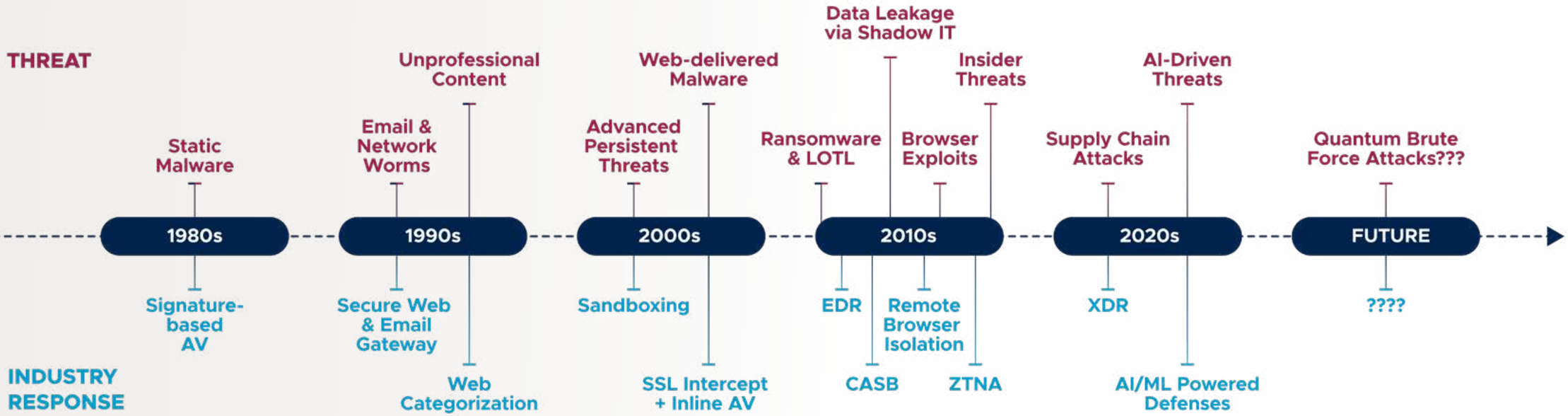

8 Ways AI is Easing Stress on the SOC
Symantec by Broadcom
Carbon Black. by Broadcom



AI: Friend or foe?

Some see artificial intelligence (AI) as a rapidly accelerating threat to organizations worldwide. They're not wrong. Others see AI as a boon to cyber defenses, and they too are correct. AI in cybersecurity is a double-edged sword. Equipping both attackers and defenders, the quest to deploy AI to each side's advantage has turned into an intense and relentless arms race of technology and talent. From automated phishing and malware generation on one side to intelligent, predictive protections on the other, AI is shaking up the way organizations approach their security.

Security vendors have spent decades developing defenses to protect against breakthrough threats (see graphic). And even before attackers began weaponizing AI, machine learning (ML) had already proven itself as a critical defensive tool. In fact, 97% of companies using ML reported tangible benefits in productivity, customer service, and human error reduction. ML's widespread adoption continues to lay the groundwork for today's rapid advancements in AI-driven cybersecurity.

AI and ML by the numbers

62%

of organizations identify ways machine learning can strengthen their security systems.

Source: Ponemon Institute

78%

of companies report using AI (up from 55% in 2023).

Source: Stanford HAI

A moving target

Whether being used to attack or defend, AI is evolving at a pace the industry has never seen before. With AI capability **doubling every seven months**, AI-enabled threats are shape-shifters, changing faster than many cybersecurity vendors can update traditional solutions. Without defenders themselves relying on AI, how can they possibly hope to keep up?

AI: From frontier to foundational

Not long ago, "AI in cybersecurity" was more tantalizing marketing buzz than bonafide protection. Eager to score an early market lead, some vendors rushed out basic GenAI-based chatbots and knowledge search functions as tools that could improve analyst productivity. While useful, these did little to actually fortify defenses and strengthen perimeters.

