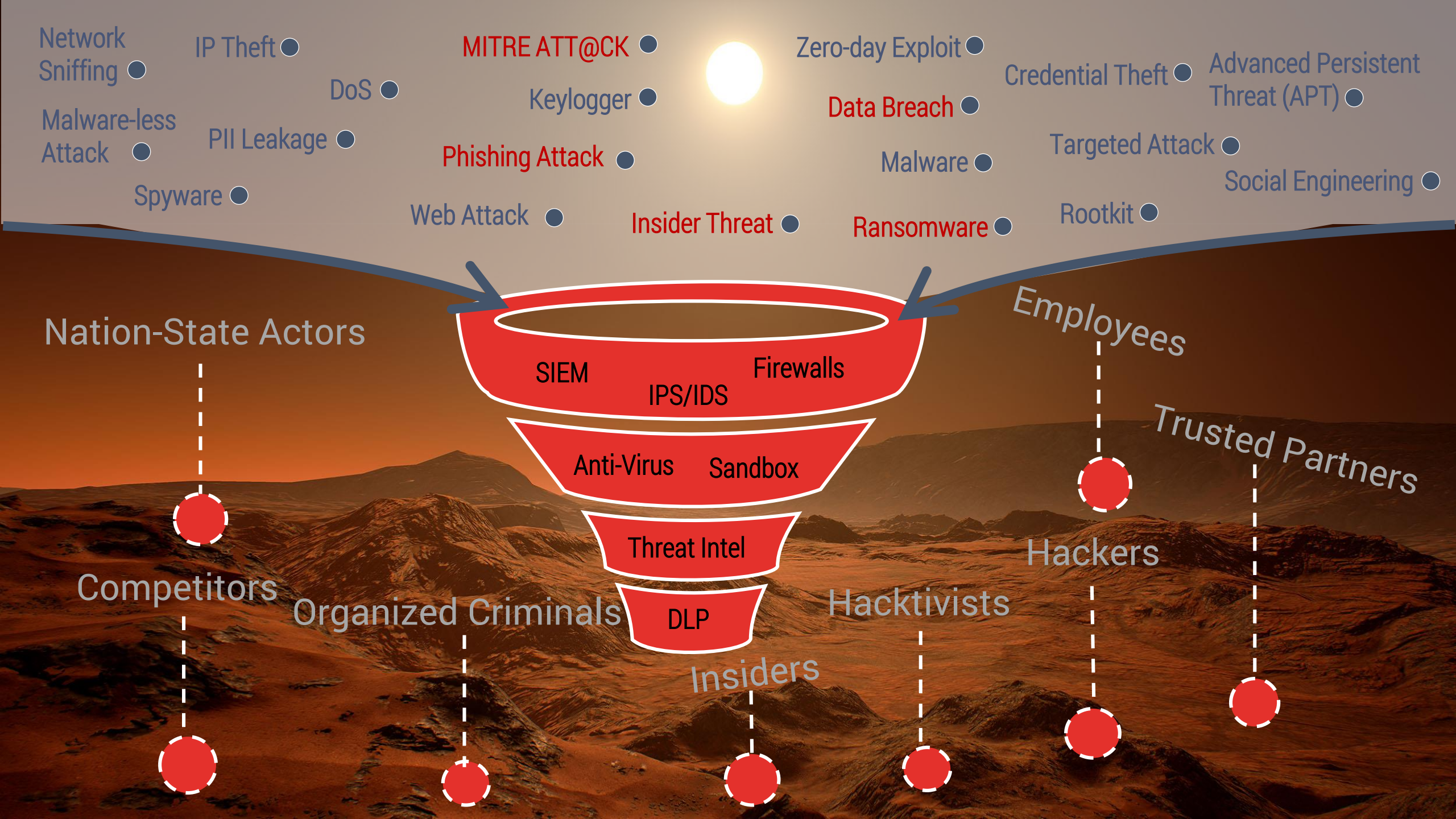
ThreatRESPONDER™

Threat < Detection + Prevention + Response + Analytics + Investigation + Hunting + Intelligence > Platform

