SentinelOne
Secure Tomorrow™

Strengthening Security Operations with Data and AI

The Value of a Unified Approach to Cybersecurity

eBook

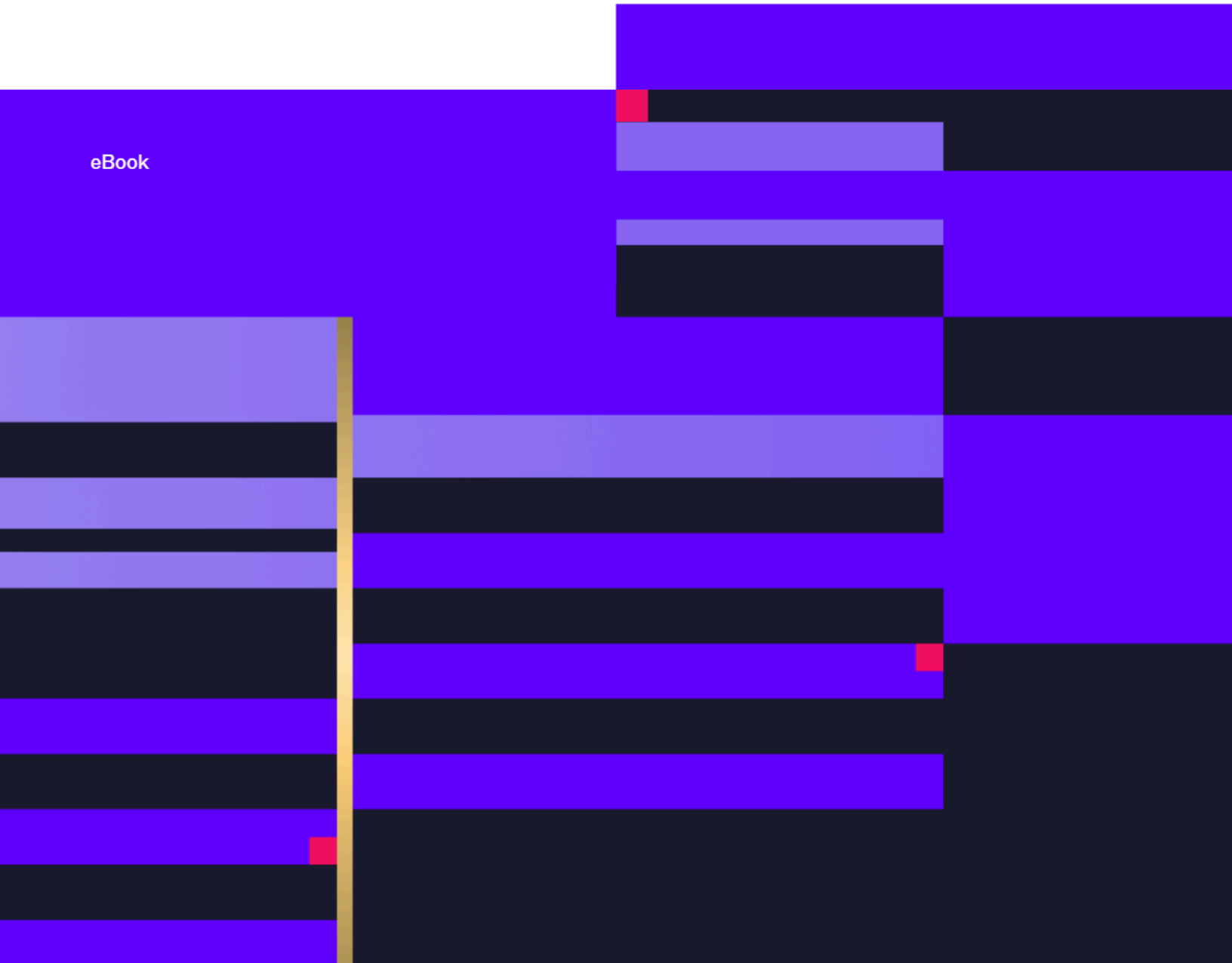


Table of Contents

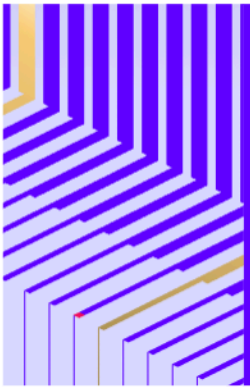
Generative AI Brings Data to Life and Elevates the Expertise of Security Professionals

If your security data could talk, what would it say? With generative AI, this question isn't rhetorical. While AI is making waves across all industries, its transformative potential is especially clear in security.

