

XDR Buyer's Guide for Strapped Security Teams

What to look for when time, budget,
and talent are stretched thin

[➤ Get Started](#)

Security teams today are expected to do a lot more with a lot less.

With the odds stacked against them, analysts still need to manage sprawling tool stacks, investigate each alert manually, respond to incidents at lightning speed, maintain visibility across hybrid environments, and somehow avoid complete burnout in the process.

Meanwhile, attackers have already outsourced much of their workflow to AI-driven automation. And nearly two-thirds (65%) of phishing attacks, helped along by generative AI, are now aimed at organizations like yours.

65% of phishing attacks now target organizations, rather than individuals.
Source: [Hox Hunt](#)

Far from ideal

The unfortunate reality is that smaller organizations now face many of the same threats as large enterprises, but without the luxury of massive SOC budgets or endless operational bandwidth. While the industry has responded with more tools, platforms, and acronyms, it all just amounts to more complexity. And more risk. That's what extended detection and response (XDR) solves for.

In this guide, we're breaking down exactly why a unified XDR platform gets the job done, including:

- Why lean security teams are uniquely vulnerable
- What a robust XDR should actually help you accomplish
- Which capabilities make the biggest impact

Because enterprise-grade security shouldn't require enterprise-sized teams or budgets.



Five challenges SOCs can't afford to overlook

Attackers got faster. *Did your team?*

If you've worked in security long enough, you already know managing vulnerabilities can feel less like a process and more like a treadmill that keeps speeding up. As nation-state actors expand their targets and AI accelerates multi-stage attacks, defenders are expected to respond faster to signals coming at them across all attack vectors. Worse yet, many attackers have shifted toward financially-motivated campaigns. Meanwhile, security teams still spend hours pivoting between tools to determine whether 10 alerts actually signal just one incident—a costly mismatch that at best erodes productivity and at worst leads to a breach.

GenAI didn't create the problem. *It accelerated it.*

Threat actors were leveraging automation long before GenAI entered the conversation. Now, large language models (LLMs) generate sophisticated phishing lures, malware, social engineering scripts, and credential-harvesting campaigns at unprecedented speed and scale. As attackers build complex, multi-step attack chains, speed has become central to cyber resilience. With Shadow AI and emergent autonomous agents, defenders struggle to secure environments evolving faster than they can adapt.

Tool sprawl was manageable. *Until it wasn't.*

Most organizations didn't intend to build fragmented security stacks—they accumulated over time. An endpoint solution here, network security there, and data loss prevention layered on top. Soon analysts spend more time switching interfaces, correlating telemetry, and reconstructing attack timelines than responding to threats. The issue isn't just complexity, but visibility. When security tools don't share context, attackers have more time to operate without raising high-confidence alerts that prompt action. Tool sprawl creates exploitable blind spots that only drive risk, especially for lean teams that lose critical time piecing together attack signals across separate systems.

The attack surface is everywhere. *And traditional perimeters are gone.*

Remote work, cloud adoption, SaaS applications, and GenAI have redefined the perimeter as we know it. Every unmanaged endpoint, overprivileged account, and exposed credential creates another opportunity for attackers to move laterally, while sensitive data continues to spread across systems and services. Security teams are now expected to maintain visibility across every layer—a near impossible task for organizations without the resources to continuously monitor and correlate activity across their endpoints, networks, and data.

Where has all the good talent gone? *Security teams need a hero.*

The security talent shortage is far from new, but the greater challenge lies in a shortage of skill. According to the latest [ISC2 Cybersecurity Workforce study](#), 95% of organizations report at least one cybersecurity skills gap—with 59% describing those gaps as critical. In fact, only 5% believe they have all the cybersecurity skills they need. It's quickly becoming one of the industry's most dangerous liabilities. As emerging AI technologies and threats continuously reshape the security landscape, upskilling has become just as critical (if not more) as hiring. For already overwhelmed SOCs, these skill gaps make it even harder to manage then endless flood of alerts competing for attention. It's no surprise that nearly three of four security professionals (74%) say [the current threat landscape is the most challenging](#) it has been in five years. Security teams are being pushed beyond their limits, and it's high time they found relief.

What the industry is saying

AI as cybersecurity's
biggest wildcard

87%

AI vulnerabilities are the fastest-growing cyber risk according to nearly 9 out of 10 professionals.

