IronNet™

Accelerated threat response with **NDR**

A GUIDE TO

Network detection and response in the security software ecosystem

Are we living with a false sense of security?

In its 2021 Cybersecurity Impact Report, which comprises results and analysis of a third-party survey of enterprise security decision-makers, IronNet discovered that most of the global survey respondents (90%) indicated the security posture of their company had improved in the past two years. However, 86% of respondents experienced a cybersecurity incident so severe in the past year that it required a C-level or Board meeting. What's more, nearly half of all respondents (46%) said the number of cybersecurity incidents they have experienced has increased over the past year.

Clearly, enterprises just can't keep up.

What is the key to solving this issue? Throwing more money at the widespread cybersecurity problem will not unlock the answer. As the 2020 Forrester Analytics Business Technographics® Security Survey revealed in a recent XDR report "Despite an increased investment in IT security, 59% of global security decision-makers [responding to the survey] say that their firm's sensitive data was breached at least once in the past year.[1]

Whether unleashing malware, rolling out ransomware campaigns, or committing data theft, adversaries are winning the cyber game. So how can we fix a broken approach to cybersecurity and flip the script? The answer is network detection and response (NDR), powered by behavioral analytics.

In this guide, you will learn:

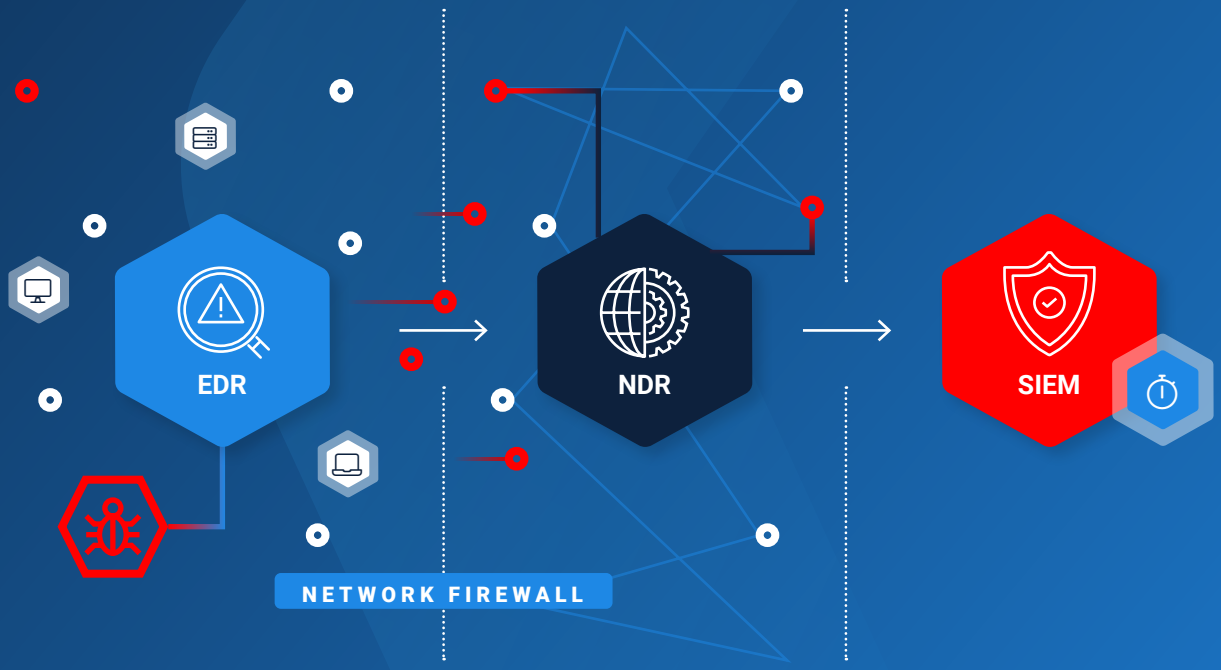
- ✓ How to detect cyber threats at the network gate
- ✓ Ways to unveil adversaries' hard-to-change tactics, techniques, and procedures (TTP)
- ✓ A practical way to rule out false positives with correlated detections
- ✓ How to achieve a 360° view of the threat landscape
- ✓ What NDR adds to your security ecosystem

59%

of global security decision-makers responding to a Forrester Security Survey say that their firm's sensitive data was breached at least once in the past year.

Catching intrusions at the network gate

Cyber attacks are slipping undetected past network firewalls and endpoint security controls (used for desktops, laptops, servers, and other endpoint devices) to exfiltrate data and/or exploit systems. Even though organizations have invested in better security controls, the increased sophistication of attacks is a key reason they continue to experience ongoing security issues. The reality is that a "sophisticated" attack can actually be quite simple: any attack that evades traditional or front-line detection systems by disguising nefarious activity using normal protocols to breach networks can be considered "sophisticated."



