AI: The Good, The Bad and The Opportunity

Solutions Guide

AI: The Good, The Bad and The Opportunity

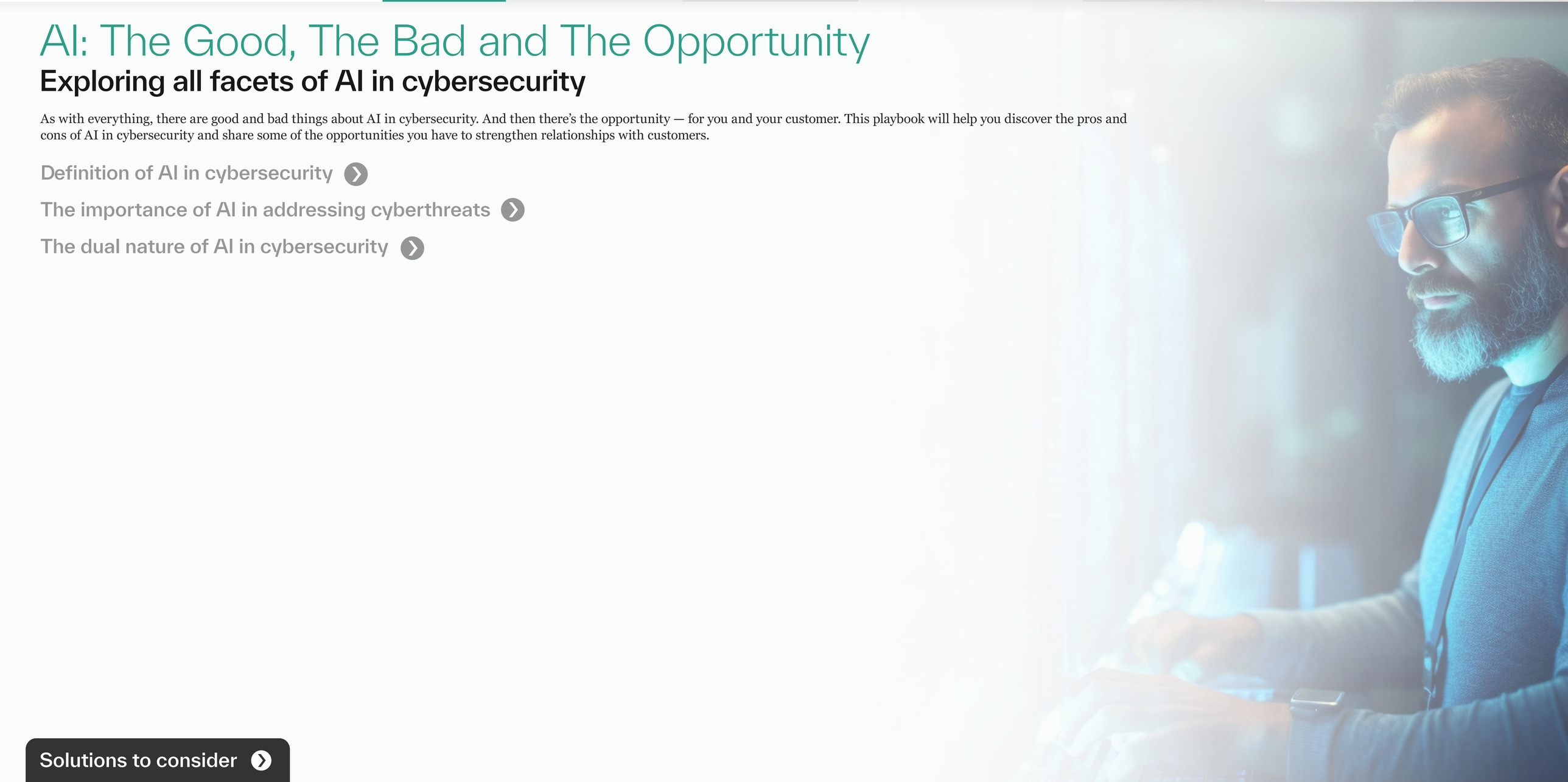
Exploring all facets of AI in cybersecurity

As with everything, there are good and bad things about AI in cybersecurity. And then there's the opportunity — for you and your customer. This playbook will help you discover the pros and cons of AI in cybersecurity and share some of the opportunities you have to strengthen relationships with customers.

Definition of AI in cybersecurity ›

The importance of AI in addressing cyberthreats ›

The dual nature of AI in cybersecurity ›



Solutions to consider ›

AI: The Good, The Bad and The Opportunity

Exploring all facets of AI in cybersecurity

As with everything, there are good and bad things about AI in cybersecurity. And then there's the opportunity — for you and your customer. This playbook will help you discover the pros and cons of AI in cybersecurity and share some of the opportunities you have to strengthen relationships with customers.

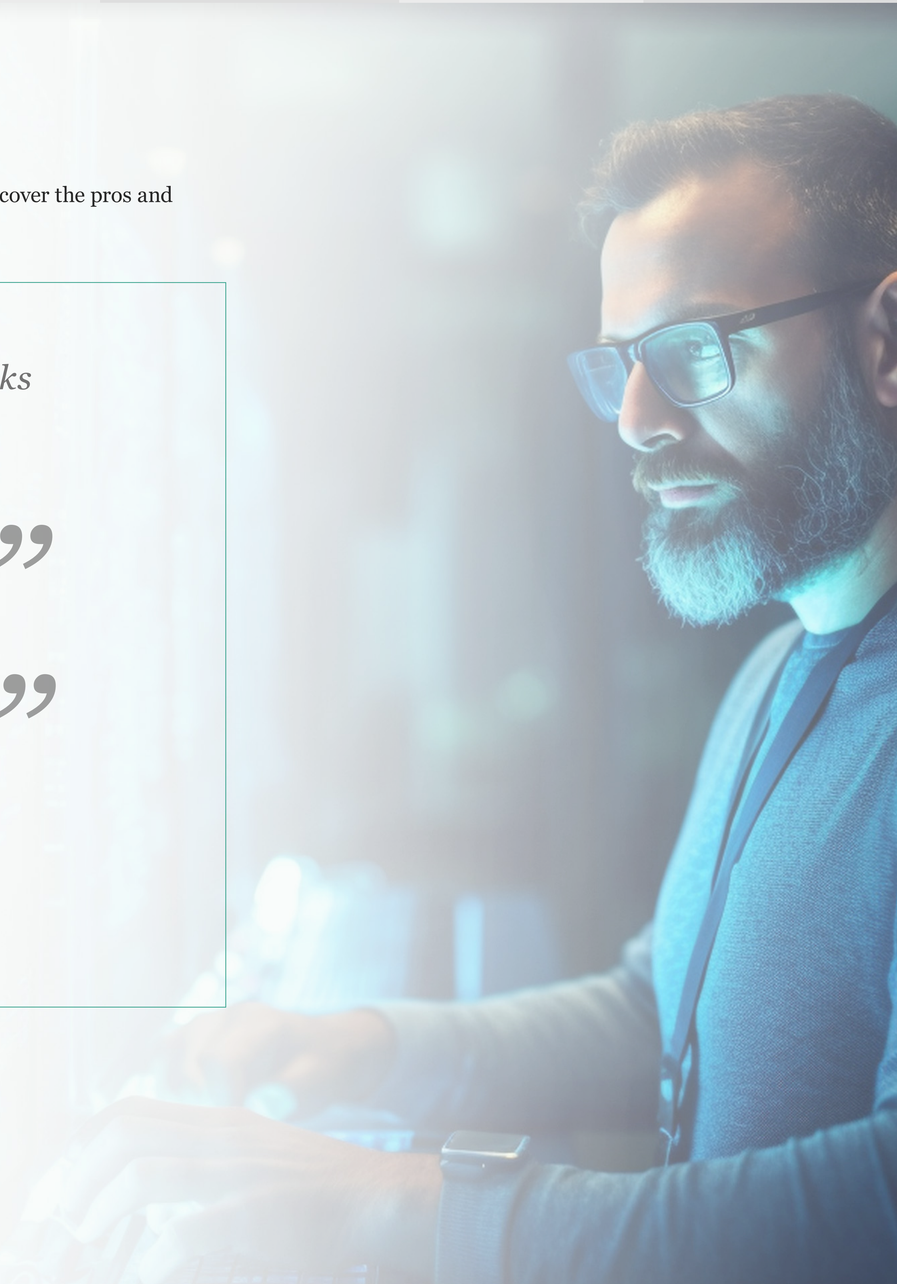
Definition of AI in cybersecurity

> *"Artificial intelligence (AI) is used in cybersecurity to help organizations protect their networks from cyberthreats and unauthorized access. AI can monitor, analyze, detect, and respond to cyberthreats in real time. It can also automate tasks that are repetitive and tedious for security analysts to complete, freeing up time and resources for more complex tasks.[1]"*

> *"Simply put.... AI is the application of applied statistics to solve cybersecurity problems.[2]"*

While AI is the bright shiny thing, inherent in this definition is data:

> *"The key to enabling outcomes in security is not about the AI; it is about the data ... data is the enabling infrastructure for security AI.[2]"*



The importance of AI in addressing cyberthreats

The dual nature of AI in cybersecurity

Solutions to consider

AI: The Good, The Bad and The Opportunity

Exploring all facets of AI in cybersecurity

As with everything, there are good and bad things about AI in cybersecurity. And then there's the opportunity — for you and your customer. This playbook will help you discover the pros and cons of AI in cybersecurity and share some of the opportunities you have to strengthen relationships with customers.

Definition of AI in cybersecurity

The importance of AI in addressing cyberthreats

In terms of data, AI offers an important ability to "separate the wheat from the chaff." For example, it can quickly break down and triage hundreds of alerts coming in at once — data that would be impossible for humans to process at machine speed. It can then prioritize alerts for immediate action and automate responses for routine alerts.

