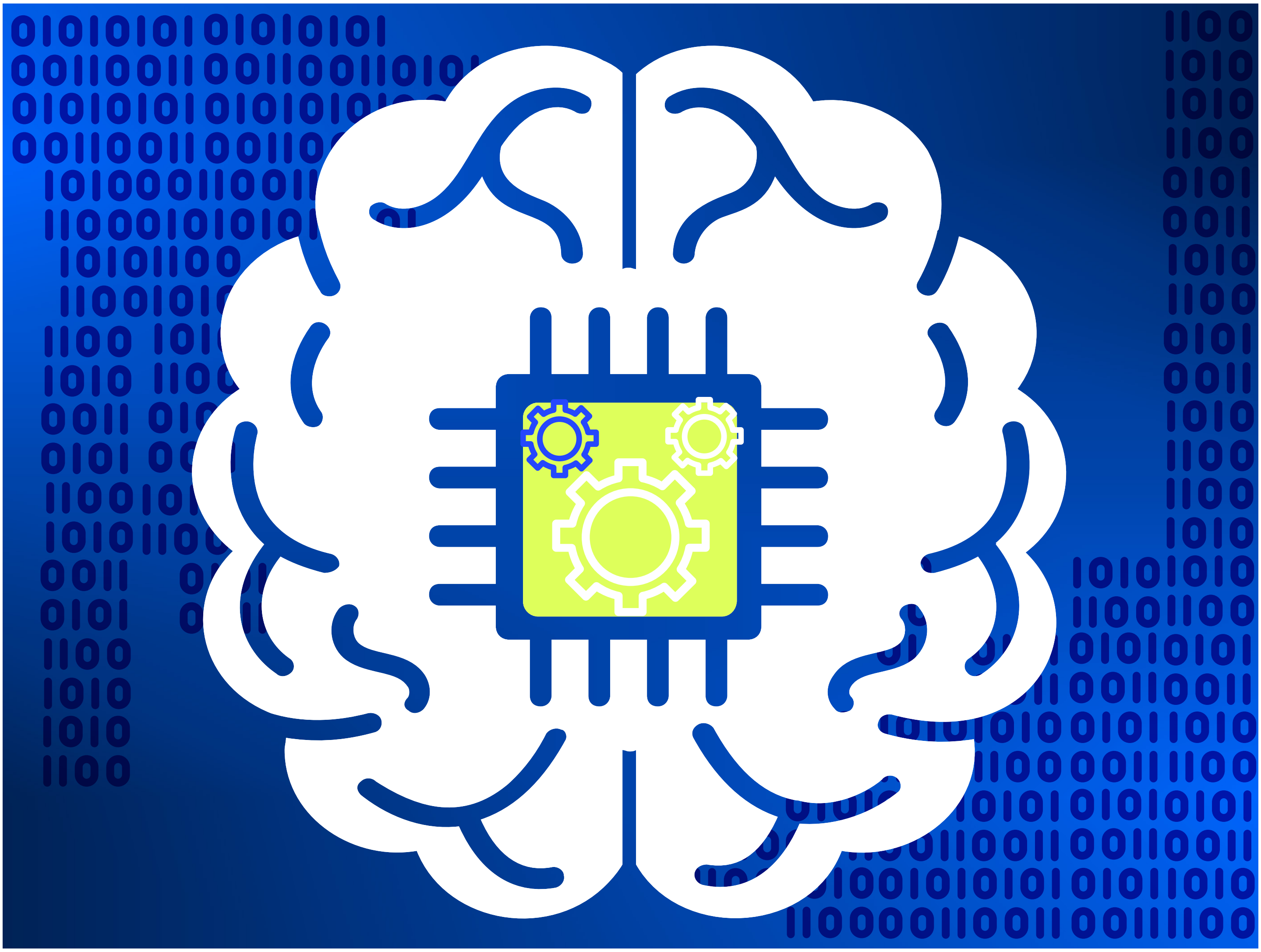
MIT Technology Review Insights

Produced in association with

deep instinct™

Enterprises need to start thinking differently about cybersecurity to get ahead of bad actors.

Deep learning delivers proactive cyber defense



Key takeaways

1 In the first quarter of 2022, U.S. data breaches increased 14% over the first quarter of 2021.

2 Deep learning offers an autonomous, highly accurate way to identify sophisticated attack patterns and predict adversarial threats before they happen, without the need for highly skilled cybersecurity experts.

3 If companies are to make headway against bad actors, they need a mindset shift from detection to prevention. As cyberattacks become more technologically sophisticated, using techniques like adversarial AI, more advanced tools like deep learning are needed to prevent breaches.