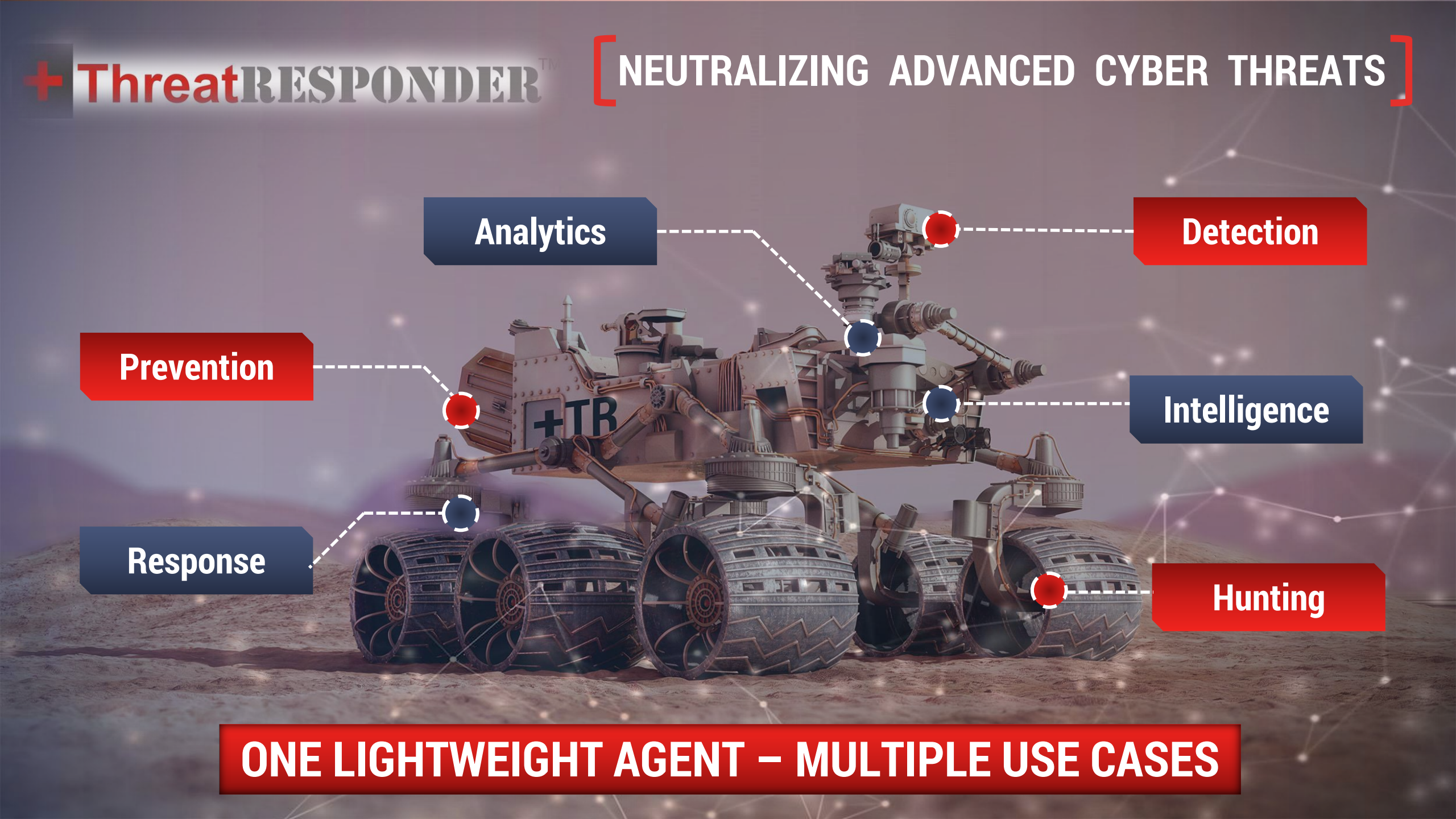
CAPABILITIES + BENEFITS + USE CASES


netSecurity®
FOUNDED
December 2004
VISION
To be the brand of choice in cyber security and forensics
15+ Years of Real-World Problem Solving and R&D in Security and Forensics
Unparalleled Innovation
Customer-Focused
World-Class Quality
Impeccable Timeliness
ThreatRESPONDER™
MISSION > To detect and prevent advanced cyber attacks and data breaches in real-time

