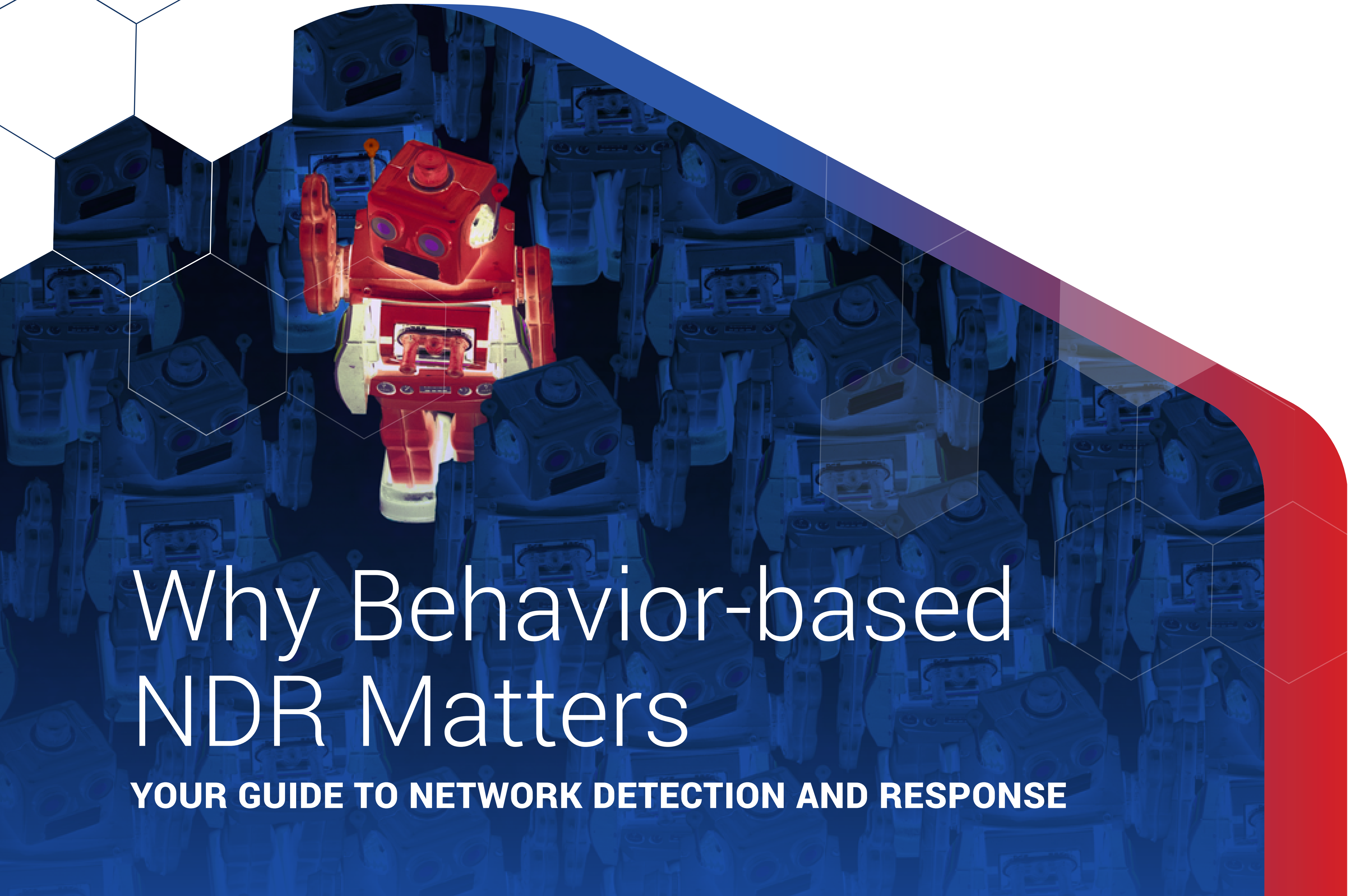
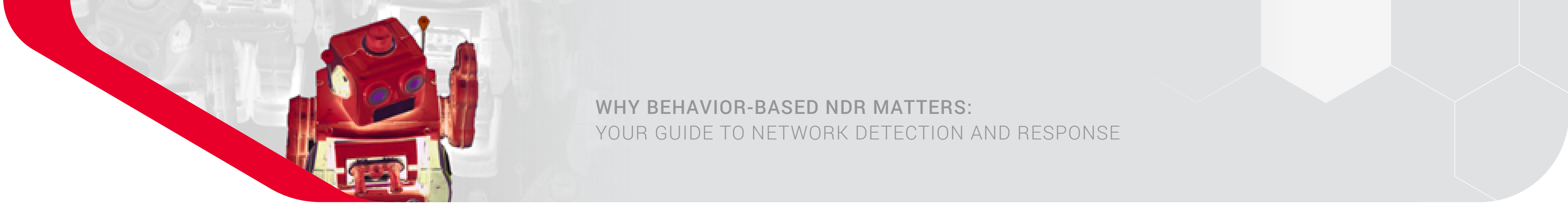
IronNet