Attackers may
already be among us

71%

of analysts fear they may already be compromised without their knowledge due to lack of visibility and confidence in threat detection capabilities.

Nearly half of
attacks are missed

47%

of attacks go undetected over a 12-month period because teams lacked the visibility and context to respond in time.

Trust is hard
to come by

36%

of security leaders said they were very confident their controls were working as intended.

Complexity comes
at a high cost

65%

of organizations say they have too many security tools, while

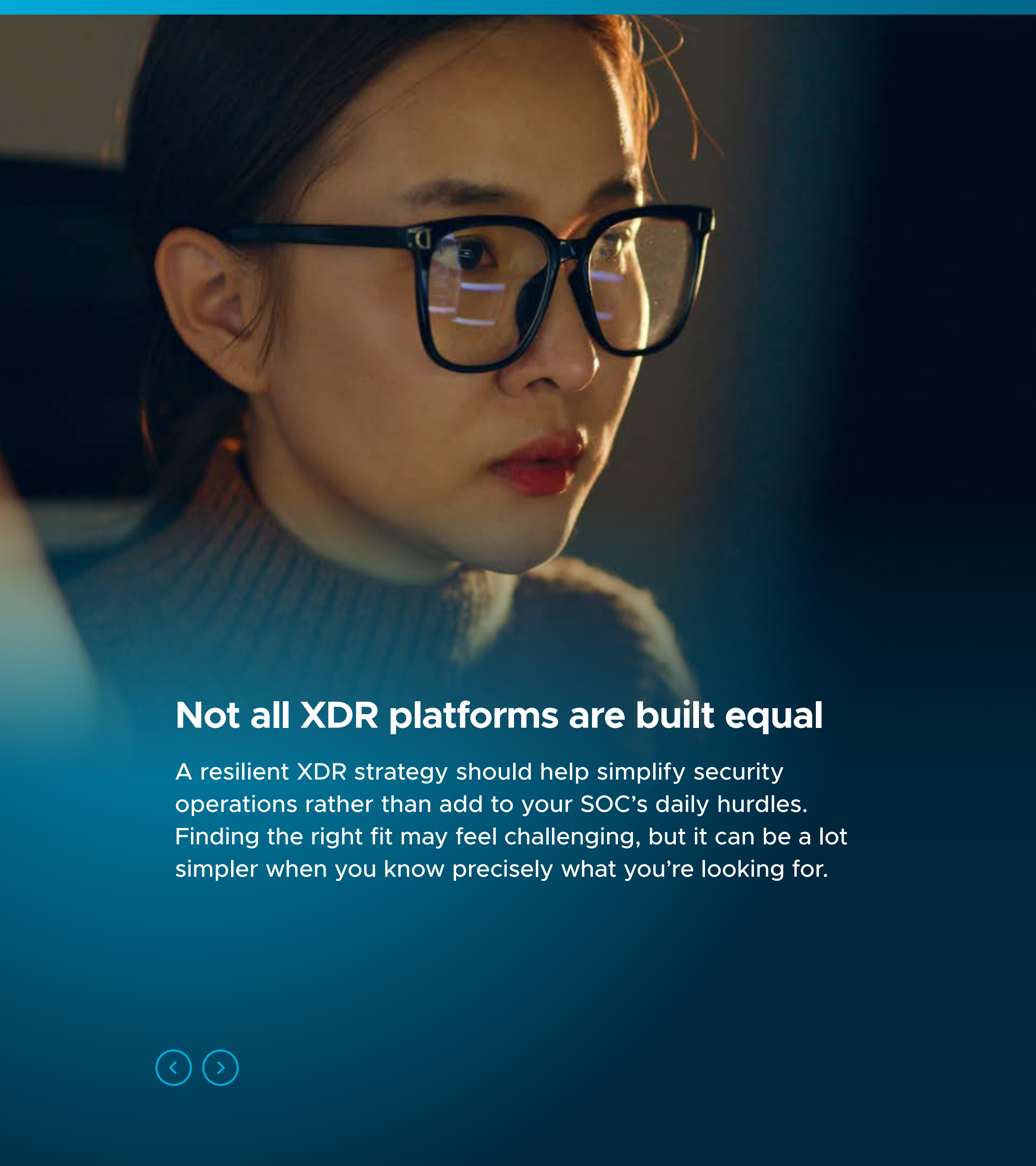
53%

say those tools can't be integrated

Consolidation
is the future

84%

of CISOs agreed their organizations are prioritizing security platformization.