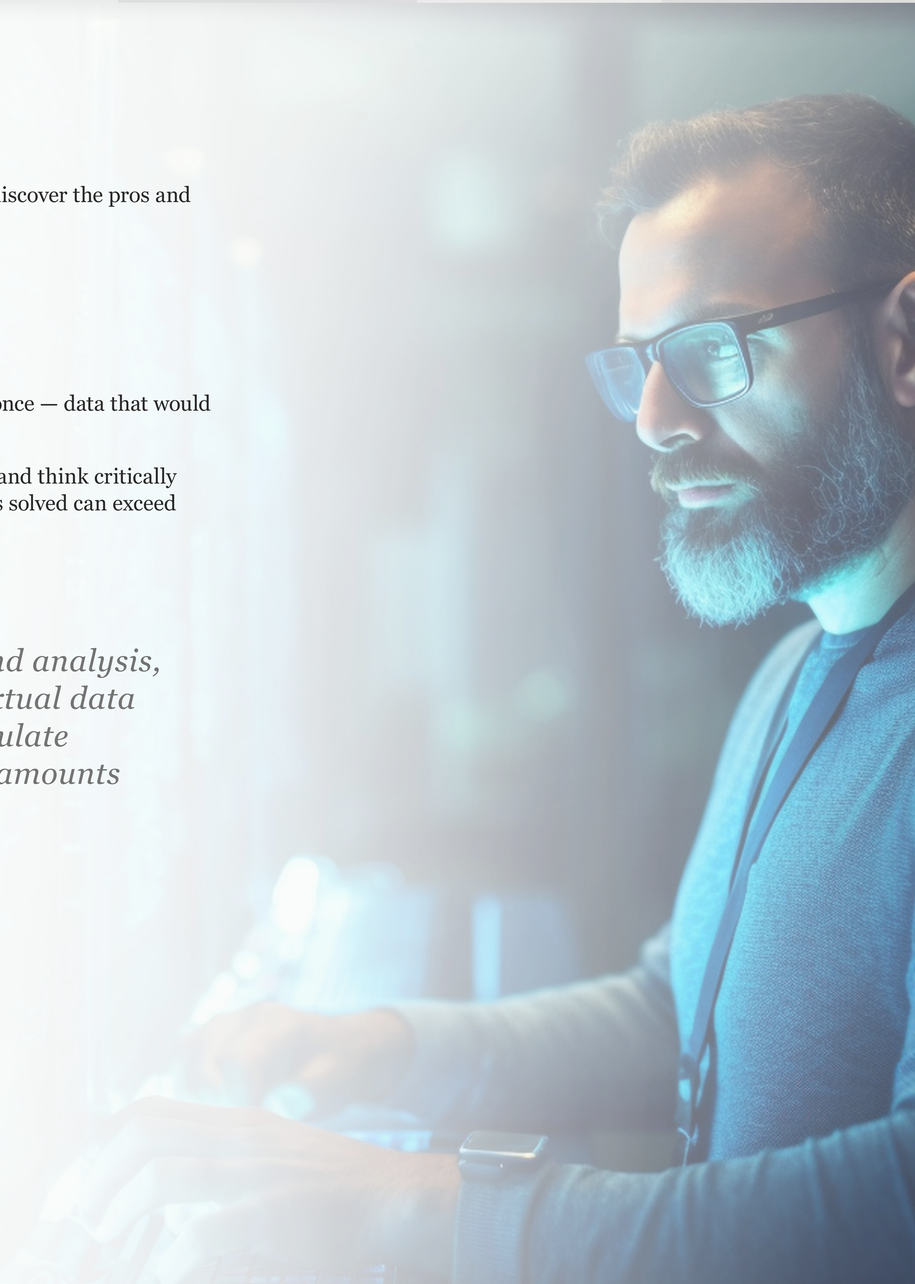
This does not mean that AI replaces human expertise. While AI is based on inarguable data, security analysts bring interpretative data to the party — they parse context and think critically and ethically — and can marry those skills with AI's capabilities. As IDC puts it: "The reality is that the scale of machine learning has grown to such a point that problems solved can exceed what a single person can pattern match in a lifetime or even a thousand lifetimes."[2]

As your customer's best advocate, your goal is to ensure that their networks and data are protected. IDC lays out the goals clearly:

> *"Using large amounts of structured and unstructured data, content analytics, information discovery, and analysis, as well as numerous other infrastructure technologies, AI-enabled security platforms use deep contextual data processing to answer questions, provide recommendations and direction, hypothesize, and formulate possible answers based on available evidence. The models are trained through the ingestion of vast amounts of content and automatically adapt and learn from their mistakes."*

That said, AI can be a double-edged sword.

The dual nature of AI in cybersecurity



Solutions to consider

AI: The Good, The Bad and The Opportunity

Exploring all facets of AI in cybersecurity

As with everything, there are good and bad things about AI in cybersecurity. And then there's the opportunity — for you and your customer. This playbook will help you discover the pros and cons of AI in cybersecurity and share some of the opportunities you have to strengthen relationships with customers.

Definition of AI in cybersecurity

The importance of AI in addressing cyberthreats

The dual nature of AI in cybersecurity

At the same time that AI is being used by the "good guys" to quickly identify and prevent threats, it's also being used by the "bad guys" to not only automate more advanced threats but also to revive publicly known threats, such as those on the Common Vulnerabilities and Exposures (CVEs) list, and reimagining them on a wider scale.

Essentially, AI is the dual-edged sword: one side attacks, the other defends.

The ease of AI makes it a much more accessible tool with which to create and launch attacks. In other words, just about anyone can do it. For example, the more enterprising bad guys are not only launching advanced attacks, but they're also serving as "mentors" by expanding their business models to offer subscription services and sell bundled "quick start" kits for aspiring bad actors. Here are some other ways that bad actors are using AI:[3]

1. **Automated attacks:** Automated attacks make it easier for them to target multiple systems simultaneously, while making it harder for defenders to detect and respond to the attack.
2. **Targeted attacks:** Targeted attacks can identify vulnerabilities in specific systems and exploit them, opening the door to exposure of sensitive information or assets.
3. **Social engineering:** AI-powered chatbots can generate fake news or social media posts that spread malware, manipulate public opinion, or trick users into divulging sensitive information.
4. **Evading detection:** AI can help bad guys bypass traditional cybersecurity tools or generate new, more difficult-to-detect malware variants.
5. **"Gain of function" malware:** AI can help bad guys create malware capable of learning and evolving, making it more challenging to preempt — or make malware "more effective" or harder to detect by adapting to changes in the environment.

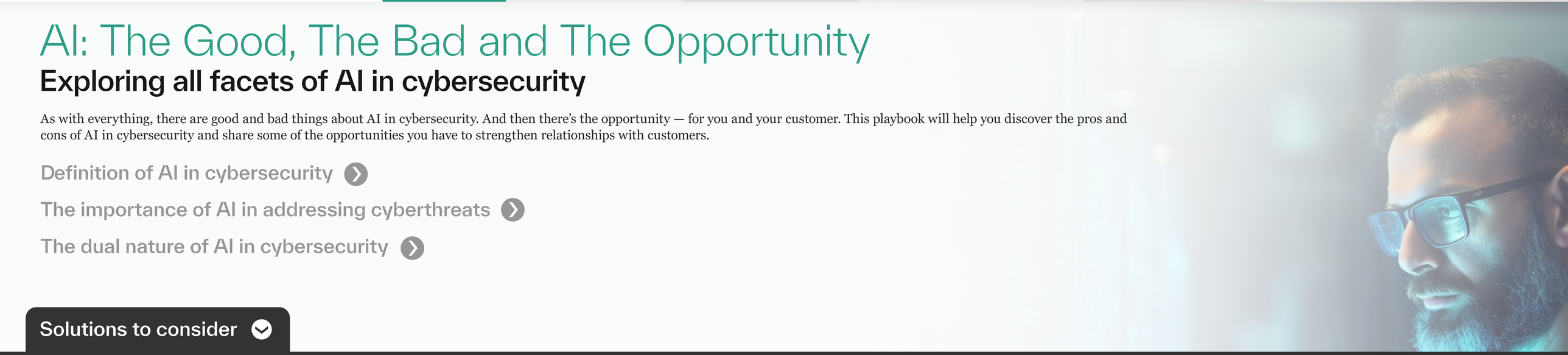
For precisely these reasons, it's crucial for you to stay on top of the fast-moving advancements in AI and how they can impact your customer's security environment.

Solutions to consider

AI: The Good, The Bad and The Opportunity

Exploring all facets of AI in cybersecurity

As with everything, there are good and bad things about AI in cybersecurity. And then there's the opportunity — for you and your customer. This playbook will help you discover the pros and cons of AI in cybersecurity and share some of the opportunities you have to strengthen relationships with customers.



Solutions to consider

Amazon Web Services (AWS)

- **Amazon Q –** Help employees to streamline tasks, accelerate decision-making and problem-solving, and spark creativity and innovation with fast, relevant information and advice from this generative AI–powered assistant.
- **Amazon SageMaker –** Enable data scientists and developers to quickly and easily build, train, and deploy machine learning models at any scale with this fully managed service.
- **Amazon Personalize –** Allow developers to create individualized recommendations for customers using their applications with this machine learning service.

Dell Technologies

- **Secureworks Taegis XD –** Leverage advanced AI for comprehensive threat detection, response, and remediation across your entire IT environment.
- **Dell PowerProtect Cyber Recovery –** Use AI-driven analytics to detect and prevent cyberthreats, ensuring critical data and systems are protected and recoverable in the event of an attack.
- **Dell EMC Integrated Data Protection Appliance (IDPA) –** Employ AI to analyze network traffic, identifying and mitigating potential security threats and ensuring efficient data protection and recovery.

HPE Aruba

- **HPE Aruba Networking Unified SASE –** Enable your organization to embrace security-first, AI-powered networking with zero-trust principles built in — no matter where users connect from.
- **HPE Aruba Networking SSE –** Simplify access control with a unified platform where ZTNA, SWG, CASB, and DEM share a single codebase and all policies are managed from a single user interface.
- **HPE Aruba Networking Central –** Empower IT to manage all networks from one dashboard on a cloud-native management solution with comprehensive AIOps and Generative AI large language models (LLMs), deeper insights, and workflow automation.

Microsoft

- **Microsoft Copilot for Security –** Increase the efficiency and capabilities of defenders and improve security outcomes at machine speed and scale with this generative AI-powered assistant.
- **Microsoft Sentinel –** Detect threats using analytics, investigate incidents with AI, and respond rapidly with automation of common tasks with the first cloud-native SIEM from a major cloud provider.
- **Microsoft Defender for Cloud –** Secure AI, data, and compute workloads in your multicloud environment with comprehensive cloud-native application protection platform (CNAPP) capabilities that protect against cyberthreats and vulnerabilities.

Palo Alto

- **AI Access Security –** Enable your workforce to confidently use AI tools, while giving your security team full visibility, robust control, data protection, and proactive threat prevention.
- **Prisma Cloud AI Security Posture Management (AI-SPM) –** Secure your AI ecosystem by identifying vulnerabilities and prioritizing misconfigurations in models, apps, and resources.
- **AI Runtime Security –** Secure your entire AI app ecosystem and confidently build AI-based apps and protect against runtime threats like prompt injections, model DoS, insecure outputs, and more.

RUCKUS Networks

- **RUCKUS R770 Indoor Access Point –** Rely on ultrafast, low latency wireless connections with improved capacity and efficiency with enterprise-class, RUCKUS AI-driven Wi-Fi 7.
- **RUCKUS One –** Deploy networks fast and deliver exceptional user experiences with turnkey NaaS and AI-driven unified management of converged multi-access public and private enterprise networks.
- **RUCKUS T670 Wireless Access Point –** Provide seamless, high-performance connectivity in rugged outdoor environments with an enterprise-grade outdoor Wi-Fi 7 solution, featuring RUCKUS AI, BeamFlex technology, and support for the 6 GHz band.

Symantec

- **Symantec SMART Security –** Improve threat hunting effectiveness — and ROI — by better predicting the next attack chain steps with Symantec Endpoint Security Complete plus Symantec Email Security.cloud — enhanced by GenAI.
- **Symantec SMART Premium –** Boost Symantec SMART Security with the addition of GenAI-powered Symantec SMART Web Protection, SMART Encryption, and SMART Multi-Factor Authentication.
- **Symantec SMART AI –** Secure your entire AI app ecosystem and confidently build AI-based apps and protect against runtime threats like prompt injections, model DoS, insecure outputs, and more.

Pros of AI in Cybersecurity

AI brings great speed, scale, and consistency to cybersecurity, enabling organizations to detect and respond to cyberthreats more quickly and effectively than humans can alone. AI can also help organizations adapt to evolving threats and protect their digital assets. These are just some of the pros of AI in cybersecurity.