Fast forward to today, and AI has found its way into core cybersecurity capabilities to keep up with surging demands, increasingly sophisticated ransomware and advanced persistent threats (APTs). As attackers leverage AI to scale their operations or ease their entry into the ransomware business, nation-state sponsored threat actors are widening their targets, putting organizations of all sizes in the crosshairs.

Think AI is a new thing? *Think again.*

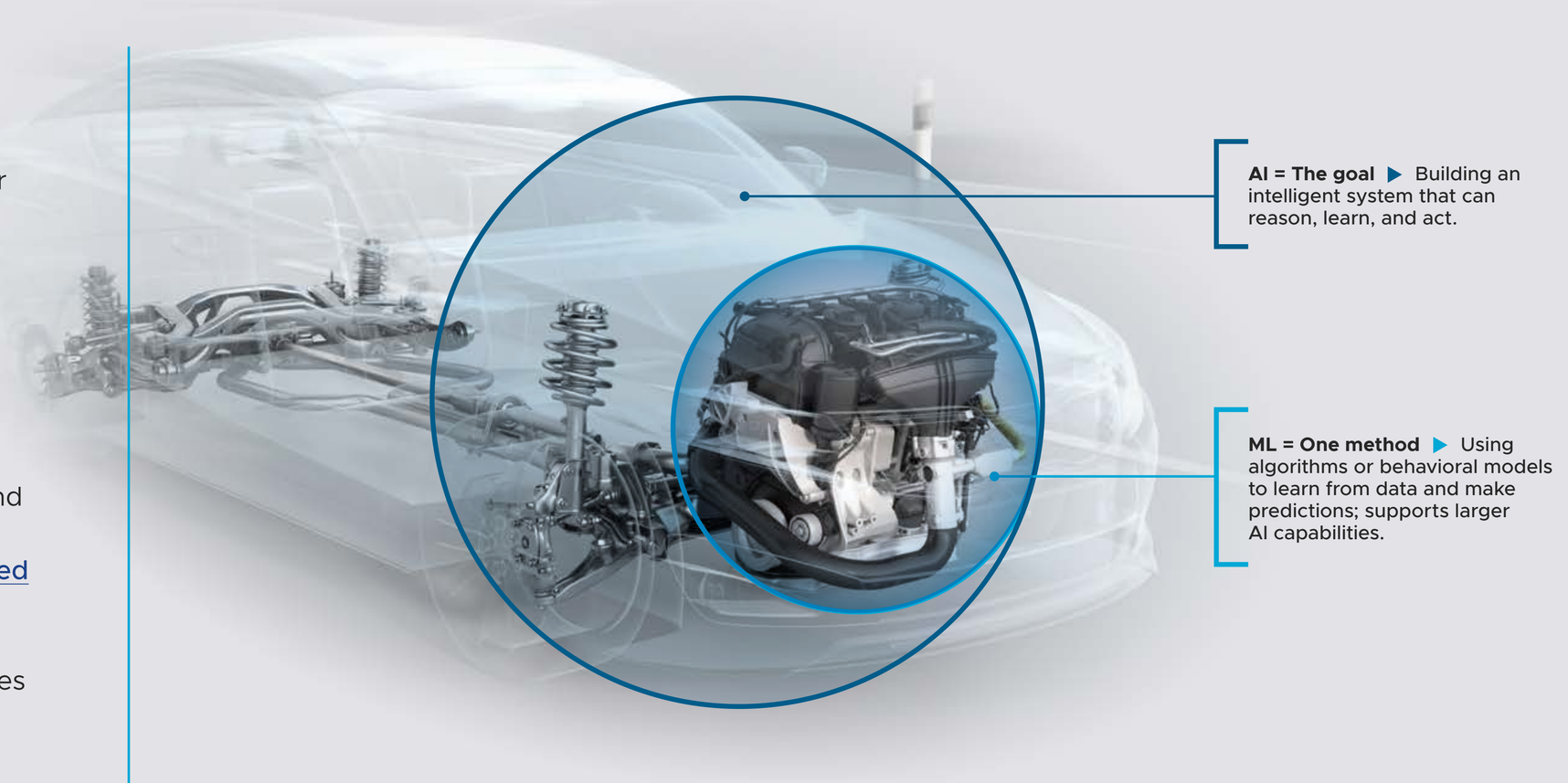
Symantec was founded back in 1982 to focus on AI and natural language processing (NLP).