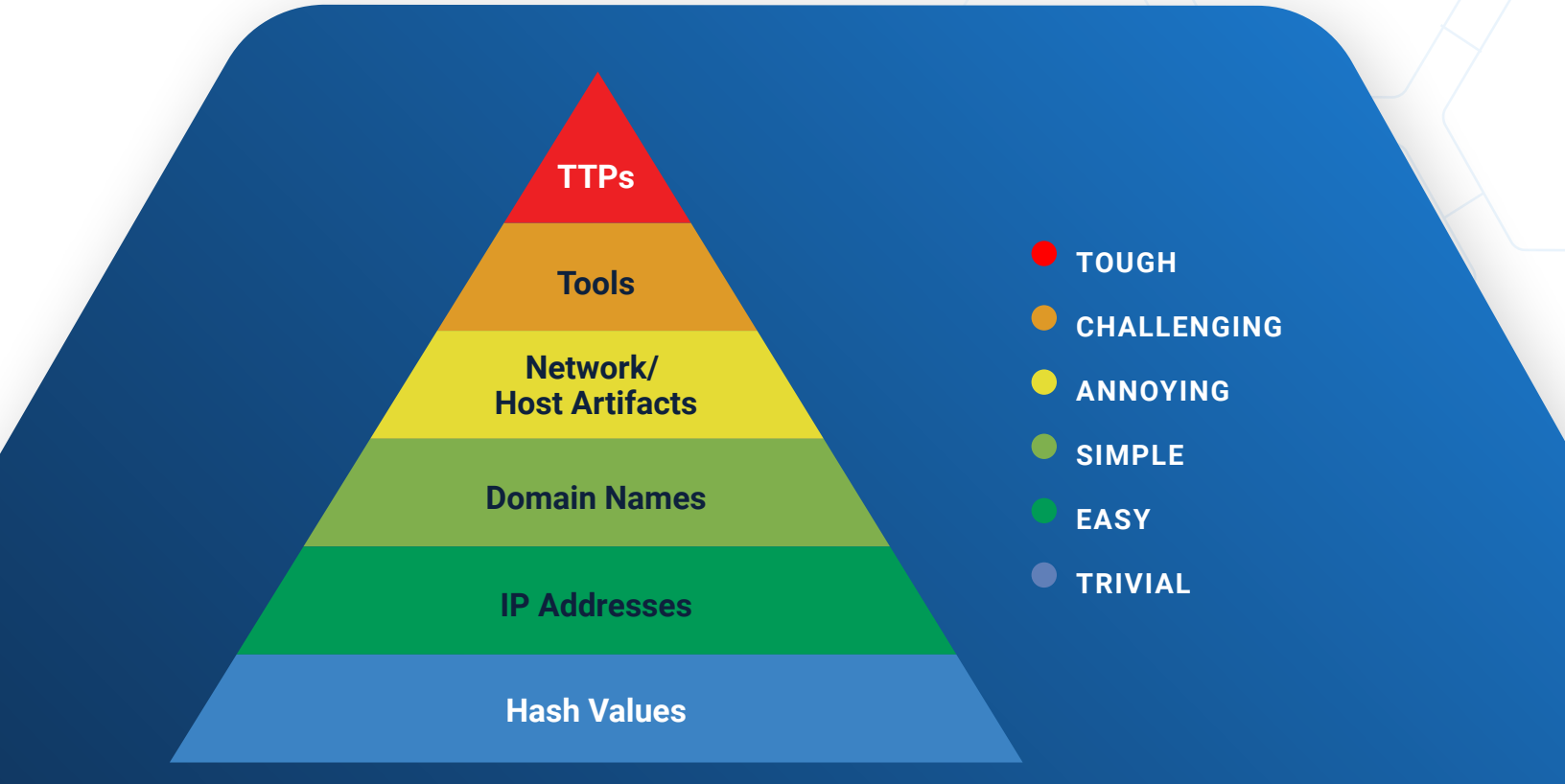
Threats to the network are slipping past firewalls and endpoint detection tools to intrude the network itself.

Detecting "left of boom"

The key to detecting and responding quickly to these attacks is to use behavioral analytics to spot anomalous network activity at the network gate. A security ecosystem that includes NDR solutions driven by behavioral analytics gives SOC analysts the full visibility of threats needed to see and contain attack campaigns early in the intrusion cycle — that is, "left of boom" — before data exfiltration, ransom demands, and system exploitation can occur. This early visibility of activity extends to the cloud, as behavioral analytics enable analysts to see the truth in the network traffic to and from the cloud.