- Enhanced threat detection and response
- Automation of routine tasks
- Behavioral analysis and anomaly detection
- Predictive analytics for risk management

The Concerning Picture of Alert Fatigue[6]

- **63%**-The size of our attack surface has increased in the past three years.
- **4,484** – Average number of alerts received by SOC teams daily.
- **Nearly 3 hours** – Time spent by SOC teams manually triaging alerts.
- **83%** - Percentage of alerts that are false positives and not worth security analysts' time.
- **32%** - Time spent on alerts that are not a threat.

Value of AI for Security Operations[7]

- **108 days** – Time saved responding to threats for organizations that invest in AI.
- **$1.76 million** – Average savings in data breach costs by organizations that invested in AI and automation, compared to those that don't.
- **Up to 40%** - Higher returns seen by organizations investing in AI and automation as those technologies mature.
- **43%** - Greater revenue growth over five years for organizations with mature security capabilities.

Solutions to consider

Pros of AI in Cybersecurity

AI brings great speed, scale, and consistency to cybersecurity, enabling organizations to detect and respond to cyberthreats more quickly and effectively than humans can alone. AI can also help organizations adapt to evolving threats and protect their digital assets. These are just some of the pros of AI in cybersecurity.

Enhanced threat detection and response

- **Rapid analysis of large datasets:** Data is central to AI-enhanced threat hunting, and that data — network traffic logs, user behavior, system logs, etc. — must be collected, consolidated, and cleaned before it can be analyzed. AI can then automatically process massive datasets to detect anomalies or irregular patterns and identify threats. With traditional threat detection systems, however, many of those threats may go undetected.
- **Identification of unknown and zero-day threats:** Traditional signature-based solutions compare suspicious activity against a database of known threats and malware signatures and throw up an alert for human consideration and/or action, creating hundreds or thousands of potentially false alerts. The challenge for security analysts then, is to wade through a haystack of alerts to find the "needle" — before an attack occurs!

  But with alert fatigue, coupled with AI now being used by bad actors to launch zero-day attacks (or even old attacks on a wider scale), traditional solutions are much less effective against these unknown threats. AI-enabled solutions can quickly plow through mountains of data and instantly identify and prioritize alerts to prevent a threat.

Automation of routine tasks

Behavioral analysis and anomaly detection

Predictive analytics for risk management

The Concerning Picture of Alert Fatigue[6]

- **63%**-The size of our attack surface has increased in the past three years.
- **4,484** – Average number of alerts received by SOC teams daily.
- **Nearly 3 hours** – Time spent by SOC teams manually triaging alerts.
- **83%** - Percentage of alerts that are false positives and not worth security analysts' time.
- **32%** - Time spent on alerts that are not a threat.

Value of AI for Security Operations[7]

- **108 days** – Time saved responding to threats for organizations that invest in AI.
- **$1.76 million** – Average savings in data breach costs by organizations that invested in AI and automation, compared to those that don't.
- **Up to 40%** - Higher returns seen by organizations investing in AI and automation as those technologies mature.
- **43%** - Greater revenue growth over five years for organizations with mature security capabilities.

Solutions to consider

Pros of AI in Cybersecurity

AI brings great speed, scale, and consistency to cybersecurity, enabling organizations to detect and respond to cyberthreats more quickly and effectively than humans can alone. AI can also help organizations adapt to evolving threats and protect their digital assets. These are just some of the pros of AI in cybersecurity.

Enhanced threat detection and response

Automation of routine tasks

- **Streamlining incident response processes:** AI can automate incident response processes by enabling you to[4]:
  - **Respond to critical events faster:** Automated IR can monitor millions of security events, enabling timely threat detection and recovery time.
  - **Assign incident response duties:** AI can automatically assign engineers, based on expertise and availability, so they can better respond to an incident based on its nature.
  - **Classify malware and perform risk analysis:** AI can identify anomalies and patterns, then evaluate and classify malware for risk analysis.
  - **Provide platform security:** Automated IR seamlessly integrates security protocols into the development process at the start of the software development lifecycle.
  - **Improve process management:** Automated IR helps to manage security alerts at scale, prioritize IR activities, and ensure the right resources are focused on high-priority tasks.
- **Reducing workloads for security analysts:** As mentioned previously, collecting, consolidating, and cleaning data is typically done by security professionals — a time-consuming task. But with AI, security teams can focus on more strategic aspects of cybersecurity and leave the mundane tasks to AI and automation. As one vendor says: "AI and machine learning is [sic] helping security analysts level the playing field by processing massive amounts of data, providing rapid insights based on analysis, and cutting through the noise of daily security alerts and false positives. This drastically improved [sic] your team's efficiency and productivity, giving them an advantage over potential cyber criminals."[5] In other words, AI and automation help analysts reduce their workloads by eliminating manual errors, streamlining processes, refocusing their efforts, and reducing mean time to detect and respond (MTTD and MTTR).

Behavioral analysis and anomaly detection

Predictive analytics for risk management

The Concerning Picture of Alert Fatigue[6]

- **63%**-The size of our attack surface has increased in the past three years.
- **4,484** – Average number of alerts received by SOC teams daily.
- **Nearly 3 hours** – Time spent by SOC teams manually triaging alerts.
- **83%** - Percentage of alerts that are false positives and not worth security analysts' time.
- **32%** - Time spent on alerts that are not a threat.

Value of AI for Security Operations[7]

- **108 days** – Time saved responding to threats for organizations that invest in AI.
- **$1.76 million** – Average savings in data breach costs by organizations that invested in AI and automation, compared to those that don't.
- **Up to 40%** - Higher returns seen by organizations investing in AI and automation as those technologies mature.
- **43%** - Greater revenue growth over five years for organizations with mature security capabilities.

Solutions to consider

Pros of AI in Cybersecurity

AI brings great speed, scale, and consistency to cybersecurity, enabling organizations to detect and respond to cyberthreats more quickly and effectively than humans can alone. AI can also help organizations adapt to evolving threats and protect their digital assets. These are just some of the pros of AI in cybersecurity.

Enhanced threat detection and response

Automation of routine tasks

Behavioral analysis and anomaly detection

- **Identifying abnormal user behavior and network activities:** Malicious attacks share a commonality: They all behave differently than normal baseline behaviors. Modern anomaly detection solutions use AI and machine learning to automatically learn and adapt to evolving patterns within data, enabling your customer to accurately and efficiently detect anomalies within their networks. AI/ML can quickly comb through network traffic logs, system logs, and user behaviors and compare them to typical threat patterns to accurately identify and respond to abnormal behaviors — such as unauthorized access to sensitive data — or anomalies like sudden spikes or dips in activity, errors in the text, or unusual temperature changes. With AI-powered user behavior and anomaly detection solutions, you can now respond proactively to preempt a threat in real time in your customer's environment rather than react to a threat in progress.

- **Early detection of insider threats and advanced persistent threats (APTs):** By leveraging AI and deep learning for behavioral analysis, organizations can detect insider threats, APTs, and other attacks that traditional systems might miss. Consider this: "Deep learning, a subset of AI, holds significant promise in detecting sophisticated and complex threats. Deep learning models can process and analyze vast amounts of unstructured data, such as network logs, packet captures, and system events, to identify hidden patterns and correlations. Deep learning algorithms excel in detecting advanced persistent threats (APTs), insider threats, and other stealthy attacks that may evade traditional security measures.[8]"

Predictive analytics for risk management

The Concerning Picture of Alert Fatigue[6]

- **63%**-The size of our attack surface has increased in the past three years.
- **4,484** – Average number of alerts received by SOC teams daily.
- **Nearly 3 hours** – Time spent by SOC teams manually triaging alerts.
- **83%** - Percentage of alerts that are false positives and not worth security analysts' time.
- **32%** - Time spent on alerts that are not a threat.

Value of AI for Security Operations[7]

- **108 days** – Time saved responding to threats for organizations that invest in AI.
- **$1.76 million** – Average savings in data breach costs by organizations that invested in AI and automation, compared to those that don't.
- **Up to 40%** - Higher returns seen by organizations investing in AI and automation as those technologies mature.
- **43%** - Greater revenue growth over five years for organizations with mature security capabilities.

Solutions to consider

Pros of AI in Cybersecurity

AI brings great speed, scale, and consistency to cybersecurity, enabling organizations to detect and respond to cyberthreats more quickly and effectively than humans can alone. AI can also help organizations adapt to evolving threats and protect their digital assets. These are just some of the pros of AI in cybersecurity.

Enhanced threat detection and response

Automation of routine tasks

Behavioral analysis and anomaly detection

Predictive analytics for risk management

- **Forecasting potential security risks and vulnerabilities:** Unlike a crystal ball, predictive analytics uses historical data, along with statistical algorithms and machine learning, to identify patterns and predict outcomes in real time. With this data, you can help your customer anticipate risks and spot vulnerabilities — such as detecting potential vulnerabilities in their security infrastructure — and identify opportunities. For example, opportunities might include prioritizing their security investments and resources by focusing on high-risk areas.

- **Proactive mitigation of security incidents before they occur:** What if, instead of just responding to threats, you could help your customer to not only predict threats, but also to proactively prevent them? Predictive analytics does just that. Using AI to quickly cull mountains of data, an AI-based solution can analyze patterns and trends from previous security incidents and current network behaviors to forecast potential threats.[9] With this information, you can help your customer to proactively implement preventative measures to ward off future attacks.

The Concerning Picture of Alert Fatigue[6]

- **63%**-The size of our attack surface has increased in the past three years.
- **4,484** – Average number of alerts received by SOC teams daily.
- **Nearly 3 hours** – Time spent by SOC teams manually triaging alerts.
- **83%** - Percentage of alerts that are false positives and not worth security analysts' time.
- **32%** - Time spent on alerts that are not a threat.

Value of AI for Security Operations[7]

- **108 days** – Time saved responding to threats for organizations that invest in AI.
- **$1.76 million** – Average savings in data breach costs by organizations that invested in AI and automation, compared to those that don't.
- **Up to 40%** - Higher returns seen by organizations investing in AI and automation as those technologies mature.
- **43%** - Greater revenue growth over five years for organizations with mature security capabilities.

Solutions to consider

Pros of AI in Cybersecurity

AI brings great speed, scale, and consistency to cybersecurity, enabling organizations to detect and respond to cyberthreats more quickly and effectively than humans can alone. AI can also help organizations adapt to evolving threats and protect their digital assets. These are just some of the pros of AI in cybersecurity.

- Enhanced threat detection and response
- Automation of routine tasks
- Behavioral analysis and anomaly detection
- Predictive analytics for risk management

The Concerning Picture of Alert Fatigue[6]

- 63%-The size of our attack surface has increased in the past three years.
- 4,484 – Average number of alerts received by SOC teams daily.
- Nearly 3 hours – Time spent by SOC teams manually triaging alerts.
- 83% - Percentage of alerts that are false positives and not worth security analysts' time.

Solutions to consider

Amazon Web Services (AWS)

- **Amazon Q –** Help employees to streamline tasks, accelerate decision-making and problem-solving, and spark creativity and innovation with fast, relevant information and advice from this generative AI–powered assistant.
- **Amazon SageMaker –** Enable data scientists and developers to quickly and easily build, train, and deploy machine learning models at any scale with this fully managed service.
- **Amazon Personalize –** Allow developers to create individualized recommendations for customers using their applications with this machine learning service.