Why Behavior-based NDR Matters

YOUR GUIDE TO NETWORK DETECTION AND RESPONSE



Seeing Beyond the Known

As hacking toolkits become more freely available across the internet, shrewd network infiltration techniques and destructive malware that were previously the realm of only the most advanced threat actors are now becoming more commonplace. Traditional approaches to network threat detection are not keeping up with the sophistication, frequency, and scale of cyber attacks.

We need a new, more advanced weapon.

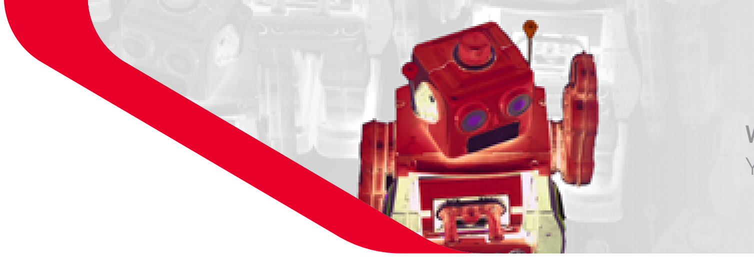
Signature-based threat detection—the mainstay method of detecting known threats—isn't going anywhere. While used largely as a reactive strategy that attackers can easily evade by adjusting code signatures or moving command and control (C2) communication infrastructure, it still plays an important triage role in an organization's cybersecurity portfolio.

Today's security executives are looking to shore up their defenses with a more proactive approach—one that can signal unknown threats steps ahead of the impact and facilitate a quick pivot to response. Network Detection and Response solutions based on behavioral analytics provide that level of sophistication missing in traditional threat detection. NDR can spot out-of-norm patterns of data in a network, detecting the unidentified and more sophisticated attacks that are now evading traditional preventative techniques.

But there are a few important things to know about this emerging category. In its Market Guide for NDR, Gartner highlights the fact that perimeter security and endpoint tools alone are not enough, adding that a behavioral-based network analysis capability is critical to an enterprise's cyber defenses.

In this ebook, you will learn:

- How NDR elevates your threat detection strategy overall
- How artificial intelligence (AI)-enhanced behavioral analytics identify the most challenging threats in your network
- Four questions to ask when evaluating NDR vendors



Contents

The Cyber Threat Continuum

Cyber threats can be organized into three main categories: Known Knowns, Known Unknowns, and Unknown Unkowns. The techniques required to detect these categories generally get more sophisticated as they progress from known to unknown.

Known Knowns

Whitelists, Correlation Rules

- Blocking malicious IP or URL addresses based on a threat intelligence feed
- Scanning for multiple account failures across X machines in Y minutes

Known Unknowns

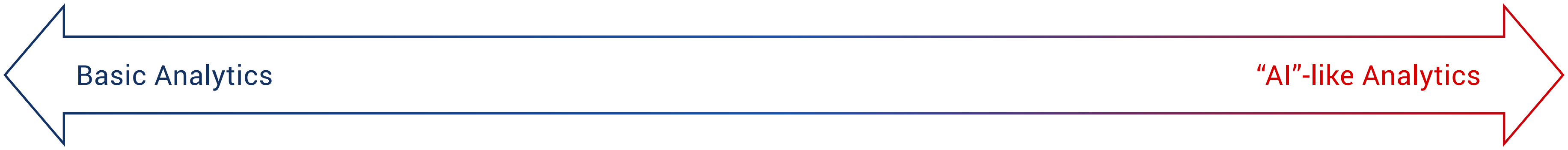
Supervised/ Unsupervised Machine Learning

- Supervised: Automating searches for vendor-identified “known bads”
- Unsupervised: Anomaly detection in a growing dataset

