AI for cybersecurity:
Separating the wheat from the chaff

May 10th , 2019

Tewfik Toum,
@Tewfik_t
Principal Advisor, IBM Europe

AI in cybersecurity is great. Or is it ?

- **Great interest:** to reduce time & resources
- **Great scepticism:** we’re at peak of the hype
- **Great caution:** lack of new skills

… but are applications of AI in cybersecurity delivering what they promised?

Still work to do, but promise for the future:

Many enterprises are using artificial intelligence (AI) technologies as part of their overall security strategy, but results are mixed on the post-deployment usefulness of AI in cybersecurity settings.

- ***By 2020, 40% of security vendors will claim AI-driven capabilities, up from 10% today.*****, Gartner 2017**

- ***AI for cybersecurity is a hot new thing—and a dangerous gamble.***
  (**MIT Technology Review, Aug. 2018)**

- ***Overall, the cybersecurity toolsets of greatest relevance to AI are incident detection and response (IDR) and endpoint detection and response*****.**
  (IDC, 2019)

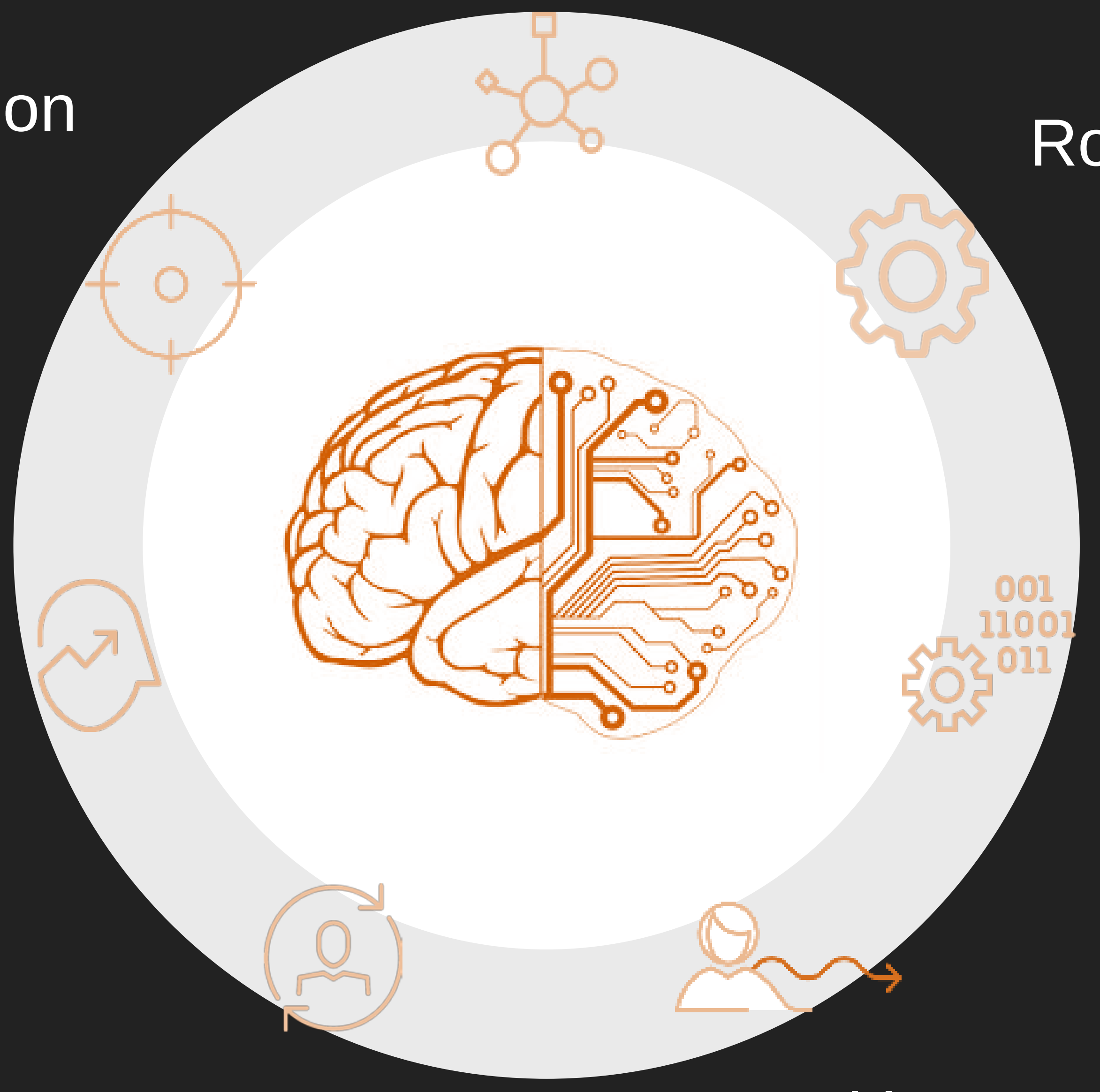
Content

1. AI in cybersecurity
2. Key use cases and application areas
3. The hype of AI in cybersecurity
4. Key take-aways

AI is underpinned by many advanced technologies and has the “power” to transform cybersecurity