Dell Technologies

- **Secureworks Taegis XD –** Leverage advanced AI for comprehensive threat detection, response, and remediation across your entire IT environment.
- **Dell PowerProtect Cyber Recovery –** Use AI-driven analytics to detect and prevent cyberthreats, ensuring critical data and systems are protected and recoverable in the event of an attack.
- **Dell EMC Integrated Data Protection Appliance (IDPA) –** Employ AI to analyze network traffic, identifying and mitigating potential security threats and ensuring efficient data protection and recovery.

HPE Aruba

- **HPE Aruba Networking Unified SASE –** Enable your organization to embrace security-first, AI-powered networking with zero-trust principles built in — no matter where users connect from.
- **HPE Aruba Networking SSE –** Simplify access control with a unified platform where ZTNA, SWG, CASB, and DEM share a single codebase and all policies are managed from a single user interface.
- **HPE Aruba Networking Central –** Empower IT to manage all networks from one dashboard on a cloud-native management solution with comprehensive AIOps and Generative AI large language models (LLMs), deeper insights, and workflow automation.

Microsoft

- **Microsoft Copilot for Security –** Increase the efficiency and capabilities of defenders and improve security outcomes at machine speed and scale with this generative AI-powered assistant.
- **Microsoft Sentinel –** Detect threats using analytics, investigate incidents with AI, and respond rapidly with automation of common tasks with the first cloud-native SIEM from a major cloud provider.
- **Microsoft Defender for Cloud –** Secure AI, data, and compute workloads in your multicloud environment with comprehensive cloud-native application protection platform (CNAPP) capabilities that protect against cyberthreats and vulnerabilities.

Palo Alto

- **AI Access Security –** Enable your workforce to confidently use AI tools, while giving your security team full visibility, robust control, data protection, and proactive threat prevention.
- **Prisma Cloud AI Security Posture Management (AI-SPM) –** Secure your AI ecosystem by identifying vulnerabilities and prioritizing misconfigurations in models, apps, and resources.
- **AI Runtime Security –** Secure your entire AI app ecosystem and confidently build AI-based apps and protect against runtime threats like prompt injections, model DoS, insecure outputs, and more.

RUCKUS Networks

- **RUCKUS R770 Indoor Access Point –** Rely on ultrafast, low latency wireless connections with improved capacity and efficiency with enterprise-class, RUCKUS AI-driven Wi-Fi 7.
- **RUCKUS One –** Deploy networks fast and deliver exceptional user experiences with turnkey NaaS and AI-driven unified management of converged multi-access public and private enterprise networks.
- **RUCKUS T670 Wireless Access Point –** Provide seamless, high-performance connectivity in rugged outdoor environments with an enterprise-grade outdoor Wi-Fi 7 solution, featuring RUCKUS AI, BeamFlex technology, and support for the 6 GHz band.

Symantec

- **Symantec SMART Security –** Improve threat hunting effectiveness — and ROI — by better predicting the next attack chain steps with Symantec Endpoint Security Complete plus Symantec Email Security.cloud — enhanced by GenAI.
- **Symantec SMART Premium –** Boost Symantec SMART Security with the addition of GenAI-powered Symantec SMART Web Protection, SMART Encryption, and SMART Multi-Factor Authentication.
- **Symantec SMART AI –** Secure your entire AI app ecosystem and confidently build AI-based apps and protect against runtime threats like prompt injections, model DoS, insecure outputs, and more.

Cons of AI in Cybersecurity

AI, machine learning, and analytics bring great promise to the cybersecurity field in terms of data processing at machine speed and scale. At the same time, there are serious considerations that must be made. Understanding the challenges and limitations of AI/ML can help you better educate your customers about AI's dual nature.

- Vulnerabilities to adversarial attacks
- Overreliance on AI without human oversight
- Privacy and ethical concerns
- Complexity and cost of implementation
- Data vulnerability and leakage

> *"The future of cybersecurity isn't about choosing between humans and automation—it's about integrating them effectively."*

Solutions to consider

Cons of AI in Cybersecurity

AI, machine learning, and analytics bring great promise to the cybersecurity field in terms of data processing at machine speed and scale. At the same time, there are serious considerations that must be made. Understanding the challenges and limitations of AI/ML can help you better educate your customers about AI's dual nature.

Vulnerabilities to adversarial attacks

- **Exploitation of AI models through manipulated inputs:** The benefits of AI are numerous. But AI is not immune from being used to generate attacks. Adversarial attacks involve bad actors deliberately attempting to subvert the functionality of AI systems by altering either the original data or the parameters or architecture in the AI model itself. These attacks are crafted to deceive AI systems, causing them to make incorrect or unintended predictions or decisions. Think about how adversarial AI attacks — including white box vs. black box, evasion, poisoning, and transfer attacks — can lead to potentially life-altering outcomes in autonomous vehicles, medical diagnosis systems, facial recognition systems, and other AI-powered applications.

  While there are ways to help your customer to mitigate these risks — including adversarial training where the AI model is trained with adversarial examples to increase its robustness and defensive distillation which involves training a secondary model to detect adversarial examples — more work needs to be done to develop more effective solutions.[10]

- **Evasion of AI-based detection systems by sophisticated adversaries:** Evasion attacks occur when bad actors manipulate data inputs to avoid detection by AI-based security systems, making it difficult to identify and respond to threats. These attacks demonstrate the value of continuous updates and improvements in AI algorithms to adapt to new evasion techniques.

  There are two types of evasion attacks: nontargeted and targeted. In both cases, the goal is to make the AI model produce incorrect output but in the nontargeted attacks it can be any incorrect output whereas in targeted attacks, it must be a specific incorrect output. It's the difference between manipulating the image of a stop sign so that AI fails to recognize it as a stop sign versus classifying a stop sign as harmful. Both lead to dangerous situations, depending on the circumstances.

  The challenge with evasion attacks is that bad actors look for the best way to confuse the model while still being undetectable by humans. This can make them difficult to detect because they take advantage of the particular characteristics or patterns an AI model picks up during its training.

Overreliance on AI without human oversight

Privacy and ethical concerns

Complexity and cost of implementation

Data vulnerability and leakage

Solutions to consider

> *"The future of cybersecurity isn't about choosing between humans and automation — it's about integrating them effectively."*

Cons of AI in Cybersecurity

AI, machine learning, and analytics bring great promise to the cybersecurity field in terms of data processing at machine speed and scale. At the same time, there are serious considerations that must be made. Understanding the challenges and limitations of AI/ML can help you better educate your customers about AI's dual nature.

Vulnerabilities to adversarial attacks

Overreliance on AI without human oversight

- **False positives and false negatives in automated systems:** Automation is key to transforming cybersecurity and speed is a key benefit. But it's easy to put all your automation eggs in the cybersecurity basket and get lulled into a false sense of security. For example, automated systems can quickly and easily generate false positives and false negatives. The risk with false positives is that, if they occur frequently, they can desensitize security teams. On the other hand, false negatives can have dire implications because a genuine threat can go undetected. The goal should be to help your customer balance the fast and cool technology with skilled security experts to help protect their systems and data.[11]

- **Lack of contextual understanding and critical thinking abilities:** Over-relying on automation can also lull organizations into believing that they need fewer human experts. The risk is that an organization may think that they need more technology and fewer experts. But the opposite is true. Automated systems lack the human intuition and context needed to evaluate the level of risk and the importance of a particular alert. Successful organizations have seasoned security experts who can interpret the data they're seeing and differentiate between a benign activity and differentiate between a benign activity that looks suspicious and a genuine threat. [11]

Privacy and ethical concerns

Complexity and cost of implementation

Data vulnerability and leakage

> *"The future of cybersecurity isn't about choosing between humans and automation—it's about integrating them effectively."*

Solutions to consider

Cons of AI in Cybersecurity

AI, machine learning, and analytics bring great promise to the cybersecurity field in terms of data processing at machine speed and scale. At the same time, there are serious considerations that must be made. Understanding the challenges and limitations of AI/ML can help you better educate your customers about AI's dual nature.

Vulnerabilities to adversarial attacks

Overreliance on AI without human oversight

Privacy and ethical concerns

- **Collection and misuse of sensitive data for AI training:** Managing and controlling the integrity and privacy of growing data stores continues to challenge already overburdened and underfunded security teams. As IDC explains:[2]

> *"Sensitive or confidential information may be uploaded into an AI model with little to no thought about the long-term implications. Individual datasets that are innocuous when standing alone may be combined, thus creating personally identifiable information (PII). Frankly, it's another (powerful) tool that requires security awareness training for users to operate appropriately."*

There are also compliance issues — such as GDPR in the European Union — and data privacy concerns to consider ensuring that personal data is not processed without individual consent.

- **Biases and discrimination in AI algorithms and decision-making:** AI is a window into the biases of the people who created it — and they are overwhelmingly men. Examples of gender and racial bias abound in generative AI tools, especially in the short time that they have accessed the open internet. This bias perpetuates itself and impacts the world around it as generative AI gains in popularity and importance.[2] Similarly, data and AI algorithms that train AI threat detection models must be scrutinized to avoid skewed results. Diverse datasets and continuous evaluation against bias are required to ensure fairness in AI models and equitable and accurate outcomes across different demographics and scenarios.

Complexity and cost of implementation

Data vulnerability and leakage

Solutions to consider

> *"The future of cybersecurity isn't about choosing between humans and automation — it's about integrating them effectively."*

Cons of AI in Cybersecurity

AI, machine learning, and analytics bring great promise to the cybersecurity field in terms of data processing at machine speed and scale. At the same time, there are serious considerations that must be made. Understanding the challenges and limitations of AI/ML can help you better educate your customers about AI's dual nature.

Vulnerabilities to adversarial attacks

Overreliance on AI without human oversight

Privacy and ethical concerns

Complexity and cost of implementation

- **Integration challenges with existing security infrastructure:** Integrating AI with existing security infrastructures and workflows can transform operations, bringing better solutions and insights. But it is a complex process, requiring thoughtful, strategic planning and execution to ensure it doesn't disrupt ongoing operations. Start with a compatibility assessment to point out technical challenges, including data formats and communication protocols. It may also help to adopt modular AI that be easily plugged into existing systems and AI tools that support leading standards for a more seamless integration. By understanding the challenges (particularly with legacy systems), following best practices, considering data management, and leveraging APIs, you can help guide your customer through a smooth AI integration process.[12]

- **High costs associated with AI development, deployment, and maintenance:** As with other technology projects, the costs for AI can quickly spin out of control if projects and costs are not carefully planned and controlled. Here are some rough estimates of development costs.[13]

  - Small-scale AI project: $10,000 to $100,000
  - Medium-sized AI project: $100,000 to $500,000
  - Large-scale AI project: $500,000 to $9,000,000
  - Enterprise-level AI project: $9,000,000+

  There are also additional costs involved in cleaning up your customer's data, any customizing of the software or hardware, and other associated costs. Maintenance and management can be handled by the in-house team or outsourced to a professional. Though outsourcing can be costly, it can eliminate in-house costs altogether, freeing up staff to focus on more strategic initiatives. (MTTD and MTTR).

Data vulnerability and leakage

Solutions to consider

> *"The future of cybersecurity isn't about choosing between humans and automation—it's about integrating them effectively."*

Cons of AI in Cybersecurity

AI, machine learning, and analytics bring great promise to the cybersecurity field in terms of data processing at machine speed and scale. At the same time, there are serious considerations that must be made. Understanding the challenges and limitations of AI/ML can help you better educate your customers about AI's dual nature.