Unknown Unknowns

Deep Learning

- Models determine network behavior features to extract and examine suspicious traffic
- Humans label the data based on context and experience
- Humans train the models, which become more intelligent over time



Basic Analytics

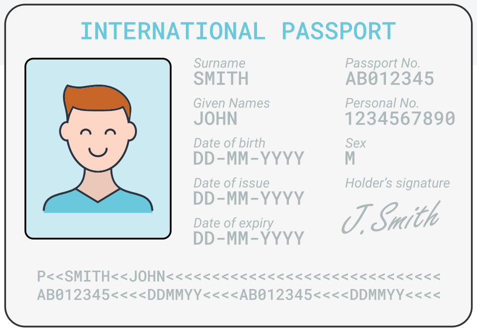
“AI”-like Analytics

The Cyber Threat Continuum: An Analogy

Let's look at how the concepts of Known Known, Known Unknown, and Unknown Unknown play out using the analogy of airport security:

Known Known

I am looking for John Smith with a passport from the Netherlands with an ID# of 123456.

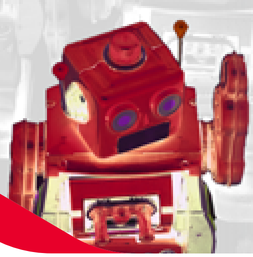


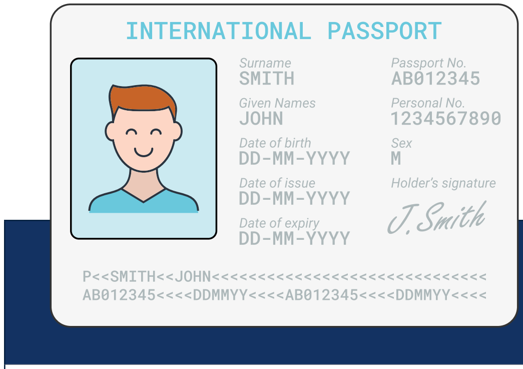
Known Unknown

I am looking for a 6'1" white male, around 40-45 years old, flying in from Europe.

Unknown Unknown

I would like to find cyber threats against the airport.





Detecting **Known Knowns**

What are Known Known threats?

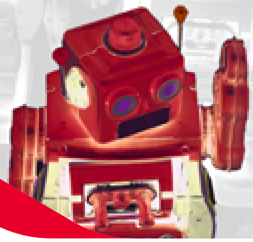
- Exact matches on code patterns or sequences associated with previously detected threats
- Matching known command and control infrastructure protocols previously used by adversaries

Characteristics and methods:

- Known bad URLs (i.e. badwebsite.com) or known bad IP address
- Hosting providers or websites that are known—by domain reputation—to be commonly compromised
- Hash values associated with known malware
- Traffic from potentially adversarial or unexpected geographies
- Easily recognizable traffic patterns such as a denial-of-service attack from a single IP address
- Account failures/modified logins

How can Known Known threats be detected?

- Identifying communications to specific IPs or URLs using the firewall or endpoint
- Identifying based on a third party reputation provider
- Looking for patterns based on simple rules



Detecting **Known Unknowns**

What are Known Unknown threats?

- Modified or recompiled known malware with minor changes to generate new hashes that bypass detection
- Use of leveraging open communication protocols for malicious purposes
- System access by way of stolen credentials to gain access to systems
- Known techniques (such as phishing) used to implant malware or steal credentials
- Data or IP loss through legitimate cloud services

Characteristics and methods:

- Malware families where code signatures are modified multiple times to bypass signature controls
- Botnet and C2 infrastructure where IP and URL launch points can be quickly moved
- DNS tunneling
- Lateral movement

How can Known Unknown threats be detected?

- Behavioral analytics backed by AI and machine learning can identify network behaviors that underlie the malware family.
- This is done by analyzing a stream of traffic and extracting anomalous behaviors. The characteristics of those behaviors are then contextualized and used to match the behaviors against known malicious activities.

! Most tools promising AI or machine learning as part of their behavioral analytics are actually based on simplistic, statistical outlier-based models that are a slight step up from the signature-based analysis of Known Knowns. Typical shortcomings of these systems include:

- The inability to analyze a group of systems, such as a sample list of URLs or IPs, and to alert when a new URL/IP is not commonly seen
- The inability to analyze data communications and to alert if the volume of bytes transferred is higher than a typical baseline

Detecting **Unknown Unknowns**

What are Unknown Unknown threats?

