eBook

IronNet™

Dynamic detection for dynamic threats

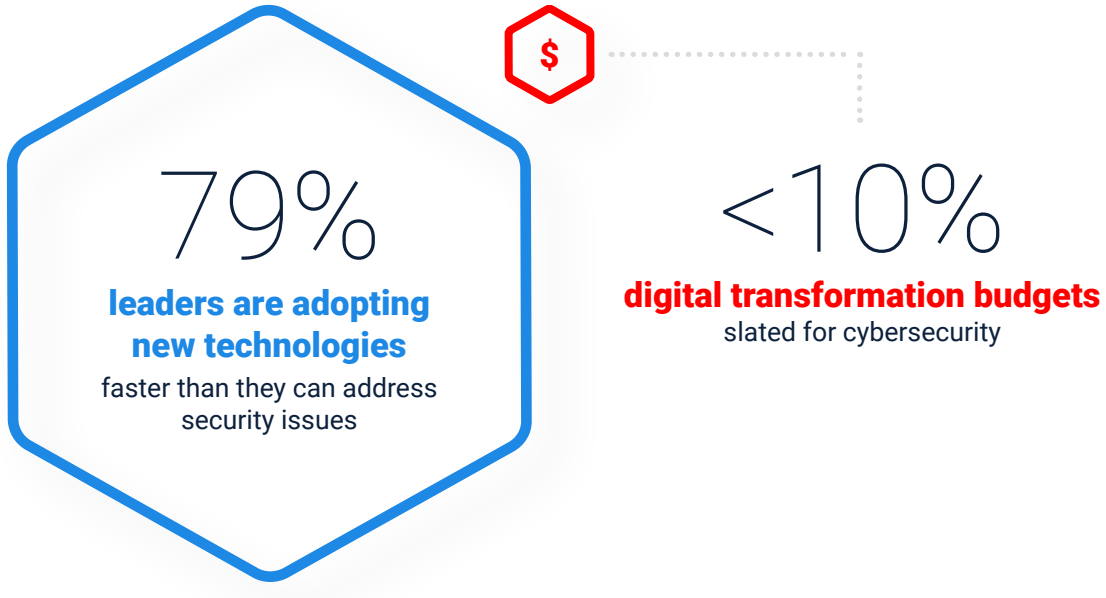
How network defense lessens cyber risk

Table of contents

Detection "left of boom"

Cyber risk is business risk.

As our world has become increasingly reliant on digital transformation, the risks of cyber threats have broadened. Cybersecurity must be integral to this transformation. Yet Deloitte's 2019 Future of Cyber Survey revealed that more than 90% of C-level executives slate less than 10% of their cybersecurity budgets to digital transformation projects. Similarly, Accenture Security has noted that 79% of corporate leaders reported "their organization is adopting new and emerging technologies faster than they can address related security issues."



This large gap between budgets and technologies creates a cyber vulnerability, where the newest and least understood digital systems are potentially unmonitored or unprotected. **Does your cybersecurity strategy address how to manage cyber threats to your entire enterprise network — regardless of whether it is an on-premise network, in the cloud, or a hybrid environment?**

The intrusion lifecycle

Whether your point of reference for identifying cyber risk and security gaps and prioritizing cyber spend is the NIST Cybersecurity Framework, the matrix-based MITRE ATT&CK Framework, or others, your goal is the same: to prevent unauthorized data access and/or system manipulation as early as possible in the intrusion lifecycle through early detection. One could argue that detections at any other point in the lifecycle are playing catch up after a breach has occurred.

Investing in capabilities to stop hackers in their tracks at the reconnaissance phase (or even before) is critical. Once an adversary moves along the intrusion path, being able to map detected observables to threat tactics is also essential for better determining the best and fastest course of remediation.