Symantec by Broadcom Carbon Black. by Broadcom

AI's double edge is making it easier for adversaries to infiltrate new markets and cause millions in damages and downtime losses.

Our current reality is clear: AI-powered capabilities are becoming increasingly essential. While 94% of organizations have increased spending on products and services supporting data readiness for AI, only 21% have fully embedded AI into their operations. And these early adopters are already reaping the rewards. 84% of large companies are seeing returns on their AI and GenAI investments.

Hype aside, what do real AI defenses look like today? Let's take a closer look.



You Can't Have AI Without ML

Think of artificial intelligence (AI) as the vehicle we all interact with when we use machines that can think, learn, and act in ways that feel intelligent. In cybersecurity, that can look like real-time queries being answered as naturally as another SOC colleague might respond, or deep analysis that helps defenders forecast future paths in an attack chain.

Now let's zoom in. Machine learning (ML) is the engine that helps power the AI vehicle. It's a subset of AI that teaches computers how to spot patterns, learn from data and make decisions—without someone needing to spell out every step in code. That could mean automated threat summaries or models that contextualize and learn to block specific threats.

8 Ways AI is Transforming Cybersecurity

How AI is shaking up security

While attackers are using AI to sharpen their tactics and accelerate their path to profit, defenders are harnessing the same fundamental technologies with creative precision to gain speed and clarity in their quest to prevent, detect, and stop threats. Today's security vendors often use AI to uncover complex patterns, disrupt attacks in real time, and transform massive data streams into visual, actionable intelligence.

Read on to see how AI is already reshaping cybersecurity and helping even smaller security teams fortify their defenses against today's known foes and tomorrow's unknowns.

Predicting next stage attacks

Cybersecurity has a next move problem.

Attackers are exploiting a gap between detection and prediction. Every year more attackers are chaining together sophisticated tactics, techniques, and procedures (TTPs) to slip past perimeter defenses and infiltrate whole systems. When one of their tactics fails, they're quick to pivot, following step-by-step instructions from shared, affiliate playbooks that keep their attack chains moving. This makes it increasingly difficult to predict their next move. As a result, in 2024 alone, their persistence cost businesses an average of $4.4 million per breach.

See into likely futures with AI.

Typically, most defenses on the market detect and stop attackers and then tell you what they've done, not what they're planning on next. That's where AI comes in. By analyzing thousands of attack chains, AI can learn the playbook directly from the attackers. Leveraging behavioral analytics and intel from past incidents, it extends visibility into a new frontier.

Use AI-powered prediction to solve this next move problem.

Defenders can go beyond what's happening and take a peek at what's likely to happen next. With detailed foresight into their attacker's plans, they can raise the proper defenses, cut the right paths, and potentially save businesses millions. Foiling multi-step spearphishing, credential theft, and sophisticated ransomware attacks are no longer beyond the reach of defenders. Because when analysts are able to see the patterns behind the noise, the cycle is broken.

Predicting the next move

An attack rarely stops at first swing. For example, after a phishing email drops a beaconing agent, analysts might see it list shares and create a remote scheduled task. But Symantec's AI-powered feature, Incident Prediction, runs its actions through a catalog of 500,000+ real-world attack chains to predict the most likely steps. The results could look like this: credential theft (72%), privilege escalation (46%), or ransomware starting (19%). Instead of waiting for the next move, analysts can intervene before it's even executed.