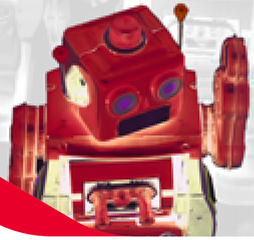
- Malware that leverages new zero-day vulnerabilities
- New Advanced Persistent Threats (APT) groups
- Attack methods that take advantage of new or legacy technologies that are poorly secured

Characteristics and methods:

- Industrial Control System (ICS) or Internet of Things (IoT) attacks on systems that are poorly defended
- Malware using techniques derived from APT groups or nation-state toolkits like WannaCry
- Insider threats that have installed keyloggers on systems or steal data from cloud repositories

How can Unknown Unknown threats be detected?

- Using predictive models to identify and classify all anomalies in a network
- Applying human intelligence and intuition at scale to network anomalies
- Working with elite threat hunters and researchers with cyber offense experience to train models to detect known methods of attack used by nation-states or APT groups
- Increasing the amount of data informing the NDR system through Collective Defense. Amassing encrypted network traffic to analyze from groups of industry, supply chain, or geography-based participants has two main advantages. First, the more data you have access to, the better trained your AI models will be. Second, more data means greater visibility into incoming threats. Similar behaviors across similar companies or across an industry may indicate reconnaissance by a threat actor planning a larger campaign. Detecting those behaviors at machine speed enables companies to put protection in place at an exponentially faster rate.



Four Questions to Ask when Evaluating an NDR Solution

Network detection based on behavioral analytics uses AI-based models to identify patterns of activity or traffic that were not previously identified as suspicious at extreme rates of speed. Think of it as automating high-end, human threat-hunting to a scale that has never been seen.

However not all behavioral analytics approaches are the same. Here are four questions to ask when evaluating behavior-based NDR solutions:

1 How could Network Detection and Response augment your current capabilities?

If you believe your organization is fully protected because your endpoints covered and/or you have a SIEM, think again. SIEMs have their own blind spots, and endpoints' detection capabilities can be evaded or disabled by a determined adversary. Both the SIEM and endpoint struggle with detecting adversaries that are not specifically malware based, such as lateral movement using stolen credentials. Full protection can only come with expanding your coverage and reducing risk by closing off those gaps. Network behavior analysis is critical to threat detection for a number of reasons. One, by its very nature, a network is the fundamental communication mechanism on which an attacker must operate and it's very difficult for attackers to hide their tracks (as compared to logs in a SIEM or endpoint agents on a device, which can be targeted and disabled or simply doctored to erase an attacker's tracks). Two, it is massive and pervasive: the sheer amount of network metadata, protocol logs, and network artifacts make it extremely difficult, if not nearly impossible, for an adversary to hide their activities across or disable an entire network. Behavioral models, ranging from simple statistical analysis to more advanced behavioral models used by expert Network Detection and Response solutions, help catch what signature-based tools miss.

2 Can the solution scale with your organization?

In a modern environment, a network could contain hundreds of gigabytes of data, multiple sites, and thousands of endpoints. Extremely large amounts of network traffic continually flow through the segments of this system. Your NDR solution should be able to analyze data at the scale of your organization — not just at individual segments — to avoid creating blind spots, a false sense of security, and increased operational and management costs that can negatively impact security operations.

Four Questions to Ask when Evaluating an NDR Solution

3

How does the NDR solution distinguish anomalous from malicious activity?

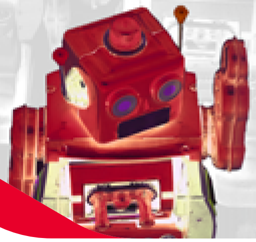
New applications, activities, or sites—like new devices that join the network, software updates, DNS communications, browser communications and streaming services like Spotify—can exhibit anomalous behaviors the first few times they are activated. A best-in-class NDR solution will be able to distinguish malicious behavior from normal anomalous behavior through both analytical techniques and human expertise that can be applied at scale. NDR vendors whose expert hunting teams use up-to-date databases of threat knowledge and insights, and apply advanced offensive techniques, offer a critical advantage for developing detection models to identify threats more quickly. Combining the judgment of these experts with the use of AI and machine learning to constantly improve security outcomes is key to increasing detection fidelity and reducing risk.

4

Does the solution offer a software-based operational model in which you can share and receive advanced notice of new threats with peers in your industry or region? How does it work?