Summiting the Pyramid of Pain

Early detection is crucial for enabling a faster response, but how can hidden threats be identified more quickly? It is broadly accepted in the analyst community that a cyber attacker can easily change hash values, IPs, and domains, the three lowest levels of David J. Bianco's "Pyramid of Pain" Threat Hunting Framework. It is also widely known that TTPs — the top level of this framework — are the most difficult for an attacker to change. Therefore, TTPs, which boil down to adversarial "behaviors," are the best type of indicators for defenders to focus on when attempting future detections based on previous knowledge.

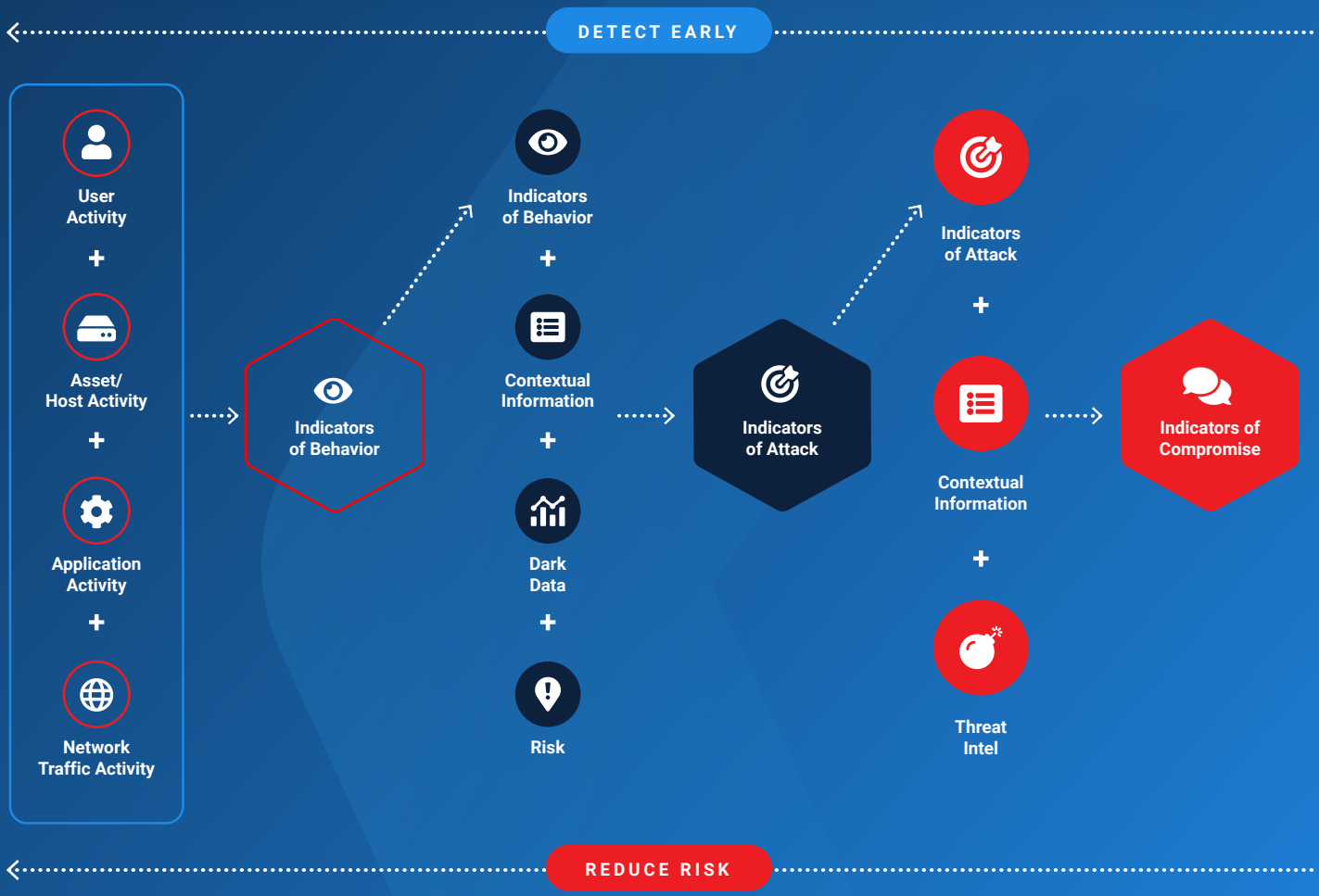


David J. Bianco's "Pyramid of Pain" Threat Hunting Framework

Knowing this, enterprises need to direct cybersecurity priorities and investments toward the apex of the pyramid. With an eye on TTPs, NDR tools yield more robust detections that tolerate changes in an adversary's Indicators of Compromise (IoC), forcing attackers to overhaul their existing tooling in order to remain undetected. Given how daunting this task is for adversaries, cyber defenders gain an upper hand by detecting campaigns before they advance along the kill chain and across companies or sectors. Even better, behavioral analytics can detect activity that does not yet have a signature," or "Indicators of Behavior." In fact, it is the only way to spot unknown threats, often fighting AI-driven attacks with AI.