When it comes to cybersecurity, generative AI must be more than just a chatbot. Combining the analytical prowess of traditional AI with an ability to learn and create, **generative AI use cases are helping organizations detect, respond, and resolve threats faster and more effectively than ever before** while using the same resources. In fact, The Ponemon Institute found that advanced generative AI models are well positioned to analyze complex systems, such as network infrastructures or software applications, to identify vulnerabilities, detect novel threats, and mitigate risks.[1]

Generative AI does this not by replacing cybersecurity teams, but by enhancing their capabilities. It transforms how teams operate by taking on tedious tasks and accelerating critical ones to help people focus on the work only a human can do. **Users can converse with AI in natural language through a simple interface as if they had a security analyst sitting next to them,** helping security professionals of all levels—from new employees to the experts—get the critical insights they need in near-real time. It accomplishes this by quickly sifting through vast amounts of data, recognizing patterns and identifying threats at machine speed, and continuously learning over time.

As such, some of the most promising applications we see today center around threat identification and investigation. Generative AI can be a powerful force in reducing alert fatigue, for example. One study found that AI capably handled an average of 51% of alerts without human supervision.[1] Similarly, sifting through data to find threats is typically time-consuming for humans, but with generative AI, querying happens much faster. AI can guide users through investigations by translating natural language into complex queries, auto-generating threat summaries, suggesting related queries, and more. With help from AI, it's possible for teams to analyze vast amounts of security data from diverse environments in minutes instead of hours, saving time in situations when every second counts.



63% of IT professionals see cybersecurity as the area of greatest potential for generative AI[2]

51% of security alerts can be handled by AI without human supervision[1]

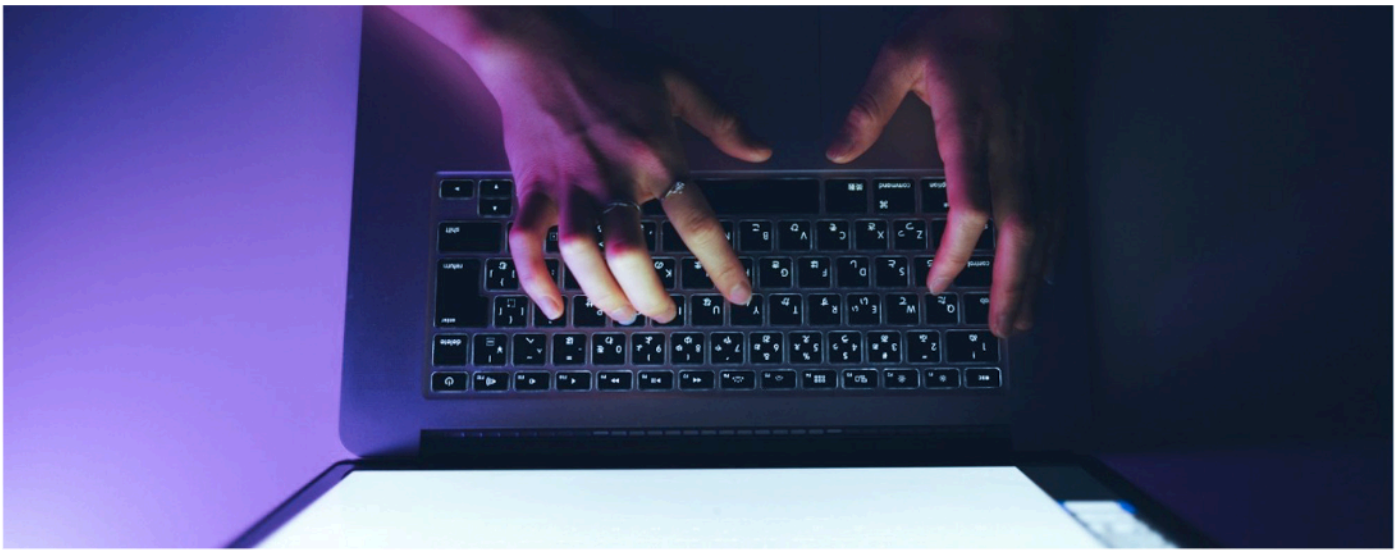
50% of organizations report their security posture has improved by adopting AI for cybersecurity[1]