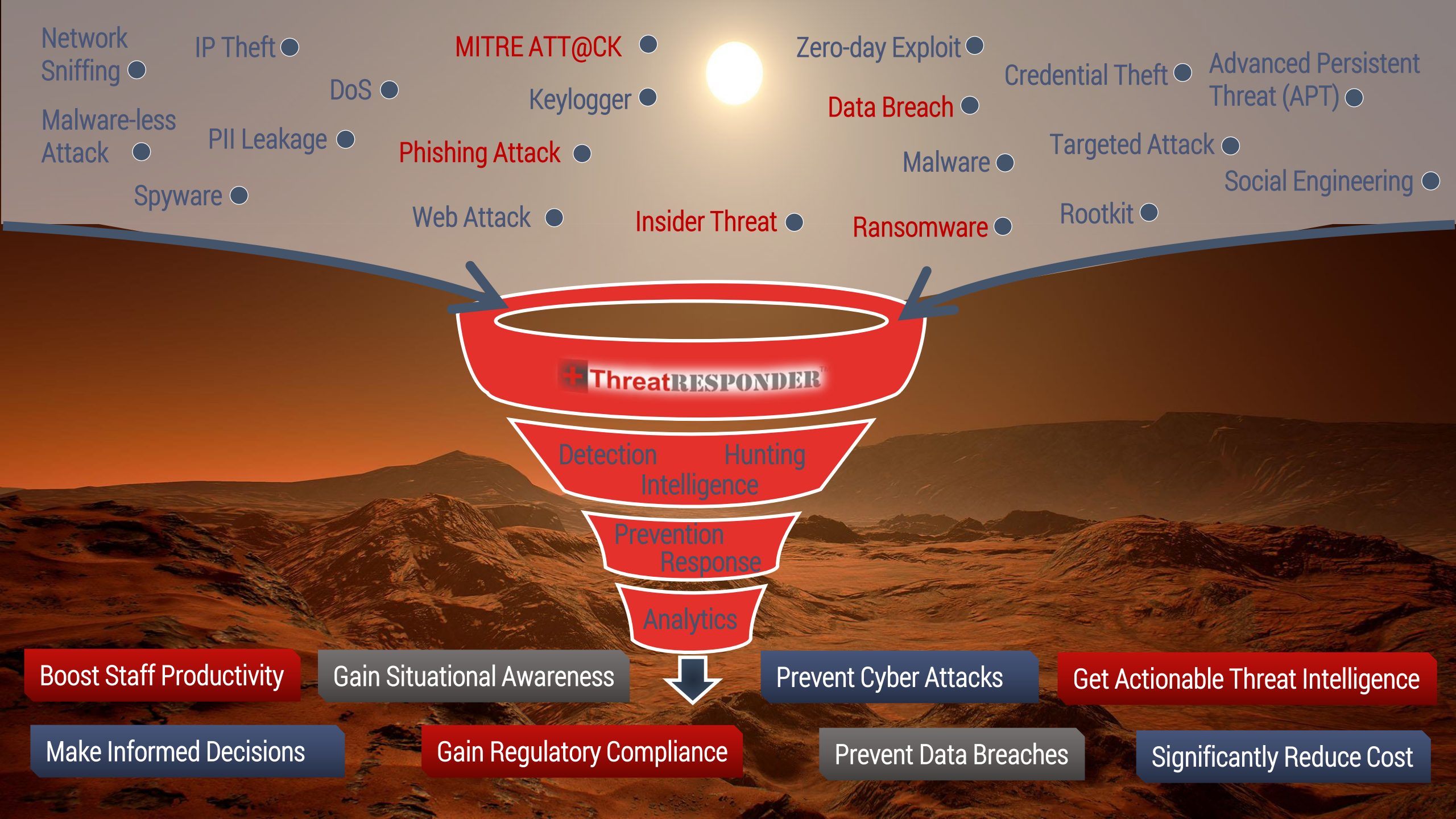

Network Sniffing
IP Theft
MITRE ATT@CK
Zero-day Exploit
Credential Theft
Advanced Persistent Threat (APT)
DoS
Keylogger
Data Breach
Malware-less Attack
PII Leakage
Phishing Attack
Malware
Targeted Attack
Social Engineering
Spyware
Web Attack
Insider Threat
Ransomware
Rootkit
Nation-State Actors
Employees
SIEM
Firewalls
IPS/IDS
Trusted Partners
Anti-Virus
Sandbox
Threat Intel
Hackers
Competitors
Organized Criminals
DLP
Hacktivists
Insiders

