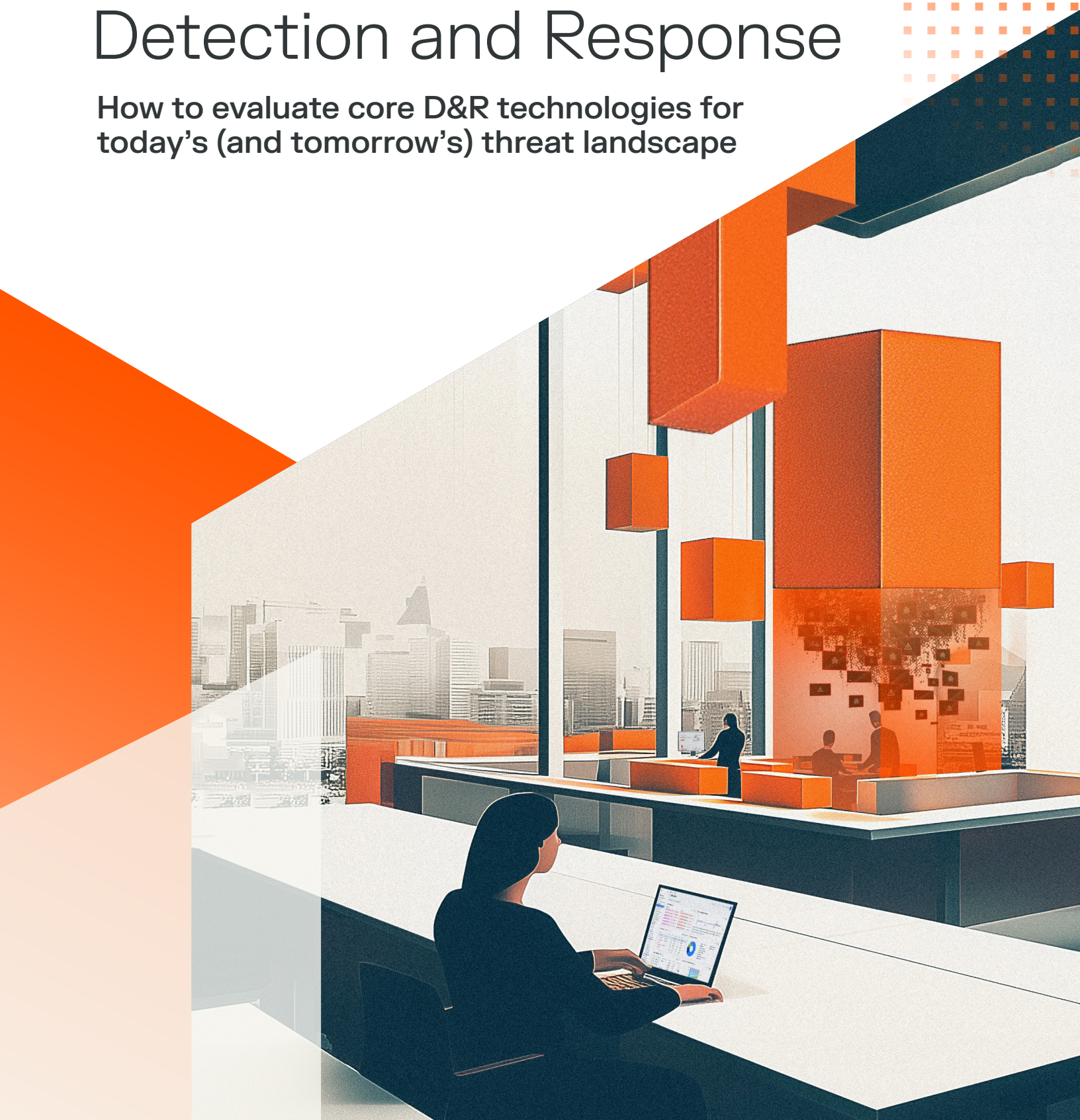
illumio

EBOOK

The Buyer's Guide to Detection and Response

How to evaluate core D&R technologies for today's (and tomorrow's) threat landscape



Contents

INTRODUCTION

When attackers move fast, you have to move faster.

In cybersecurity, timing is everything.