69% of organizations believe that they cannot respond to cyber threats without AI[3]

[1] The State of AI in Cybersecurity Report. The Ponemon Institute and MixMode, 2024

[2] Using generative AI to strengthen cybersecurity. KPMG, 2023

[3] The Real-World Impact of AI on Cybersecurity Professionals. ISC2, 2024



In the Wrong Hands, Generative AI is Equally Disruptive

Attackers see the power of generative AI, too—and they're exploiting it to become faster and more effective

Many types of cyberattacks look familiar because strategies that work stick around. But make no mistake, attackers are always innovating, and like many of us, **they see the value generative AI holds to evolve their tactics.** From lowering the barrier of entry to cybercrime to using data to find vulnerabilities in software, generative AI is making attacks more destructive, efficient, and harder to detect. In fact, the National Cyber Security Centre (NCSC) in the United Kingdom reports that all types of cyber threat actors—state and non-state, skilled and less skilled—are already using AI to varying degrees in their attacks.[1]

Take phishing, for example. Hackers are using WormGPT, a nefarious offshoot of OpenAI's ChatGPT, to write more convincing phishing messages without telltale grammatical errors, eliciting users to disclose sensitive information.[2] Threat actors are also using generative AI to generate malicious code that can exploit vulnerabilities in security systems, helping them gain access to sensitive data and remain undetected for periods of time. Unfortunately, these use cases are just the tip of the iceberg. The rise of the ransomware-as-a-service (RaaS) model[3] has created a black market where sophisticated, AI-driven tools are sold at scale. This has lowered the barrier to entry for threat actors and opened the door to further innovation and greater damage in the future. That is, if attackers are left unchecked.

The best defense is to beat them at their own game

Though the threat posed by AI in the wrong hands is real, current trends suggest that AI favors defenders. The NCSC also reports that the impact of AI on cyber threats will be offset by the use of AI to enhance cybersecurity resilience through better detection and improved security by design.[1] Generative AI can help provide meaningful insights into threat prioritization by identifying vulnerabilities and assessing the impact of potential threats—much in the way a malicious actor might use it, albeit for good.

[1] The Impact of AI on Cyberthreats. National Cyber Security Centre, 2024

[2] WormGPT – The Generative AI Tool Cybercriminals Are Using to... SlashNext.com, 2023

[3] The Good, the Bad, and the Ugly in Cybersecurity. Week 15. SentinelOne, 2024

Data is the Fuel that Powers AI Security Operations

Harnessing AI for cybersecurity starts with data

To effectively combat threats, generative AI models need data.

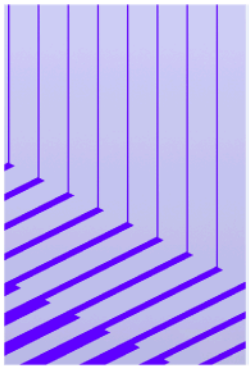
Without enough useable, high-quality data, AI algorithms may lack the baseline information required to offer informed recommendations and actionable insights. They may even provide inaccurate or biased results—reducing their efficacy with potentially harmful outcomes.

AI-ready security operations require a shift in data strategy and a unified data estate

Providing generative AI and traditional AI models with the data they need to be accurate and performant requires organizations to establish a single foundation of high-quality, standardized data. But getting there can be challenging for numerous reasons:

- Organizations often have **multiple data lakes** using different schemas, data formats, data governance practices, and more
- They may be storing **massive volumes of data** that require a significant investment to bring together
- They use **disparate tools or solutions that don't integrate** with one another, creating data, product, and workflow siloes
- They may not have **the resources** needed to unify a data estate, such as talent or capital

What's needed is a holistic approach to data and AI—an approach that accounts for everything from the data sources, to the AI models, to the process of surfacing insights to the security team while keep costs manageable. It's time to move away from a siloed approach to data, solutions, and workflows.