ThreatRESPONDER™

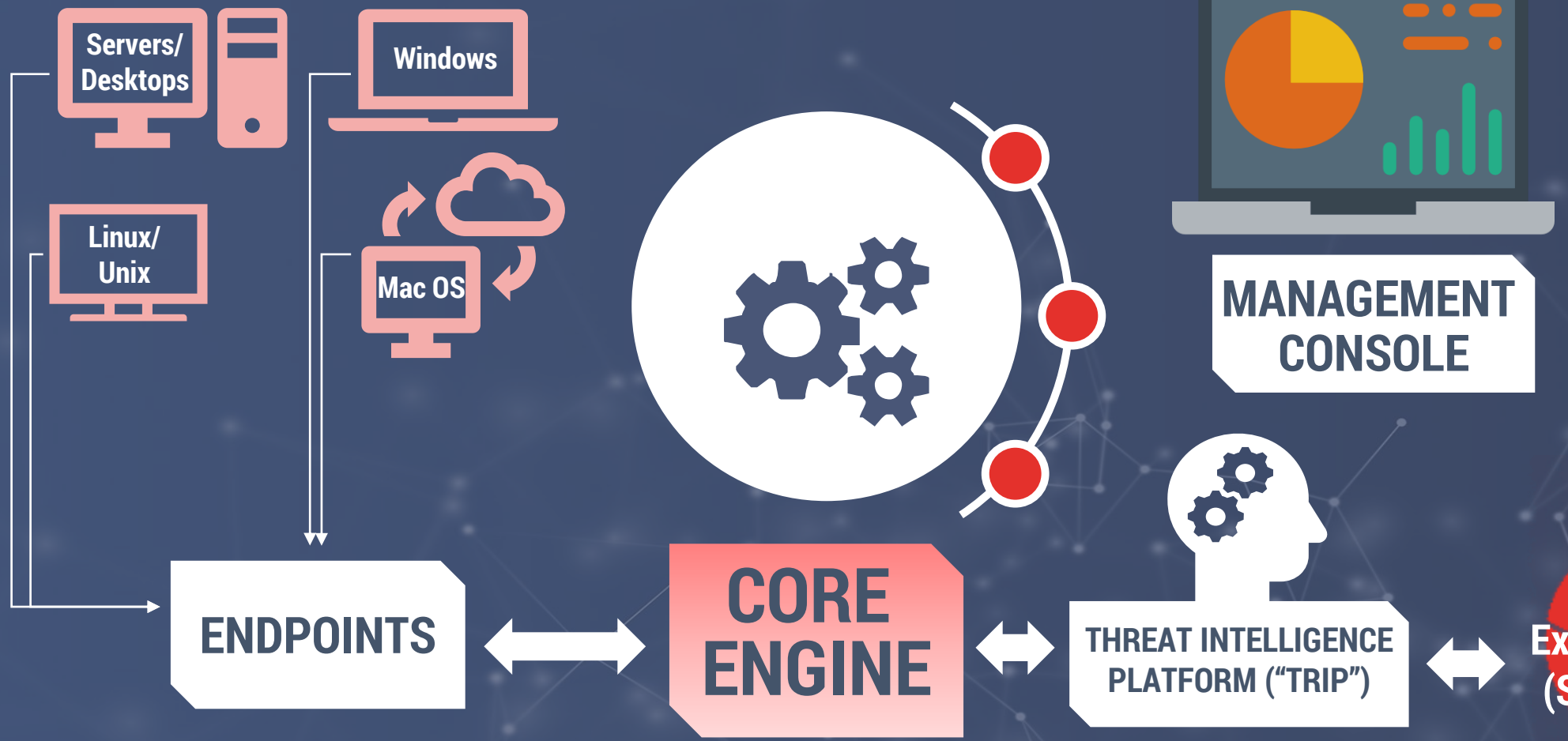
NEUTRALIZING ADVANCED CYBER THREATS



ONE LIGHTWEIGHT AGENT – MULTIPLE USE CASES


Network Sniffing
IP Theft
MITRE ATT@CK
Zero-day Exploit
Credential Theft
Advanced Persistent Threat (APT)
DoS
Keylogger
Data Breach
Malware-less Attack
PII Leakage
Phishing Attack
Targeted Attack
Malware
Social Engineering
Spyware
Web Attack
Insider Threat
Ransomware
Rootkit
ThreatRESPONDER
Detection
Hunting
Intelligence
Prevention
Response
Analytics
Boost Staff Productivity
Gain Situational Awareness
Prevent Cyber Attacks
Get Actionable Threat Intelligence
Make Informed Decisions
Gain Regulatory Compliance
Prevent Data Breaches
Significantly Reduce Cost

THREATRESPONDER® PLATFORM ARCHITECTURE



- Dashboard
- Threat Hunting & Investigation
- Data Loss Prevention
- Policy Enforcement
- User Behavior Analytics
- Malware Analysis

Machine Learning (ML) & Behavior-based Algorithms

- ML-based detection
- Behavior of malware and threat actors
- Attackers' TTPs
- Malware-less techniques

Signatures + Known Indicators

- Signature of known malware
- Indicators of Compromise (IoCs)
- Policy Enforcement

Threat Intelligence (Internal/External)

- File Hashes/Names/Paths
- C&C IP Addresses, URLs, Domain Names, Email Addresses
- User Agents, Mutexes, etc.

Core Engine

- Ingests Threat Data
- Combines ML and Behavior-based Algorithms, Signatures, IoCs, and Threat Intelligence

ACTIONABLE THREAT INTELLIGENCE

PROTECTING AGAINST SENSITIVE DATA LOSS

Data Loss Vectors

:: Clipboard ::
Copy
Paste

:: Email ::
Outlook
Thunderbird

:: Web ::
Internet Explorer
Edge
Firefox
Chrome
Safari

:: Places ::
Removable Storage
CD/DVD/USB
Local Drive
Printing
Print Screen
Network Shares