"Left of boom"

In military vernacular, the phrase "left of boom" refers to disrupting insurgent activity before the adversaries can build or plant bombs. The same holds true for cyber activity: You must stop the adversaries before they reach the exploitation or exfiltration phases. If you do not — or cannot — act fast enough, you're giving valuable dwell time to the network intruder to achieve a successful heist of your organization's data; gain control of your network, systems, or assets; or drain monetary assets. Being able to detect unknown, sophisticated threats is critical for mitigating their impact, as the average dwell time of a breach is 206 days, with another 73 days on average to contain it.

Although you want your security operations center (SOC) team to mature "left of boom," your "right of boom" defenses need to be strong as well. Network detection and response (NDR) is the way to catch behaviors on the network to build strong cyber defense. You can use the MITRE ATT&CK® Framework to evaluate your defense capabilities against these threats.

What is network defense?

How do you detect threats that have infiltrated your network? These are the threats by adversaries who have managed to slip past your firewall and/or taken advantage of an insecure endpoint to get inside your network. Once inside, adversaries often lurk there to determine the best way to steal money or data, including personally identifiable information (PII) or intellectual property. They may then move laterally across networks from their entry point to find the systems or data they are targeting.

Network Detection and Response solutions complement the firewall and Endpoint Detection and Response (EDR) tools to catch these network threats, which don’t have traditional security “calling cards,” or signatures. Occasionally, the nemesis could even be an insider threat, such as an employee who has been given access to your network.

Either way, your organization must have the capabilities to scrutinize suspicious behaviors on your network to stop them “left of boom,” or, in a worst case scenario, as the adversaries start to move laterally across your network. Your goal is to respond before they successfully capture the intended payload or take over your critical systems remotely. And if they do reach this point (or have progressed along the intrusion path), you need a reliable way to detect that the dire adversarial techniques are in play on your network.

Fighting what you can't see

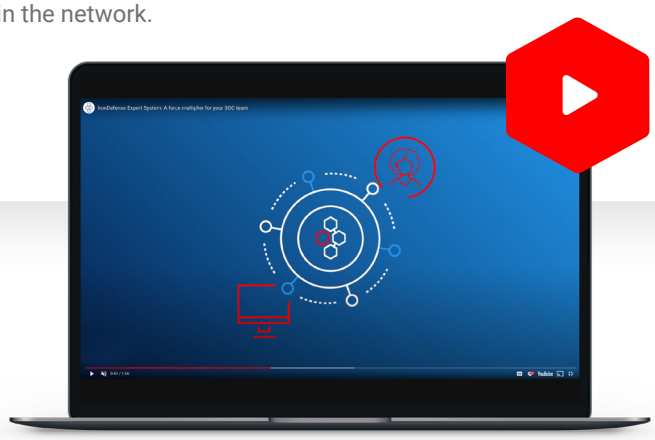
Defending in the dark

You can't fight what you can't see. Firewalls and endpoint protection tools have known visibility gaps in the current threat landscape. NDR tools can fill those voids, rounding out your security stack to provide broader visibility across the threat landscape. Leveraging advanced behavioral analytics, NDR systems can detect unknown threats that do not yet have associated signatures or known Indicators of Compromise (IoCs). Behavioral analytics detect what signatures miss, shining a brighter light on possible malicious activity.

Your SOC. Multiplied.