Regulatory pressures complicate efforts to unify data

Regulatory pressures are increasing, with new security and compliance regulations released every year. In fact, the SEC brought **over 50 cyber-related enforcement actions** in 2023.[1]

Navigating these requirements is challenging, and it only becomes more expensive and cumbersome as organizations archive data for compliance purposes and create more data siloes, further complicating efforts to create a unified data estate.

[1] Newfront Cyber Update: New Cyber Rules Coming into Force in 2024. Newfront, 2024

A Unified Platform Approach is Essential to Fully Leveraging Data and AI—and Reducing Risk

Maximize the value of data and enter the era of AI

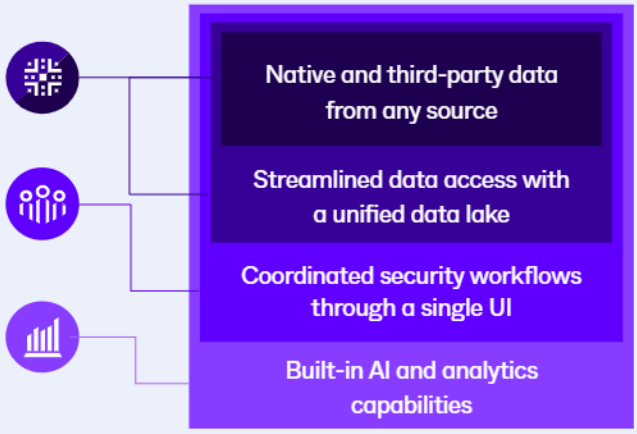
So, how do you harness security data and use it to fuel generative AI for better security operations? The answer is a unified platform approach to cybersecurity. This approach provides the foundational infrastructure for managing, analyzing, and leveraging an organization's data assets effectively. But a unified approach does more than just organize data—it enables better, more holistic visibility into the threat intelligence lifecycle, from detection and investigation to response and beyond. By consolidating tools and processes, a unified platform makes it easier to automate tasks with AI and surface more meaningful insights to the humans on security teams. This reduces costs and effort while also enhancing an organization's overall security posture and mitigating risk.

More than meets the UI: The elements of a unified platform approach

But what exactly do we mean by a "unified platform approach"? At the most fundamental level, a unified approach is a comprehensive and fully integrated platform that consolidates security solutions into a **single back-end data estate and front-end user interface (UI).**

It's always evolving to keep pace with new kinds of threats, and **it's extensible** to accommodate cutting-edge approaches to protection. A unified approach has the following qualities:

- Improves access to information by making it easier and faster to get insights with a **unified data foundation** that includes all of an organization's data
- Streamlines the user experience by enabling **coordinated security workflows** across capabilities, increasing the speed and efficacy of security teams
- Includes a built-in **analytics and AI layer** that supercharges security teams and enables future innovation



Let's take a closer look at these qualities and how they unlock value for security operations, starting with a unified data foundation.