By the time most teams detect an attack, it's already well underway. The intruder is inside. Data might be exfiltrated. Systems could be compromised. Your board is calling. That's why detection and response (D&R) is more than just another layer of defense — in today's threat landscape, it's your lifeline.

But not all D&R solutions are created equal. Vendors throw around big claims and buzzwords, and it's getting harder to tell what actually works or what your organization actually needs.

That's where this guide comes in.

We're cutting through the noise to give you a clear, practical breakdown of the most common D&R technologies: what they do well, where they fall short, and how they fit into a modern security strategy. We'll also explain why the industry is shifting toward cloud detection and response (CDR) and what that means for you.

If you want to understand what tools are worth your time and which ones still leave you exposed, you're in the right place.

What detection and response really means today

Detection and response (D&R) tools are designed to spot malicious activity quickly and act on it even faster. They're your second line of defense when prevention fails. And make no mistake prevention will fail.

In the past, cybersecurity was all about building walls: stopping attackers at the perimeter and assuming everything inside was safe. But that model no longer holds.

Within the last year:

75%
of organizations report being victims of a ransomware attack

90%
have detected a security incident involving lateral movement in their network

58%
had to shut down operations due to an attack for an average of 12 hours

The reality is that attackers are getting in. The perimeter has dissolved, and waiting for perfect prevention is no longer an option.

That's why D&R is critical. It gives you the ability to catch what prevention misses, contain threats before they spread, and limit the damage before it becomes catastrophic.

In this section, we'll break down the core types of D&R technologies, how they work, where they shine, and where they fall short, so you can choose what's right for your environment.

EDR
(endpoint detection and response)

Endpoints—such as laptops, desktops, servers, and mobile devices—are among the most common entry points for attackers. That's where EDR solutions focus.

EDR continuously monitors endpoint activity, collects telemetry, and uses behavioral analysis to detect suspicious or malicious behavior. When something looks off, EDR tools can alert security teams, record forensic details, and often take automated actions like isolating the device or killing a malicious process.

They're designed to give SOC analysts visibility into what's happening on endpoints and the tools to investigate and remediate quickly.

EDR is great at:

- **Stopping endpoint-focused attacks:** EDR excels at catching malware, ransomware, and insider threats that start at the device level.
- **Behavioral detection:** beyond signatures, modern EDR tools spot suspicious patterns, like unusual process execution or privilege escalation.
- **Forensics and investigation:** EDR stores rich endpoint data, letting analysts reconstruct how an attack unfolded.
- **Response capabilities:** many EDRs can isolate compromised machines, stop processes, and roll back changes to contain damage fast.
- **Coverage of remote and mobile devices:** with remote work, EDR has become critical for securing endpoints outside the corporate perimeter.

But EDR struggles with:

- **Limited scope:** EDR sees only what happens on the endpoint. It can't detect lateral movement across the network or malicious traffic between cloud workloads.
- **Noise and false positives:** analysts may get flooded with alerts about activity that looks suspicious but isn't truly malicious.
- **Resource overhead:** endpoint agents can consume CPU and memory, and maintaining them at scale can be a challenge.
- **Evasion tactics:** advanced attackers can disable or bypass EDR agents, leaving blind spots.
- **Fragmented visibility:** without integration into network or cloud monitoring, EDR gives a partial view of the overall attack surface.

NDR
(network detection and response)

While EDR focuses on what happens on devices, NDR looks at what flows between them.

NDR solutions monitor network traffic, from packet-level data to flow logs, to spot anomalies, suspicious communication patterns, and indicators of compromise. The goal is to detect threats that have slipped past the perimeter and are now moving inside the network.

NDR tools often use a mix of signature-based detection, heuristics, and machine learning to flag unusual behaviors. For example, a server suddenly talking to an unfamiliar IP, or large amounts of data being exfiltrated at odd hours.

Because attackers often rely on lateral movement to escalate their access once inside, NDR is particularly valuable for spotting these hidden movements before they turn into full-scale breaches.