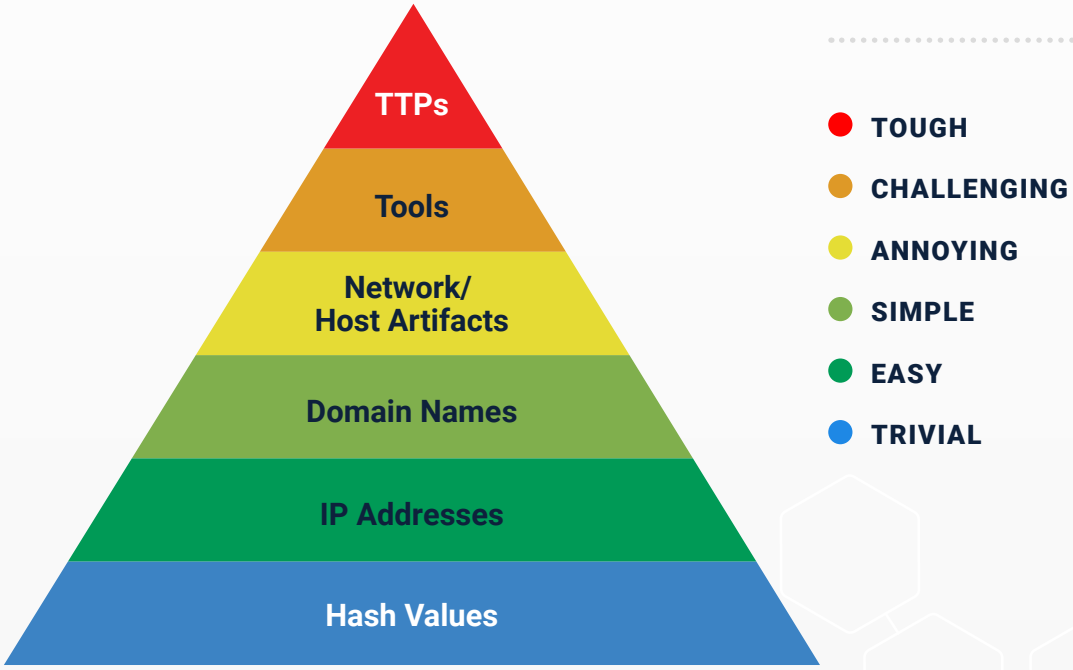
Looking for behaviors, and using a common reference such as the MITRE ATT&CK Framework, can help your SOC team prioritize response by alert level. In some cases, your team can even attribute the threats to certain adversary groups — based on typical tactics, techniques, and procedures (TTPs) — to anticipate their moves and sector targets. By automating early investigation into alerts, advanced NDR tools can help analysts triage and respond faster to threats in the network.

See how



Achieving full visibility

Why is network defense a stronger defense? Simply put, it's hard for adversaries to change their TTPs, or behaviors, quickly. To make headway toward weakening cyber adversaries, therefore, you must find them where they are most susceptible by adding network detection and response to your cybersecurity arsenal. In fact, your defense efforts are most effective at this top level of what security researcher David J. Bianco calls the threat hunting framework "Pyramid of Pain."



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

BIANCO EXPLAINS,

> When you detect and respond at this level, you are operating directly on adversary behaviors, not against their tools … From a pure effectiveness standpoint, this level is your ideal. If you are able to respond to adversary TTPs quickly enough, you force them to do the most time-consuming thing possible: learn new behaviors.

You want to direct your cybersecurity priorities and investments to the apex of the pyramid. NDR tools that draw on advanced behavioral analytics can raise cyber defense to this level. How? By giving your SOC team insight to more and earlier indicators of malicious activity, so they can detect and respond faster to these sophisticated threats.

Use case: "Finally, greater visibility of cyber threats to the financial sector"

Although this innovative, global financial firm has one of the most in-depth and capable security controls architectures in the financial services sector, it knew it had limited ability to detect and respond to behavioral-based threats, especially advanced persistent threats (APTs).

Discover how this company improved its capabilities for detecting unknown threats.

The Gartner SOC Visibility Triad

It's important to keep in mind that a NDR solution no longer is a "nice to have" complement to a traditional cybersecurity stack; instead, it is a must-have. NDR tools, together with EDR and SIEM capabilities, are key for achieving greater visibility for 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. While it is important to secure all of them, there are limitations to an endpoint-only approach.