Bolster Security Operations with Easily Accessible, High-Quality Data

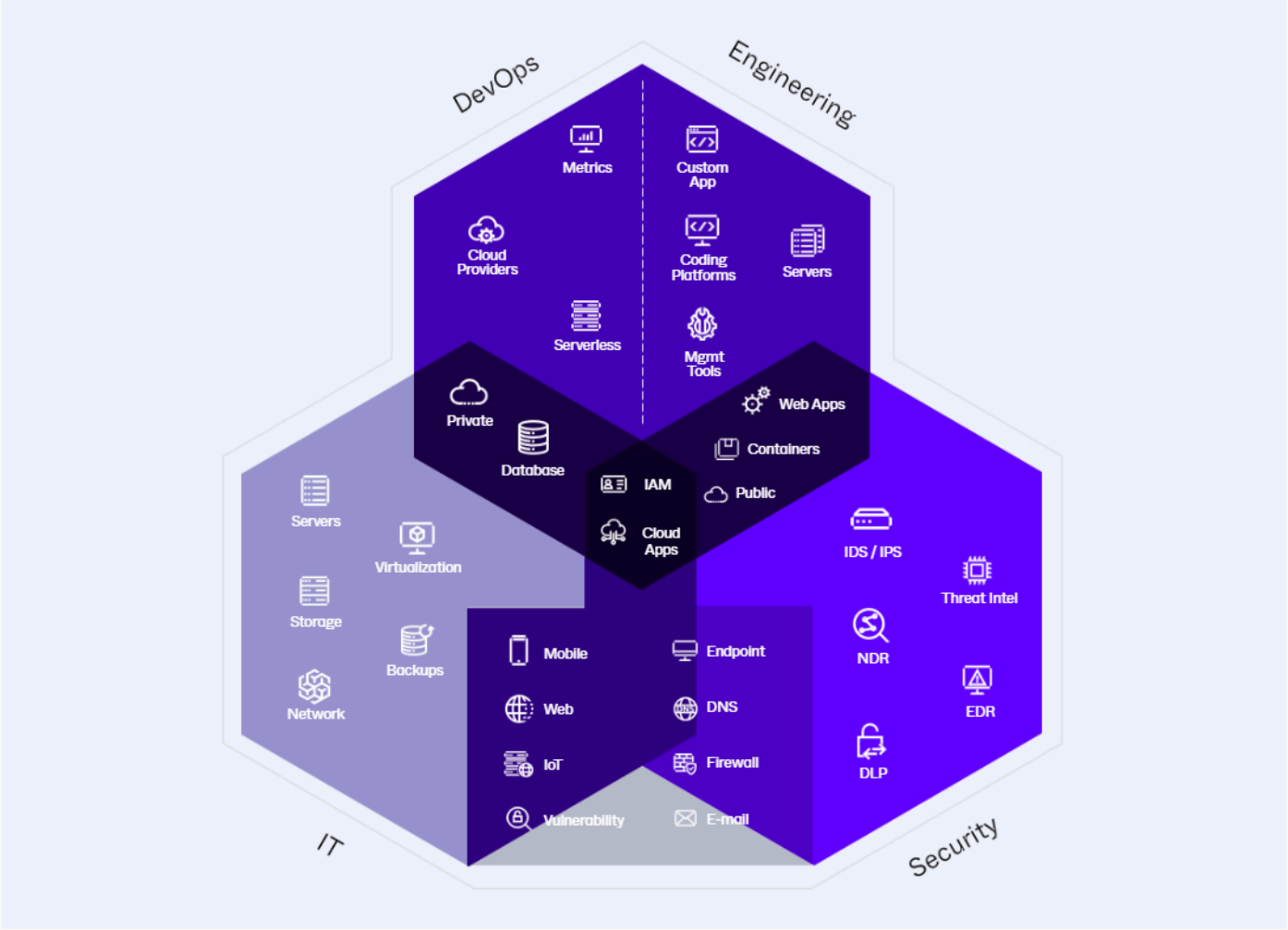
A unified data lake enables applications to contextualize and share native and third-party data

Many vendors claim to have a "unified platform," but in reality, they're offering disparate solutions connected by a UI. Others offer a suite of products that leverage multiple different data lakes. The problem with these "platforms" is that they're no more than a centralized user interface—**to be truly effective, applications must share data and context on the backend as well.** That's why a unified data lake is key.

A **unified data lake** gives surfaces across environments a single repository from which to draw and deposit data. The hallmark of a strong data lake is that it ingests, stores, and manages both first- and third-party data, including all logs and forensics, while remaining manageable and cost-effective.

By centralizing data in a single location, teams can search across all ingested data to find insights faster, reducing mean-time-to-detection (MTTD) and mean-time-to-respond (MTTR). A unified data lake also reduces storage costs by eliminating the need for multiple lakes.

For generative AI specifically, a single lake increases models' breadth of visibility and the scope of data that can be queried. With a richer pool of information to draw from, models improve their decision-making process and provide more accurate and insightful outputs.



A Strong Data Strategy Goes Beyond Collecting Data

Streamline access with open cybersecurity data standards and data portability

Beyond data aggregation, a unified data lake includes **connectors and parsers that normalize and contextualize data** from applications into a common framework to avoid redundancy and reduce storage costs. Ideally, this framework is built on open standards, such as the Open Cybersecurity Schema Framework (OCSF), to improve interoperability now and in the future. Open standards greatly speed threat detection, analysis, and response while reducing workloads for cybersecurity teams, because teams don't need to spend time compiling and standardizing data and instead can focus on proactive security enhancements. Open standards also enable **data portability,** so that organizations can adopt more security tools as needed and ensure business continuity with the seamless migration of data.