NDRs are great at:

- **Lateral movement detection:** if an attacker compromises one endpoint and tries to pivot deeper into the network, NDR can flag the unusual east-west traffic.
- **Unknown threat discovery:** by monitoring behavior rather than relying only on known signatures, NDR can surface previously unseen attack patterns.
- **Wide coverage:** NDR sees activity across the network, not just individual devices, giving SOC teams visibility into connections between endpoints, servers, and cloud gateways.
- **Incident investigation:** packet captures and flow data provide forensic evidence of how an attacker moved through the network.
- **Complementing EDR and XDR:** NDR can fill the visibility gap that endpoint-only tools miss, especially for unmanaged or IoT devices.

But NDRs struggle with:

- **Encrypted traffic**: with so much traffic now encrypted (TLS/SSL), NDR can lose visibility into the actual content, forcing reliance on metadata and behavioral patterns.
- **Hybrid and cloud architectures:** modern workloads move between on-premises data centers, public clouds, and endpoints. This makes it harder for traditional network-based tools to keep up.
- **Volume and noise:** network traffic is massive, and NDR tools can generate high numbers of alerts which requires strong tuning and analyst expertise.
- **Blind spots for off-network devices:** remote endpoints that don't route traffic through corporate networks can evade NDR visibility.
- **Resource-intensive:** collecting, storing, and analyzing packet-level data can be costly in terms of infrastructure and bandwidth.

XDR
(extended detection and response)

XDR is designed to break down silos across security tools. Instead of having separate consoles for endpoint (EDR), network (NDR), email, cloud, and identity systems, XDR platforms pull telemetry from all of them into a single view.

By correlating signals across multiple domains, XDR aims to give security teams faster, more accurate detections and reduce the alert fatigue that comes from juggling too many point solutions.

Most XDR solutions combine detection, investigation, and response into one workflow that:

- Ingests signals
- Correlates these signals into higher-fidelity incidents
- Allows analysts to take action directly from the XDR console, such as isolating an endpoint, disabling a user account, or blocking malicious domains

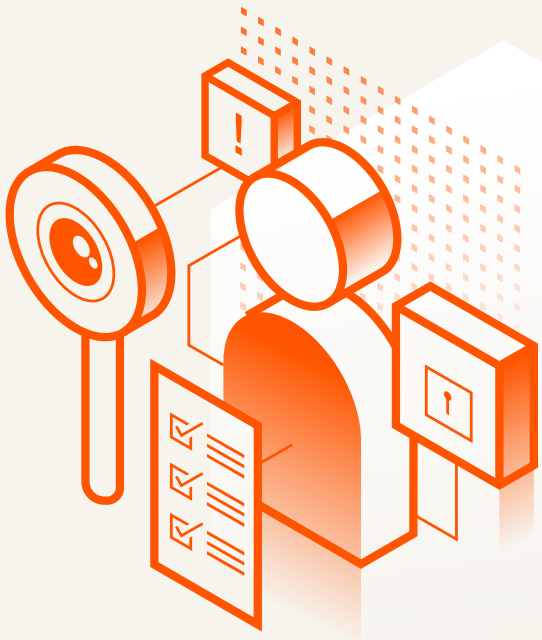
Some vendors market XDR as the evolution of EDR, expanding protection from just endpoints to the broader IT ecosystem. And while XDR is often marketed as an "all-in-one" tool, it can still lead to coverage gaps and alert fatigue.

XDRs are great at:

- **Cross-domain correlation:** by stitching together events across endpoint, network, email, and identity, XDR helps analysts see the full attack chain instead of isolated alerts.
- **Reducing alert noise:** XDR platforms typically consolidate thousands of low-level alerts into a smaller set of actionable incidents.
- **Single-pane-of-glass visibility:** analysts can monitor and respond to threats without bouncing between multiple tools.
- **Streamlined response:** many XDRs allow direct action, such as quarantining devices, suspending accounts, and blocking IPs, from within the platform.
- **Improved detection of advanced threats:** correlating subtle signals across domains makes it easier to detect stealthy or multi-stage attacks that might otherwise slip through.

But they struggle with:

- **Data overload:** while XDR reduces alert volume, the sheer amount of telemetry can still overwhelm storage, processing, and analyst attention.
- **Integration gaps:** XDR platforms often work best within a single vendor's ecosystem. Connecting third-party tools can be inconsistent or limited.
- **Maturity:** XDR is still evolving, and capabilities vary widely between vendors. Some resemble "EDR-plus," while others are closer to SIEM replacements.
- **False sense of completeness:** XDR is marketed as "all-in-one," but coverage depends entirely on what sources are integrated. Gaps remain if important signals, such as OT or IoT, aren't fed in.
- **Resource requirements:** running XDR effectively still demands skilled analysts to tune detections, investigate incidents, and manage integrations.