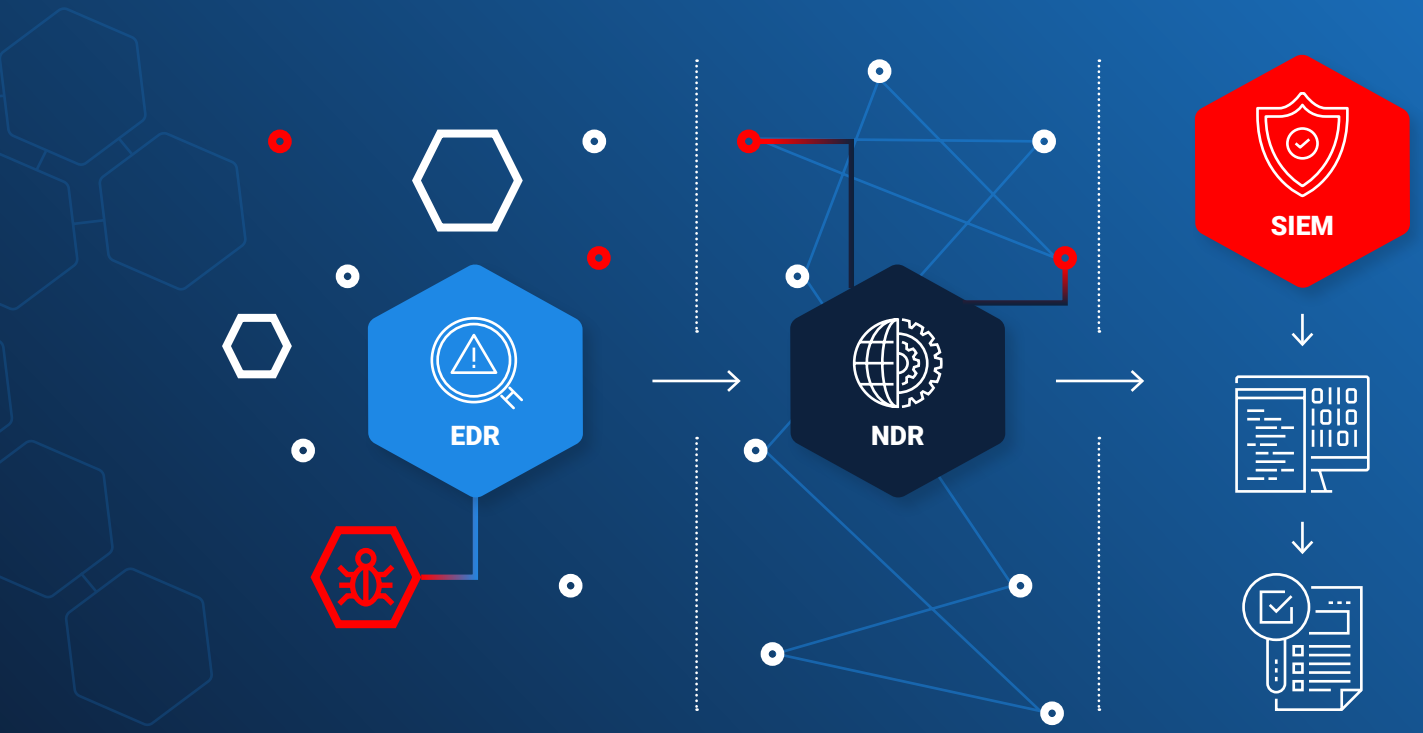
Since every company or organization operating today relies on an extended matrix of partners, third-party service suppliers, and supply chain vendors, EDR simply is not sufficient to catch all threats. Endpoint agents cannot be installed on everything, and EDR doesn't work for Internet of Things (IoT) and cloud capabilities. Not to mention the management challenges. Adversaries can target endpoints and readily neutralize them.

SECTION 2: FIGHTING WHAT YOU CAN'T SEE

This is where the NDR is so crucial. In short, the truth is in the traffic. Given that the network is ubiquitous, all movement to and from an endpoint is via the network. What's more, the network is so vast that it is nearly impossible for an attacker to fully cover his or her tracks.