Why Indicators of Behavior matter most

NDR solutions that use advanced behavioral analytics place emphasis on Indicators of Behavior (IoBs) instead of just known Indicators of Compromise. Simply put, detecting only IoCs with traditional, signature-based tools is too late in the intrusion cycle to minimize the risk. The earlier the detection, the lesser the risk of serious impact.



The earlier the threat detection, the lower the risk and business impact.

A practical way to rule out false positives

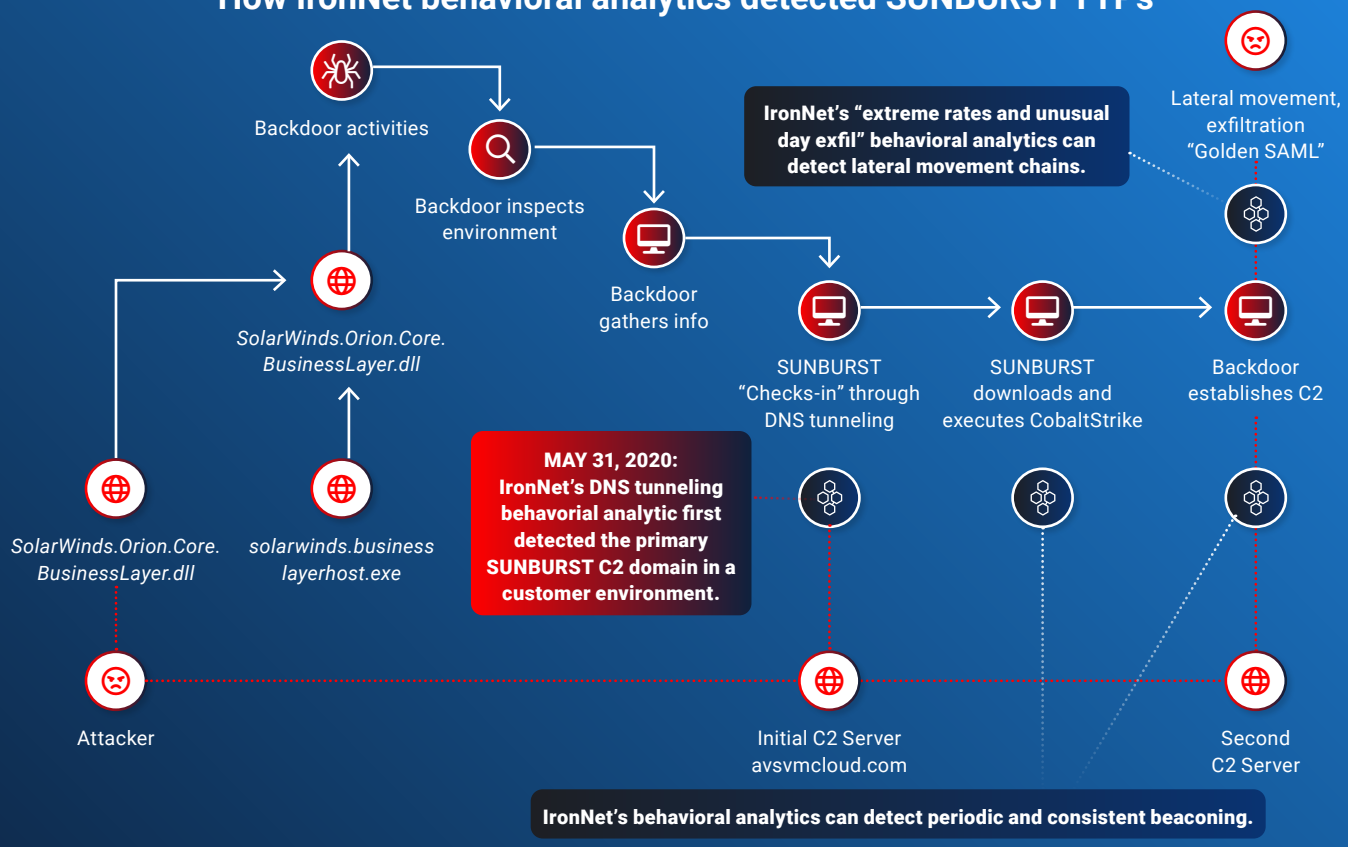
Focusing detection efforts on TTPs is the only way to discover novel or "zero day" threats early in the intrusion cycle, before they have known signatures associated with them. However, there is a catch: machine learning and algorithmic threat detections can alert on too many false positives when tuned to be sensitive to unknowns. One of the main reasons for this thorn in any SOC analyst's side is that behavioral anomalies and threat signals manifest in real-world networks in myriad ways, which often vary based on specific configurations of infrastructure, IT policy, and user conventions.