Not all XDR platforms are built equal

A resilient XDR strategy should help simplify security operations rather than add to your SOC's daily hurdles. Finding the right fit may feel challenging, but it can be a lot simpler when you know precisely what you're looking for.



Here's what to look for



Comprehensive protection Coverage that matches your priorities

First, get clear on which domains matter most to your security strategy—visibility without alignment can lead to dangerous blind spots. If your biggest concerns are endpoint activity, network security, cloud workloads, or data protection, your XDR solution should reflect that.



Proven prevention Keep threats in check

An XDR platform can't just detect and respond. It also needs strong prevention. With endless false positives and low-fidelity alerts draining analyst time, a platform should reduce noise early. That way teams can stop common threats earlier in the attack chain, before bad actors have a chance of pivoting tactics and causing massive damage.



Intuitive workflows

Roadmaps that won't slow you down

Security teams already juggle enough responsibilities without fighting fragmented and siloed tools along the way. You want the path of least resistance. An XDR platform should present insights in a way that's easy to understand, investigate, and act on—with handoffs between teams feeling seamless. A single console platform will get teams there without multiple dashboards slowing them down.



AI-powered capabilities

With humans at the helm

AI in XDR should enable security teams—not sideline them. The best AI-driven capabilities put your teams first, such as helping analysts:

- Prioritize alerts
- Summarize investigations
- Map threat incidents
- Predict attacker moves

AI that makes management easier—from automating routine tasks to relieving operational burden—will keep decision-making where it belongs: with the human experts defending your organization.



Unified security

Less stitching, more impact

A lot of teams know the pain of managing dozens of integrations just to get partial visibility across their environment. But XDR shouldn't make them assemble coverage piece by piece. Look for a platform with native telemetry across key domains, so endpoint, network, and data signals can work together from the start. The more unified, the easier it is for teams to maintain consistent coverage without stitching signals together by hand.



Simplified reporting

Detailed reports anytime you need them

There's no reason why analysts should get pulled away from more important work to spend hours putting together a report—especially when an XDR platform can take care of it. Simple, built-in reporting makes it easier for teams to share updates, hand off data, and show progress, all while building the credibility and proof of value stakeholders want to see.



The right XDR platform will empower teams to:

- ⚡ Prevent attacks and stop data loss before they lead to disruptions, financial penalties, or reputational damage
- ⚡ Accelerate threat detection and response with clearer, actionable insights
- ⚡ Reduce alert fatigue, boosting SOC efficiency from top to bottom
- ⚡ Improve security outcomes without needing to grow headcount
- ⚡ Simplify compliance, reporting, and day-to-day data privacy efforts
- ⚡ Cut operational overhead and lower security costs without sacrificing visibility
- ⚡ Prove security value with reports that stakeholders can easily understand
- ⚡ Maintain customer trust and business continuity when incidents happen