Cognitive technologies

Artificial intelligence



Recommendation engines

Robotics

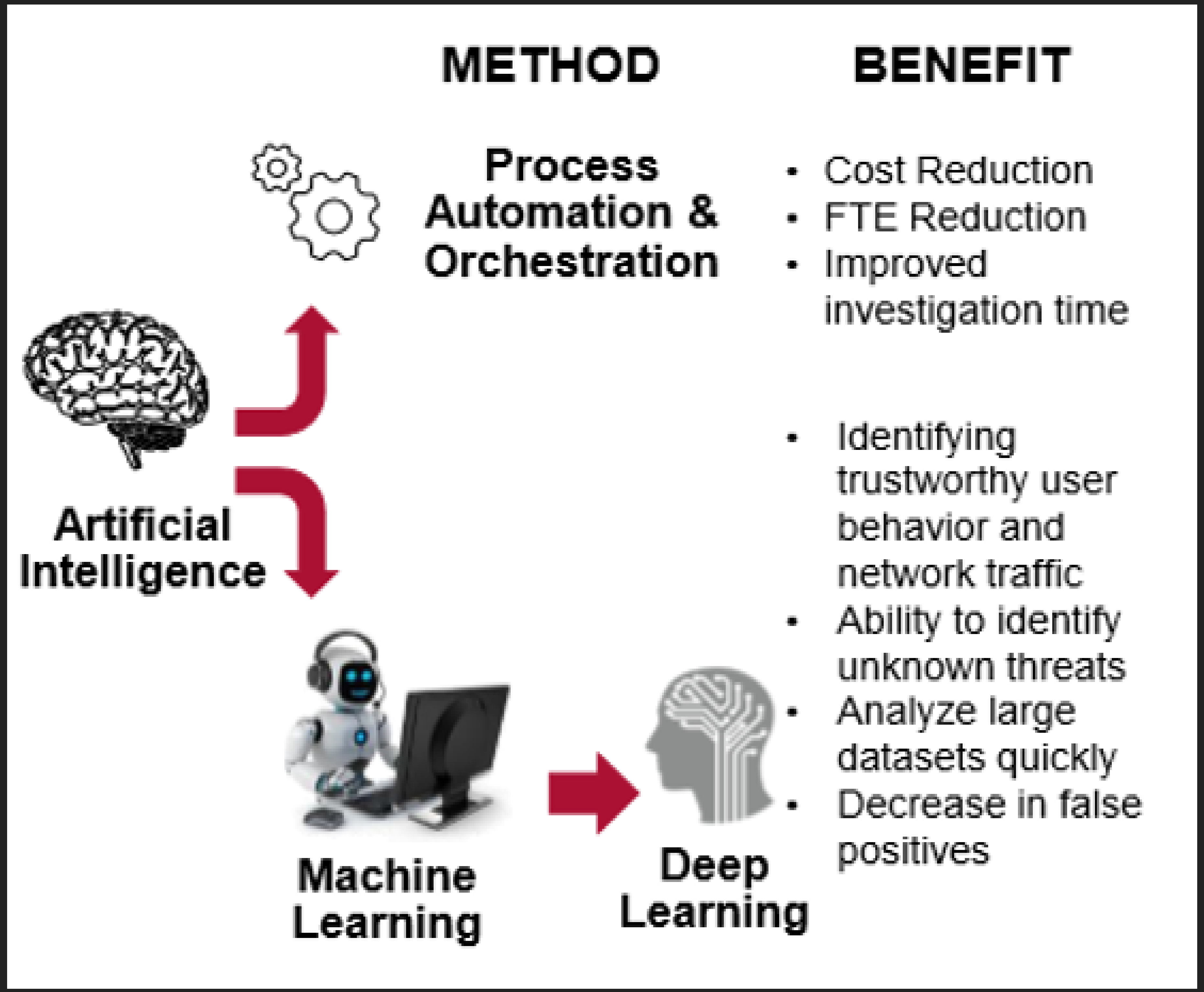
Predictive analytics

Machine learning systems

Deep learning

Natural language processing

Cognitive security will enable organizations to improve their ability to prevent and detect threats, as well as accelerate and automate responses.