2 Mapping the threat landscape

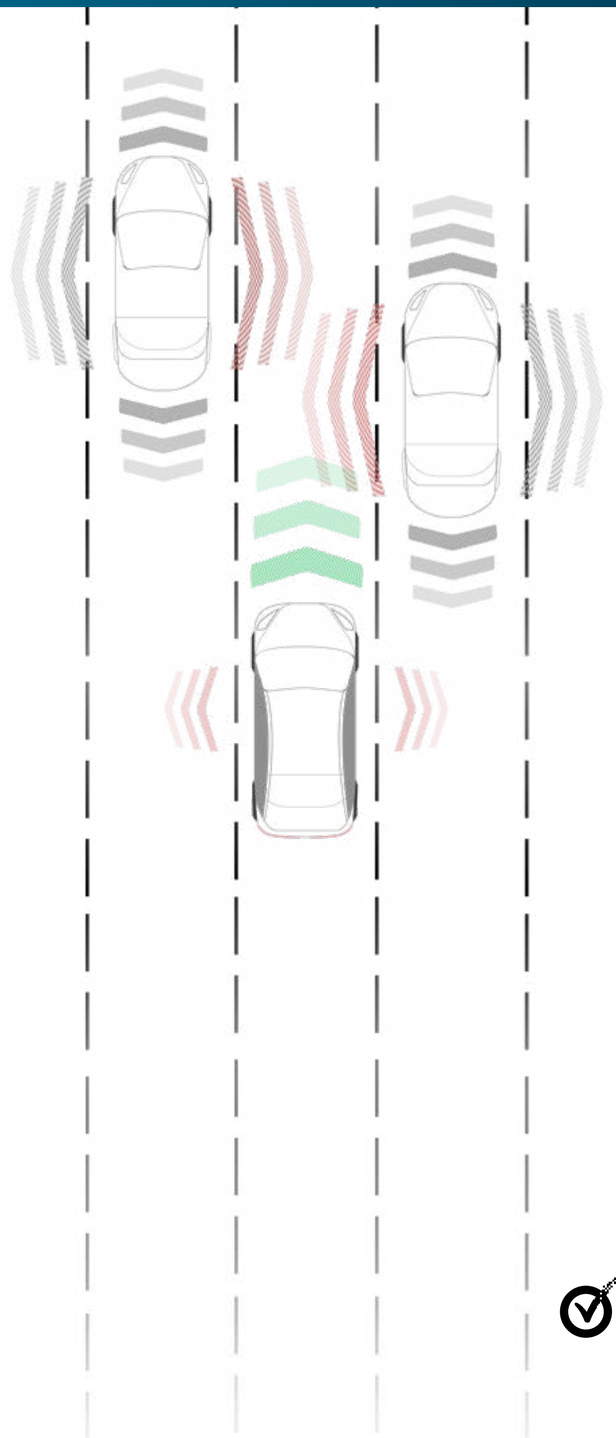
Once upon a time, threats were simpler.

Today, attackers leverage AI to sharpen their phishing lures, refine polymorphic codes, and better disguise activities. Meanwhile, analysts face hundreds of false alerts every day—wading through the noise like it's some exhausting, sisyphean challenge. Even when they do uncover the real threat, they're racing against the clock to gather enough context to remediate, with risk mounting by the second.

Let AI shoulder the boulder.

By marshalling numerous agents to respond to queries, AI assistants can tap into reputation databases, threat bulletins, blogs, intel APIs, and technical documentation in seconds. Agentic AI assistants can even automatically flag and prioritize alerts, leverage existing tools for threat containments, and identify security gaps. Precious time goes back on the clock for analysts while faster answers and smarter containment make their work a little easier.