Vulnerabilities to adversarial attacks

Overreliance on AI without human oversight

Privacy and ethical concerns

Complexity and cost of implementation

Data vulnerability and leakage

- Losing sensitive or personally identifiable data (PII) is probably the biggest risk with AI, simply due to the massive data volumes and the data generated. As part of training or using AI models, vast amounts of personal data may be used, processed, or created, resulting in a risk of data leakage. There are several ways to help your customer manage this risk:
  - Implement strong encryption to protect sensitive data in transit and at rest.
  - Employ strict access controls and authentication methods.
  - Conduct regular cyber range exercises using adversarial techniques to try to breach the AI system. These exercises serve to both test and improve the resilience of your customer's environment and mitigation strategies.

"The future of cybersecurity isn't about choosing between humans and automation—it's about integrating them effectively."

Solutions to consider

Cons of AI in Cybersecurity

AI, machine learning, and analytics bring great promise to the cybersecurity field in terms of data processing at machine speed and scale. At the same time, there are serious considerations that must be made. Understanding the challenges and limitations of AI/ML can help you better educate your customers about AI's dual nature.

Vulnerabilities to adversarial attacks

Overreliance on AI without human oversight

Privacy and ethical concerns

Complexity and cost of implementation

Data vulnerability and leakage

> *"The future of cybersecurity isn't about choosing between humans and automation—it's about integrating them effectively."*

Solutions to consider

Amazon Web Services (AWS)

- **Amazon Q –** Help employees to streamline tasks, accelerate decision-making and problem-solving, and spark creativity and innovation with fast, relevant information and advice from this generative AI–powered assistant.
- **Amazon SageMaker –** Enable data scientists and developers to quickly and easily build, train, and deploy machine learning models at any scale with this fully managed service.
- **Amazon Personalize –** Allow developers to create individualized recommendations for customers using their applications with this machine learning service.

Dell Technologies

- **Secureworks Taegis XD –** Leverage advanced AI for comprehensive threat detection, response, and remediation across your entire IT environment.
- **Dell PowerProtect Cyber Recovery –** Use AI-driven analytics to detect and prevent cyberthreats, ensuring critical data and systems are protected and recoverable in the event of an attack.
- **Dell EMC Integrated Data Protection Appliance (IDPA) –** Employ AI to analyze network traffic, identifying and mitigating potential security threats and ensuring efficient data protection and recovery.

HPE Aruba

- **HPE Aruba Networking Unified SASE –** Enable your organization to embrace security-first, AI-powered networking with zero-trust principles built in — no matter where users connect from.
- **HPE Aruba Networking SSE –** Simplify access control with a unified platform where ZTNA, SWG, CASB, and DEM share a single codebase and all policies are managed from a single user interface.
- **HPE Aruba Networking Central –** Empower IT to manage all networks from one dashboard on a cloud-native management solution with comprehensive AIOps and Generative AI large language models (LLMs), deeper insights, and workflow automation.

Microsoft

- **Microsoft Copilot for Security –** Increase the efficiency and capabilities of defenders and improve security outcomes at machine speed and scale with this generative AI-powered assistant.
- **Microsoft Sentinel –** Detect threats using analytics, investigate incidents with AI, and respond rapidly with automation of common tasks with the first cloud-native SIEM from a major cloud provider.
- **Microsoft Defender for Cloud –** Secure AI, data, and compute workloads in your multicloud environment with comprehensive cloud-native application protection platform (CNAPP) capabilities that protect against cyberthreats and vulnerabilities.

Palo Alto

- **AI Access Security –** Enable your workforce to confidently use AI tools, while giving your security team full visibility, robust control, data protection, and proactive threat prevention.
- **Prisma Cloud AI Security Posture Management (AI-SPM) –** Secure your AI ecosystem by identifying vulnerabilities and prioritizing misconfigurations in models, apps, and resources.
- **AI Runtime Security –** Secure your entire AI app ecosystem and confidently build AI-based apps and protect against runtime threats like prompt injections, model DoS, insecure outputs, and more.

RUCKUS Networks

- **RUCKUS R770 Indoor Access Point –** Rely on ultrafast, low latency wireless connections with improved capacity and efficiency with enterprise-class, RUCKUS AI-driven Wi-Fi 7.
- **RUCKUS One –** Deploy networks fast and deliver exceptional user experiences with turnkey NaaS and AI-driven unified management of converged multi-access public and private enterprise networks.
- **RUCKUS T670 Wireless Access Point –** Provide seamless, high-performance connectivity in rugged outdoor environments with an enterprise-grade outdoor Wi-Fi 7 solution, featuring RUCKUS AI, BeamFlex technology, and support for the 6 GHz band.

Symantec

- **Symantec SMART Security –** Improve threat hunting effectiveness — and ROI — by better predicting the next attack chain steps with Symantec Endpoint Security Complete plus Symantec Email Security.cloud — enhanced by GenAI.
- **Symantec SMART Premium –** Boost Symantec SMART Security with the addition of GenAI-powered Symantec SMART Web Protection, SMART Encryption, and SMART Multi-Factor Authentication.
- **Symantec SMART AI –** Secure your entire AI app ecosystem and confidently build AI-based apps and protect against runtime threats like prompt injections, model DoS, insecure outputs, and more.

Opportunities Presented by AI in Cybersecurity

The opportunities in AI are immense, both for you and your customers. A recent report indicated that, from April 2023 to January 2024, enterprise AI usage skyrocketed by 595%.[14] No longer are AI, machine learning, and automation innovations. They're now embedded in most every organization. Here are just some of the opportunities presented by AI in cybersecurity.

- Advanced threat detection and response capabilities
- Scalability and efficiency improvements
- Augmented decision-making and contextual insights
- Evolution of adaptive and self-learning security systems
- Role of AI assistants in augmenting cybersecurity analyst abilities
- Role of data loss prevention solutions in preventing unauthorized leakage of company data

Solutions to consider

Opportunities Presented by AI in Cybersecurity

The opportunities in AI are immense, both for you and your customers. A recent report indicated that, from April 2023 to January 2024, enterprise AI usage skyrocketed by 595%.14 No longer are AI, machine learning, and automation innovations. They're now embedded in most every organization. Here are just some of the opportunities presented by AI in cybersecurity.

Advanced threat detection and response capabilities

- **Real-time monitoring and adaptive security controls:** Integrating Real-time adaptive security flexes with multiple, moving perimeters and increasingly advanced threats targeting enterprises. It can monitor a network for malicious traffic and behavioral anomalies, ferret out endpoint vulnerabilities, identify real-time changes to systems, automatically enforce endpoint protections and access rules, block malicious traffic, and more. It starts with a security platform to share and correlate information (instead of point solutions) and includes finer-grained controls, automation, on-demand security services, security as a service, and integration of security and management data.

- **Proactive threat hunting and incident response automation:** Proactive threat hunting and incident response automation are two different approaches to threat monitoring and mitigation that can help organizations stay ahead of cyberthreats:

  - **Proactive threat hunting:** A focused process that involves identifying triggers that could indicate a potential threat, such as anomalies, unusual patterns, or suspicious activities. Once a trigger is identified, threat hunters search for anomalies that could prove or disprove a hypothesis. The goal is to find vulnerabilities and attacks before they happen. Threat hunting can help organizations identify more threats, detect them earlier, and improve incident response.

  - **Incident response automation:** Using automation in the threat hunting process can help organizations respond more quickly and in a more coordinated way. Threat hunters can use automation to study adversary behaviors, quantify what they observe, and test techniques to create detection content and determine the most effective response actions. Automated threat detection can be a critical component of modern cybersecurity approaches and can help organizations bolster their defenses and mitigate risks.[1]

Scalability and efficiency improvements

Augmented decision-making and contextual insights

Evolution of adaptive and self-learning security systems

Role of AI assistants in augmenting cybersecurity analyst abilities

Role of data loss prevention solutions in preventing unauthorized leakage of company data

Solutions to consider

Opportunities Presented by AI in Cybersecurity

The opportunities in AI are immense, both for you and your customers. A recent report indicated that, from April 2023 to January 2024, enterprise AI usage skyrocketed by 595%.14 No longer are AI, machine learning, and automation innovations. They're now embedded in most every organization. Here are just some of the opportunities presented by AI in cybersecurity.

Advanced threat detection and response capabilities

Scalability and efficiency improvements

- **Real-time monitoring and adaptive security controls:** Your customer's security teams must monitor and protect their organization's digital assets, but managing large volumes of data and alerts can be overwhelming due to resource limitations and the sheer number of alerts. To address these challenges, security teams must leverage intelligent automation and advanced analytics. With automation, your customer can triage alerts, categorize them based on severity, and prioritize incident response. By automating routine tasks, the security team can focus their efforts on investigating and mitigating critical security incidents. Advanced analytics, such as machine learning and behavioral analysis, can help to identify patterns and anomalies within the alert data and enable faster and more accurate threat detection.[15]
- **Optimizing resource allocation and workforce productivity:** Clearly, AI/ML presents a massive opportunity for your customer to rethink their cybersecurity team. Because they operate at machine speed and scale — something humans can never attain — it can reduce MTTD and MTTR and increase analyst productivity. Instead of babysitting alerts that don't amount to anything, they can get alerts for only high priority threats that require human critical thinking skills.

Augmented decision-making and contextual insights

Evolution of adaptive and self-learning security systems

Role of AI assistants in augmenting cybersecurity analyst abilities

Role of data loss prevention solutions in preventing unauthorized leakage of company data

Solutions to consider

Opportunities Presented by AI in Cybersecurity

The opportunities in AI are immense, both for you and your customers. A recent report indicated that, from April 2023 to January 2024, enterprise AI usage skyrocketed by 595%.14 No longer are AI, machine learning, and automation innovations. They're now embedded in most every organization. Here are just some of the opportunities presented by AI in cybersecurity.

Advanced threat detection and response capabilities

Scalability and efficiency improvements

Augmented decision-making and contextual insights

- **Real-time monitoring and adaptive security controls:** Enriching security analysis with predictive analytics and contextual data – Predictive analytics in cybersecurity offers a slew of benefits, each contributing to a more effective and proactive security posture for your customer:[16]
  - **Early detection and prevention:** By analyzing anomalies, predictive models can often detect threats at their nascent stage. This early warning system allows for a head start on preventing a breach rather than just mitigating its aftermath.
  - **Better resource optimization:** With predictive analytics, security teams can focus their efforts and resources where they're most needed. By prioritizing high-risk areas, organizations can optimize their cybersecurity strategies, ensuring they are resilient in the face of targeted attacks.
  - **Improved incident response:** Incorporating predictive analytics into a cybersecurity framework also improves incident response. Predictive models can model attack scenarios, which then prepare teams with response plans, mitigating the time taken to assess and act when a real-time incident occurs.
  - **Demonstrate compliance:** Predictive analytics can help organizations in regulated industries meet compliance requirements by demonstrating the proactive measures taken to secure data and prevent breaches.