METHOD

BENEFIT

Process Automation & Orchestration

- Cost Reduction
- FTE Reduction
- Improved investigation time

Artificial Intelligence

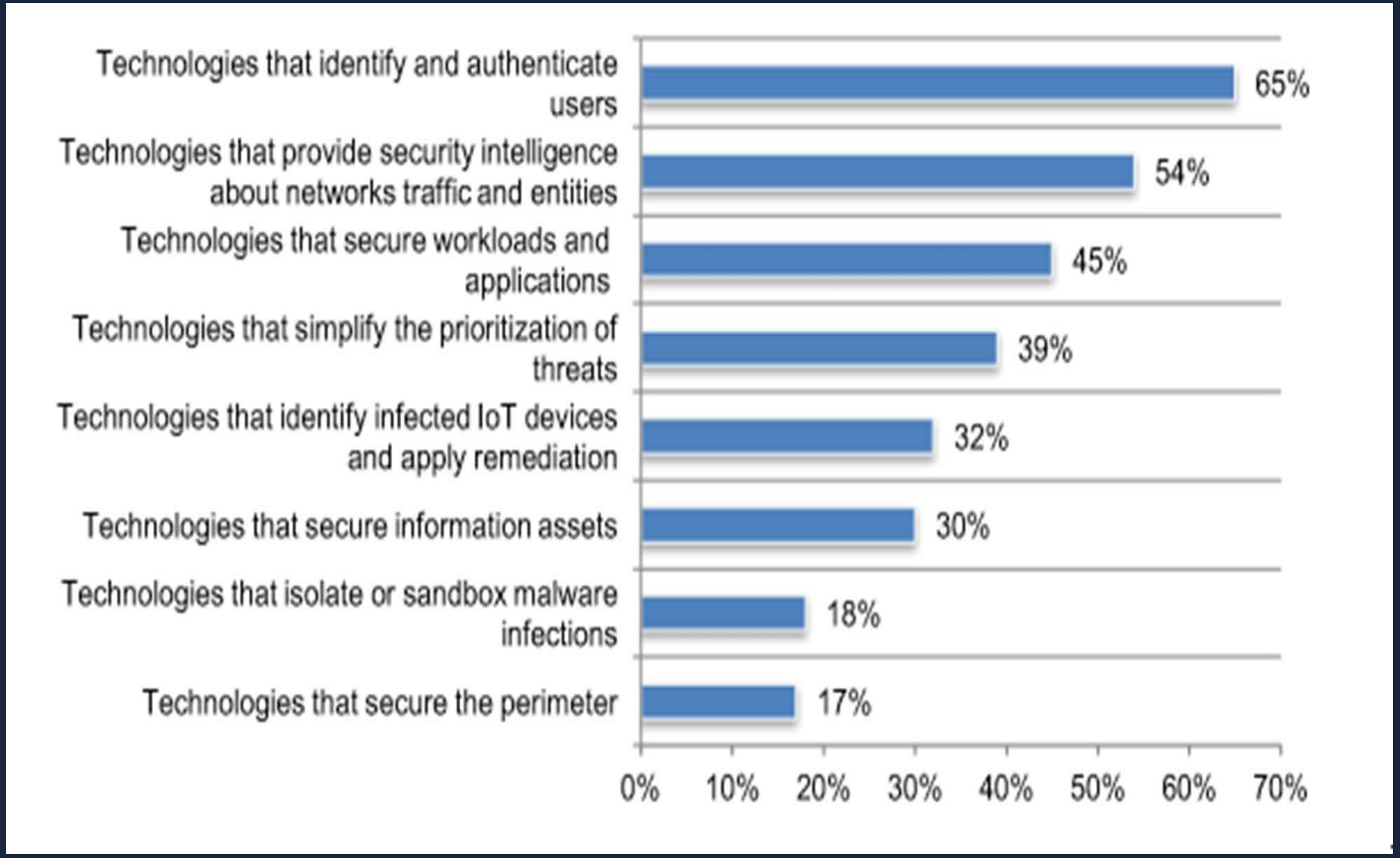
Machine Learning

Deep Learning

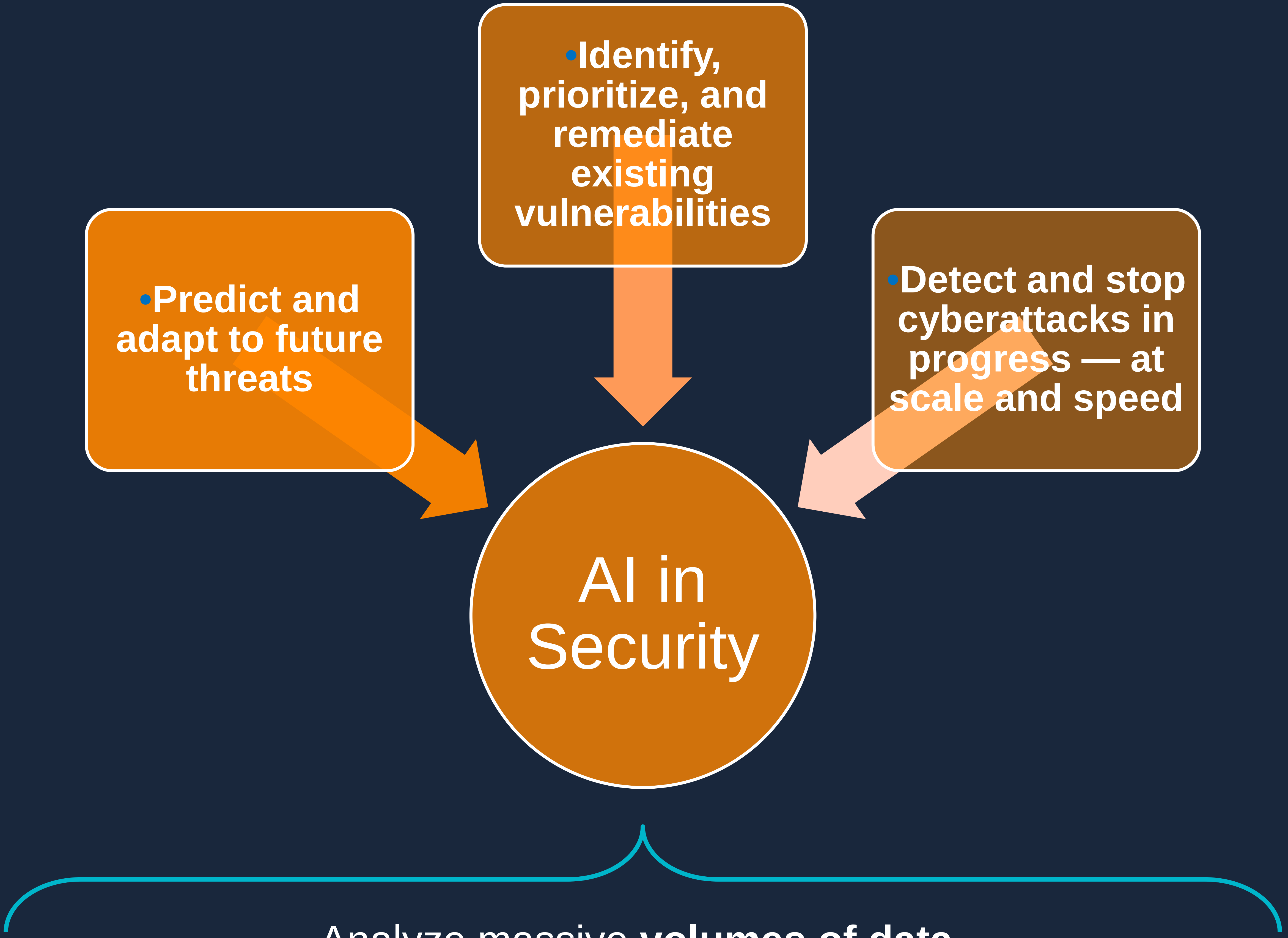
- Identifying trustworthy user behavior and network traffic
- Ability to identify unknown threats
- Analyze large datasets quickly
- Decrease in false positives