Simplify data querying and retrieval while controlling storage costs

A true unified data lake supports a **unified query language** to promote interoperability between systems while simplifying data access for users. With a unified query language, analysts don't have to struggle to learn and use multiple syntaxes across different data sources and systems, saving them time and reducing opportunity for errors. When a unified query language is paired AI models that support open standards like OCSF, the possibilities of AI expand. AI improves the speed and efficiency of security operations by querying, leveraging, and assessing native and third-party data in a normalized way.

Finally, a unified data lake also facilitates efficient data retrieval for faster incident response and streamlined investigations. It does this by enabling **integration and communication between disparate data sources,** as well as through **column-based storage.** With column-based storage, data is stored for each column separately, making retrieval and querying much faster. When paired with **cloud-native architecture and multi-tenant design,** this approach enables scale as organizations evolve.

Did you know? Open standards are gaining momentum

Open standards, specifically OCSF, are emerging as a global trend,[1] and for good reason. As many organizations find themselves adopting more security tools to keep pace with threats, open standards are needed to ensure that these tools can communicate with one another and operate to their fullest extent.

Currently, vendor-specific proprietary standards cause applications to operate in data siloes. Not only does it create more work for security teams as they spend time integrating tools, but it also inhibits the efficacy of security solutions due to insight bottlenecks.

OCSF enables the integration of these systems while preserving their confidentiality and integrity, helping businesses to adjust quickly to evolving threats and ensure their future tools—regardless of vendor—can be integrated as needed. It saves time for security teams, because they no longer need to compile and standardize data from multiple entries to collect meaningful insights. What's more is that the benefit of open standards is vast—developers can build on each other's work, paving the way for industry-wide innovation.

[1] The 2023 State of Open Standards. The Linux Foundation, 2023.

Improve the Analyst Experience with Coordinated Security Workflows and Real-Time Analytics

Disjointed workflows are a security liability

Ideally, security teams spend their time mitigating risk and taking a proactive stance against threats. The reality is, navigating complex workflows creates inefficiencies. Current cybersecurity workflows are often disjointed because organizations use a variety of disconnected tools and processes for tasks like threat detection, incident response, and vulnerability management. This can lead to gaps in visibility and coordination, which at best means slower response times and wasted resources. At worst, it means a costly breach that has serious implications for an organization.

A centralized console eliminates the need to "swivel" between security tools

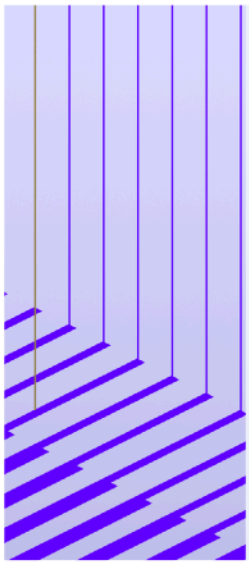
By enabling teams to access tools from a single user interface, a platform approach **improves visibility and ease-of-use.** With a centralized management and operational console, security teams spend less time navigating between multiple tools and processes. This console serves as a hub for managing policies, monitoring events, and orchestrating incident response activities, helping them better understand their entire environment. And with the right level of customizability, analysts can work in the way that's best for them.

Boost foundational capabilities while priming security operations for the future

One of the most powerful benefits of a unified platform approach is that it **boosts speed without sacrificing efficacy.** Using capabilities like XDR is easier and more effective through a single UI, so security teams can quickly access the information they need. With integrated AI and analytics, a unified platform helps users analyze threat intelligence feeds from various sources and enrich security telemetry with contextual information about known threats. AI applies detection logic and analytics to all of an organization's data faster than humanly possible, saving teams time and enabling them to cover more ground than before.

Finally, a unified approach creates an **extensible foundation for the future.** Extensibility enables organizations to easily incorporate new first-party and third-party solutions—even if they're using legacy systems—to help scale and combat evolving threats. This allows for adoption of the latest innovations in cybersecurity while maintaining interoperability and compatibility with existing tools and processes.

Mitigate Risk with a Generative AI Layer that Accelerates Security Operations for the Entire Team



What's the difference? Demystifying common AI terms

Artificial Intelligence (AI)
Systems that use advanced analysis and logic to mimic intelligent behaviors, including understanding artifacts/language, producing new artifacts/language, and toking or automating actions.

