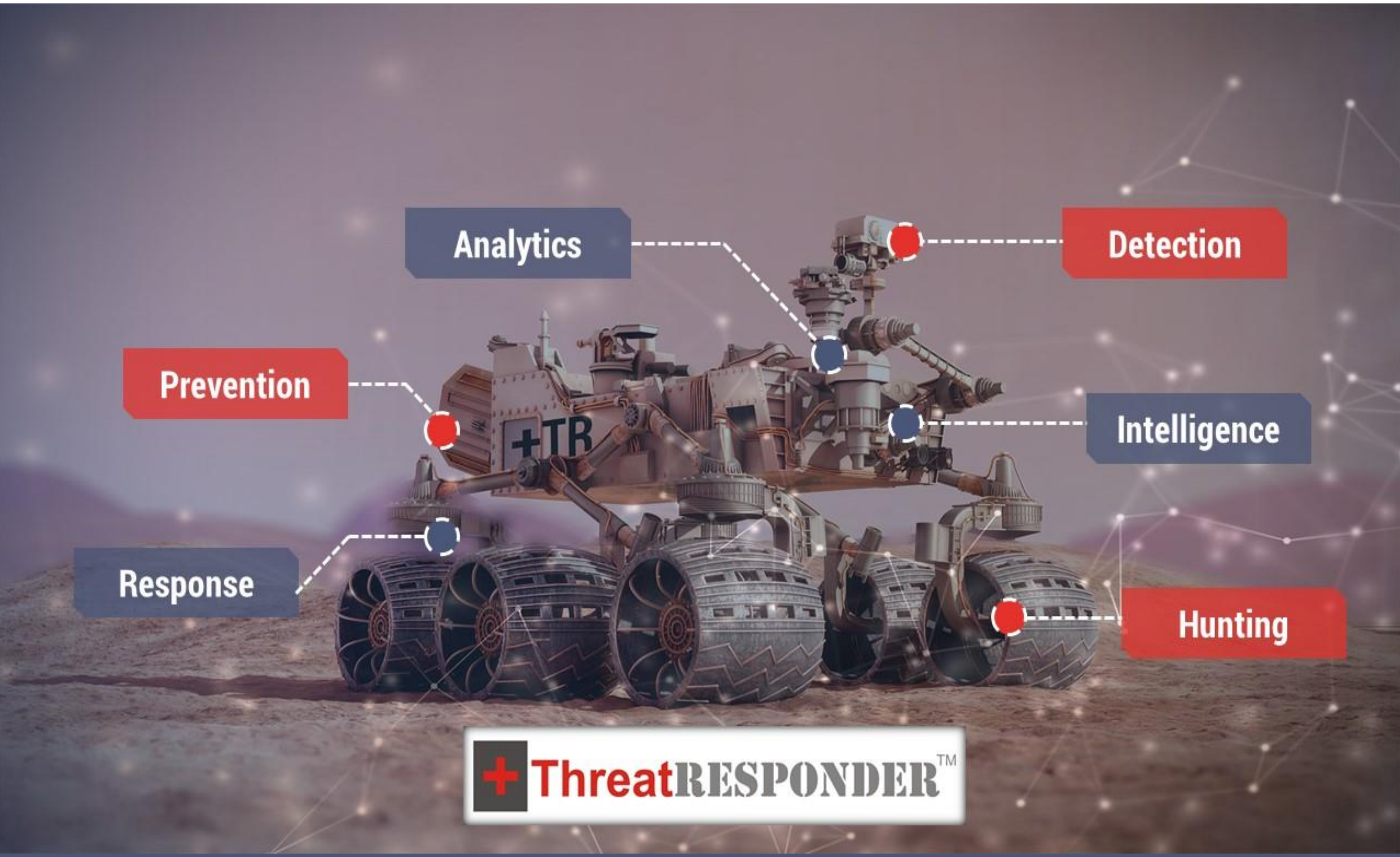
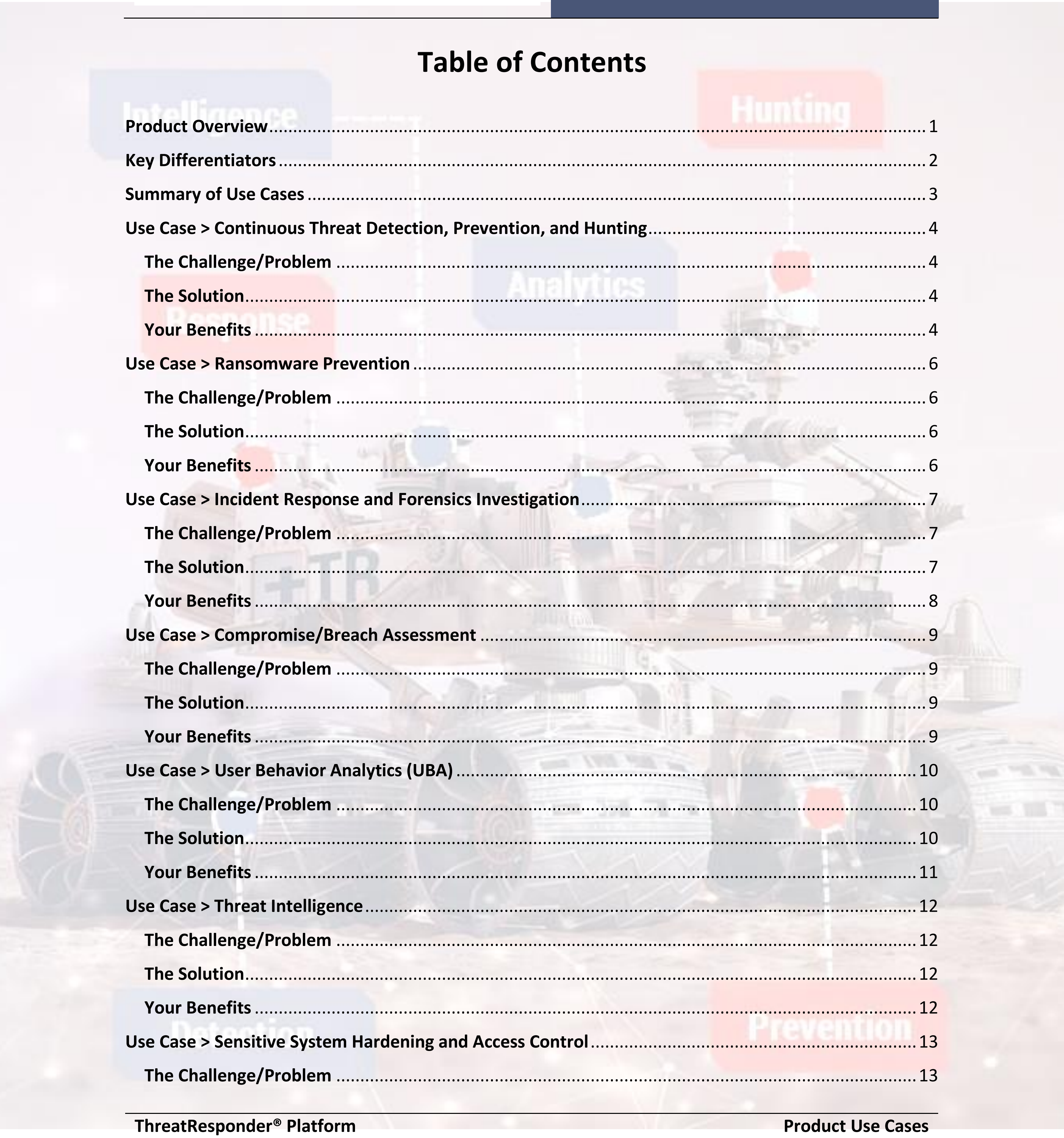