GAINING VISIBILITY INTO INSIDER THREATS

ThreatRESPONDER® | Ask Curiosity | 20 | inno.demo

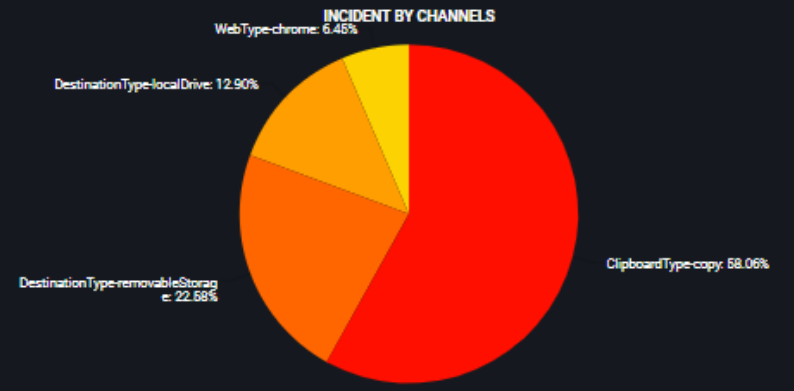
- Dashboard
- Alerts
- Live View
- Investigate
- Forensics
- Hunt
- Data Loss Prevention
- Behavior Analytics
- Policies
- LaunchPad
- Rovers
- Preferences
- User Guide

You are on: Data Loss Prevention - Dashboard

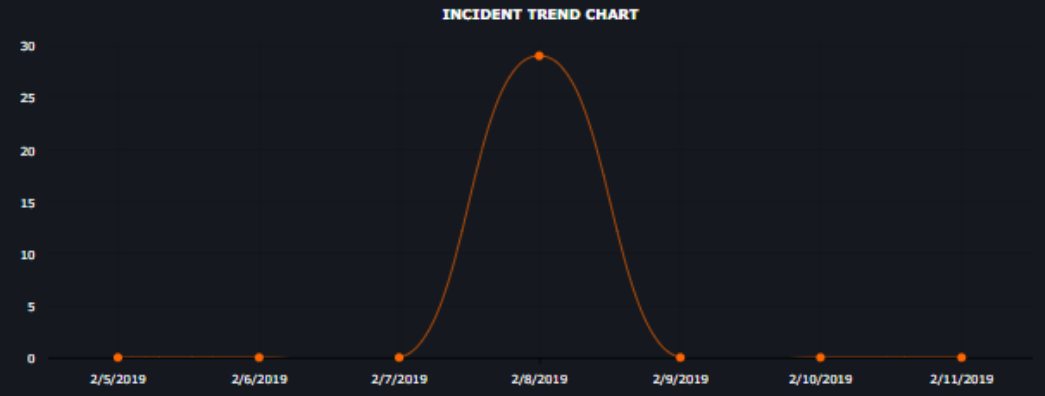
DASHBOARD | REPORTS | POLICIES | ADD NEW POLICY