> "With its AI technology, we're seeing a more reasonable number of alerts, and our false positive ratio has gone down significantly over the last three years as the tool continues to get better at being able to analyze and catalog threats, as well as alerting when required."
>
> — IT director, manufacturing, on Symantec Endpoint Security (SES) Complete



Turning alert fatigue into decisive, informed action

SymantecAI, an agentic AI component of Symantec Endpoint Security (SES) Complete and Symantec CBX, surfaces actionable insights and data from internal threat analysis tools. It analyzes a threat's behavior, breaks it down into plain language, and maps which existing defenses are best positioned to detect, block, and remove the threat. The result? Analysts move quickly and decisively when an attack is underway.

Symantec by Broadcom Carbon Black. by Broadcom

3 Illustrating attack paths

Go beyond traditional process trees.

Bad actors often operate from the shadows, making threat detection and response a complex challenge for resource-strapped SOC teams combing through alerts. Traditional security tools and process trees identify isolated indicators of compromise, but they fall short when it comes to mapping out the full scope and progression of an attack. That's left to defenders to figure out manually, slowing response time and remediation.

Rely on ML foundation for more insights.

ML has quietly powered processes in the background for years like Google's email spam filters or Microsoft's smart email threat detection. It's no surprise that the same ML principles and capabilities are now driving some of cybersecurity's most effective tools, analyzing vast streams of data to help humans connect the dots faster.

View the blast radius of an attack.

As defenders chase threats, they spiral 10 tabs deep into a dead end, struggling to recall how they got there in the first place. Fed by alerts curated and filtered by ML, Carbon Black Threat Tracer examines every entity related to an attack—files, parent processes, and impacted devices—and turns process trees into dynamic, actionable visualizations. Now, analysts can quickly grasp the extent of a threat and explore multiple angles, pivoting between processes and assets all in one window for a wider, comprehensive visual on everything happening in their systems.

Detect ▸ Correlate ▸ Visualize

WITHOUT Threat Tracer	WITH Threat Tracer
Unfiltered alerts muddy the contextual view of attacks.	ML filters and curates alerts so Threat Tracer can focus on what matters.
Isolated IOC and static process trees make it hard to see the full picture.	Real-time, ML-powered correlation across files, processes and devices reveals the complete attack chain in seconds.
Analysts have to dig through complex tools and multiple tabs to piece incidents together.	Dynamic visualization all under one unified, interactive view helps analysts connect the dots faster.
Handoffs between colleagues can be incomplete or complex, slowing investigations and limiting junior analysts' growth.	Able to log comments on every action, finding, or alert, analysts get comprehensive context for investigations, making collaborations smooth and easy.
As teams chase leads to try to map lateral movement, response is delayed and risk rises.	Instant clarity on the scope and impact of an attack speeds up containment and remediation.

4 Summarizing complex incidents

Analysts are drowning in a sea of false positives.

SOC teams spend too much time bailing out their boat. On average, one third (33%) of companies have responded late to cyber attacks because security teams were tied up investigating incidents that don't actually pose a threat. Still, they're locked in place until every alert is validated, especially the false ones. Meanwhile real threats are given time to move laterally across systems and escalate.

AI could be the SOC's lifeboat.

They know exactly what would help. One survey shows 39% of defenders believe AI and automation offer the best opportunity to improve response time. And they're not wrong. GenAI adoption has been associated with a 30% reduction in security incident mean time to resolution (MTTR). Analysts can expedite triage by allowing GenAI to sift through all the variables and produce an incident summary they can flick through in seconds. Comprehensive insights are available at the click of a button, saving defenders precious time they can put to better use hunting threats.

Cutting through false starts

Both Symantec Endpoint Security (SES) Complete and Symantec CBX deliver instant. AI-generated incident summaries that help analysts cut through false positives (FPs). This capability quickly surfaces and distills the details of an attack, providing a clear, easily understood narrative in seconds.

Each summary outlines the attack chain, suspicious commands, behaviors and even recommended next steps, enabling analysts to assess the urgency and scope of an attack at a glance. With actionable insights right on their dashboards, teams have more time for critical thinking and mitigating the potential impact of an otherwise unmanaged incident.