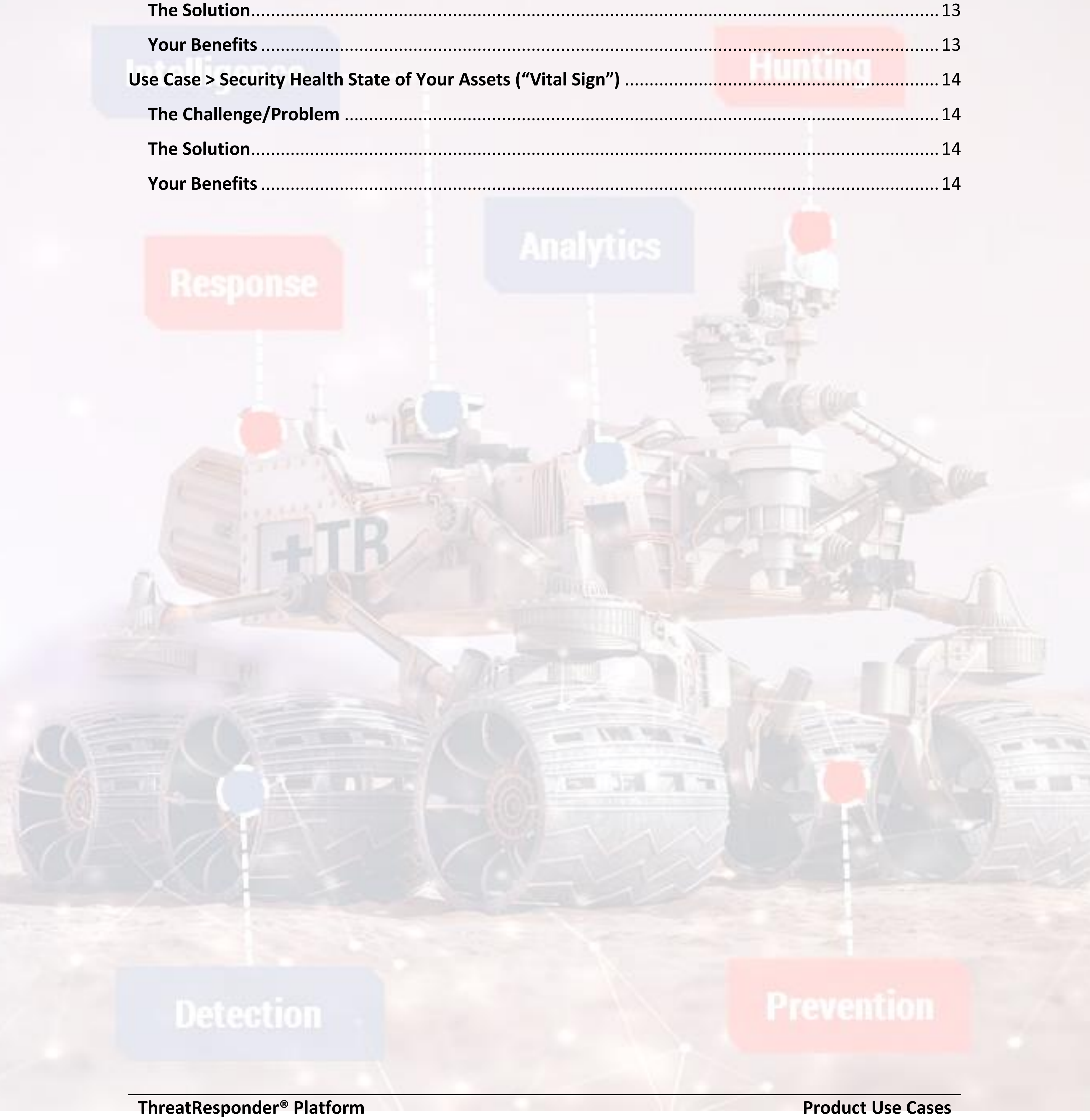
Product Use Cases

Founded in 2004, NetSecurity's vision is "to be the brand of choice in security, forensics, and training." The company's mission is to detect and prevent advanced attacks and data breaches in real-time. NetSecurity provides unparalleled innovation, world-class quality, customer-focused, and timely solutions.