Machine Learning (ML)
Class of algorithms whose behavior changes based on the data given.

Generative AI
Subset of highly-scaled ML models that can learn from a representation of artifacts, and when prompted, can generate new related artifacts.

Large Language Models (LLMs)
Type of generative AI models trained on large volumes of text to understand text inputs and generate human-like text outputs.

Generative AI puts real-time insights and automated capabilities at analysts' fingertips

A conventional approach to cybersecurity data analysis often results in processing time lags of hours or more, making it ineffective against the swift pace of sophisticated threats. Building **generative AI solutions on top of a unified platform bridges the response gap by reducing processing time and enabling near real-time analysis of data.** This not only improves the efficiency of cybersecurity activities, but it also provides a comprehensive view of an organization's security posture.

An AI and analytics layer breathes life into a data estate by turning it into a teammate

The power of generative AI and analytics lies in their ability to bring data to life. To start, generative AI enables security teams to interact with data in **natural language** as if they had an additional expert on their team. This has major implications for users of all skillsets—for junior analysts, it uplevels their abilities because they no longer need to spend time learning and refining queries in a specific language but instead can query data conversationally. Similarly, senior analysts can rely on generative AI to write queries, freeing up time for tasks that only they can do.

Generative AI also **streamlines threat detection and investigation** by applying detection logic and analytics to data. Acting as a sentry, it can generate real-time insights across surfaces that might signal an attack, such as spikes in network activity. It also **reduces alert fatigue** by advising teams on which threats to prioritize with guided recommendations, and it can speed the resolution of alerts by triggering automated workflows, like integrations to ticketing systems. It's ever-vigilant, running auto-investigations in the background to truly reduce the monitoring burden for all teams.

Finally, it's a powerful **threat response tool.** When applying policies, generative AI enables one-click migration actions and orchestration integrations for customized, automated playbook responses. When a threat is resolved, it also offers auto-summaries, so users don't have to spend time documenting their findings.

Altogether, a Unified Platform Approach Enables Powerful Generative AI Use Cases and Helps Security Teams Scale

A unified platform with generative AI doesn't just reduce workloads without sacrificing protection—it redefines what's possible in cybersecurity

We're seeing numerous transformative use cases enabled by a unified platform plus generative AI, and because AI will only improve over time, there's still much more to come. Today, the most impactful use cases we're encountering are:

AI-powered anomaly detection across third-party log sources

AI provides powerful detection capabilities that automatically detect anomalies from events across connected log sources. If an organization connects logs from third-party sources to be ingested into their unified data lake, AI will identify potential security threats, such as a possibly hijacked account detected from events in suspicious geolocations.

Automated alert triage and global similarity analysis

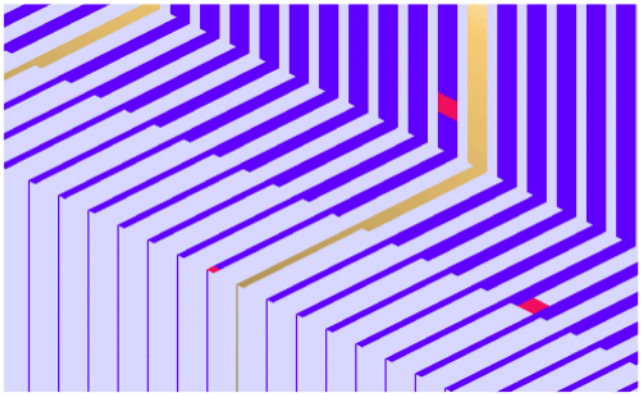
AI automates the process of triaging alerts by analyzing trillions of anonymized data signals on a global scale to identify similar alerts and understand how analysts have responded to them. For example, when an analyst reviews an alert, they'll see that "93% of alerts like these" were marked True Positive, therefore also making the AI's verdict True Positive. Analysts can also see that "32 alerts like these are open" in their environment, helping them make efficient, evidence-based decisions on the optimal response. AI will then learn from analysts' responses to continually improve its similarity analysis and recommended verdicts.