- **Real-time monitoring and adaptive security controls:** Actionable threat intelligence gives analysts timely and relevant insights with which to effectively detect, analyze, and respond to threats. Actionable cyberthreat intelligence provides analysts with timely, relevant, and contextual insights into potential threats, enabling them to make informed decisions and take proactive measures to mitigate risks. Unlike raw data or generic threat feeds, intelligence is actionable and specific to your customer's environment, enabling analysts to effectively prioritize their responses.[17]

Evolution of adaptive and self-learning security systems

Role of AI assistants in augmenting cybersecurity analyst abilities

Role of data loss prevention solutions in preventing unauthorized leakage of company data

Solutions to consider

Opportunities Presented by AI in Cybersecurity

The opportunities in AI are immense, both for you and your customers. A recent report indicated that, from April 2023 to January 2024, enterprise AI usage skyrocketed by 595%.14 No longer are AI, machine learning, and automation innovations. They're now embedded in most every organization. Here are just some of the opportunities presented by AI in cybersecurity.

Advanced threat detection and response capabilities

Scalability and efficiency improvements

Augmented decision-making and contextual insights

Evolution of adaptive and self-learning security systems

- **Continuous improvement and adaptation to emerging threats:** Continuous improvement and adaptation help your customer to build resilience and navigate unexpected challenges. By regularly evaluating and optimizing cybersecurity processes, you can help your customer to identify vulnerabilities and proactively make changes to mitigate risks.[17]
- **Self-healing and resilience against evolving attack techniques:** NIST lays out four goals that can be used to help your customer build their cyber resiliency strategy:[18]

1. **Automated attacks:** Maintain a state of informed preparedness for adversity.
2. **Targeted attacks:** Continue essential mission or business functions despite adversity.
3. **Recover:** Restore mission or business functions during and after adversity.
4. **Adapt:** Modify mission or business functions and/or supporting capabilities in response to predicted changes in the technical, operational, or threat environments.

In other words, your customer must improve resiliency by recovering from the threat and then modifying processes, practices, and technologies to better anticipate and withstand the next threat.

Role of AI assistants in augmenting cybersecurity analyst abilities

Role of data loss prevention solutions in preventing unauthorized leakage of company data

Solutions to consider

Opportunities Presented by AI in Cybersecurity

The opportunities in AI are immense, both for you and your customers. A recent report indicated that, from April 2023 to January 2024, enterprise AI usage skyrocketed by 595%.14 No longer are AI, machine learning, and automation innovations. They're now embedded in most every organization. Here are just some of the opportunities presented by AI in cybersecurity.

Advanced threat detection and response capabilities

Scalability and efficiency improvements

Augmented decision-making and contextual insights

Evolution of adaptive and self-learning security systems

Role of AI assistants in augmenting cybersecurity analyst abilities

Some security solutions come with AI chatbots that act as assistants to capacity-challenged security analysts. These generative AI chatbots aim to increase your customer's organizational efficiency by giving security analysts an AI engine that can help them identify, analyze, and mitigate threats using conversational prompts and interactive dialogue. An AI assistant not only transforms how analysts view their jobs, but it can also empower them: New analysts can learn from data-driven insights, while experienced analysts can focus on more important tasks — all while reducing the chances of missing important data.

Role of data loss prevention solutions in preventing unauthorized leakage of company data

Solutions to consider

Opportunities Presented by AI in Cybersecurity

The opportunities in AI are immense, both for you and your customers. A recent report indicated that, from April 2023 to January 2024, enterprise AI usage skyrocketed by 595%.14 No longer are AI, machine learning, and automation innovations. They're now embedded in most every organization. Here are just some of the opportunities presented by AI in cybersecurity.

Advanced threat detection and response capabilities

Scalability and efficiency improvements

Augmented decision-making and contextual insights

Evolution of adaptive and self-learning security systems

Role of AI assistants in augmenting cybersecurity analyst abilities

Role of data loss prevention solutions in preventing unauthorized leakage of company data

Data loss prevention (DLP) solutions can help detect and prevent data theft, accidental data sharing, and unauthorized data leakage by protecting endpoints and preventing unauthorized access. They combine standard cybersecurity measures — such as firewalls, endpoint protection, monitoring services, and antivirus software — with advanced solutions like AI/ML and automation to help your customer identify sensitive data, monitor data usage, and ensure regulatory compliance. DLP solutions can also help improve an organization's overall cybersecurity posture, especially on devices that are sensitive to threats, and protect intellectual property and ensure customer trust.[1]

Solutions to consider

Opportunities Presented by AI in Cybersecurity

The opportunities in AI are immense, both for you and your customers. A recent report indicated that, from April 2023 to January 2024, enterprise AI usage skyrocketed by 595%.14 No longer are AI, machine learning, and automation innovations. They're now embedded in most every organization. Here are just some of the opportunities presented by AI in cybersecurity.

Advanced threat detection and response capabilities

Scalability and efficiency improvements

Augmented decision-making and contextual insights

Evolution of adaptive and self-learning security systems

Role of AI assistants in augmenting cybersecurity analyst abilities

Role of data loss prevention solutions in preventing unauthorized leakage of company data

Solutions to consider

Amazon Web Services (AWS)

- **Amazon Q –** Help employees to streamline tasks, accelerate decision-making and problem-solving, and spark creativity and innovation with fast, relevant information and advice from this generative AI–powered assistant.
- **Amazon SageMaker –** Enable data scientists and developers to quickly and easily build, train, and deploy machine learning models at any scale with this fully managed service.
- **Amazon Personalize –** Allow developers to create individualized recommendations for customers using their applications with this machine learning service.

Dell Technologies

- **Secureworks Taegis XD –** Leverage advanced AI for comprehensive threat detection, response, and remediation across your entire IT environment.
- **Dell PowerProtect Cyber Recovery –** Use AI-driven analytics to detect and prevent cyberthreats, ensuring critical data and systems are protected and recoverable in the event of an attack.
- **Dell EMC Integrated Data Protection Appliance (IDPA) –** Employ AI to analyze network traffic, identifying and mitigating potential security threats and ensuring efficient data protection and recovery.

HPE Aruba

- **HPE Aruba Networking Unified SASE –** Enable your organization to embrace security-first, AI-powered networking with zero-trust principles built in — no matter where users connect from.
- **HPE Aruba Networking SSE –** Simplify access control with a unified platform where ZTNA, SWG, CASB, and DEM share a single codebase and all policies are managed from a single user interface.
- **HPE Aruba Networking Central –** Empower IT to manage all networks from one dashboard on a cloud-native management solution with comprehensive AIOps and Generative AI large language models (LLMs), deeper insights, and workflow automation.

Microsoft

- **Microsoft Copilot for Security –** Increase the efficiency and capabilities of defenders and improve security outcomes at machine speed and scale with this generative AI-powered assistant.
- **Microsoft Sentinel –** Detect threats using analytics, investigate incidents with AI, and respond rapidly with automation of common tasks with the first cloud-native SIEM from a major cloud provider.
- **Microsoft Defender for Cloud –** Secure AI, data, and compute workloads in your multicloud environment with comprehensive cloud-native application protection platform (CNAPP) capabilities that protect against cyberthreats and vulnerabilities.

Palo Alto

- **AI Access Security –** Enable your workforce to confidently use AI tools, while giving your security team full visibility, robust control, data protection, and proactive threat prevention.
- **Prisma Cloud AI Security Posture Management (AI-SPM) –** Secure your AI ecosystem by identifying vulnerabilities and prioritizing misconfigurations in models, apps, and resources.
- **AI Runtime Security –** Secure your entire AI app ecosystem and confidently build AI-based apps and protect against runtime threats like prompt injections, model DoS, insecure outputs, and more.

RUCKUS Networks

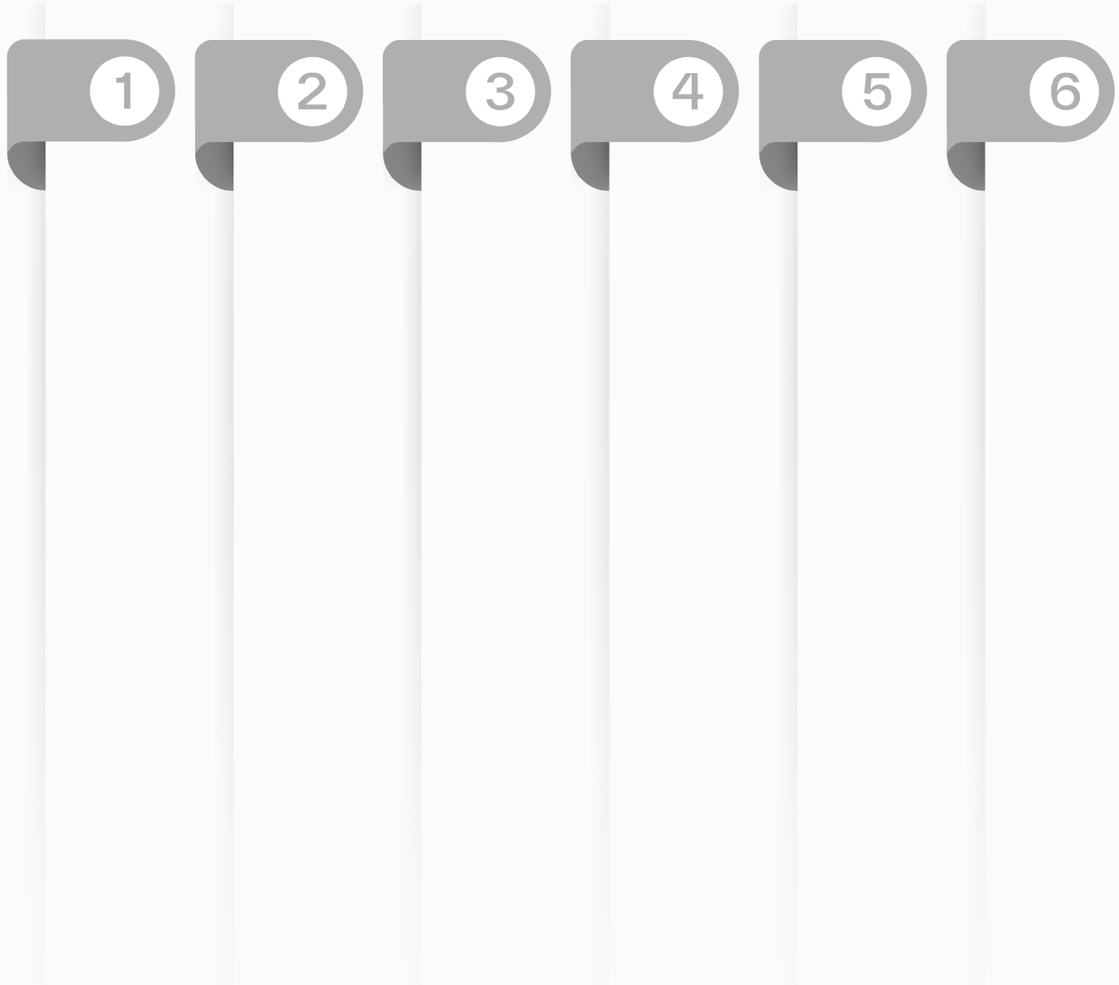
- **RUCKUS R770 Indoor Access Point –** Rely on ultrafast, low latency wireless connections with improved capacity and efficiency with enterprise-class, RUCKUS AI-driven Wi-Fi 7.
- **RUCKUS One –** Deploy networks fast and deliver exceptional user experiences with turnkey NaaS and AI-driven unified management of converged multi-access public and private enterprise networks.
- **RUCKUS T670 Wireless Access Point –** Provide seamless, high-performance connectivity in rugged outdoor environments with an enterprise-grade outdoor Wi-Fi 7 solution, featuring RUCKUS AI, BeamFlex technology, and support for the 6 GHz band.