© **NetSecurity® Corporation** | 22375 Broderick Drive, Suite 210, Dulles, VA 20166
Phone: (703) 444-9009 | Toll Free: 1-855-NETSECURITY | Web: netsecurity.com | Email: 911@netsecurity.com

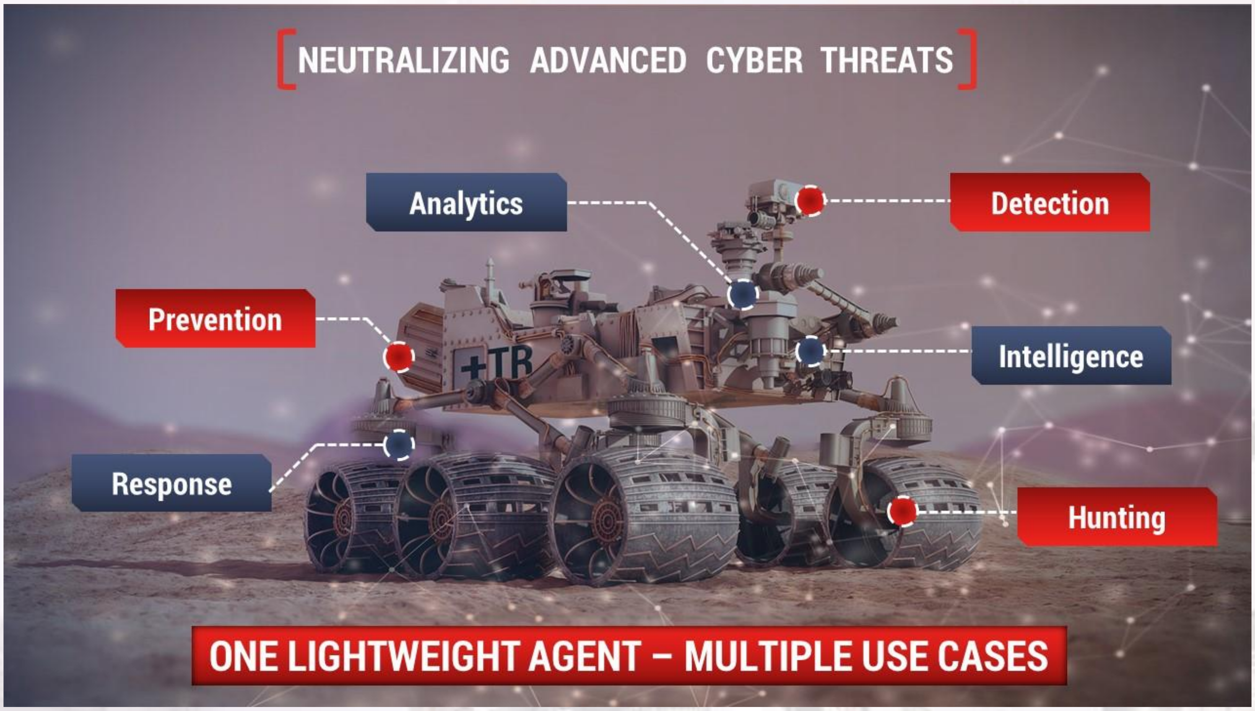
Table of Contents




Intelligence
Hunting
Analytics
Response
+TR
Detection
Prevention

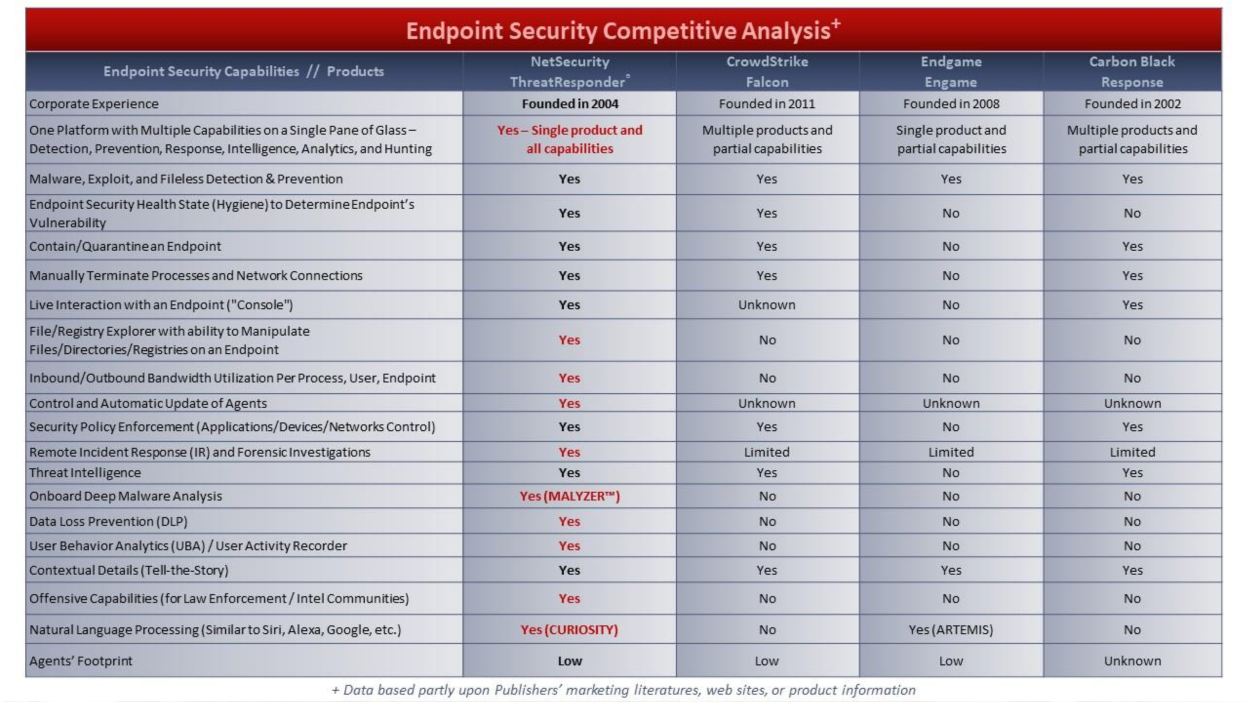
Product Overview

ThreatResponder® Platform is an All-in-One Threat **Intelligence**, **Analytics**, **Detection**, **Prevention**, **Response**, and **Hunting** platform that provides **361º Threat Visibility™** of your enterprise. The product detects and prevents advanced cyber attacks and data breaches perpetrated by nation-state adversaries and insider threat actors.