The value of human insights

How do you increase the signal-to-noise ratio in detections spotted by behavioral analytics? Fortunately, there is an activity that is both essential to threat hunting and directly in support of false-positive reduction: identifying corroborating evidence by enriching behavioral analytics with human insights. This scenario gets us closer and closer to eliminating false positives and helps reduce the margin of error. This was the main goal in designing the Expert System and integrated threat hunting platform of IronNet's IronDefense NDR solution.

USE CASE

How IronNet behavioral analytics detected SUNBURST TTPs

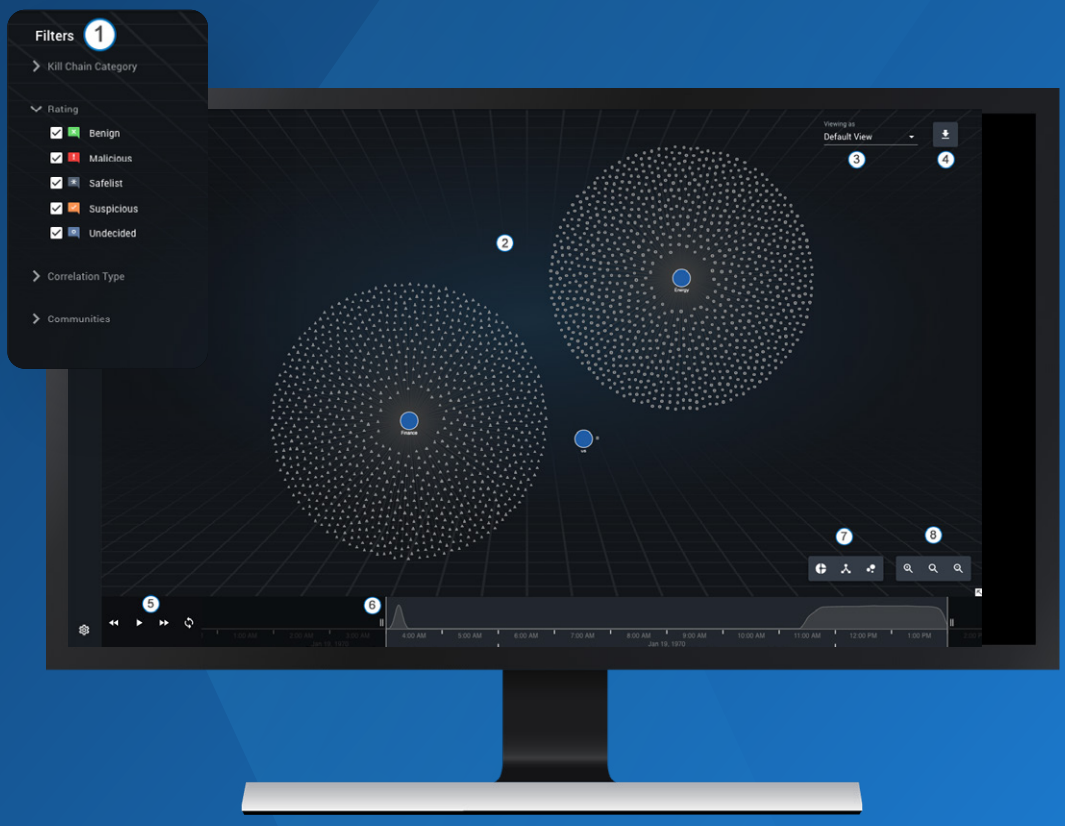


Flipping the script on attackers with **Collective Defense**

Alert correlation within a single enterprise as a principled method reduces false positives while maintaining high recall, and IronNet's IronDefense takes this approach. Truly novel attack vectors, however, require additional measures to create a fuller picture of the threat landscape at any given time. This is where Collective Defense comes in.

Collective Defense means that enterprises that may be related targets of the same attacker, such as electrical companies or banks, agree to share anonymized metadata about the threats they are seeing on an ongoing basis on their networks. This flips the script on the attacker, a brilliant move against the adversary given how hard it is to change TTPs.

Collective Defense raises the defensive capabilities of any one player, as there is strength in numbers when analysts across sectors can share threat intelligence in real time. Within IronNet's Collective Defense platform, IronDome, IoCs that may get lost in the noise at an individual company can take on greater prominence and, hence, relevance and priority when seen in multiple networks, or over a period of time. This approach creates a cyber radar view of threats across a Collective Defense community.