5 Analyzing sandbox scripts

Sifting through scripts is old news.

Attackers know defenders can't block critical tools like Powershell, which is why scripts have long been a perfect cover for malicious inactivity and living off the land (LOTL) attacks. Traditional sandboxes run those scripts in safe environments, but they usually stop short of explaining why the behavior is dangerous or how it fits into a larger attack chain. That means analysts have to run through logs, trying to decipher the intent behind the attack while burning up time that puts them a step behind bad actors.

Understand how ML and AI strengthen one another.

With ML, analysts can automatically identify the nature of a script and leverage GenAI to narrate its behavior. As ML surfaces these patterns and their relevance, AI hands it to analysts in plain language. This gives teams a clear description of a script's intent and context within seconds—more of what they need to make faster, well-informed decisions.

Reimagining the sandbox with AI

Symantec Cloud Sandbox makes itself adaptive—feeding context back into your defenses rather than just keeping attacks isolated in a box. Whether it's a Powershell script disabling defenses or a Python code escalating privileges, this clarity and precision strengthen sandbox verdicts, taking raw data and turning it into actionable insights. Symantec Cloud Sandbox guides analysts toward quicker, smarter responses before threats can spread further inside the network.

> "It's the difference between operating in the dark in a house that you kind of were familiar with. Whereas with Carbon Black, the lights are on all day and all night. We can go to exactly what we want to see and wherever we want to see it."
>
> — Cyberdefense team leader, financial services

6 Detecting suspicious patterns

A bad actor's dream is an admin's worst nightmare.

There's been an undeniable uptick in LOTL techniques used by ransomware groups since 2021, with well over half employing LOTL attacks. These attackers exploit trusted, essential tools—like Powershell, VMI, PSExec, AnyDesk, and even native Windows processes—as cover for malicious activity. Because system administrators depend on these tools to keep things running, they become the perfect camouflage.

> "Based on the alert information we get from SES Complete, we have developed an automated response system based on criticality. There's a 30% to 40% reduction in the MTTR for known threats and exploits."
>
> — Cybersecurity manager, financial services

Flag threats with precision.

Without clear visibility, it's nearly impossible to distinguish routine operations from hostile intent. That's where behavioral analytics steps in. When ML powers the analytics engine, it continuously learns from an organization's day-to-day behavioral data. Once it knows the environment, it can identify anomalies and pinpoint the combinations that don't fit the norm.

Get your SOC team's peace back.

Beyond spotting anomalies and learning what "normal" looks like across an organization, ML gives analysts behavioral insight they can turn into tangible advantages. By detecting and stopping any abnormal activity quietly and efficiently, SOC teams can focus on higher-value targets instead of chasing after false positives.

When normal is anything but

LOTL techniques aren't going anywhere, but detective capabilities like Adaptive Protection—found in Symantec Endpoint Security (SES) Complete and Symantec CBX—make sure your essential tools can't be misused in plain sight. Routine operations continue without disruption, while its granular security model and powerful global threat telemetry flag suspicious behaviors and block them before attackers can blend in.

That means the next time Powershell launches at 3:00 AM on a server that rarely sees activity at that hour, it'll be instantly flagged. And over time, Adaptive Protection becomes even more precise, automatically blocking abnormal usage of tools while letting legitimate tasks continue. Admins are free to run their tools, attackers lose their precious cover, and organizations effortlessly shrink their attack surface—all while reducing the amount of alerts plaguing their SOC teams.

7 Correlating telemetry across domains

More tools doesn't always mean stronger security.

Fragmented tools may promise more coverage, but they often create more visibility gaps, preventing analysts from seeing the full picture. Worse yet, smaller security teams—already short on time and resources—rely on a patchwork of integrations, only to end up with overwhelming volumes of data that are much too difficult to correlate and interpret. Sure, some tools may try to bridge the gaps with API integrations, but they're often incomplete. Analysts may know something is happening but they won't always know what it is—or what to even do about it. Instead of adding costly layers, organizations of any size can benefit from AI-driven telemetry correlation.