Security professionals are poised to embrace the high potential of AI technologies

Technologies most likely to be supported by AI



Source: The 4th Annual Study on the Cyber resilient organization, Ponemon Institute, April 2019



•**Identify, prioritize, and remediate existing vulnerabilities**

•**Predict and adapt to future threats**

•**Detect and stop cyberattacks in progress — at scale and speed**

AI in Security

Analyze massive **volumes of data**
Address the cybersecurity **skills gap**
Constantly adapt to **evolving threats** and **attack patterns**
Limit the **impact** of cyberattacks and breaches

Source: Artificial Intelligence Will Revolutionize Cybersecurity, Forrester, Sep 2017

Machine learning uses in security: supervised and unsupervised learning

Supervise
d

Supervised ML is used to identify patterns of "badness" that are similar to other known examples that can be detected by an algorithm.

Fits the problems of phishing, spam and malware classification, spam classification

Unsupervised

Unsupervised ML helps detect otherwise elusive anomalies that may indicate malicious intent.

- Domain name classification, look up, frequencies

- Threat intelligence
- Tier 1 Analyst automation
- User and Entity behavior analytics and rule-based approaches

Many products being rolled out involve "supervised learning," which requires firms to choose and label data sets that algorithms are trained on—for instance, by tagging code that's malware and code that is clean.

Does “artificial intelligence” automatically mean “better product” in security today? The Jury is still out

Many products being rolled out involve “supervised learning,” which requires firms to choose and label data sets that algorithms are trained on—for instance, by tagging code that’s malware and code that is clean.

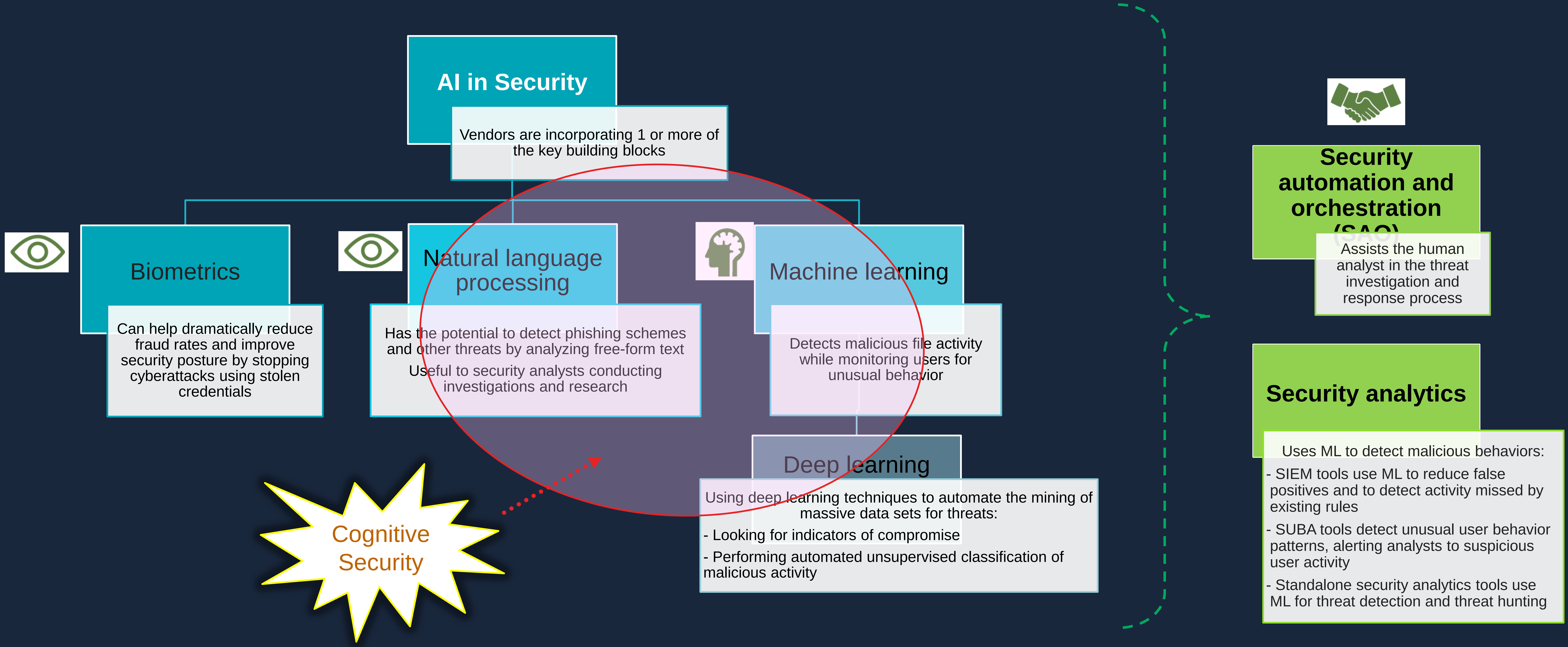
Organizations looking to implement commercial solutions based on ML should not focus on the type of ML algorithm being applied. Rather, organizations should focus on the data required to feed the solution and on the results delivered by the implementation.
Gartner, May 2019