SIEM + SOAR

(security information and event management) + (security orchestration, automation, and response)

These two technologies are often paired together because they complement each other. But neither is a true detection tool on its own.

SIEMs act as the central hub for logs and events. They ingest data from across the IT ecosystem, including firewalls, endpoints, servers, applications, identity systems, and cloud platforms. Then, they normalize, store, and correlate the data.

Analysts use SIEM dashboards and queries to detect anomalies, investigate incidents, and satisfy compliance requirements.

SOARs pick up where SIEM leaves off. They don't detect threats, but they automate responses once alerts arrive. They run playbooks to enrich data, assign tickets, block IPs, quarantine endpoints, or notify the right teams.

In short, SIEM gives you the "eyes and memory," while SOAR provides the "hands and reflexes."

SIEMs and SOARs are great at:

- **Centralizing logs and events:** SIEMs make it easier to search across mountains of data for security and compliance.
- **Correlation and context:** SIEM rules can combine multiple alerts into higher-level incidents.
- **Forensics and reporting:** SIEMs store historical data for audits and breach investigations.
- **Automation and consistency:** SOAR playbooks speed up response and ensure repeatable processes.
- **Reducing SOC workload:** together, SIEM + SOAR can take tedious, repetitive triage and response tasks off analysts' plates.

But they struggle with:

- **Not true detection engines:** both rely on EDR, NDR, XDR, or threat intel feeds to provide meaningful signals.
- **Alert fatigue:** SIEMs can generate overwhelming noise, which SOARs may then automate into unnecessary or disruptive actions.
- **Complexity and cost:** standing up SIEM pipelines and SOAR integrations is resource-intensive, often requiring ongoing tuning and maintenance.
- **Limits of automation:** SOAR can't replace human judgment for complex incidents and still needs analysts to make critical decisions.

What's missing from traditional D&R

The fact is that none of the tools listed above were built for the cloud-first, hybrid-everything world we live in now.

Modern environments are:

- Distributed across public cloud, private data centers, and endpoint environments
- Constantly changing with ephemeral workloads and dynamic policies
- Built for speed, not security

Traditional D&R tools can't keep up. The problem? Blind spots.

Endpoint tools miss unmanaged devices. Network tools miss cloud-native apps. Even XDR solutions lead to data overwhelm and alert fatigue.

By the time alerts surface, it's already too late to contain the blast radius.

Why cloud detection and response (CDR) is the future of D&R

CDR is the next evolution of detection and response. It's built for today's and tomorrow's hybrid environments.

CDR is a security capability that identifies, contextualizes, and contains threats within cloud workloads, virtual machines, containers, and inter-application communications.

Why it matters now:

- **The cloud is the new perimeter.** It's where your apps, data, and users live. And it's more distributed than ever. CDR gives you visibility into those dynamic, multi-cloud environments.
- **Lateral movement is the number one attack tactic.** CDR helps you spot and fix lateral movement risk so breaches can't spread through your network.
- **AI and automation are table stakes.** You can't respond to breaches fast enough if you're only using manual processes. CDR automates breach containment. Isolate attacks on the stop.

Choosing the right D&R strategy

The key to modern cybersecurity is building a strategy that fits your environment, supports your team, and delivers real control fast.

Here's what to consider as you build or refine your detection and response approach.

Know your environment

Cloud, containers, unmanaged assets, hybrid infrastructure — today's environments are sprawling, dynamic, and constantly shifting.

Yet many D&R tools still rely on static assumptions or narrow visibility. Traditional endpoint or perimeter-focused tools can't see workload-to-workload traffic in the cloud. They also often miss malicious movement across distributed environments.

To close the gap, you need tools that ingest and analyze data from everywhere attackers could hide, not just where it's convenient.

Find your blind spots

Most D&R tools are specialists. For example, EDR sees activity at the device level, NDR monitors traffic patterns, and SIEM aggregates logs.

But on their own, they don't offer complete context. And stitching together those signals is slow, manual, and often incomplete.