Say hello to Symantec® CBX

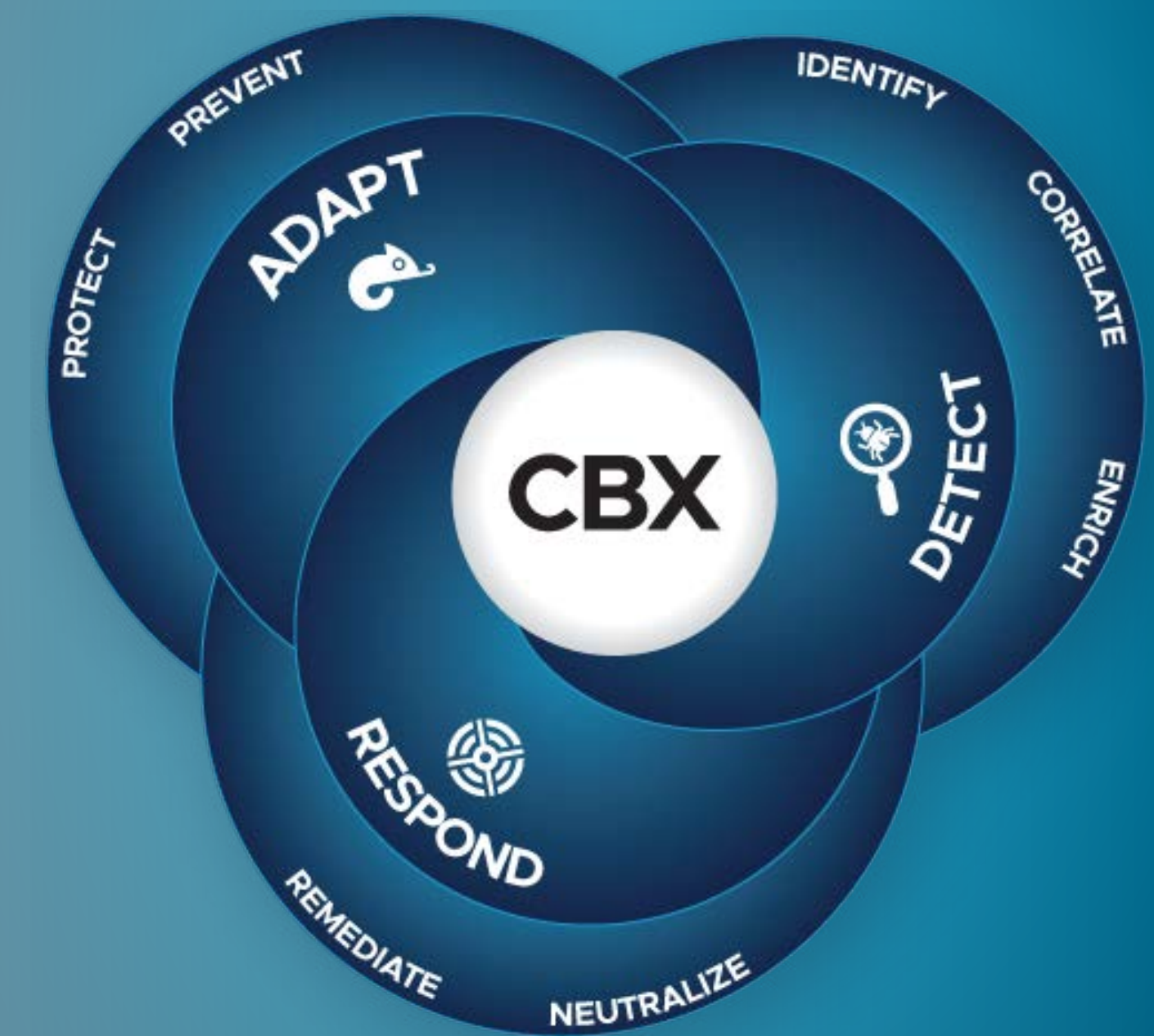
We built Symantec CBX, a unified XDR platform featuring award-winning capabilities from both Symantec and Carbon Black®, to give resource-strapped security teams a simpler, clearer path to reliable security.

Intentionally designed for lean teams fighting ever more sophisticated threats, CBX helps organizations cut through the noise faster with native correlation of telemetry across endpoints, networks, and data. With zero need for manual stitching, fragmented integrations become a thing of the past. Security teams can finally gain a full view of an attacker's activity—understanding what is happening, what it means, and what to do about it.

Everyone deserves peace of mind. CBX delivers enterprise-grade security at a fraction of the cost.

With CBX, analysts can reduce alert fatigue, boost productivity, and simplify compliance and day-to-day operations using AI-powered capabilities that:

- Surface attacker activity in a single pane
- Make sense of complex incidents and provide next steps for action
- Visualize the blast radius of attacks
- Predict an attacker's next four to five moves
- Block living off the land (LOTL) attacks before they can do damage.