Source : GBS Scorecards (based on QMV2Q19 & WD4 revenue), $M

Content

1. AI in cybersecurity
2. Key use cases and application areas
3. The hype AI in cybersecurity
4. Key take-aways

AI in cybersecurity is concentrated around machine learning and deep learning



AI in Security

Vendors are incorporating 1 or more of the key building blocks

Biometrics

Can help dramatically reduce fraud rates and improve security posture by stopping cyberattacks using stolen credentials

Natural language processing

Has the potential to detect phishing schemes and other threats by analyzing free-form text

Useful to security analysts conducting investigations and research

Machine learning

Detects malicious file activity while monitoring users for unusual behavior

Deep learning

Using deep learning techniques to automate the mining of massive data sets for threats:

- Looking for indicators of compromise
- Performing automated unsupervised classification of malicious activity

Cognitive Security

Security automation and orchestration (SAO)

Assists the human analyst in the threat investigation and response process

Security analytics

Uses ML to detect malicious behaviors:

- SIEM tools use ML to reduce false positives and to detect activity missed by existing rules
- SUBA tools detect unusual user behavior patterns, alerting analysts to suspicious user activity
- Standalone security analytics tools use ML for threat detection and threat hunting

Source: Artificial Intelligence Will Revolutionize Cybersecurity, Forrester, Sep 2017

Threat detection is the area with the highest potential for ML

Applying ML techniques to cybersecurity

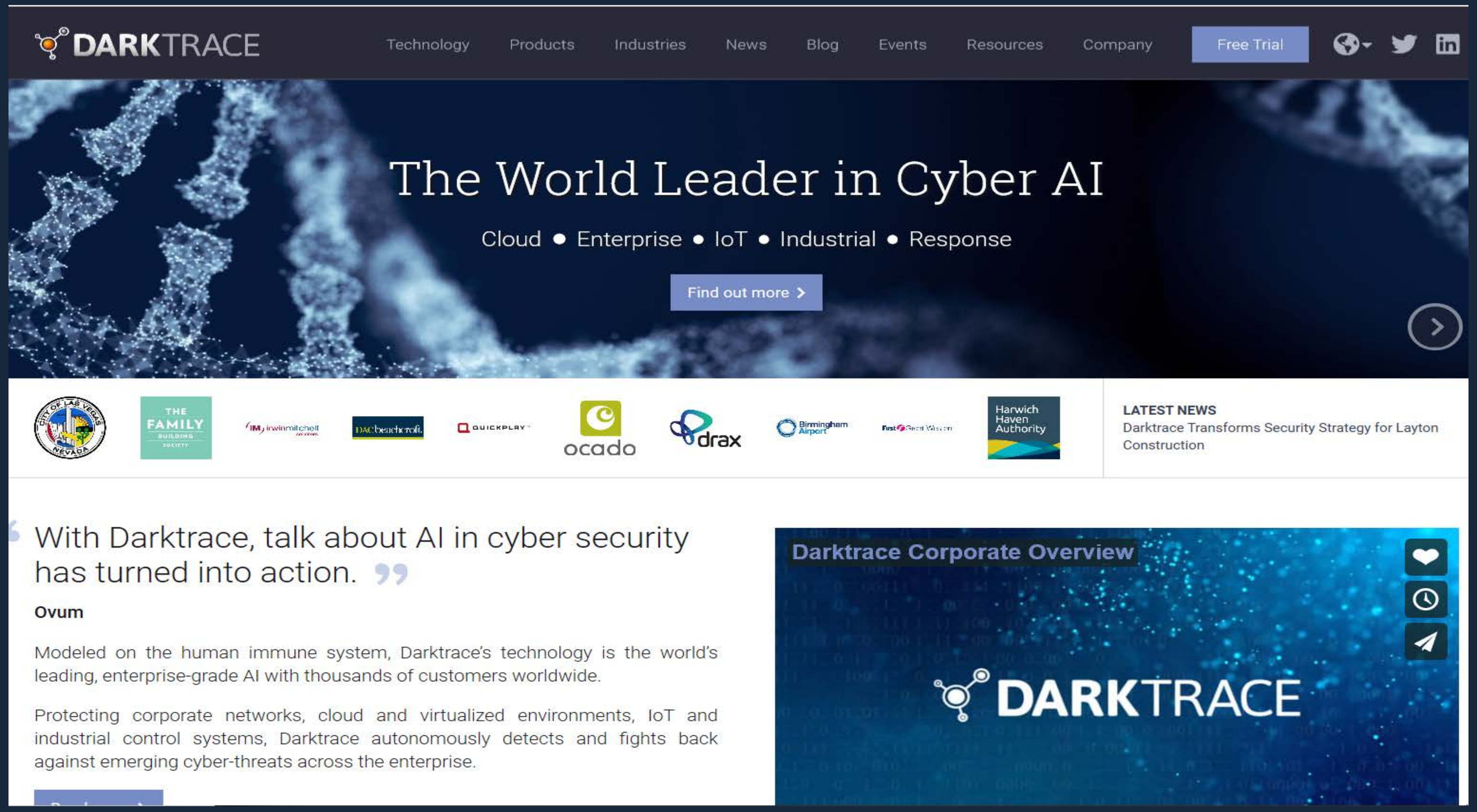
Technique	Description	Cybersecurity use case
Classification	This is a method of comparing an unknown data point against a larger data set that has a variety of known characteristics. The more data available with previously identified entries, the faster the new classification will likely be. However, if the comparative data has not been accurately classified or contains invalid data points, the new classification will be inaccurate and will grow in its inaccuracy as the machine “learns” from that data set.	Applied to cybersecurity, this is the ability of a solution to take an unknown, seemingly benign data point — a file sample, email, or log entry — and compare it to a large data set (such as data lake or other data repository) of previously identified data and have the system say this is malicious. For many current security solutions that use **ML for malware categorization and identification systems, this is the current state of the art**.
Clustering	With clustering, the goal is to find data points that naturally appear similar in nature. In cybersecurity, clustering is possible but challenging because of the wide variety of data possibilities present in items like log entries, text alerts, and file samples. This makes it difficult for an ML algorithm to cluster items correctly without wide variances in accuracy and without significant human-assisted contouring of the data. However, when cybersecurity vendors target clustering for a specific use case, it can be very effective at identifying anomalies.	In cybersecurity, security teams use clustering to identify network attacks by analyzing alert outliers visually plotted on a clustering map. In a modern SOC that has a network analysis and visibility (NAV) solution employing this technique, a data map would display a graphical representation of attack data and normal data**.. Clustering is also a technique used in security user behavior analysis (SUBA) solutions that attempt to highlight anomalous user activity.**
Regression	With regression, the goal is to measure the statistical relationship between variables based on historical data or a training data set. The variable attempting to be predicted is the dependent variable. The variables that have an impact on the dependent variable are the independent variables. In cybersecurity, for example, vendors use regression analysis to determine which factors have the most impact on the determination of whether something is malware or malicious activity.	Best exemplified by security solutions such as Cylance and Trend Micro’s and Deep Insights systems. These solutions looking at a variety of sample data and a variety of other data (e.g., a classification) and then compare specific mathematical measurements of the data as they relate to a standard mean value. **Data points measured as being too far from the standard mean value are likely the ones that merit further analysis.**