The best strategies use tools that enrich your existing telemetry with context, like how workloads are connected or which communications are normal versus high risk. That kind of visibility helps analysts spot lateral movement early and act decisively.

Prioritize action over alerts

On average, security teams report managing more than 2,000 alerts per day on average.

That's simply not sustainable.

Modern D&R platforms must do more than detect. They should distill alerts into clear action, surface what matters most, and integrate with workflows your analysts already use.

The goal isn't just knowing something's wrong but knowing exactly where to look and what to do next.

Detect lateral movement, not just initial access

Most tools are built to spot the breach, not what happens after. But it's the lateral movement that happens after the initial breach where the real damage happens. Attackers pivot from system to system, escalating privileges and working their way towards your most critical assets.

Choose D&R platforms that don't just alert on initial compromise, but also reveal how attackers are navigating your environment.

5

Understand your exposure in real time

Knowing there's a threat is one thing, but knowing what's at risk is another.

Look for tools that help you visualize the potential blast radius of an attack and help you answer questions like:

- Which workloads can the attacker reach?
- What critical systems are connected?
- What's the shortest path to your crown jewels?

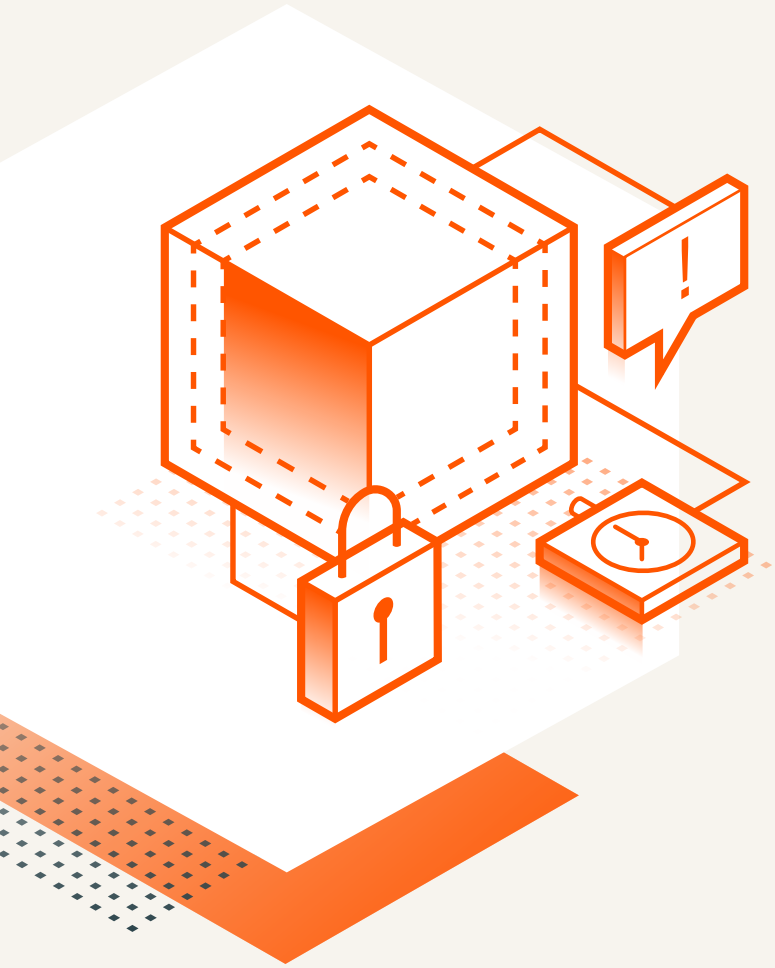
The ability to answer these questions in real time turns detection into decisive action.

6

Reduce dwell time with proactive breach containment

The faster you isolate a threat, the less damage it can do. But most detection tools stop at alerting and leave breach containment to manual processes or disconnected platforms.

The right D&R strategy includes proactive, integrated containment. A platform should connect detection with segmentation controls, so you can isolate suspicious activity instantly and prevent spread, even before your team is finished with a full investigation.



7

Support your Zero Trust goals

Detection is only half the job. The right solution should also contain threats immediately, before they spread.

If a D&R tool can't isolate compromised systems, visualize blast radius, or enforce segmentation in real time, it's not built to support a complete Zero Trust strategy in practice.