Symantec CBX enables you to



ADAPT

your defenses
to stop attacks
sooner and
improve security
posture



DETECT

attacks
across your
environment
and see the full
attack story



RESPOND

with speed
and clarity
from a unified
console

Unparalleled prevention, detection, and response

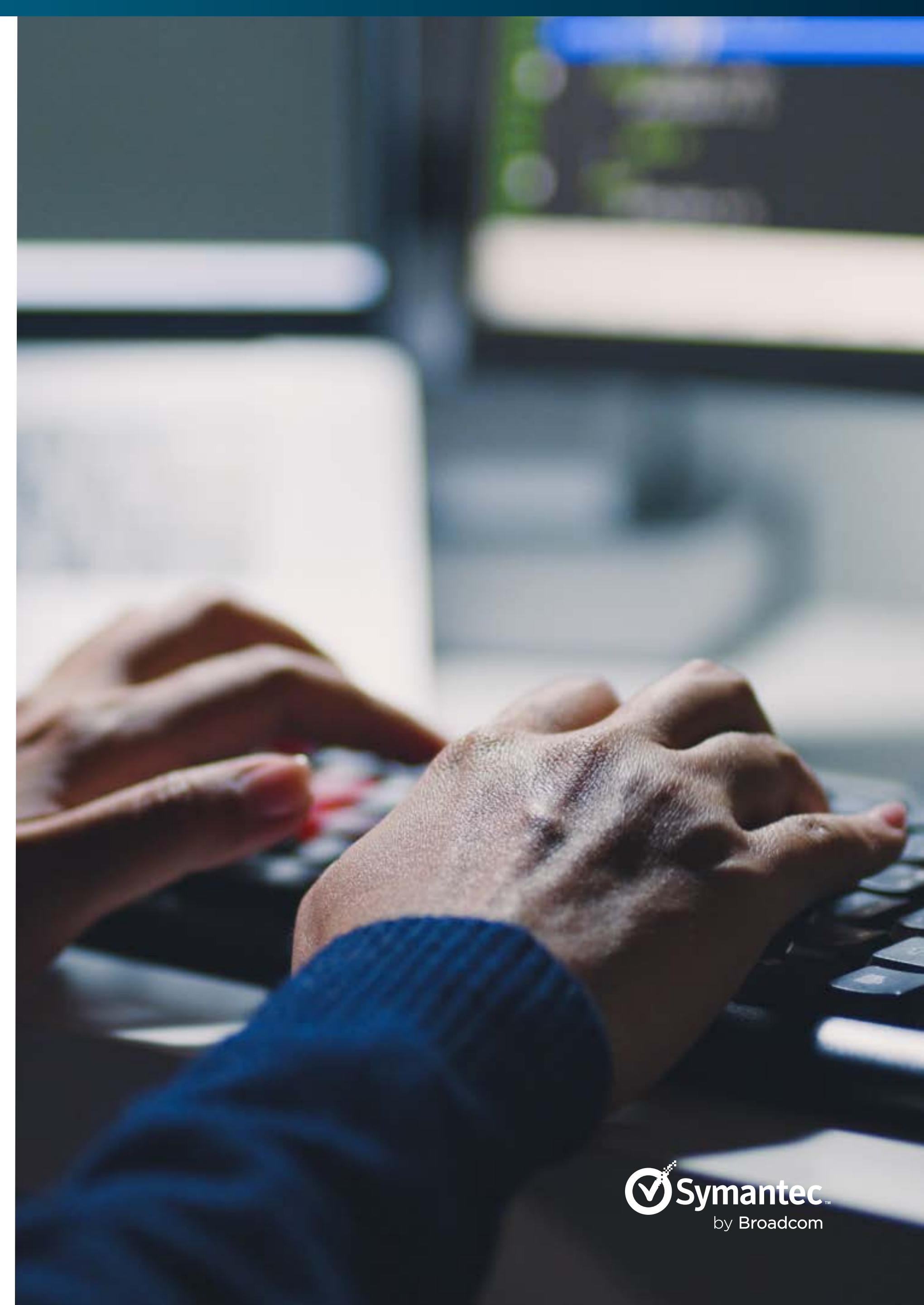
Attackers obsessively target endpoints as the fastest path into an organization's environment. From there, they enact multi-step tactics to move laterally across domains and avoid detection, wreaking havoc every step of the way.

Symantec CBX stops attackers in their tracks. Unlike traditional security tools that generate isolated alerts, CBX provides deep visibility into endpoint activity and automatically correlates that telemetry with network and data security events to reveal the full scope of an attack.

Leveraging Symantec's award-winning prevention capabilities and Carbon Black's pioneering EDR technology, CBX secures all your devices before attackers can make the jump.