A united front across endpoints, networks, and data.

Rather than forcing analysts to manually piece together disparate telemetry, AI can identify correlations that might otherwise go unnoticed, especially by fatigued or less experienced teams. Combined with cloud native telemetry, these insights can surface deeper context and visibility across the attack surface. Analysts can finally prioritize more precise threat hunting and decisive response. Freed from log-centric ingestion and fragmented data pipelines, security teams gain clearer detections, regaining confidence in their defenses and skills. (They might even be able to reduce their reliance on costly SIEM platforms.)

Shift left and stop attacks sooner

Symantec CBX, the unified XDR platform from Symantec and Carbon Black, helps security teams improve performance and reduce friction by simplifying operations with a single management console and cross-domain native telemetry. By correlating endpoint process activity, network connection logs, and DLP content inspections, CBX allows teams to "shift left" and stop attacks sooner while also gaining the full picture faster than is possible with standard endpoint or SIEM solutions. This breadth of context helps analysts identify the correlations that matter, reducing alert fatigue, speeding time to resolution, and lowering SIEM and operational costs. And for leaner teams, out-of-the-box policy configurations make it easier to rapidly achieve measurable security outcomes.

8 Upskilling SOC teams

Cybersecurity professionals are a precious resource.

With the World Economic Forum estimating a global shortage of 4 million practitioners and pressures mounting in the SOC, cybersecurity personnel are stretched thin every day trying to keep up with escalating attacks, emerging regulations, and expanding responsibilities.

For junior analysts, keeping up is especially rough. In an industry that demands speed and adaptability, massive datasets, complex tools, and high volumes of false positives all combine to stall their growth. Collaborations within the SOC start to break down and remediation slows while the talent gap only widens.

> "We had a ransomware attack two weeks after I joined the team. It was all hands on deck (15 of us working together) for 16 hours a day for a month to remediate and fully resume operations. We have not had another incident like that since starting to use Carbon Black."
>
> — Information security administrator, call center services

Ease the burden across the whole SOC

Closing the cybersecurity skills gap is essential for SOCs of every size. Symantec and Carbon Black help organizations upskill teams without compromising protection. Purpose-built for under-resourced, overstretched SOCs, Symantec CBX unifies endpoint, network, and data telemetry to simplify operations while delivering enterprise grade security. By leveraging proven AI, the cloud-based XDR platform equips smaller teams to surface threats faster, stop attacks sooner, prioritize response, and act confidently without having to manage disconnected tools. Meanwhile, SymantecAI Security Assistant, available in Symantec Endpoint Security (SES) Complete and Symantec CBX, allows analysts to ask questions freely and receive immediate, contextual explanations of scripts and activity.

1 in 4 companies report adopting AI due to labor or skills shortages.

67% of organizations report a moderate-to-critical cybersecurity skills gap.

Source: World Economic Forum

	How Do AI-Powered Features Benefit SOC Teams?				
	Visibility	Time Savings	Response Speed	Response Effectiveness	Upskilling
Incident Prediction	✓	✓	✓	✓	
Threat context	✓	✓	✓	✓	✓
Adaptive Protection (Anomaly detection)	✓	✓	✓	✓	
Incident summaries	✓	✓	✓	✓	✓
Threat Tracer (Attack visualization)	✓	✓	✓	✓	✓
Secure sandboxing		✓	✓	✓	
Cross-domain telemetry correlation	✓	✓	✓	✓	✓
Natural language processing (SOC team upskill)		✓	✓	✓	✓

Outpace AI-Powered Threats with AI-Powered Protections

Across every industry, organizations are investing in AI to strengthen defenses and accelerate threat response. But the playing field cuts both ways. Bad actors are just as quick to weaponize AI, lowering the bar to entry and enabling complex multi-stage attacks that are trickier to detect and even harder to predict.