NEUTRALIZING ADVANCED CYBER THREATS
Analytics
Detection
Prevention
+TR
Intelligence
Response
Hunting
ONE LIGHTWEIGHT AGENT – MULTIPLE USE CASES

Key Differentiators

ThreatResponder® Platform differentiates itself from other endpoint security products in the following ways:



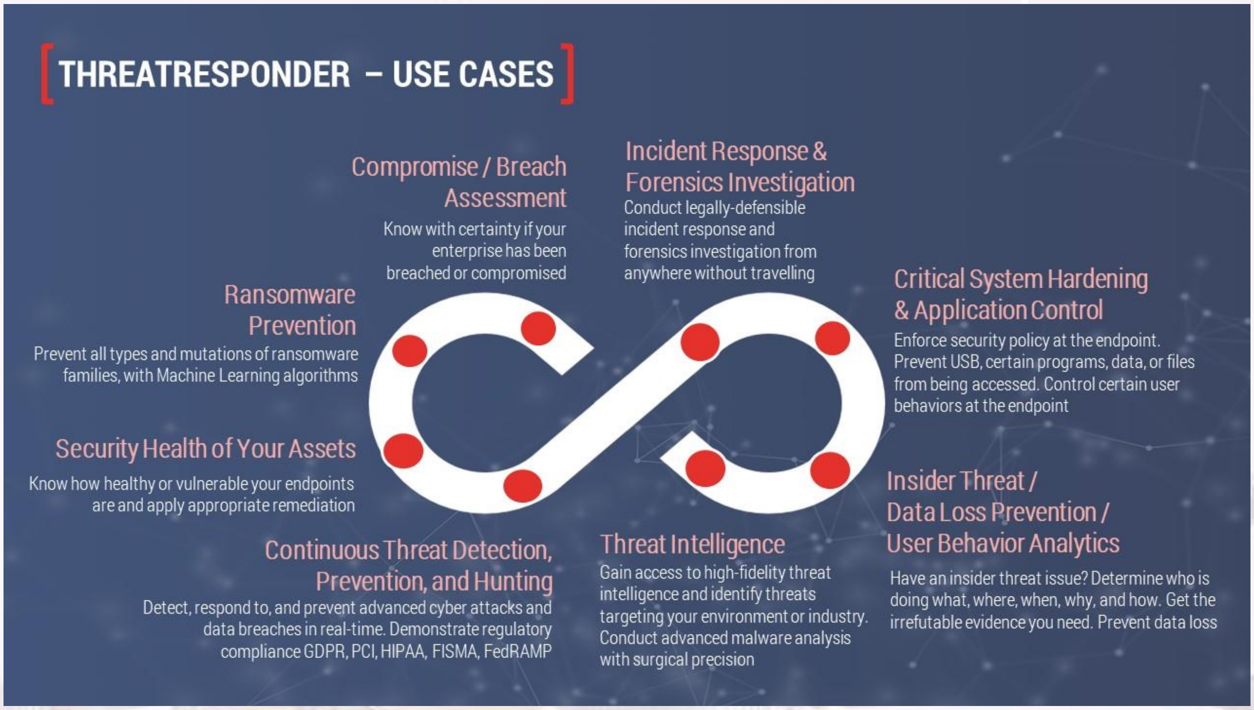
Endpoint Security Competitive Analysis[+]

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

Summary of Use Cases

This document describes how ThreatResponder® may be used to solve today's advanced cyber threat and data breach challenges and the benefits of using the product in your enterprise network. The use cases described in this document are summarized in the graphics shown below:



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

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

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

Use Case > Continuous Threat Detection, Prevention, and Hunting

ThreatResponder® Platform allows you to detect, respond to, and prevent advanced cyber attacks and data breaches in real-time.

The Challenge/Problem

Read the news and you are likely to hear about a data breach or computer hacking incident. Cyber attacks and data breaches continue to be on the rise, with attackers continually crafting their techniques to fly below the radar of defensive measures. Today's adversaries are very sophisticated, leveraging both malware and malware-less (fileless) techniques to infiltrate their targets. Insider threat actors (such as employees, consultants, partners) pose a significant risk to an organization. Most endpoint security solutions only address threats to Windows platform with no visibility into the threats hidden in Mac OS, Linux, Unix, enterprise logs, and network traffic. Traditional security technologies (such as anti-virus, firewalls, SIEM, IPS/IDS, and DLP) are ineffective in solving these cyber security problems. This is evident in the continued rise in data breaches in major organizations.

The Solution

ThreatResponder® neutralizes today's advanced adversarial threats through the following activities:

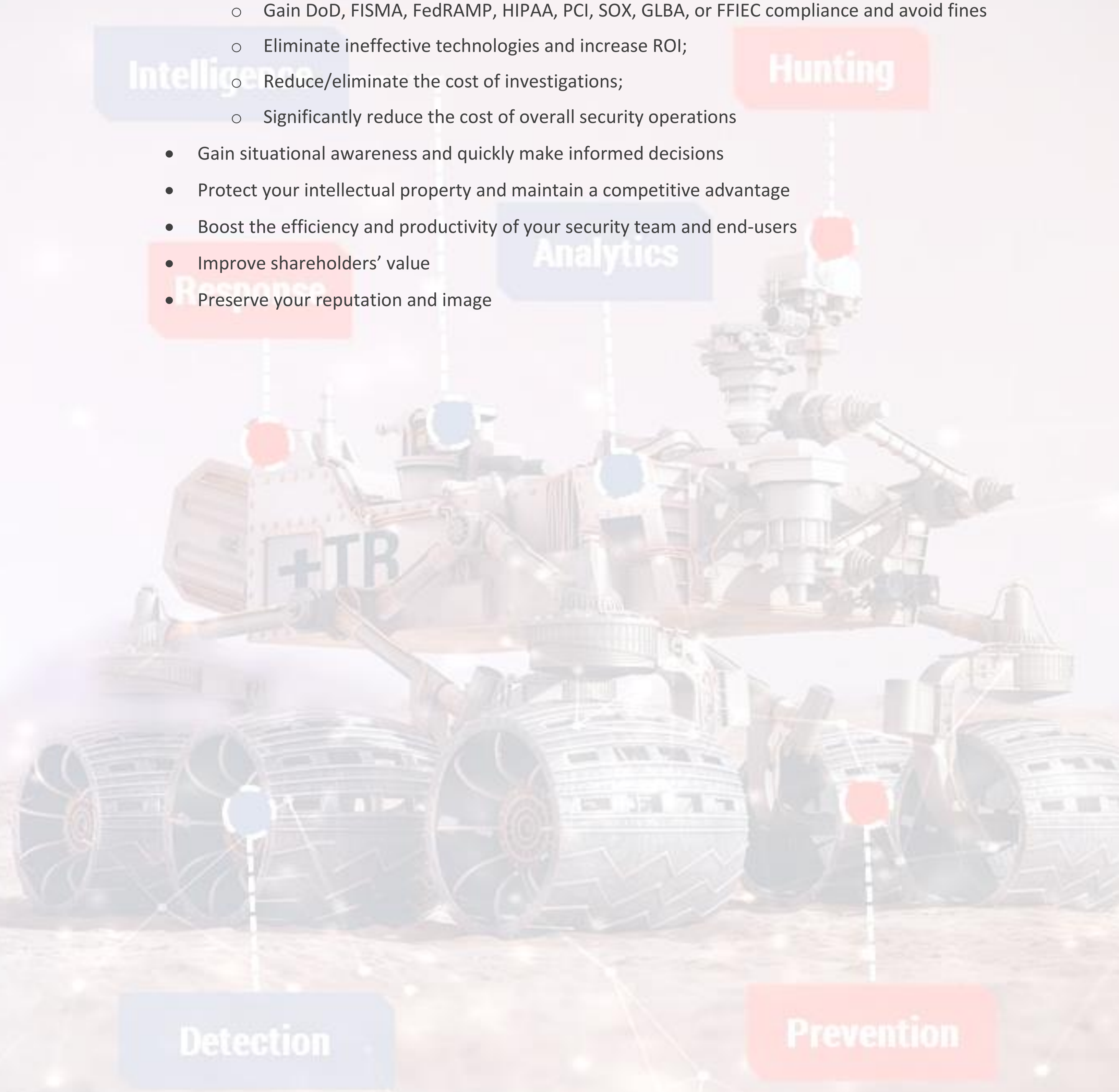
- **Detection:** Leverages threat intelligence, signatures, behavior, and machine-learning algorithms to detect threats related to processes, network connections, and user activities
- **Prevention:** Prevents attacks in real time and evicts the adversary
- **Analytics:** Ingests data from millions of endpoints, performs threat/forensics and user behavior analytics (UBA)
- **Response:** Interacts live with an endpoint, neutralizes the threat, and contains ("quarantines") the hosts to restrict the spread of the attack
- **Intelligence:** Consumes threat intel from various sources—including US-CERT, commercial, and open-source threat intelligence feeds. Enriches data collected to detect threats in your environment
- **Hunting:** Sweeps millions of endpoints for indication of threats or policy violation and pinpoints risky activities; mitigates the risk identified across the enterprise

Your Benefits

ThreatResponder® protects you against advanced cyber attacks and data breaches in real-time. The product benefits you in many ways, including:

- Save money:
    - Prevent costly cyber attacks and data breaches

  - Gain DoD, FISMA, FedRAMP, HIPAA, PCI, SOX, GLBA, or FFIEC compliance and avoid fines
  - Eliminate ineffective technologies and increase ROI;
  - Reduce/eliminate the cost of investigations;
  - Significantly reduce the cost of overall security operations
- Gain situational awareness and quickly make informed decisions
- Protect your intellectual property and maintain a competitive advantage
- Boost the efficiency and productivity of your security team and end-users
- Improve shareholders’ value
- Preserve your reputation and image



Use Case > Ransomware Prevention

According to Wikipedia, “Ransomware is a type of malicious software from cryptovirology that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid. While some simple ransomware may lock the system in a way which is not difficult for a knowledgeable person to reverse, more advanced malware uses a technique called cryptoviral extortion, in which it encrypts the victim's files, making them inaccessible, and demands a ransom payment to decrypt them.” Examples of ransomware include: WannaCry, Petya, CryptoLocker, Locky, Cryptowall, and Bad Rabbit.

The Challenge/Problem

Ransomware has dominated the news recently with major organizations falling victim to this category of crimeware. Companies spend a large amount of money to recover from ransomware attacks. Could you be the next victim? Without a mechanism in place to detect and prevent your systems from ransomware attacks, you could be vulnerable, resulting in business interruption, reputational damage, and access to your data by unknown adversaries. The Windows operating system is not the only target of ransomware; Mac and Linux are not immune.

The Solution

ThreatResponder® is a threat detection, response, prevention, hunting, and analytics platform. Through machine learning, behavioral indicators, and signature-based detection, our algorithms automatically detect and prevent potential ransomware attacks against your enterprise assets. ThreatResponder® will notify you of ransomware detection in your entire enterprise and systems/endpoints where ransomware may have been detected, regardless of the geolocation of that enterprise asset. We tell you which of your enterprise assets are protected by ThreatResponder® and which are not so that vulnerable assets can be protected as well.

Your Benefits

By deploying ThreatResponder® to protect your enterprise assets, you can rest assured that your organization does not become a victim of ransomware. This ensures that your reputation remains intact so you can improve shareholders’ equity, maintain competitive advantage, and focus on growing your business. Avoid ransomware attacks by deploying ThreatResponder® to all your enterprise assets – Linux, Mac OS, and Windows.

Use Case > Incident Response and Forensics Investigation

ThreatResponder® Platform allows you to conduct legally-defensible incident response and forensics investigation against thousands of endpoints from anywhere without traveling or waiting for evidence media to arrive.

The Challenge/Problem

Today's networks are continuously under cyber attacks and data breaches, which may be caused by insiders, trusted partners, customers, or nation-state actors. When a cyber incident does occur, there is the need to perform incident response or computer forensics investigation. There is a scarcity of trained and certified incident responders or investigators. Moreover, investigating hundreds or thousands of systems simultaneously becomes an uphill battle. The days when a forensics investigator or incident handler must travel to the location of the evidence source (computer system) or wait for days/weeks for the evidence to be shipped are long gone. There is now the need to conduct investigation regardless of the geolocation of the evidence while avoiding business interruption.

Do you have an unknown file, binary, or malware to analyze? Are you spending hours, days, or weeks to understand the capabilities of malicious software? Since advanced malware are known to evade detection or reversing, you now have an effective option.