Source: Forrester, Artificial Intelligence Will Revolutionize Cybersecurity

Content

1. Introduction to AI in cybersecurity
2. Key use cases and application areas
3. The hype of AI in cybersecurity
4. Key take-aways

A plethora of AI tools and platforms claim ML as a major game changer



The World Leader in Cyber AI

Cloud ● Enterprise ● IoT ● Industrial ● Response

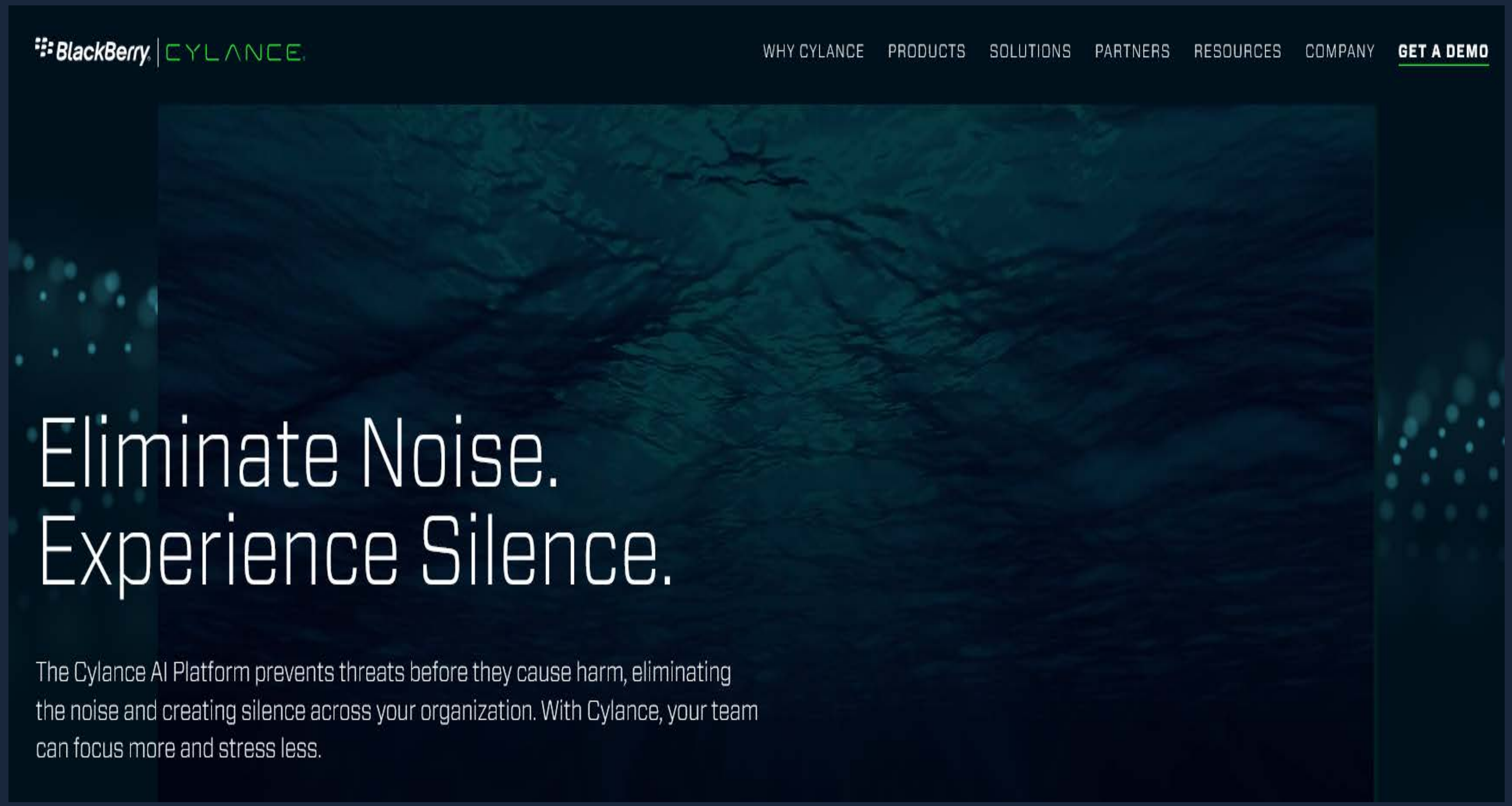
LATEST NEWS
Darktrace Transforms Security Strategy for Layton Construction