Symantec

- **Symantec SMART Security –** Improve threat hunting effectiveness — and ROI — by better predicting the next attack chain steps with Symantec Endpoint Security Complete plus Symantec Email Security.cloud — enhanced by GenAI.
- **Symantec SMART Premium –** Boost Symantec SMART Security with the addition of GenAI-powered Symantec SMART Web Protection, SMART Encryption, and SMART Multi-Factor Authentication.
- **Symantec SMART AI –** Secure your entire AI app ecosystem and confidently build AI-based apps and protect against runtime threats like prompt injections, model DoS, insecure outputs, and more.

Opportunities for MSPs and MSSPs

Your customers require a new security approach as they seek to move from perimeter-based security to zero trust to help protect against targeted threats and improve business performance. It can also mitigate supply chain risk and secure cloud environments. Is your customer ready to take their first steps? Start by offering these services:



Vendor Solutions for AI-Powered Cybersecurity

- AI-Powered Threat Detection and Prevention
- User and Entity Behavior Analytics (UEBA)
- Security Orchestration, Automation, and Response (SOAR)
- Next-Generation Endpoint Protection
- AI-Powered Network Traffic Analysis
- AI-Based Vulnerability Management

Solutions to consider ›

Opportunities for MSPs and MSSPs

Your customers require a new security approach as they seek to move from perimeter-based security to zero trust to help protect against targeted threats and improve business performance. It can also mitigate supply chain risk and secure cloud environments. Is your customer ready to take their first steps? Start by offering these services:

1 Build a Zero-Trust Roadmap

2 3 4 5 6

Success starts with a comprehensive zero-trust roadmap that outlines the activities needed to implement your customer zero-trust strategy. This strategy document will provide a clear view of the deliverables, budget, and business outcomes expected.

- Determine a framework, whether it's the NIST or CISA framework or a framework from Gartner, Forrester, or others. TD SYNNEX can help you select the right vendors to craft a zero-trust vision.
- Recruit business and IT stakeholders—from IT operators to enterprise architects to business unit leaders to C-suite executives—who can help build your customer's zero-trust roadmap and evangelize the need for new or shifting investments or significant cultural and organizational change.
- Identify interdependencies between the zero-trust implementation and other IT and business projects.

Vendor Solutions for AI-Powered Cybersecurity

- AI-Powered Threat Detection and Prevention
- User and Entity Behavior Analytics (UEBA)
- Security Orchestration, Automation, and Response (SOAR)
- Next-Generation Endpoint Protection
- AI-Powered Network Traffic Analysis
- AI-Based Vulnerability Management

Solutions to consider ›

Opportunities for MSPs and MSSPs

Your customers require a new security approach as they seek to move from perimeter-based security to zero trust to help protect against targeted threats and improve business performance. It can also mitigate supply chain risk and secure cloud environments. Is your customer ready to take their first steps? Start by offering these services:

1 | **2 Refine the Business Continuity Plan** | 3 | 4 | 5 | 6

Every organization today should have a business continuity plan that outlines what happens when (not if) they're attacked. The next step is to help them adopt or periodically stress-test and refine their business continuity plan.

Then, put together an up-to-date inventory of systems and their criticality to make it easy to prioritize actions in case there's a threat or attack. Create playbooks, conduct tabletop exercises, and test backups for critical assets.

The more you can help them prepare, the better off they'll be in the event of a cyberattack or other disaster.

Vendor Solutions for AI-Powered Cybersecurity

- AI-Powered Threat Detection and Prevention
- User and Entity Behavior Analytics (UEBA)
- Security Orchestration, Automation, and Response (SOAR)
- Next-Generation Endpoint Protection
- AI-Powered Network Traffic Analysis
- AI-Based Vulnerability Management

Solutions to consider ›

Opportunities for MSPs and MSSPs

Your customers require a new security approach as they seek to move from perimeter-based security to zero trust to help protect against targeted threats and improve business performance. It can also mitigate supply chain risk and secure cloud environments. Is your customer ready to take their first steps? Start by offering these services:

1 2 **3 Assess Their Environment** 4 5 6

Next, help your customer understand their unique risks by identifying vulnerabilities in their environment and providing recommendations. Take advantage of these assessments:

- **Security Maturity Assessment –** Get a complimentary 45-minute assessment of your customer's security practices and controls and provide a graded report with a customized action plan to improve their security posture.
- **Penetration Testing –** Show them how bad actors exploit their systems to access and disclose sensitive data, and how to best prioritize vulnerabilities for remediation.
- **Vulnerability Assessments –** Point out the pathways that attackers use to exploit their systems and provide a complete financial risk analysis with ways to re-allocate limited resources to ensure they're protected.
- **Additional Assessments –** Access additional assessment capabilities, including Security Risk Assessments, Physical Security Assessments, Physical Penetration Testing, GDPR Assessments, and many others.

Vendor Solutions for AI-Powered Cybersecurity

- AI-Powered Threat Detection and Prevention
- User and Entity Behavior Analytics (UEBA)
- Security Orchestration, Automation, and Response (SOAR)
- Next-Generation Endpoint Protection
- AI-Powered Network Traffic Analysis
- AI-Based Vulnerability Management

Solutions to consider ›

Opportunities for MSPs and MSSPs

Your customers require a new security approach as they seek to move from perimeter-based security to zero trust to help protect against targeted threats and improve business performance. It can also mitigate supply chain risk and secure cloud environments. Is your customer ready to take their first steps? Start by offering these services:

1 2 3 **4 Offer Comprehensive Services** 5 6

Help customers focus on their core business by leveraging our advanced managed and other security services.

- **Incident Response Services –** Comprehensive Incident Response (IR) services—including Plan Development, Readiness Review, and Emergency Response—ensure they have the right capabilities to respond to and recover from threats.
- **Compliance Services –** Governance and compliance readiness services for HIPAA, HITRUST, PCI-DSS, NIST 801-171, ISO 27001, NERC-CIP, SOC 1and2, GDPR, and others—ideal for businesses that face a high regulatory burden.
- **Implementation Services –** Services for new installations, integrations, patch services, configurations, and staff augmentations to help you design the best solution for them.
  - **SOC-as-a-Service –** Have a bench of cyber experts who can monitor, analyze, manage, and act on threats across your customer's business.
  - **Firewall Services –** Help your customer focus on their core business while you administer, monitor, and maintain their firewall infrastructure.
  - **ISAO Threat Feed –** Join a very large community of companies, local governments, and security professionals to collaborate, share intelligence, and participate in training and conferences and leverage competent collaborative analysis.

Vendor Solutions for AI-Powered Cybersecurity

- AI-Powered Threat Detection and Prevention
- User and Entity Behavior Analytics (UEBA)
- Security Orchestration, Automation, and Response (SOAR)
- Next-Generation Endpoint Protection
- AI-Powered Network Traffic Analysis
- AI-Based Vulnerability Management

Solutions to consider ›

Opportunities for MSPs and MSSPs

Your customers require a new security approach as they seek to move from perimeter-based security to zero trust to help protect against targeted threats and improve business performance. It can also mitigate supply chain risk and secure cloud environments. Is your customer ready to take their first steps? Start by offering these services:

1 2 3 4

5 Engage through training and engagement experiences

6

Engage your customer's team with numerous training and engagement experiences for both new and advanced users.

Training

- **Foundational –** Develop the foundational cybersecurity skills needed to advance to the next level through the Cyber Essentials Series.
- **Accelerated –** Access over 50 cloud-based, instructor-led classroom learning courses to prepare for cybersecurity careers and train on a hyper-realistic network within a cloud-hosted cyber range using the tools your team uses every day.
- **Virtual –** Choose from an extensive set of courses for new cybersecurity team members or, for more advanced users, an upgraded training program that includes the entire course library, 200+ Virtual Lab Environments, a guided mentor, and industry certification practice tests.
- **Advanced threat training –** Learn how to contain threats, fix weaknesses, and use the latest threat hunting tools via online, gamified training using real-world simulations within a protected environment.

Engagement

- **Demos –** Test and engage with leading cybersecurity offerings to see how they work in real time.
- **Engagement –** Engage in an "up close and personal" live cyber experience to test the responses of your team and/or environment in a cyber range.

Vendor Solutions for AI-Powered Cybersecurity

- AI-Powered Threat Detection and Prevention
- User and Entity Behavior Analytics (UEBA)
- Security Orchestration, Automation, and Response (SOAR)
- Next-Generation Endpoint Protection
- AI-Powered Network Traffic Analysis
- AI-Based Vulnerability Management

Solutions to consider ›

Opportunities for MSPs and MSSPs

Your customers require a new security approach as they seek to move from perimeter-based security to zero trust to help protect against targeted threats and improve business performance. It can also mitigate supply chain risk and secure cloud environments. Is your customer ready to take their first steps? Start by offering these services:

1 2 3 4 5

6 Sell and Build SASE and XDR into the Security Stack

According to Gartner, "by 2025, at least 60% of enterprises will have explicit strategies and timelines for SASE adoption encompassing user, branch, and edge access, up from 10% in 2020."[15] Security leaders will also want to consolidate their products/vendors, be more proactive in their response to threats, and drive greater efficiency—and they're increasingly turning to MSPs and MSSPs who truly understand their security challenges.

- Perform a gap analysis and establish a high-level SASE strategy and roadmap that's closely aligned with business goals and wider organizational strategic initiatives (such as cloud migration, cybersecurity policies, and IT strategy plans). Ensure the plan leverages the customer's existing assets and enables them to transition to a SASE model over time.
- Assess your client's current network and security environment, and the resources they have available, to determine which services they need, the processes to be used, what technologies will be deployed, and the training required.
- If your customer already has an SD-WAN, they may only need SSE capabilities. If they don't, determine whether they can benefit from SASE now or whether SSE can be an on-ramp for SASE.
- Evaluate the point solutions your customer has and any underutilized functionality, as well as the level of automation and integration between them, and consider a consolidation strategy anchored with XDR.
- Help your customer understand the synergistic value offered by XDR—for example, underlying data lake foundation with lower-cost and flexible data storage, functional orchestration and automation, and advanced security analytics—and not just in how you can pare down the number of solutions and/or vendors.
- Deliver XDR as a service to minimize maintenance for you and your customer.
- Cut time to sale by packaging up or bundling solutions you've already vetted—or provide a menu of pre-vetted vendor solutions from which to choose.

Vendor Solutions for AI-Powered Cybersecurity

- AI-Powered Threat Detection and Prevention
- User and Entity Behavior Analytics (UEBA)
- Security Orchestration, Automation, and Response (SOAR)
- Next-Generation Endpoint Protection
- AI-Powered Network Traffic Analysis
- AI-Based Vulnerability Management

Solutions to consider ›

Opportunities for MSPs and MSSPs

Your customers require a new security approach as they seek to move from perimeter-based security to zero trust to help protect against targeted threats and improve business performance. It can also mitigate supply chain risk and secure cloud environments. Is your customer ready to take their first steps? Start by offering these services:

Vendor Solutions for AI-Powered Cybersecurity

- AI-Powered Threat Detection and Prevention
- User and Entity Behavior Analytics (UEBA)
- Security Orchestration, Automation, and Response (SOAR)

Solutions to consider

Amazon Web Services (AWS)

- **Amazon Q –** Help employees to streamline tasks, accelerate decision-making and problem-solving, and spark creativity and innovation with fast, relevant information and advice from this generative AI–powered assistant.
- **Amazon SageMaker –** Enable data scientists and developers to quickly and easily build, train, and deploy machine learning models at any scale with this fully managed service.
- **Amazon Personalize –** Allow developers to create individualized recommendations for customers using their applications with this machine learning service.