In this fast-moving environment, relying on fragmented or outdated security stacks isn't always advisable. Building resilience means choosing trusted, proven solutions that reinforce the core pillars of cybersecurity while staying ahead of emerging regulations and the continuous threat of more complex, advanced attacks.

It’s not just about keeping up.

At Symantec and Carbon Black, we’re not interested in our customers just keeping pace—we want defenders to stay well ahead of impending threats. Backed by one of the most aggressive R&D engines in the industry, our future-ready and AI-powered innovations like Incident Prediction, Adaptive Protection, and Incident Summaries redefine what it means to stay ahead of the curve. By blending prevention, detection, analysis, and response—supercharged with AI—our combined portfolio fortifies your defenses and empowers your teams to make smarter, more precise decisions.

Proactive, comprehensive defenses like Symantec Endpoint Security (SES) Complete, Symantec CBX, and and Carbon Black Cloud give your SOC the tactical advantage they need to predict, outmaneuver, and contain attacks before bad actors even get a chance to pivot. With Adaptive Protection, actionable incident summaries, and AI-driven insights into an attacker’s most likely moves, your defenses are sharpened into a cohesive, battle-ready force.

Can you measure the ROI of AI-powered security? How does 180% sound?

Adaptive Protection, an AI-powered feature of Symantec Endpoint Security Complete (SESC), automatically flags deviations and blocks malicious behaviors. In studying the results over three years of a composite organization representing the results of actual SESC customers, the number of security alerts requiring manual response dropped by 20% and the composite organization was able to respond 33% faster. Meanwhile, the composite organization saw a total three-year return of 180% on its investment in SESC.

Forrester Total Economic Impact™ of SES Complete, a study commissioned by Broadcom

Symantec Endpoint Security Complete

80% reduction in likelihood of a breach caused by an external attack, an attack on remote networks, or an internal incident.

33% reduction in time to investigate each security alert.

$561K in annual security solution costs avoided.

Source: Forrester Total Economic Impact™ of SES Complete, a study commissioned by Broadcom

Carbon Black

Return on investment (ROI) **427%**

Reduction in risk of a large-scale data breach with Carbon Black. **40%**

MTTR reduction for iinvestigation of security incidents by Year 3. **GROSS: 75%** **NET: 75%**

Source: Forrester Total Economic Impact™ of Carbon Black, a study commissioned by Broadcom

Symantec by Broadcom

Carbon Black. by Broadcom

SAY HELLO TO Symantec CBX

Threats may be growing more complex and volatile, but that doesn't mean modern security has to be. That's why we built Symantec CBX, the first unified XDR platform combining award-winning capabilities from both Symantec and Carbon Black, to give resource-strapped security teams a simpler, clearer path to reliable security.

With cross-domain telemetry from endpoints, networks, and data, CBX helps teams move beyond disconnected alerts to total visibility—a full view of an attacker's activity that can help prevent attacks before they do damage. By including AI-powered capabilities, CBX delivers something long overdue: enterprise-grade prevention, detection, and response in a unified platform designed to reduce complexity and strengthen resilience.

The AI powering Symantec CBX

Capabilities	Function	Outcomes
Cross-Domain Telemetry Correlation	Links activity across endpoints, networks, and data to surface insights	Total visibility, preventing attacks before they do damage and facilitating investigations
Threat Tracer	Maps attacker activity across environments in a single view	Faster investigations and clearer attack timelines
Incident Summaries	Explains incidents and remediation steps	Automated executive summaries inform decision-making and streamline response
Adaptive Protection	Detects and stops anomalous use of legitimate software	Blocks living-off-the-land (LOTL) attacks
Incident Prediction	Forecasts an attacker's likely next four moves	Strengthens defenses by stopping lateral movement of attacks in progress

Symantec by Broadcom

Symantec by Broadcom

Carbon Black. by Broadcom

Item No: ebook_8WaysAI_v8 4/26