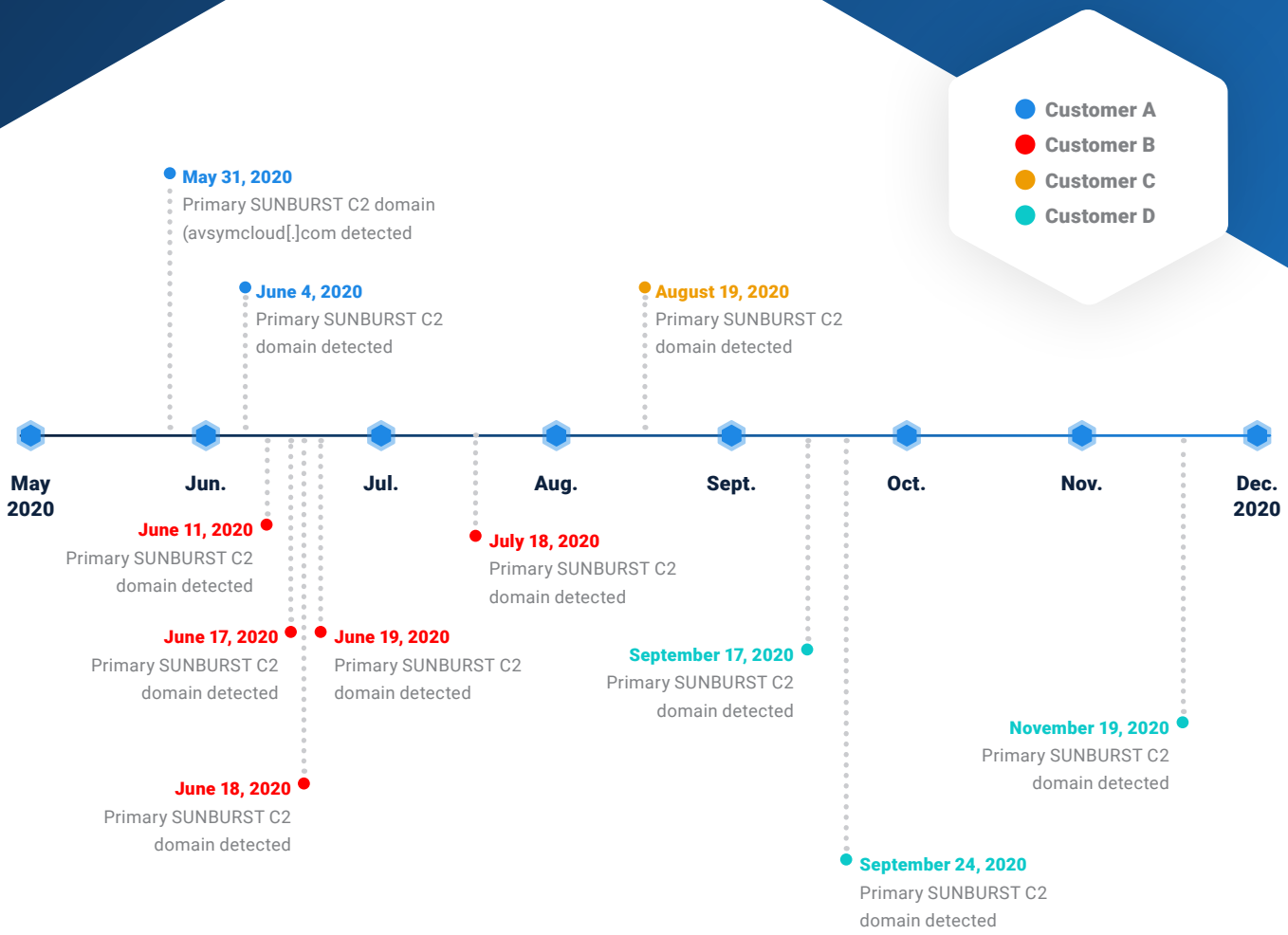


A cyber radar view of the threat landscape in the IronDome Collective Defense platform.

CASE STUDY:

Collective Defense in Action with SolarWinds/SUNBURST detection

In the SolarWinds attack, a single DNS tunnel to a Microsoft domain was not very suspicious on its own. However, when seen within a broader Collective Defense community made up of multiple companies, this activity becomes a cluster of signals on the radar that serve as a warning, because others are seeing the same anomaly around the same time. When companies have the opportunity to collaborate with this data, the strength (and speed) in numbers becomes apparent.



IronNet first spotted the SUNBURST anomaly in a customer environment in May 2020, more than six months before public disclosure. Imagine if all 18,000 affected companies could correlate the same detection in real time. The result? Faster detection and response.

Achieving a 360° view of the threat landscape

NDR capabilities are no longer an optional component of a holistic cybersecurity strategy. NDR tools, together with endpoint detection and response (EDR) and security information and event management (SIEM) capabilities, are critical for achieving greater visibility and a stronger cybersecurity defense.

Armed with all three technologies working together, you gain the comprehensive visibility you need to monitor your whole enterprise and lessen cyber risk, especially as digital transformation efforts accelerate. EDR detects only what is on the endpoint device. It is a key foundational piece for visibility and detection at the endpoint, but an enterprise is made up of countless endpoints, connected on a network. It is clear that NDR is a critical technology in the SOC Visibility Triad, ensuring that you are protecting your entire network, not just the perimeter.