With Darktrace, talk about AI in cyber security has turned into action.

Ovum

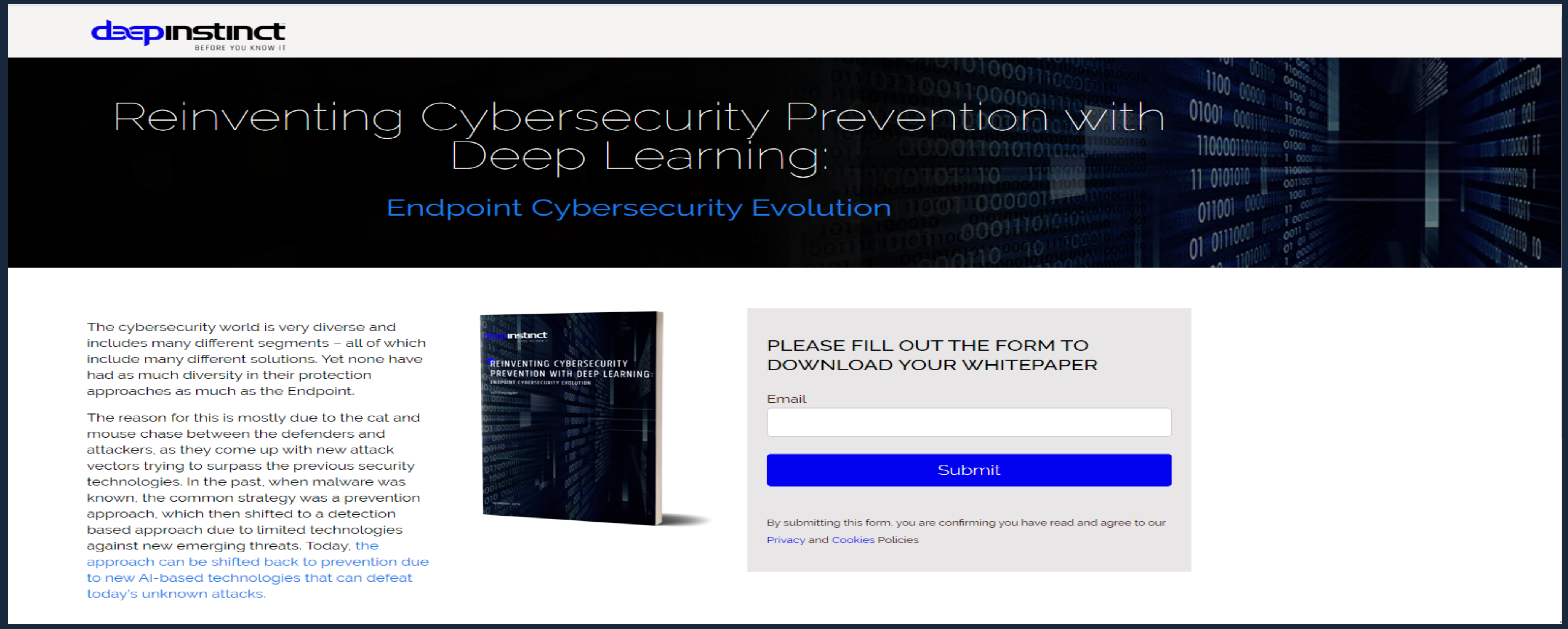
Modeled on the human immune system, Darktrace's technology is the world's leading, enterprise-grade AI with thousands of customers worldwide.

Protecting corporate networks, cloud and virtualized environments, IoT and industrial control systems, Darktrace autonomously detects and fights back against emerging cyber-threats across the enterprise.



Eliminate Noise.
Experience Silence.