Collective Defense threat intelligence sharing can dramatically increase an organization's speed to detection and mitigation. But most sharing today happens through threat intelligence feeds and informal channels, which don't provide context, urgency ratings, or actionable recommendations for mitigation. Learning about threats that have affected peers or others gives you the ability to protect before damage is done, similar to preventative maintenance or a vaccine.

NDR solutions that can share anomalies with other peers for higher-order analysis are crucial to helping identify new threats and classify unknown suspicious behavior. Collective Defense goes even further by sharing those insights and actionable information in machine speed, so all peers can detect and protect quickly.



Assessing your Security Risk: Where Behavior-based NDR can Help

A truly secure network requires investments in all areas of the organization, from an engaged and accountable leadership team to a highly talented workforce and an effective and efficient security infrastructure.

Leadership and Talent

- Ensure board support and involvement
- Define cross-functional accountability and decision-making
- Manage security budget
- Organize program structure, design architecture
- Plan, recruit, and develop workforce

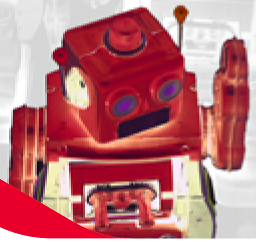
Security Infrastructure and Operations

- Define security strategy
- Develop performance measures
- Develop risk controls
- Manage third party risk
- Secure the network, perimeter, endpoints, and data
- Solidify discovery, response, and remediation of vulnerabilities and security events
- Implement rapid threat detection and tracking

Network detection backed by behavioral analytics optimizes and strengthens the heart of the threat detection and mitigation operation.

Risk and Compliance

- Manage privacy and compliance policies
- Support security audits
- Define and conduct risk assessments
- Manage security policies



Future-proof your Cybersecurity Strategy With Behavior-based NDR

Though signature-based detection does lower the level of threat noise, it is no match for more sophisticated threats. By applying behavioral analytics, IronDefense NDR provides the means for cross-entity correlation and association — which means your organization can find more threats and defend against them earlier.

IronNet's cyber analytic models are informed by experts in cyber operations who have a deep understanding of the tradecraft of APT, cyber adversaries, cyber criminals, and other bad actors.

Key Benefits of IronDefense

Find the truth within the traffic. Existing security tools can be fooled and log management stores can be altered. That's why IronDefense examines the network traffic itself, making it much harder for an attacker to evade detection.

Find unknown threats. The IronDefense platform uses advanced analytics, machine learning, and AI techniques to identify anomalous network traffic behavior patterns associated with advanced threats.

Results, not just anomaly detection. In most enterprise networks, anomalies are a standard occurrence, and detection alone is not enough. IronDefense orchestrates the collection of contextual data from multiple sources, then automates and applies the collective wisdom of the nation's top cyber offensive and defensive operators to distinguish the malicious from the anomalous and ranks them by risk to the enterprise.

Seamlessly pivot from detection to response. IronDefense integrates easily with existing tools, such as SIEMs (security information and event management) and SOARs (security orchestration, automation, and response), to enhance investigations and speed up response to detected threats using your existing endpoint, firewall, network access control, or other security tools.

Future-proof your Cybersecurity Strategy With Behavior-based NDR

By combining network behavioral analysis, forensics, and innovative intrusion detection capabilities, IronDefense delivers full network visibility and defense:

Advanced Behavioral Analysis

Leverages predictive models and behavioral analytics developed by data scientists from national government agencies to identify threats at an unmatched speed and scale.

Integrated Cyber Hunt

Enables seamless pivot from detection to investigation by providing packet-level visibility and integrated data enrichments to help investigate threats at the "speed of thought."

Expert System

Orchestrates the acquisition of contextual data and application of tradecraft cyber expertise to determine the risk of identified anomalies to the organization.

Collective Defense

Seamless integration with IronDome to deliver industry-level threat insights and visibility between public and private sector participants, enabling faster detection and collective response to threats targeting the industry.

This approach can improve your organization's overall cybersecurity metrics, as reported in highly mature and elite security operations center (SOC) environments:

- **More threats detected:** Better detection through behavioral analysis. IronNet identifies 1-2 unique detections — missed by other security tools — per customer, per week.
- **Faster response time:** More than 45% decrease in triage time from alert to action
- **Improved productivity:** More than 40% improvement in productivity (from detection to analysis, alerting and action)

Know more. Defend faster.

IronNet's Network Detection and Response solutions,
at ironnet.com/NDR

IronNet