Which gaps in your security ecosystem does NDR fill?

1. **Legacy signature-based products**
2. **Log and event management products**
3. **Endpoint detection and response tools**
4. **First-generation network-based behavioral analysis products**
5. **Infrastructure monitoring/ network performance monitoring and diagnostic-based products**
6. **Threat intelligence sharing products**
7. **Information Sharing and Analysis Centers (ISAC) and other threat sharing groups**

1. Legacy signature-based products

Signature-based products are designed to detect known attacks using a repository of previously identified IoCs, but they are not capable of detecting or responding to unknown threats. What's more, these products:

- Have resulted in many significant breaches due to the failure of legacy defenses to detect a previously unknown or modified version of a previously known attack
- Can miss a large swath of dangerous threats that evade detection, as evidenced by the major SolarWinds/SUNBURST supply chain attack and the Microsoft Exchange server attack

2. Log and event management products

While these systems provide useful correlation capabilities, SIEMs and similar log management products are designed for compliance, reporting, and security incident management purposes. They tend to:

- Struggle with the scale and processing capability required to deliver the behavioral-analysis capabilities across current and historical data to detect new or modified versions of known threats
- Are inherently designed for central aggregation points for workflow, ticketing, and case management rather than detection
- Are only as good as the underlying logs that they collected (which can be doctored or limited to what the cybersecurity tool actually "sees")

3. Endpoint detection and response tools

- EDR is key foundational piece for visibility and detection at the endpoint, but it detects only what is on the endpoint device. An enterprise is made up of countless endpoints, and EDR
- Does not cover Internet Things (IoT) devices, operational technology (OT), smart systems, and other connected devices or workloads operating in the cloud where endpoints are not available or not ideal
- Can be disabled or defeated

4. First-generation network-based behavioral analysis products

First-generation network-based behavioral analysis products provide a basic level of outlier detection using Bayesian analysis or other statistical methods to identify obvious patterns in small networks. As such, these products:

- Lack the scale, correlation, or analysis capabilities needed to detect threats hiding in plain sight within networks commonly seen at mid-sized or larger enterprises with thousands of devices, hundreds of applications, multiple physical sites, and multi-cloud architectures
- Are often marketed as artificial intelligence solutions despite not being based truly on behavioral analytics that are continually trained to spot novel threats

5. Infrastructure monitoring/network performance monitoring and diagnostic-based products

Traditional network infrastructure providers provide infrastructure monitoring products designed to identify network bottlenecks and other network reliability or performance issues. These products:

- Are essentially bolted-on cybersecurity capabilities that can provide security teams' networks with asset discovery and some network visibility
- Struggle with the algorithmic analysis needed to detect new and unknown threats with high fidelity or the forensic capabilities required by security operations teams to investigate, triage, and respond to an identified network anomaly

6. Threat intelligence sharing products

Threat intelligence products are designed to share massive amounts of non-specific signature-based IoCs that commonly focus on IP addresses and domains of known threats, and often only after a substantial period of time by the contributing organization. Threat intelligence platforms (TIPs):

- Are known to lack timeliness or specificity to an enterprise, severely limiting the effectiveness of the shared information from a cyber defense perspective
- Allow for threat actors to change tactics during the lag time in sharing threat information, because by the time this information is shared (usually weeks or months after an attack), a sophisticated attacker only needs to slightly modify their methods to bypass cyber defenses of their targeted enterprises, industries, or nations

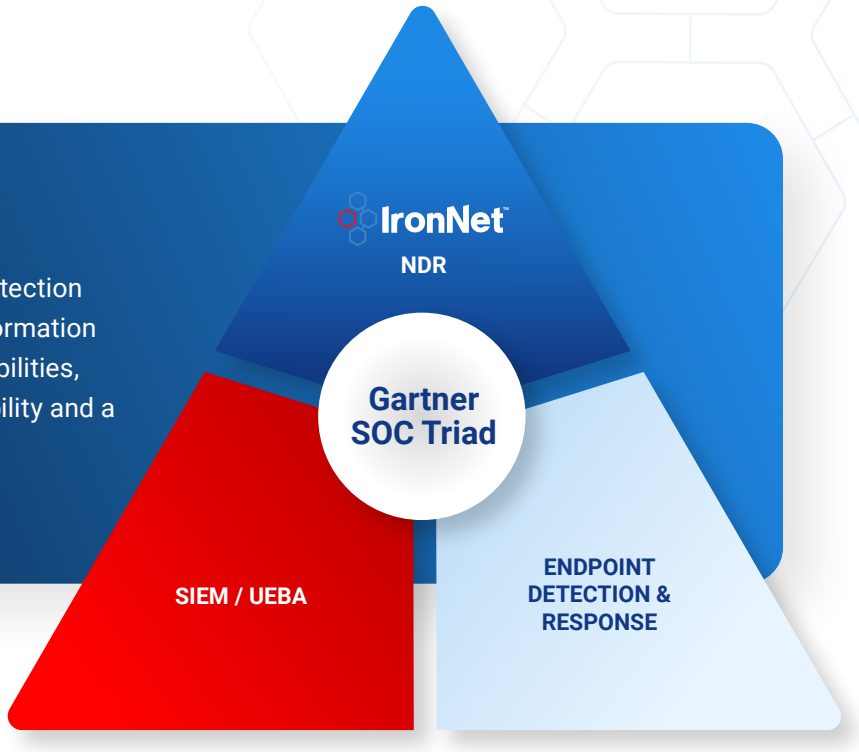
7. Information Sharing and Analysis Centers (ISAC) and other threat sharing groups