INCIDENTS BY POLICIES

INCIDENTS BY CHANNELS



INCIDENTS TREND CHART



LIST OF THE LAST 10 INCIDENTS

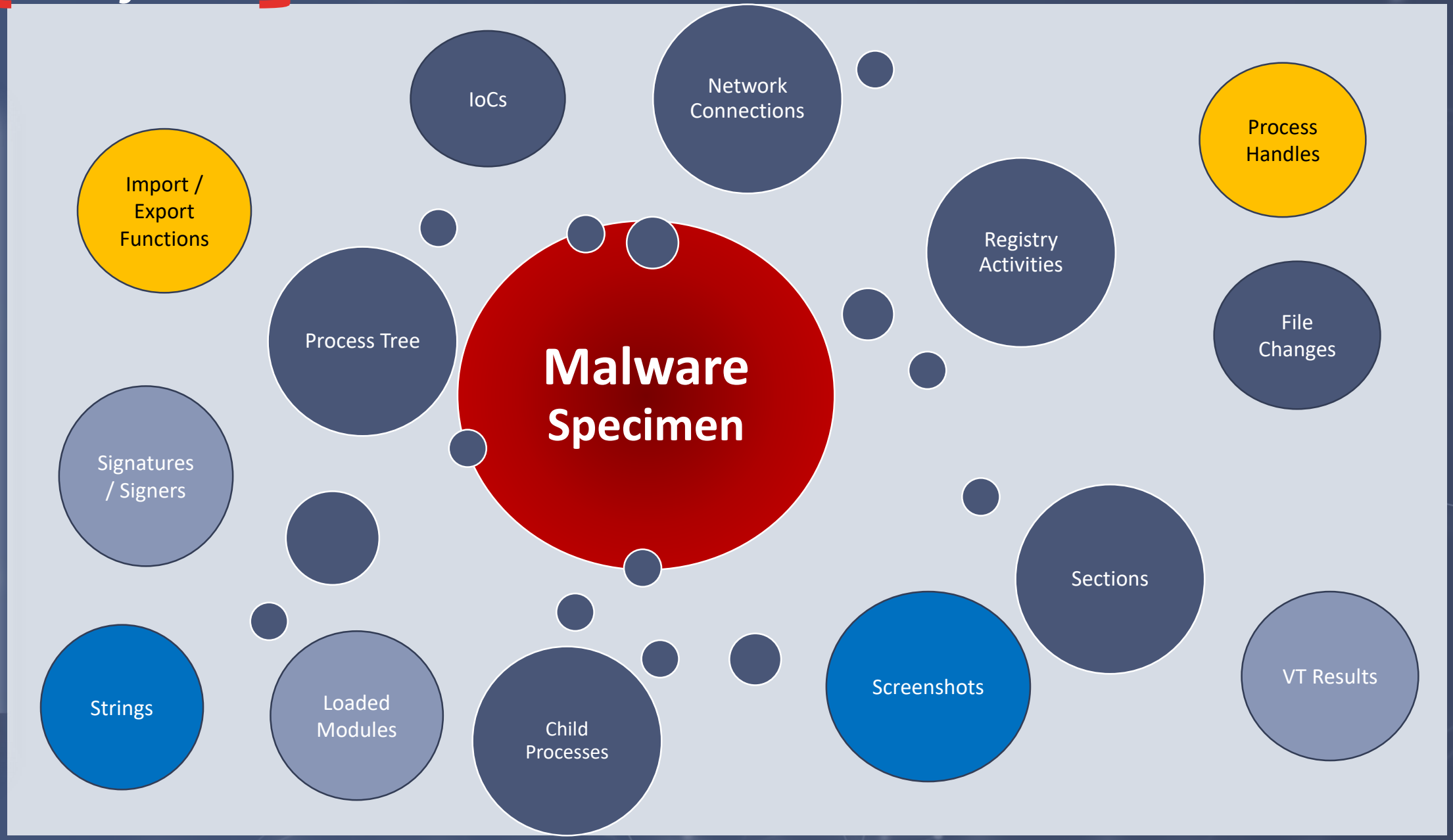
#	HOSTNAME	FILE NAME	PROCESS NAME	USER NAME	CREATED AT
1	WIN-FNDR871	[redacted]	explorer.exe	WIN-FNDR871\Win764Test	Feb 8, 2019 9:05:02 AM
2	WIN-FNDR871		explorer.exe	WIN-FNDR871\Win764Test	Feb 8, 2019 9:05:01 AM
3	WIN-FNDR871		explorer.exe	WIN-FNDR871\Win764Test	Feb 8, 2019 9:05:01 AM
4	WIN-FNDR871		explorer.exe	WIN-FNDR871\Win764Test	Feb 8, 2019 9:04:59 AM
5	WIN-FNDR871	magic.docx	explorer.exe	WIN-FNDR871\Win764Test	Feb 8, 2019 9:04:56 AM
6	WIN-FNDR871	aaaaaaaaaaaaaaa.txt	explorer.exe	WIN-FNDR871\Win764Test	Feb 8, 2019 9:04:55 AM
7	WIN-FNDR871	test.txt	explorer.exe	WIN-FNDR871\Win764Test	Feb 8, 2019 9:04:55 AM
8	WIN-FNDR871	magic.docx	explorer.exe	WIN-FNDR871\Win764Test	Feb 8, 2019 9:04:46 AM
9	WIN-FNDR871	magic.docx	explorer.exe	WIN-FNDR871\Win764Test	Feb 8, 2019 9:04:40 AM
10	WIN-FNDR871	test.txt	explorer.exe	WIN-FNDR871\Win764Test	Feb 8, 2019 9:04:33 AM

HIGHEST OFFENDERS (USERS)

LIST OF LAST 10 OFFENDERS

#	NAME	DOMAIN
1	Win764Test	WIN-FNDR871
2	Win8-x64	WIN-97EVDR36H72
3	Windows10x64Test	DESKTOP-WINT

Malyzer™ Malware Analysis with a Click of a Mouse



ThreatRESPONDER™

THREATRESPONDER – USE CASES

Compromise / Breach Assessment

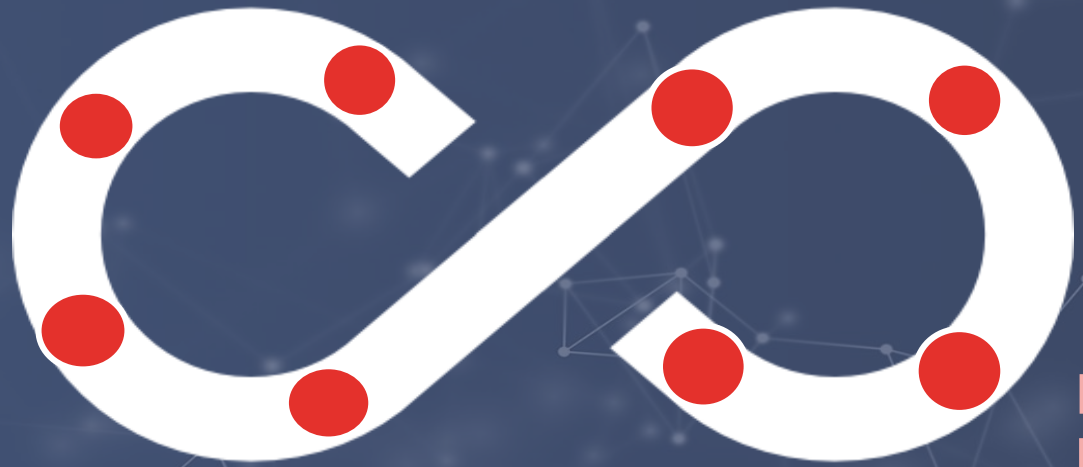
Know with certainty if your enterprise has been breached or compromised