While SIEMs have some basic analytics and play an integral role in the SOC as the central workflow system, this is not enough in today's world. SIEMs are limited by the types of logs they can collect, narrowing visibility and lacking ready-built analytics that can accelerate detection efficacy. It is hard for a system to be a reporting/workflow tool and a hunt/analytics engine at the same time.

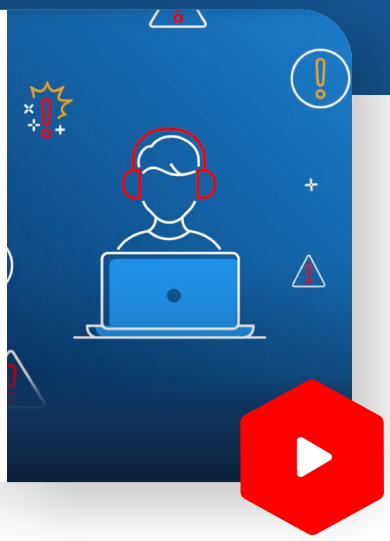
This is why companies are increasingly turning to NDR. With the right artificial intelligence (AI)/machine learning (ML) algorithms in your defense portfolio, you can tackle the challenge of processing voluminous amounts of network data to detect indicators of malicious behaviors. Armed with behavioral analytics, an NDR solution such as IronDefense completes the kind of security toolset needed for effective cyber defense.



Is your SOC team overloaded?

Your SOC manager may be concerned about balancing full threat visibility and the potential for alarm overload.

Learn more about how to achieve this balancing act.



Dynamic detection for dynamic threats

Revisiting the "SOC Visibility Triad"

We believe it's time to envision the static triad of NDR, EDR, and SIEM as a powerfully adaptive system, where each of the inextricable points on the triangle can work together — to make each other stronger.

A dynamic detection framework

SIEMs have traditionally been considered the top of the two-dimensional triad, as they are user-facing and the only one in the group to be able to ingest, correlate, and analyze the data. There is a way to add an even higher level of threat intelligence insight to the SOC visibility triad, however. Turn it into a robust and ever-evolving pyramid with all three corners of the triad contributing to an interconnected system of cybersecurity teams. In this collaborative detection framework, each node strengthens the others and forms the strongest cyber defense posture possible, collectively reducing the cyber margin of error. It's a win-win-win scenario.