This is where most legacy tools fall short — and where new approaches like cloud-native breach containment fill the gap.

Illumio Insights: CDR for modern networks

Illumio Insights is the CDR of the future.

Insights is built on an AI security graph, which is an AI-powered map of every workload, traffic flow, and relationship in your environment.

You're not only getting a map of everything in your environment. But you're getting the context you need to understand what's happening in your network, what's at risk, and where you need to prioritize your resources.

Here's how it works:

Rapid, cloud-scale deployment

Agentless push-button deployment delivers AI security graph-powered insights across millions of workloads in minutes.

Unmatched threat detection with AI observability

Significantly reduces the mean time to detect (MTTD) by uncovering unseen risks, hidden attack paths, and active threats in real time.

One-click attack containment

Neutralize potential threats with our one-click dynamic quarantine feature. Contain and isolate compromised resources to dramatically reduce the mean time to respond (MTTR). Take control and safeguard your assets with confidence.

What makes Illumio Insights different from traditional D&R tools?

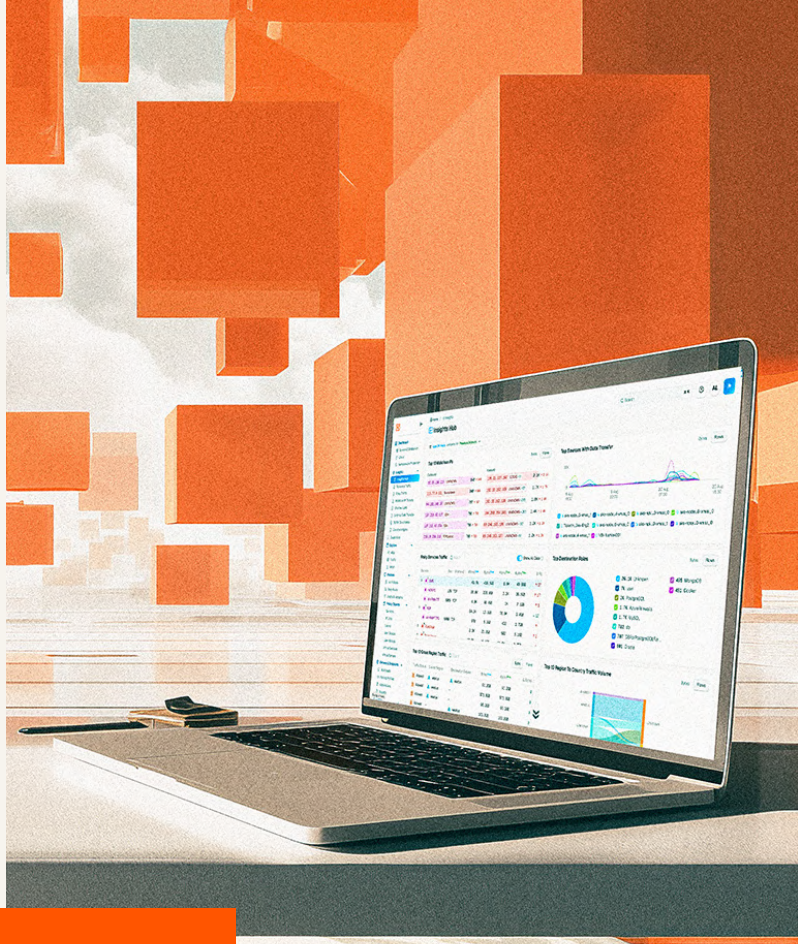
- No deep packet inspection or agent sprawl
- Purpose-built for hybrid cloud and containers
- Built-in response, not just alerts
- Uses AI to expose unseen risks, not just react
- Offers real-time observably, not just a snapshot of your environment

Ready for whatever comes next

We're living in a world where prevention is no longer enough. Attackers will get in.

Illumio Insights gives you the context to detect threats and the controls to contain them instantly.

That's real cyber resilience that's ready for the future.



Try Illumio Insights today

Explore AI CDR that identifies lateral movement risks, detects attacks, contains instantly — all at cloud scale.

- Detect cloud lateral movement others miss
- Build a visual security graph of your environment
- Enforce real-time breach containment policies
- Respond faster, smarter, and more strategically

Get started at illumio.com/insights-free-trial.