Incident Response & Forensics Investigation

Conduct legally-defensible incident response and forensics investigation from anywhere without travelling

Ransomware Prevention

Prevent all types and mutations of ransomware families, with Machine Learning algorithms



Critical System Hardening & Application Control

Enforce security policy at the endpoint. Prevent USB, certain programs, data, or files from being accessed. Control certain user behaviors at the endpoint

Security Health of Your Assets

Know how healthy or vulnerable your endpoints are and apply appropriate remediation

Continuous Threat Detection, Prevention, and Hunting

Detect, respond to, and prevent advanced cyber attacks and data breaches in real-time. Demonstrate regulatory compliance GDPR, PCI, HIPAA, FISMA, FedRAMP

Threat Intelligence

Gain access to high-fidelity threat intelligence and identify threats targeting your environment or industry. Conduct advanced malware analysis with surgical precision

Insider Threat / Data Loss Prevention / User Behavior Analytics

Have an insider threat issue? Determine who is doing what, where, when, why, and how. Get the irrefutable evidence you need. Prevent data loss

BENEFITS

Save Money

- ✓ Prevent Costly Cyber Attacks and Data Breaches
- ✓ Eliminate Ineffective Technologies and Gain High ROI
- ✓ Reduce/Eliminate Cost of Investigations
- ✓ Significantly Reduce the Cost of Security Operations

Boost Efficiency and Productivity of Your Security Team and End-Users

Gain Compliance (FISMA, PCI, GDPR, SOX, HIPAA) and Avoid Fines

Gain Situational Awareness and Quickly Make Informed Decisions

Improve Shareholders' Value

Protect Your Intellectual Property and Maintain Competitive Advantage

Preserve Your Reputation and Image

KEY DIFFERENTIATORS

One Platform. One Single Pane of Glass. Many Capabilities (Detection, Prevention, Response, Intelligence, Hunting, Analytics, DLP)

Multi-Platform (Windows, Mac OS, and Linux)

Endpoint Security Health ("Vital+Sign")