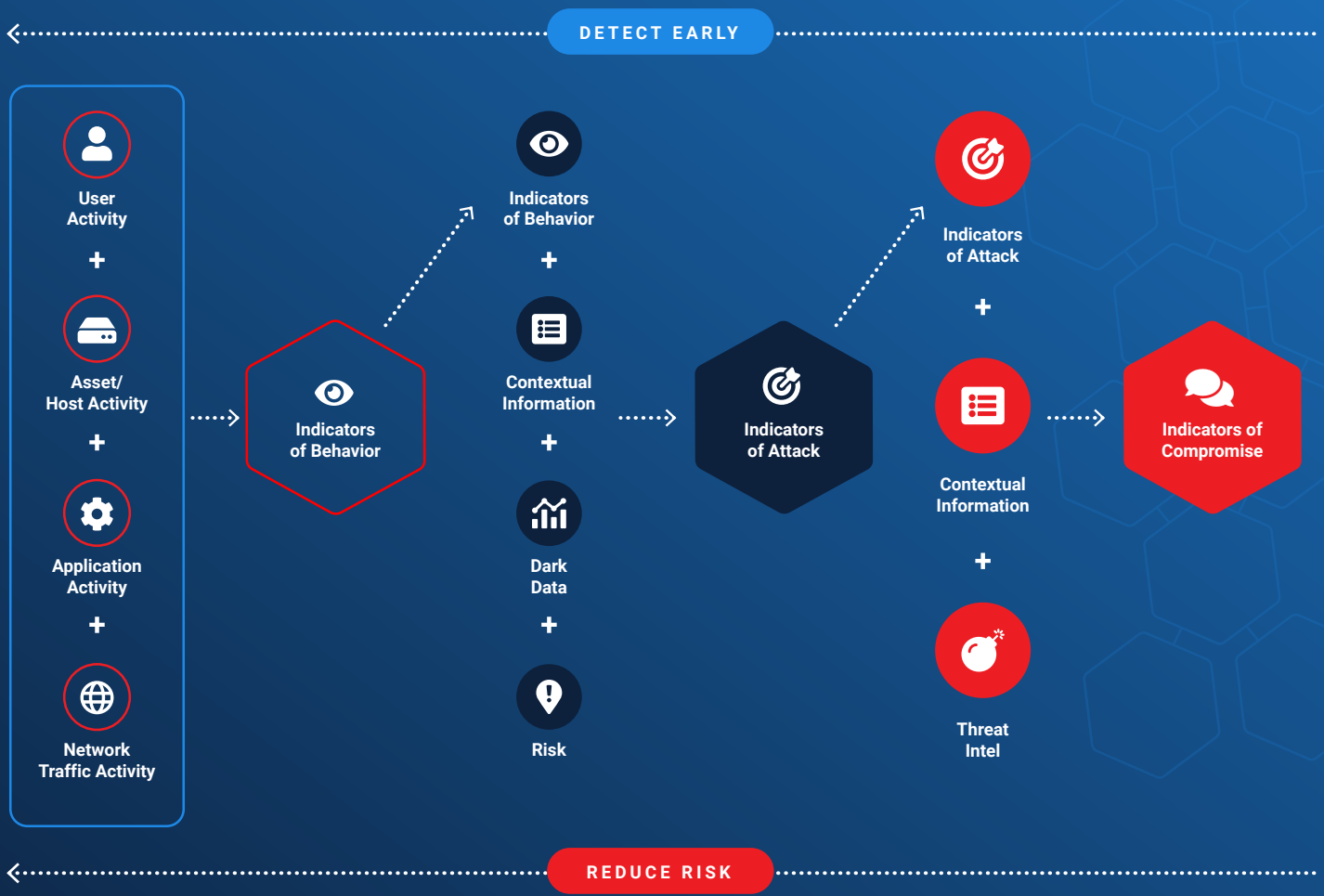
How can you generate a dynamic relationship among SIEM, EDR, and NDR tools? The answer is Collective Defense, which draws on behavioral analytics and orchestrates threat information sharing in real time — and in situational context. IronNet's IronDome, the platform that empowers this collaborative engagement, is the engine that can transform the SOC Visibility Triad into a dynamic pyramid. Each point communicates with each other at machine speed, always interconnected to strengthen each other for complete visibility across the threat landscape.

Stages of detection: moving the needle

It is understandable that organizations looking to secure their enterprise have long-treated log-based detection as a SIEM-only function. NDR solutions that use advanced behavioral analytics, such as IronDefense, are challenging and changing that notion, by placing emphasis on Indicators of Behavior (IoBs) instead of just Indicators of Compromise. Simply put, detecting only Indicators of Compromise is too late in the intrusion cycle to minimize the risk. The earlier the detection, the lesser the risk.

What is an Indicator of Behavior?

Indicators of Behavior across users, hosts, applications, and the network allow you to detect TTPs regardless of whether the underlying IoCs change. Behavioral analysis can identify potential attempts in the staging of an attack, either by an insider or an external actor.