USE CASES:

- Rapid incident response
- Proactive prevention
- Remote remediation
- Alert triage
- Attack visualization
- Threat hunting
- Forensic investigation



Fighting smarter beats fighting harder

The best defense continuously adapts

A core component of CBX's endpoint protection is Adaptive Protection. Rather than relying on static controls, Adaptive Protection uses AI and machine learning to establish a baseline of normal behavior across your environment. From there, it continuously identifies and blocks anomalous activity that may signal an attempted LOTL attack. Security teams can quickly reduce their attack surface and defend against emerging threats earlier without getting lost in thousands of alerts. That's the kind of proactive security your teams so rightfully deserve.

What if you could see four moves ahead?

Experienced analysts recognize attack patterns because they've seen them many times before. With Incident Prediction, CBX gives that same advantage to every team. Powered by AI models trained on 500,000+ real-world attack chains, Incident Prediction analyzes attacker behavior to predict their next four to five likely steps, giving security teams the power to stop them in their tracks. Instead of reacting after privilege escalation, lateral movement, or ransomware deployment, analysts can take decisive action sooner, cut down on attacker dwell time, and prevent small incidents from becoming major ones.

See into the whole attack chain with Threat Tracer

Most investigations start with a single alert and a lot of questions. How did the attacker get in? Where did they go? Did they reach any sensitive data? Threat Tracer helps analysts find answers faster by automatically bringing together all of the attacker's activity into a single, dynamic visual timeline of the attack path. Analysts can trace activity from initial access through lateral movement—and potential data exposure—without switching consoles or manually piecing together evidence. With attack visualizations and AI-driven insights, teams can quickly understand what happened, why, and what to do next.

Take the friction out of web security

With more employees shifting their work to browsers and SaaS applications, web traffic has quickly become the new frontline of cybersecurity. At the same time, risks like Shadow AI, SaaS sprawl, and careless user behavior create dangerous blind spots that many organizations struggle to monitor and control. To keep pace, organizations will need deeper visibility, especially around their web activity.

Symantec CBX protects the network domain by combining advanced detection and response with key capabilities from Symantec Cloud Secure Web Gateway (SWG) to identify malicious activity and block threats at the network

edge. Resource-constrained teams gain the clarity and control they need to proactively deflect malicious traffic before it can reach the endpoint. But prevention is only one part of the arsenal.

Unlike traditional environments that rely on API integrations and disconnected tools, CBX natively correlates endpoint, network, web, and data telemetry into a single pane view of attacker activity. With native web security telemetry built right in, analysts can easily see key intel during investigations like browser activity, web traffic, and application usages.

USE CASES:

Gain control over Shadow AI and SaaS

Achieve governance maturity and compliance

Secure your remote or hybrid workforce

Cut data noise without cutting visibility

With thousands of alerts flooding analysts every day, security teams are under growing pressure to protect data across its entire lifecycle. But the kind of visibility organizations need to keep up with AI-powered threats isn't always accessible.

Symantec CBX solves that, lowering the barrier to data protection and unlocking better security outcomes leadership can get behind. Incorporating industry-leading data security capabilities from Symantec Data Loss

Prevention (DLP), CBX extends visibility so teams can see what sensitive data was accessed, if it was exposed, and which users, systems, or locations were involved.

By correlating data security telemetry with endpoint and network activity, analysts gain a clearer understanding of the impact of an incident, without having to switch consoles or involve separate teams. CBX helps organizations ensure their sensitive data stays right where it belongs while simplifying compliance, privacy, and governance initiatives.