The Solution

ThreatResponder® Platform allows an organization or third-party investigators to conduct an incident response or a computer forensics investigation on any endpoint, regardless of geolocation, as long as the target system has an Internet connection. Even if the storage medium (hard drive) of the target system has been removed, ThreatResponder® gains raw-disk access to a target endpoint with all its mounted storage devices (local, external, network). ThreatResponder® provides the crucial evidence and timeline of evidence you need related to an incident or investigation – the evidence may be of activities happening currently or that occurred within the past several months. Some of the evidence that is discovered or produced by ThreatResponder® includes:

- User activities – browsing history, Internet search terms, file deletion/creation/edits, etc.
- Presence of malware
- Process (malware) executions (including number, dates)
- User accounts on the system
- Scheduled tasks and persistence locations
- Log files
- User activity timeline

Do you need to perform malware analysis? Stop spending hours or weeks analyzing an unknown binary. All you need is to deploy ThreatResponder® on an analyst workstation, execute the malware, and review the activities of the malicious software in the dashboard. We help you “tell the story” – everything you want to know about the malware’s intent, capabilities, and risk will be presented to you, including:

- Processes information
- Child and parent processes
- Network activities (connections, DNS resolutions, etc.)
- Registry changes (creation, deletion, modifications, etc.)
- File system activities (creation, deletion, modifications, etc.)

Your Benefits

By leveraging ThreatResponder®, you:

- Eliminate or substantially reduce the cost of forensics investigation and incident response
- Perform incident response and most forensics investigations without the need to travel to the location of the subject or evidence source
- Perform incident response and investigation on hundreds or thousands of target systems and endpoints simultaneously
- Find the evidence you are looking for quickly
- Gain contextual information, allowing you to “tell the story” of the incident
- Analyze and run a malware, allowing you to understand its full capabilities and risk to your organization

Use Case > Compromise/Breach Assessment

A compromise/breach assessment helps determine whether your assets have been compromised by an insider threat actor or a nation-state adversary.

The Challenge/Problem

The vast majority of the organizations that have been compromised today perform some due diligence to ensure that their network infrastructures are protected. These entities perform penetration testing (to simulate an adversarial attack) or security audit to satisfy regulatory or compliance (such as DoD, FISMA, FedRAMP, HIPAA, PCI, SOX, GLBA, and FFIEC) requirements. What do the results of these exercises say? Perhaps your goal is to determine if your enterprise can be compromised by an adversary or gauge the susceptibility of your network to an attack at a given point in time (security “snapshot” or “pulse”). Security snapshots or pulses are not proactive nor do they provide a barometer for detecting active threat activities.

Does the fact that your network was not hacked during the penetration engagement mean that you are secure and data is not being exfiltrated from your enterprise? Regardless of the outcome of penetration testing, these exercises do not reveal if an adversary is currently on your network, exfiltrating data from your company, or hibernating for the right opportunity to strike. What do you know about the insider threat actor who is pilfering your sensitive data and sending it outside the organization?

The Solution

Augmenting your auditing or security testing with compromise/breach assessment helps you determine whether your assets have been or are likely to be compromised. ThreatResponder® helps you determine whether there are adversarial or insider threat activities in your enterprise within minutes. Regardless of the location of the endpoint or the operating system – Linux, Mac OS, or Windows – platform. We sweep your assets to determine behavior or indicators of data breach or compromise. ThreatResponder® detects these indicators, alerts you, and prevents these attacks from causing grave harm and damaging your reputation.

Your Benefits

Whether you deploy ThreatResponder® for a few days, weeks, months, or years, you can be assured that persistent connections or attacks are detected, prevented, and reported in real-time. ThreatResponder® ensures that your reputation remains intact and you continue to maintain a competitive edge.

Use Case > User Behavior Analytics (UBA)

Do you know for sure if you have an insider threat problem? How do you know who is doing what, where, when, why, and how to your high-value assets? How can you be sure that you have the irrefutable evidence you need to neutralize the threat or launch a civil or criminal investigation?

The Challenge/Problem

Today's technology landscape has erased traditional perimeter security defenses with data stored in the cloud, under the control of service providers (or another third-party), or on-premises. Companies rely on vetted users and trusted partners to support their business operations. How do you know what these personnel, staff, or consultants are doing on your network or with your crucial assets? Do you know whether the employee who has worked for your company for years is stealing customers' list, trade secret, or other intellectual capital with them to the competitors or to start their own business?

Below are some of the challenges faced by modern enterprises:

- Low staff productivity – due to heavy Internet or personal (non-work-related) activities
- Unnecessary or unauthorized access to database or data of high-value assets
- Employees sending exfiltrating data to their personal email accounts, external storage devices (USB, DVD, flash drives, etc.), or personal computer
- Device access (USB, microphone, webcam, etc.)
- Abnormal use of application, network, or computer resources
- Using corporate computing resources for personal gain
- Web usage habits (surfing, searching, streaming audio/videos, and other non-work activities)

When there is a need to monitor an employee, organizations are left looking for "employee monitoring" software to purchase. The problem with this is, the subject is likely to know that they are being monitored and may modify behavior while under scrutiny. Further, the subject may attempt to disarm the monitoring apparatus. Worse, the subject may notify their colleagues or co-workers who may also be under investigation. Furthermore, some anti-virus software may flag these "employee monitoring" software as malicious, causing your monitoring operation to fail. Rest assured.