AI-powered response and hyperautomation suggestions to put response on autopilot

AI suggests intelligent mitigation actions to reduce MTTR and drastically scale protections. Analysts will see a recommendation for each alert based on common responses to similar alerts. They can apply that action to all similar open alerts in their environment or create a hyperautomation rule that will automatically act on them for any new similar alert.

24/7 auto-investigations to shift security in the favor of defenders

After auto-triaging an alert and determining whether it needs further investigation, AI will automatically run the investigation steps, review logs, and collect evidence—all in an easily digestible view for analysts. With auto-investigations, security teams can skip labor-intensive investigative work and instead focus on reviewing the results of AI's already completed investigations.



Stay a Step Ahead of Current and Future Threats with Trusted Cybersecurity Partners

Of course, it's not all about technology

Experienced partners play an essential role in helping organizations bring cybersecurity strategies to life. The best partners have both a clear vision for the future of cybersecurity and the capabilities to deliver on that promise. When looking for a strong partner to help implement a unified platform approach that includes AI, make sure they offer the following:

- A clear **vision for cybersecurity** that's aligned to your business's top strategies and priorities
- The expertise to provide **managed detection and response and proactive planning services**
- **Cloud native SaaS management** for high-scale requirements
- **Flexible, on-premises management** to meet customers' specific, unique needs
- A willingness to **help customers build the connectors** they need to adopt the platform
- A commitment to addressing **emerging regulations,** such as for AI or data privacy, to ensure the tools they build and maintain will remain compliant
- An adherence to **data privacy.** Providers that train their solutions on customer data, such as security information, processes, and insights, may not have high standards for data privacy

Confidently Enter the Era of Data and AI-Driven Cybersecurity with SentinelOne

More capability. Less complexity. That's SentinelOne.

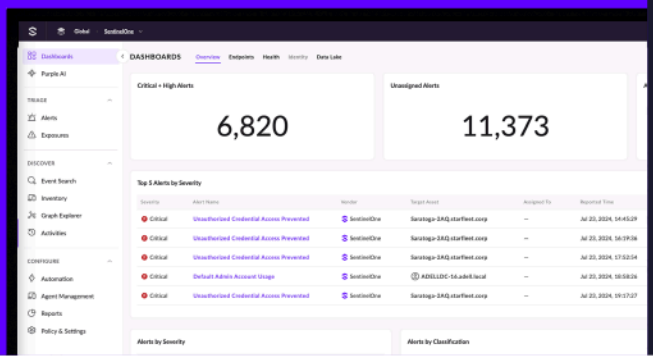
With the leading security AI platform, SentinelOne is uniquely positioned to help organizations harness the power of data and AI for frictionless defense. Learn more about our unified approach with the following resources.

- Visit SentinelOne.com to see how we're defining the future of cybersecurity
- Read our Singularity Platform webpage for details about the world's most advanced cybersecurity platform
- Learn how our Singularity Data Lake can centralize and transform your data into near-real-time intelligence
- Discover the power of Purple AI, the world's most advanced AI-powered security analyst

Ready for a Demo?

Visit the SentinelOne website for more details, or give us a call at +1-855-868-3733

sentinelone.com



Innovative. Trusted. Recognized.

Gartner

A Leader in the 2023 Magic Quadrant™ for Endpoint Protection Platforms

MITRE ENGENUITY

Record Breaking ATTACK Evaluation

+ 100% Protection. 100% Detection
+ Top Analytic Coverage, 3 Years Running
+ 100% Real-time with Zero Delays

Gartner Peer Insights.

96% of Gartner Peer Insights™ EDR Reviewers Recommend SentinelOne Singularity

FedRAMP · TEVORA PCI DSS Attestation HIPAA Attestation · AICPA SOC · STAR LEVEL ONE · 100 VIRUS · SE Labs BEST Innovator WINNER 2021 · Trusted Cloud Provider CSA

SentinelOne
Secure Tomorrow™

Contact us

sales@sentinelone.com
+1-855-868-3733

sentinelone.com

About SentinelOne

SentinelOne (NYSE:S) is pioneering autonomous cybersecurity to prevent, detect, and respond to cyber attacks faster and with higher accuracy than ever before. Our Singularity XDR platform protects and empowers leading global enterprises with real-time visibility into attack surfaces, cross-platform correlation, and AI-powered response. Achieve more capability with less complexity.

SentinelOne Data and AI eBook 2024 08 02_08072024