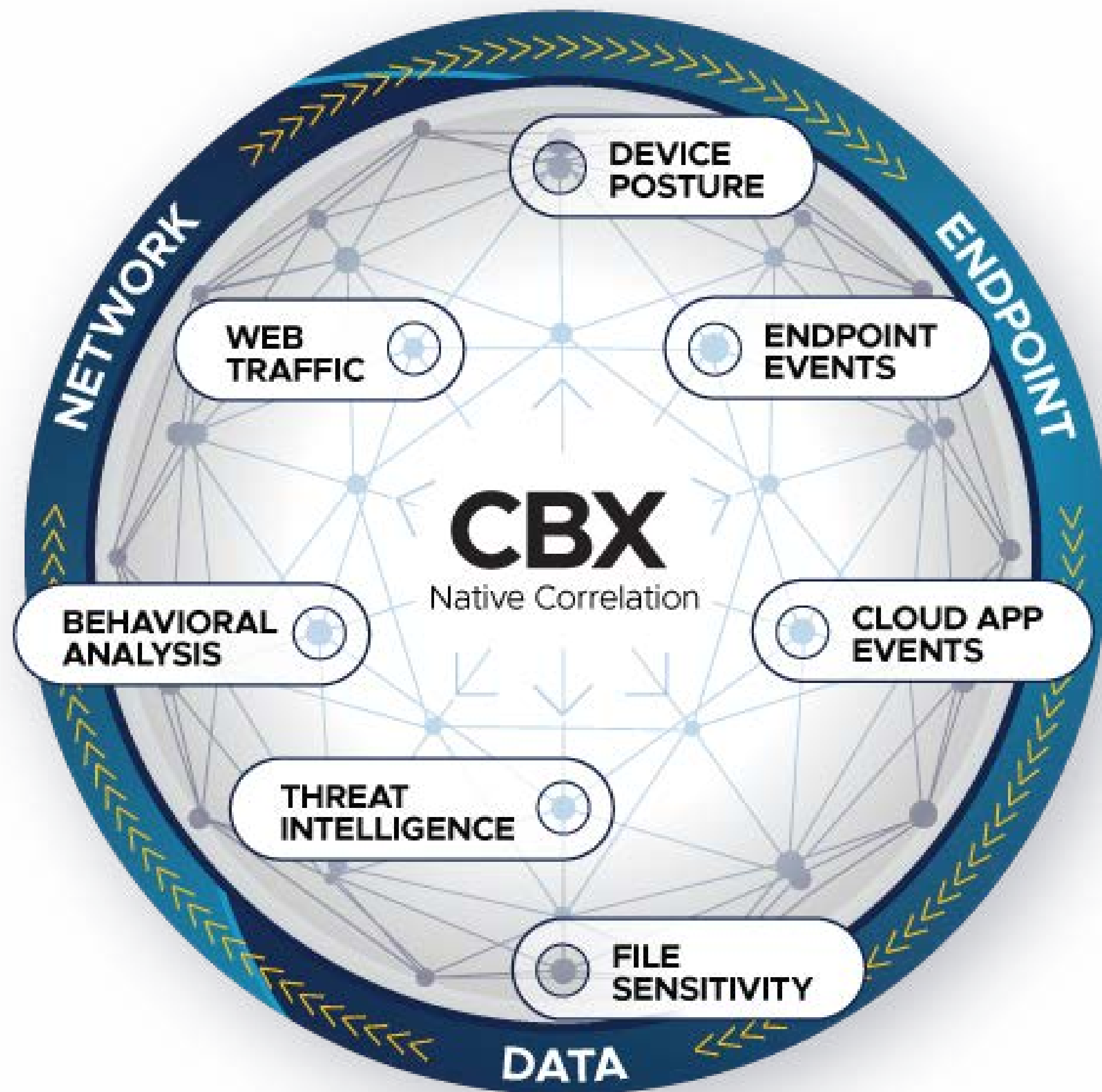
USE CASES:

Monitor data usage and movement

Streamline incident response

Prevent disastrous data leaks

Meet regulatory compliance



How CBX Works

STRONGER protection against breaches and data loss

SIMPLIFIED compliance and data privacy

FASTER detection and response

LOWER costs

GREATER efficiency

Enterprise-grade protection for all— without enterprise-level complexity

As bad actors and nation-state threats grow more opportunistic by the day, organizations of every size need access to security capabilities that will keep them safe. We designed Symantec CBX to give overwhelmed teams the clarity, visibility, and control they've been missing.

What enterprise-grade protection really means to us

What you need	How Symantec CBX gets you there
Threat prevention	AI-powered prevention, EDR, DLP, and network security work together to help stop attacks before they do damage
Faster incident response	Native telemetry correlation for clearer, actionable insights
Reduced alert fatigue	AI-driven summaries and unified visibility to cut straight through the noise and surface what matters
Optimized workflows	Centralized management and out-of-the-box configurations reduce operational burden
Simplified compliance	Built-in reporting and data privacy policies support current and emerging governance efforts
Lower overall costs	Reduces tool sprawl, manual integrations, and SIEM overhead
Bridge the talent gap	Guided remediation and AI-driven support help analysts of any experience level investigate and respond with confidence
Boost efficiency	Automates repetitive, time-consuming tasks, freeing analysts for more important matters
True resilience	Enterprise-grade protection across your entire ecosystem with security tools designed to work better together

Built for teams that don't want to fall behind

With AI-driven threats catapulting the current landscape into volatile territory, one thing is certain: Smaller organizations can't continue to rely on security through obscurity.