Dell Technologies

- **Secureworks Taegis XD –** Leverage advanced AI for comprehensive threat detection, response, and remediation across your entire IT environment.
- **Dell PowerProtect Cyber Recovery –** Use AI-driven analytics to detect and prevent cyberthreats, ensuring critical data and systems are protected and recoverable in the event of an attack.
- **Dell EMC Integrated Data Protection Appliance (IDPA) –** Employ AI to analyze network traffic, identifying and mitigating potential security threats and ensuring efficient data protection and recovery.

HPE Aruba

- **HPE Aruba Networking Unified SASE –** Enable your organization to embrace security-first, AI-powered networking with zero-trust principles built in — no matter where users connect from.
- **HPE Aruba Networking SSE –** Simplify access control with a unified platform where ZTNA, SWG, CASB, and DEM share a single codebase and all policies are managed from a single user interface.
- **HPE Aruba Networking Central –** Empower IT to manage all networks from one dashboard on a cloud-native management solution with comprehensive AIOps and Generative AI large language models (LLMs), deeper insights, and workflow automation.

Microsoft

- **Microsoft Copilot for Security –** Increase the efficiency and capabilities of defenders and improve security outcomes at machine speed and scale with this generative AI-powered assistant.
- **Microsoft Sentinel –** Detect threats using analytics, investigate incidents with AI, and respond rapidly with automation of common tasks with the first cloud-native SIEM from a major cloud provider.
- **Microsoft Defender for Cloud –** Secure AI, data, and compute workloads in your multicloud environment with comprehensive cloud-native application protection platform (CNAPP) capabilities that protect against cyberthreats and vulnerabilities.

Palo Alto

- **AI Access Security –** Enable your workforce to confidently use AI tools, while giving your security team full visibility, robust control, data protection, and proactive threat prevention.
- **Prisma Cloud AI Security Posture Management (AI-SPM) –** Secure your AI ecosystem by identifying vulnerabilities and prioritizing misconfigurations in models, apps, and resources.
- **AI Runtime Security –** Secure your entire AI app ecosystem and confidently build AI-based apps and protect against runtime threats like prompt injections, model DoS, insecure outputs, and more.

RUCKUS Networks

- **RUCKUS R770 Indoor Access Point –** Rely on ultrafast, low latency wireless connections with improved capacity and efficiency with enterprise-class, RUCKUS AI-driven Wi-Fi 7.
- **RUCKUS One –** Deploy networks fast and deliver exceptional user experiences with turnkey NaaS and AI-driven unified management of converged multi-access public and private enterprise networks.
- **RUCKUS T670 Wireless Access Point –** Provide seamless, high-performance connectivity in rugged outdoor environments with an enterprise-grade outdoor Wi-Fi 7 solution, featuring RUCKUS AI, BeamFlex technology, and support for the 6 GHz band.

Symantec

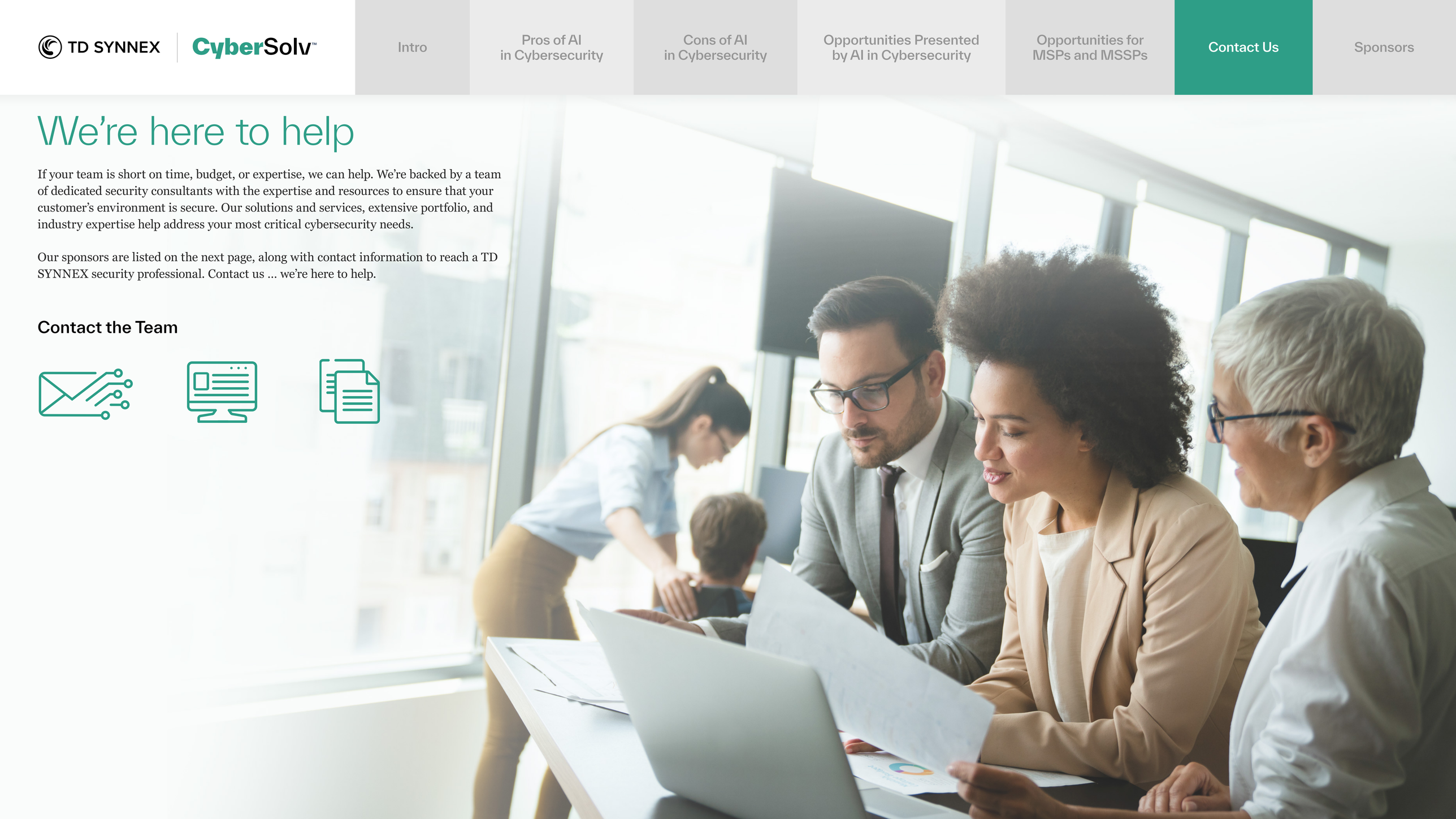
- **Symantec SMART Security –** Improve threat hunting effectiveness — and ROI — by better predicting the next attack chain steps with Symantec Endpoint Security Complete plus Symantec Email Security.cloud — enhanced by GenAI.
- **Symantec SMART Premium –** Boost Symantec SMART Security with the addition of GenAI-powered Symantec SMART Web Protection, SMART Encryption, and SMART Multi-Factor Authentication.
- **Symantec SMART AI –** Secure your entire AI app ecosystem and confidently build AI-based apps and protect against runtime threats like prompt injections, model DoS, insecure outputs, and more.

We're here to help

If your team is short on time, budget, or expertise, we can help. We're backed by a team of dedicated security consultants with the expertise and resources to ensure that your customer's environment is secure. Our solutions and services, extensive portfolio, and industry expertise help address your most critical cybersecurity needs.

Our sponsors are listed on the next page, along with contact information to reach a TD SYNNEX security professional. Contact us … we're here to help.

Contact the Team



Thank you to our sponsors

For more information on any one of these or other TD SYNNEX security solutions or services, please contact the security professionals below.

To harness the power of AI to drive innovation and growth in your business via TD SYNNEX, visit https://www.tdsynnex.com/na/us/dell/ or reach out to EnterpriseCloudSales@tdsynnex.com.

If you're interested in these solutions, check out TD SYNNEX's exclusive Dell AI Program at Pathw.ai or contact DellAI@tdsynnex.com to learn how to leverage Pathw.ai for your Cyber AI needs.

For help configuring and quoting HPE Aruba Networking SASE, SSE, and AIOps solutions, email Kristen.Vargo@tdsynnex.com.

Learn more about our solutions here: Contact Microsoft Cloud

For more information, please reach out to panwbd@tdsynnex.com.

Contact us for more information at https://www.tdsynnex.com/na/us/cybersolv/ruckus/.

For more information, visit https://www.tdsynnex.com/na/us/cybersolv/symantec/ or contact BroadcomBD@tdsynnex.com .

References and Further Reading

1. Generated by AI, 07/10/2024.
2. "A CISO's Guide to Artificial Intelligence," IDC, #US50933923, 07/20230.
3. "The Dual Nature of Artificial Intelligence (AI) in Cybersecurity," LinkedIn.com, 07/10/2023.
4. "AI in Cybersecurity: Incident Response Automation Opportunities," SISAInfoSec.com.
5. "What is AI in Cybersecurity?," Sophos.com, retrieved 07/14/2024.
6. "67% of daily security alerts overwhelm SOC analysts," HelpNetSecurity.com, 07/20/2023.
7. "Cost of a Data Breach Report 2023," IBM.com, 2023.
8. "Empowering Cybersecurity: The Role of AI in Advanced Threat Detection," Medium.com, 06/30/2023.
9. "A Predictive Future for Cybersecurity Analytics," TrueFort.com, 12/07/2023.
10. "What is Adversarial AI in Machine Learning?," PaloAltoNetworks.com, https://www.paloaltonetworks.com/cyberpedia/what-are-adversarial-attacks-on-AI-Machine-Learning, retrieved 07/14/2024.
11. "The Danger of Overreliance on Automation in Cybersecurity," gca.ISC.org, 2023.
12. "Integrating AI with Existing Systems," Spoke.ai, 03/18/2024.
13. "How Much Does It Cost to Build Artificial Intelligence Software in 2024," Medium.com, 10/12/2023.
14. "ThreatLabz 2024 AI Security Report," Zscaler.com, 2024.
15. "The Challenges of Monitoring Large Volumes of Security Alerts: A Focus on Internal Information Security Teams," LinkedIn.com, 06/22/023.
16. "Harnessing Predictive Analytics in Cybersecurity."
17. "The Human Factor: Empowering Analysts with Actionable Cyber Threat Intelligence," LinkedIn.com, 05/16/2024.
18. "Achieving Continuous Improvement and Adaptation," FasterCapital.com, 06/12/2024.
19. "Developing Cyber-Resilient Systems: A Systems Security Engineering Approach," NIST Special Publication 800-160, Volume 2 Revision 1, 12/2021.
20. "2021 Strategic Roadmap for SASE Convergence," Gartner.com, 03/24/2021.