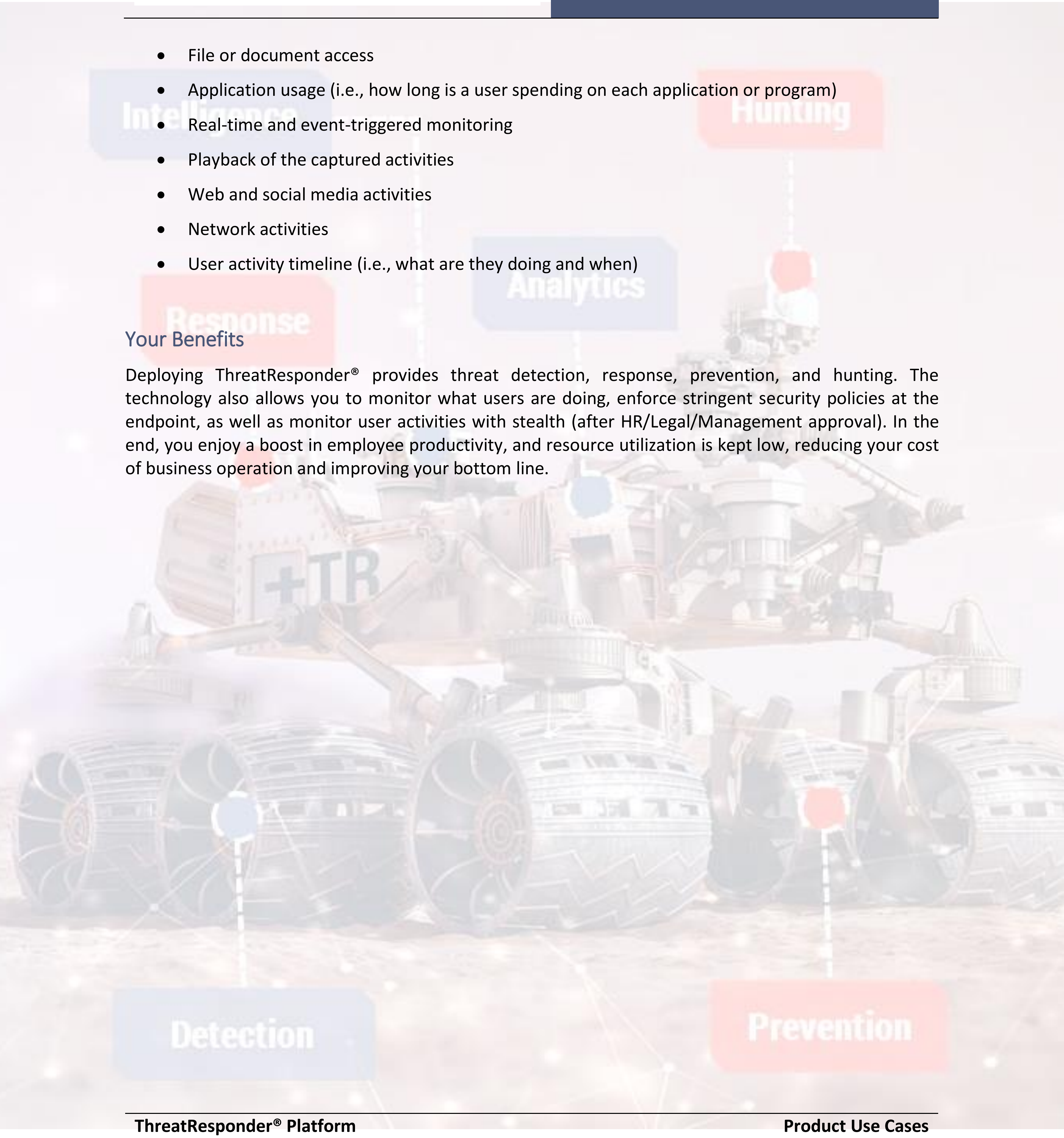
The Solution

With ThreatResponder® agent ("rover") deployed at every endpoint, you can capture all the evidence needed for internal, civil, or criminal investigation. The rover is deployed deep into the operating system kernel with no way for a user to detect its presence or operation. When triggered and upon HR/Legal/Management approval, the user behavior analytics (UBA) engine captures the raw evidence including video, screenshots, keystrokes, web activities, and listings of files that were accessed, modified, or created by a user. ThreatResponder® UBA provides insight into:

- File or document access
- Application usage (i.e., how long is a user spending on each application or program)
- Real-time and event-triggered monitoring
- Playback of the captured activities
- Web and social media activities
- Network activities
- User activity timeline (i.e., what are they doing and when)

Your Benefits

Deploying ThreatResponder® provides threat detection, response, prevention, and hunting. The technology also allows you to monitor what users are doing, enforce stringent security policies at the endpoint, as well as monitor user activities with stealth (after HR/Legal/Management approval). In the end, you enjoy a boost in employee productivity, and resource utilization is kept low, reducing your cost of business operation and improving your bottom line.



Use Case > Threat Intelligence

ThreatResponder® provides you with access to high-fidelity threat intelligence that identifies cyber security threats targeting your business or industry, providing you situational awareness to help you make informed decisions.