That's where Symantec CBX comes in.

Through cross-domain correlation and AI-powered capabilities, CBX helps teams connect the dots and see what is actually happening across their entire environment. Within seconds, massive volumes of security telemetry transform into actionable intelligence that any analyst can understand.

CBX gives organizations an advantage that has historically been reserved for the largest enterprises by giving security teams access to premium protections that were previously priced and configured beyond their reach. Uniting prevention, detection, and response capabilities under a single agent console, CBX simplifies resilience without sacrificing the level of protection today's threat landscape demands.

THE CBX ADVANTAGE

- See the full attack chain
 - Investigate faster with less effort
 - Reduce alert fatigue and burnout
 - Make confident decisions in seconds
 - Protect sensitive data across its lifecycle
 - Lower SIEM and operational costs
 - Empower your team to outpace attackers
 - Simplify compliance and governance
-

How Symantec CBX compares

	Symantec CBX	Other XDR Platforms
Endpoint visibility	✓	✓
Network visibility	✓	✓
Threat detection	✓	✓
AI-assisted investigations	✓	✓
Automated response actions	✓	✓
Attack visualization	✓	Varies by platform
AI-driven incident summaries	✓	Varies by platform
Incident Prediction	✓	
Cross-domain correlation across endpoints, network, and data	✓	
Secure Web Gateway (SWG) filtering	✓	Often separate
Data Loss Prevention (DLP) capabilities	✓	Often separate
Out-of-the-box deployment	✓	May require significant tuning
Single-agent console	✓	Varies by platform
Fast time to value	✓	Varies by platform
Reduced tool sprawl	✓	May rely on additional integrations
Simplified compliance & data privacy support	✓	May depends on additional solutions
Built for lean security teams, with scalability to enterprise level	✓	Usually optimized for larger SOCs

You told us what you need, and we listened

Fueled by the combined power of Symantec and Carbon Black, CBX was designed for the largest segment of the cybersecurity market: organizations with limited budgets, lean teams, and little to no room for error. As AI-powered attacks escalate the threat landscape, teams need more than another security platform. They need an advantage.

CBX delivers just that—with prevention, detection and response, network security, and data protection built to work better together—for security teams tired of fighting complexity at every turn.



Vendor Evaluation Checklist

Ask these questions before signing the dotted line

- | | | |
|--|--|---|
| ☐ Does it provide native telemetry across your entire environment? | ☐ Are AI capabilities designed to support analysts rather than replace them? | ☐ Is it practical for lean security teams with limited resources? |
| ☐ Can it correlate activity across domains without manual stitching? | ☐ Can investigations be completed from a single console? | ☐ Can junior analysts use it to easily investigate incidents and respond? |
| ☐ Does it include strong prevention capabilities, not just detection and response? | ☐ Does it help teams understand the business impact of an incident? | ☐ Does it accelerate time-to-value while lowering operational overhead? |
| ☐ Can analysts see the full attack chain from initial access to impact? | ☐ Does it support compliance, reporting, and data privacy initiatives? | ☐ Will it help your team become more resilient as threats continue to evolve? |
| ☐ Does it help reduce alert fatigue or add to your team's daily tasks? | ☐ Can it be deployed quickly without extensive customization or tuning? | |

If the answer isn't "yes" to most of these questions, it may be time to keep looking.

Explore XDR from the pioneers of EDR

Dive further into the capabilities that make Symantec CBX's unified visibility and prevention unmatched.

GET THE DETAILS

Watch it work firsthand in a [1:1 demo](#), guided by an in-region expert.

Or jump right in and [start your free trial](#).

It's time the odds tipped in your favor.



Copyright © 2026 Broadcom. All rights reserved.

The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries. For more information, go to www.broadcom.com. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies. Broadcom reserves the right to make changes without further notice to any products or data herein to improve reliability, function, or design. Information furnished by Broadcom is believed to be accurate and reliable. However, Broadcom does not assume any liability arising out of the application or use of this information, nor the application or use of any product or circuit described herein, neither does it convey any license under its patent rights nor the rights of others.
Item No: ebook_Buyers-Guide_20260930 9/26