The Cylance AI Platform prevents threats before they cause harm, eliminating the noise and creating silence across your organization. With Cylance, your team can focus more and stress less.


deepinstinct
REINVENTING CYBERSECURITY PREVENTION WITH DEEP LEARNING:
ENDPOINT CYBERSECURITY EVOLUTION
Submit

Reinventing Cybersecurity Prevention with Deep Learning:

Endpoint Cybersecurity Evolution

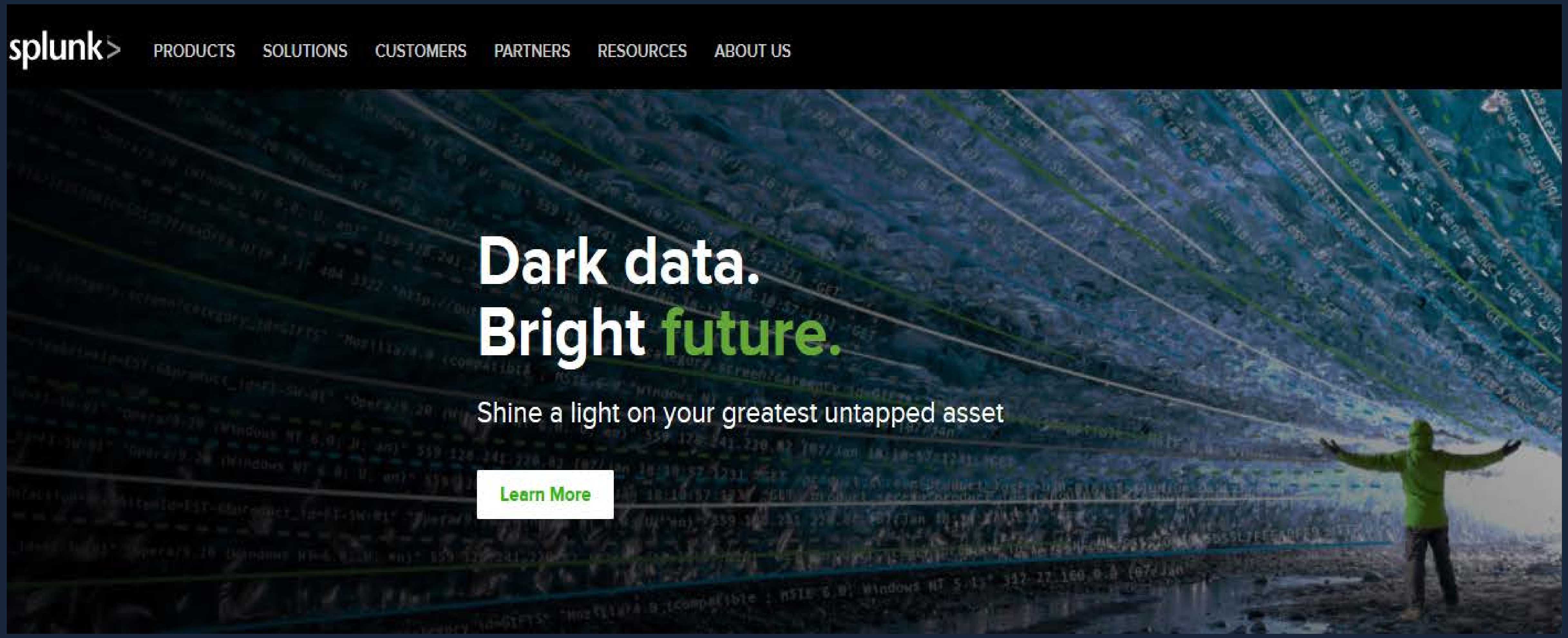
The cybersecurity world is very diverse and includes many different segments – all of which include many different solutions. Yet none have had as much diversity in their protection approaches as much as the Endpoint.

The reason for this is mostly due to the cat and mouse chase between the defenders and attackers, as they come up with new attack vectors trying to surpass the previous security technologies. In the past, when malware was known, the common strategy was a prevention approach, which then shifted to a detection based approach due to limited technologies against new emerging threats. Today, the approach can be shifted back to prevention due to new AI-based technologies that can defeat today's unknown attacks.

PLEASE FILL OUT THE FORM TO DOWNLOAD YOUR WHITEPAPER

Email

By submitting this form, you are confirming you have read and agree to our Privacy and Cookies Policies



Dark data.
Bright future.

Shine a light on your greatest untapped asset

ML is a capability not a tool but a capability

- Machine learning is still not mature enough to be the **only** layer standing between you and the cyber attackers.
- ML has its limitations in order to understand the ways in which you can ensure you've properly secured your organisation.
- The emergence of fileless attacks - machine-learning-based tools analyzing files were not able to detect those attacks. "They were just looking at the wrong place. And who does tell them where they should be looking? Humans."
- Multi-layered solutions, combined with talented and skilled people, will be the only way to stay a step ahead of the hackers as the threat landscape continues to evolve.

Despite what the shiny marketing materials might say, true artificial intelligence does not yet exist and machine learning is still not mature enough to be the only layer standing between businesses and the cyber attackers.

Content

1. Introduction to AI in Cybersecurity
2. Key use cases and application areas
3. The Hype of AI in Cybersecurity
4. Key take-aways

AI in cybersecurity can be the “silver platted bullet” for **augmenting** human capabilities …some issues to consider

1. Who is the enemy ?

2. Volume & quality of data?

3. Transparency / Auditability ?

4. Use case-based strategy?

5. How easy is the system to defeat?

“We (IBM) believe that data is the phenomenon of our time. It is the world’s new natural resource. It is the new basis of competitive advantage, and it is transforming every profession and industry. If all of this is true – even inevitable – then ***cyber crime, by definition, is the greatest threat to every profession, every industry, every company in the world.”***

Ginny Rometti, IBM CEO and Chairman

Back-up