The Challenge/Problem

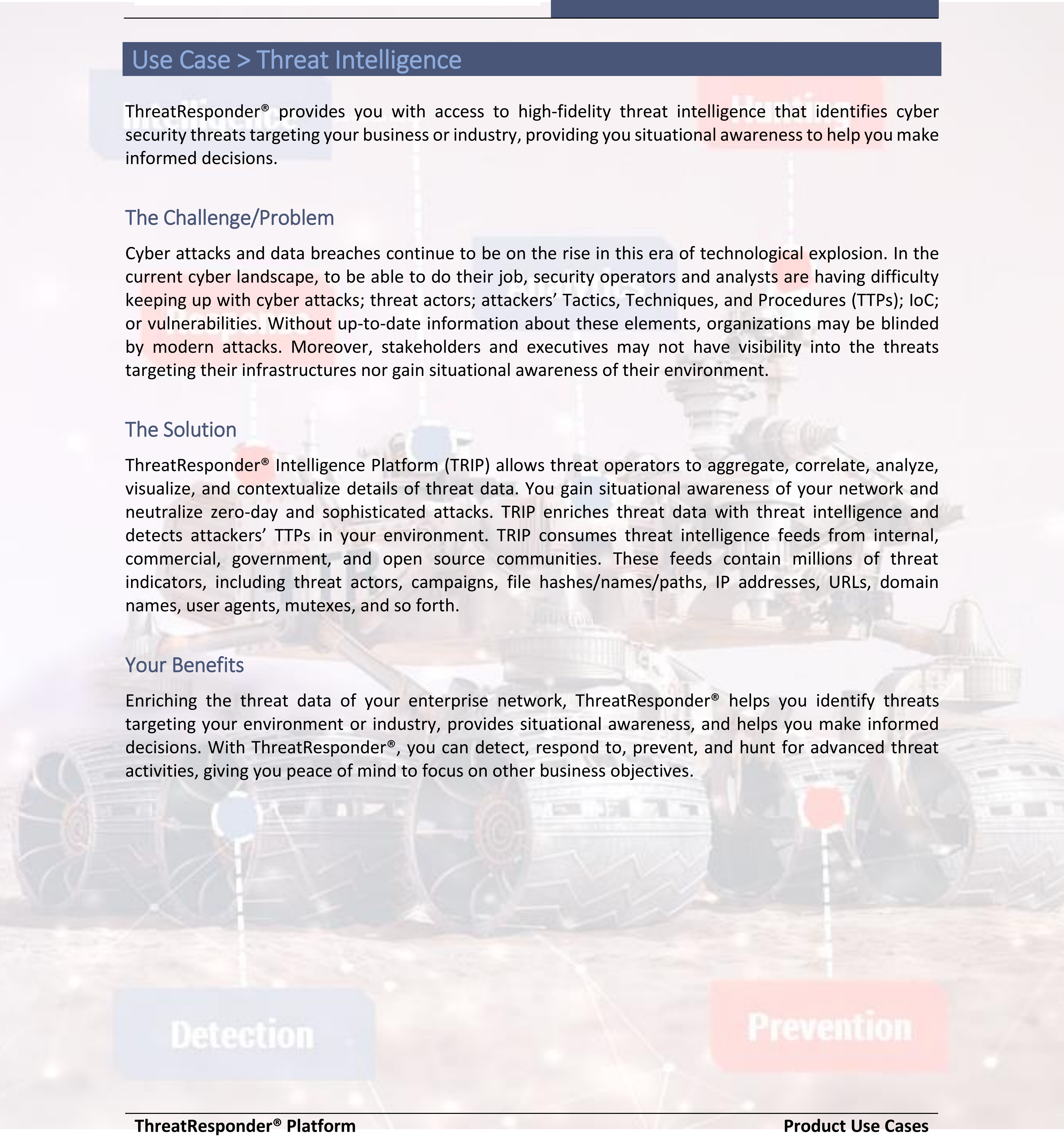
Cyber attacks and data breaches continue to be on the rise in this era of technological explosion. In the current cyber landscape, to be able to do their job, security operators and analysts are having difficulty keeping up with cyber attacks; threat actors; attackers' Tactics, Techniques, and Procedures (TTPs); IoC; or vulnerabilities. Without up-to-date information about these elements, organizations may be blinded by modern attacks. Moreover, stakeholders and executives may not have visibility into the threats targeting their infrastructures nor gain situational awareness of their environment.

The Solution

ThreatResponder® Intelligence Platform (TRIP) allows threat operators to aggregate, correlate, analyze, visualize, and contextualize details of threat data. You gain situational awareness of your network and neutralize zero-day and sophisticated attacks. TRIP enriches threat data with threat intelligence and detects attackers' TTPs in your environment. TRIP consumes threat intelligence feeds from internal, commercial, government, and open source communities. These feeds contain millions of threat indicators, including threat actors, campaigns, file hashes/names/paths, IP addresses, URLs, domain names, user agents, mutexes, and so forth.

Your Benefits

Enriching the threat data of your enterprise network, ThreatResponder® helps you identify threats targeting your environment or industry, provides situational awareness, and helps you make informed decisions. With ThreatResponder®, you can detect, respond to, prevent, and hunt for advanced threat activities, giving you peace of mind to focus on other business objectives.



Use Case > Sensitive System Hardening and Access Control

ThreatResponder® helps you to enforce granular security policy at the endpoint, including those of high-value assets. For example, with ThreatResponder®, you can prevent USB, certain programs, data, or files from being accessed/executed, or control certain user behaviors at the endpoint.

The Challenge/Problem

Some employees and end-users are less productive at their job because of the urge to get on the Internet – search, research, shop, or browse. Organizations often face the challenge of their staff using certain applications and programs excessively, such as streaming videos or audio services that may not be related to their work. Enterprises that cannot prevent certain programs or devices—such as USB, webcams, flash drives, and microphones—from being used risk having a decline in staff productivity. High-value assets such as database servers and other applications may be compromised using "normal" user credentials or programs. How would you know if a legitimate user (or service) account that has been compromised is being used to perform illegitimate database queries?

The Solution

ThreatResponder® helps you enforce stringent endpoint security by:

- Preventing certain programs from executing (programs that are banned, unsigned, signed by certain publishers, etc.)
- Preventing certain USB or storage devices from being used
- Preventing microphones and webcams from being used
- Preventing users from performing certain operations on their system
- Preventing abnormal access to critical systems (such as a database) from other systems

Your Benefits

Using ThreatResponder® allows you to improve productivity, secure/harden your endpoints, and enforce granular security at the endpoint that is not possible to enforce by network security devices. ThreatResponder® allows you to detect and prevent access to critical data, ensuring that you are not paying ransom to cybercriminals.

Use Case > Security Health State of Your Assets (“Vital Sign”)

ThreatResponder® helps you to identify the security health state (“vital sign”) of each endpoint, allowing you to apply appropriate remediation to ensure that the system is up to date, secure, and can defend against some attacks.

The Challenge/Problem

Some organizations perform patch management, vulnerability assessment, and penetration testing against their assets. These activities can help detect some vulnerabilities and identify patches that may be missing from an endpoint. The problem is that often, these exercises do not cover all enterprise assets. A vulnerability assessment or penetration test may not provide the true security health state of the system on a continuous real-time basis.

The Solution

ThreatResponder® reports the security health state (“vital sign”) of each endpoint by providing you with the patch level, logging state, user accounts and their permissions, script executions, network/remote system access, applications running on the endpoint, and so forth. Below are some of the indicators for detecting security health state, which the above exercises do not always cover:

- The patch level of the endpoint (i.e., is the system running a supported version of OS, and is it fully patched?)
- Whether local firewalls and logging facilities are enabled
- Unusual logon to a system with administrative privileges
- Excessive PowerShell, WMI, or VBA operations or executions
- Logons via interactive methods (RDP, remote access, or terminal services)
- If vulnerable or unsupported versions of an application or process are running

Your Benefits

ThreatResponder® helps identify the security health state of each asset in your network infrastructure, regardless of the geolocation of each asset. The technology ensures that risks associated with high-value assets are identified and mitigated. A good “vital sign” of each endpoint provides you the risk posture of your vital assets. Armed with this knowledge, you reduce the attack surfaces of your systems and minimize your risks.