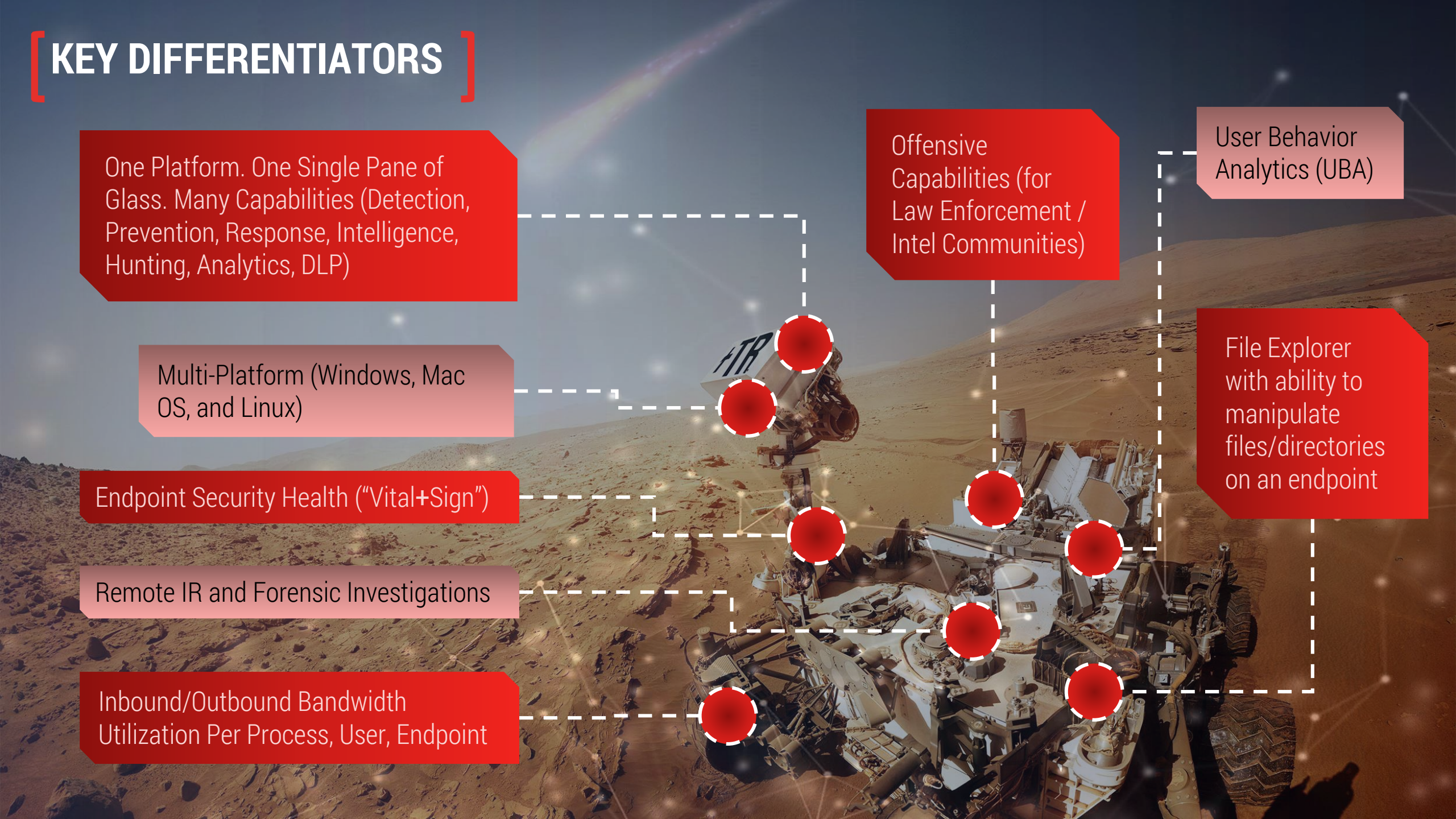
Remote IR and Forensic Investigations

Inbound/Outbound Bandwidth Utilization Per Process, User, Endpoint

Offensive Capabilities (for Law Enforcement / Intel Communities)

User Behavior Analytics (UBA)

File Explorer with ability to manipulate files/directories on an endpoint



Endpoint Security Competitive Analysis+

Endpoint Security Capabilities // Products	NetSecurity ThreatResponder®	CrowdStrike Falcon	Endgame Engame	Carbon Black Response
Corporate Experience	**Founded in 2004**	Founded in 2011	Founded in 2008	Founded in 2002
One Platform with Multiple Capabilities on a Single Pane of Glass – Detection, Prevention, Response, Intelligence, Analytics, and Hunting	**Yes – Single product and all capabilities**	Multiple products and partial capabilities	Single product and partial capabilities	Multiple products and partial capabilities
Malware, Exploit, and Fileless Detection & Prevention	**Yes**	Yes	Yes	Yes
Endpoint Security Health State (Hygiene) to Determine Endpoint's Vulnerability	**Yes**	Yes	No	No
Contain/Quarantine an Endpoint	**Yes**	Yes	No	Yes
Manually Terminate Processes and Network Connections	**Yes**	Yes	No	Yes
Live Interaction with an Endpoint ("Console")	**Yes**	Unknown	No	Yes
File/Registry Explorer with ability to Manipulate Files/Directories/Registries on an Endpoint	**Yes**	No	No	No
Inbound/Outbound Bandwidth Utilization Per Process, User, Endpoint	**Yes**	No	No	No
Control and Automatic Update of Agents	**Yes**	Unknown	Unknown	Unknown
Security Policy Enforcement (Applications/Devices/Networks Control)	**Yes**	Yes	No	Yes
Remote Incident Response (IR) and Forensic Investigations	**Yes**	Limited	Limited	Limited
Threat Intelligence	**Yes**	Yes	No	Yes
Onboard Deep Malware Analysis	**Yes (MALYZER™)**	No	No	No
Data Loss Prevention (DLP)	**Yes**	No	No	No
User Behavior Analytics (UBA) / User Activity Recorder	**Yes**	No	No	No
Contextual Details (Tell-the-Story)	**Yes**	Yes	Yes	Yes
Offensive Capabilities (for Law Enforcement / Intel Communities)	**Yes**	No	No	No
Natural Language Processing (Similar to Siri, Alexa, Google, etc.)	**Yes (CURIOSITY)**	No	Yes (ARTEMIS)	No
Agents' Footprint	**Low**	Low	Low	Unknown

+ Data based partly upon Publishers' marketing literatures, web sites, or product information

PROCUREMENT / PROOF OF VALUE (POV)

Corporate Information

Toll Free: 1-855-NETSECURITY

Telephone: +1-703-444-9009

Email: 911@netsecurity.com

Web: www.threatresponder.io / www.netsecurity.com

Government Data

- SBA Certified 8(a) SDB
- DUNS: 122657005 | CAGE Code: 3CJJ4
- GSA IT Schedule # GS-35F-0288Y
- GSA 8(a) STAR II # GS00Q17GWD2269
- Army INSCOM
- Army ITES-3S
- DoD Facility Clearance: Call