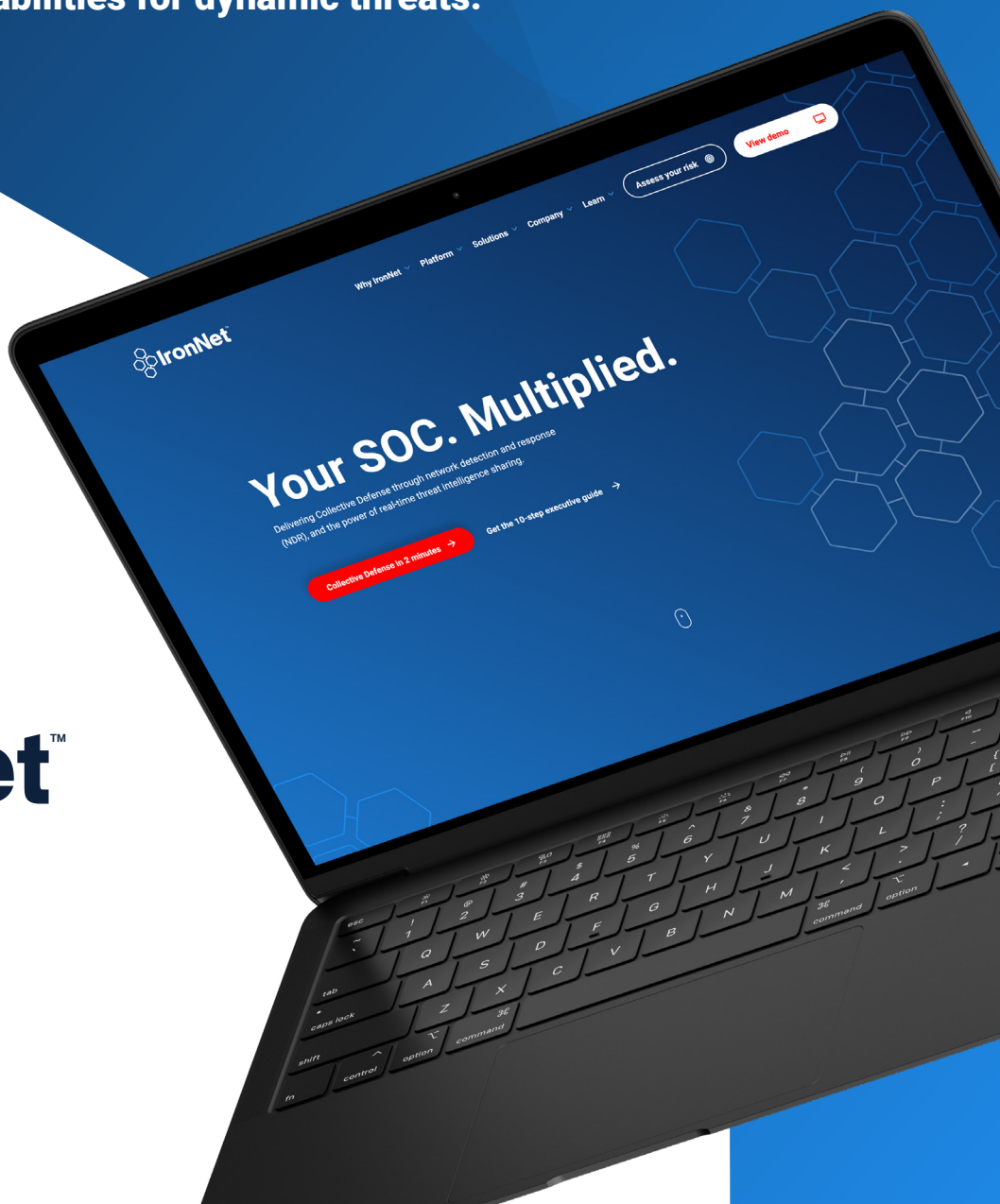


Stronger network defense with IronDefense

With its proprietary behavioral analytics, which help map threat alerts in IronDefense to the intrusion cycle, and IronDome Collective Defense platform, IronNet enables your SOC team to adopt a truly dynamic defense. While NDR in general looks in the best hiding spots, IronNet analytics are smarter because they are better informed; stronger because they turn a flat, individual triad into a connected pyramid; and quicker to adapt to new threat information in real time.

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 dynamic detection capabilities for dynamic threats.



IronNet™