Threat sharing groups emerged more than 20 years ago as a way for security teams to work together to collect, analyze, and share threat information within their members communities.This is a substantial step in the right direction, but there are some limitations. Specifically, ISACS:

- Rely largely on signature-centric threat intelligence platforms that struggle with timeliness and specificity of their intelligence or ad hoc manual forms of communication, such as email, and only with a subset of security defenders with whom an analyst has a personal relationship
- Lack technological solutions that enable them to share contextual, relevant, and timely information in real time across the full community

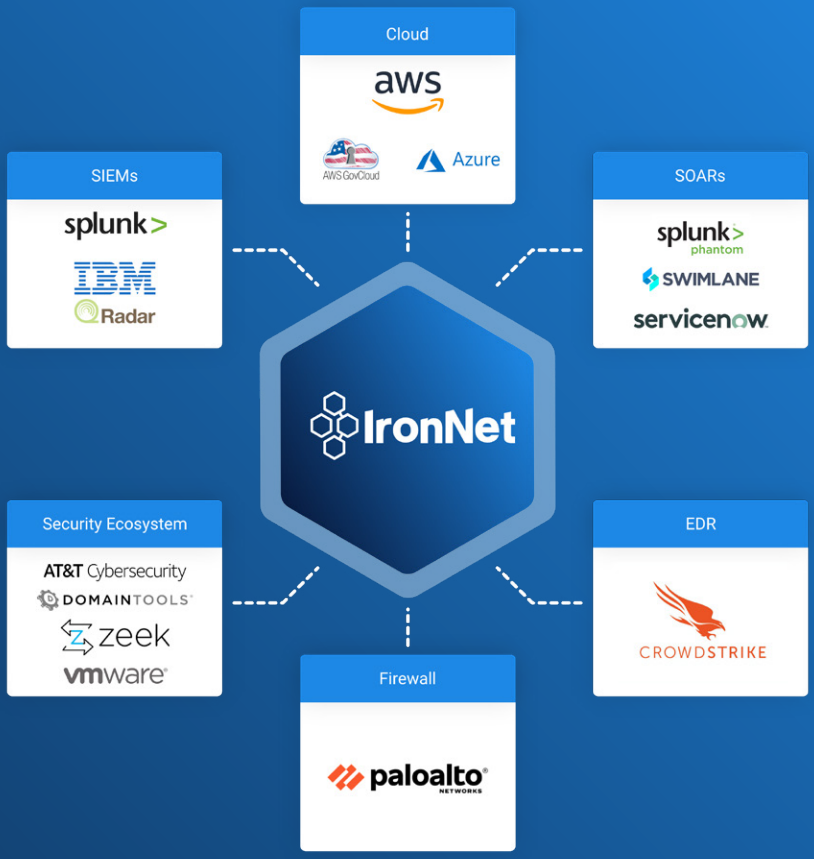
SOC Visibility Triad

NDR tools, together with endpoint detection and response (EDR) and security information and event management (SIEM) capabilities, are critical for achieving greater visibility and a stronger cybersecurity defense.



IronNet's integrations with best-of-breed technology partners

To deliver full visibility in a single pane of glass, IronNet has partnered with CrowdStrike, Palo Alto, Splunk, Amazon Web Services (AWS), Microsoft Azure, AWS GovCloud, and additional technology partners to ensure seamless NDR integration as part of your broader security ecosystem.



IronNet's technology partners for an integrated security ecosystem

Stronger network defense with IronDefense

IronNet's NDR solution, IronDefense, ensures that your security ecosystem delivers the level of detection needed to take on sophisticated, unknown cyber threats. Combining threat security analytics, operational analytics, and threat detection as a unified outcome allows detection and analysis at every step of the threat cycle. In this way, you can mature your cyber risk profile as close to "left of boom" as possible, while keeping your "right of boom" defensive posture strong and ready.

Visit **IronNet.com** to schedule a live demo of our integrated security capabilities

IronNet™