Cybersecurity professionals are constantly looking for new and innovative ways to stay one step ahead of attackers. Yet, in the first quarter of 2022 alone, there were 404 publicly reported data breaches in the U.S. – a 14% increase compared to the first quarter of 2021, **according** to the Identity Theft Resource Center. Of particular concern is the alarming rise in ransomware breaches, which increased by 13% in a single year – representing a jump greater than the past five years combined, according to the **2022 Verizon Data Breach Investigations Report (DBIR)**.

No wonder an increasing number of organizations are beginning to explore how deep learning, and its ability to mimic the human brain, can outsmart and outpace the world's fastest and most dangerous cyber threats.

The most advanced form of artificial intelligence (AI) technology, and a type of machine learning, deep learning uses neural networks to instinctively and autonomously anticipate and prevent unknown malware and zero-day attacks before they can wreak havoc on an IT environment.

Most cybersecurity technologies, such as endpoint detection and response (EDR) solutions, simply identify, track, record, and contain a threat once it has already entered an environment. Machine learning–based cybersecurity solutions are also an essential part of any security strategy, and use pre-labeled data, classified as either benign or malicious, to detect dangerous patterns.

But neither set of cybersecurity solutions can proactively defend against sophisticated attacks without constant human tweaking. Fortunately, deep learning can mimic the functionality and connectivity of neurons in the human brain, enabling neural networks to independently learn from raw and un-curated data and automatically recognize unknown threats.

"Deep learning is the only family of algorithms that works on raw data to identify cybersecurity threats with unmatched speed and accuracy," says Guy Caspi, CEO of Deep Instinct, a cybersecurity company.

The result is a powerful solution that can accurately identify highly sophisticated attack patterns at record speeds.

Time for a different line of defense

Although deep learning has been around since the 1940s, the high cost and complexity of graphics processing units (GPUs) have kept the technology out of reach for many organizations. But that's changing with the increasing processing power and lower costs of graphics chips.

> "If we are to ever get ahead of our adversaries, the world needs to change the mindset from detection to one of prevention."
> **Guy Caspi, CEO of Deep Instinct**

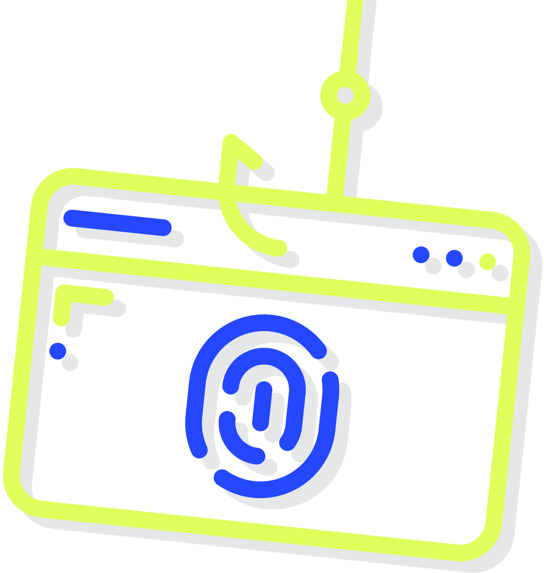
The timing couldn't be better. The increasing availability of ransomware-as-a-service offerings, such as ransomware kits and target lists, are making it easier than ever for bad actors – even those with limited experience – to launch a ransomware attack, causing crippling damage in the very first moments of infection. Other sophisticated attackers use targeted strikes, in which the ransomware is placed inside the network to trigger on command.

Another cause for concern is the increasing disappearance of an IT environment's perimeter as cloud compute storage and resources move to the edge. Today's organizations must secure endpoints or entry points of end-user devices (such as desktops, laptops, and mobile devices) from being exploited by malicious hackers – a challenging feat, according to Michael Suby, research vice president, security and trust, at International Data Corporation (IDC). "Attacks continue to evolve, as do the endpoints themselves and the end users who utilize their devices," he says. "These dynamic circumstances create a trifecta for bad actors to enter and establish a presence on any endpoint and use that endpoint to stage an attack sequence."

The increased pace of high-profile threats (e.g., ransomware) is up to double-digit (15.8%) growth. The result is a dangerous path most likely to lead to continued losses for organizations that fall victim to a cyberattack without any gains in defensive powers. Indeed, a 2021 data breach report by IBM and the Ponemon Institute **reveals** that the average cost of a data breach is $4.24 million.

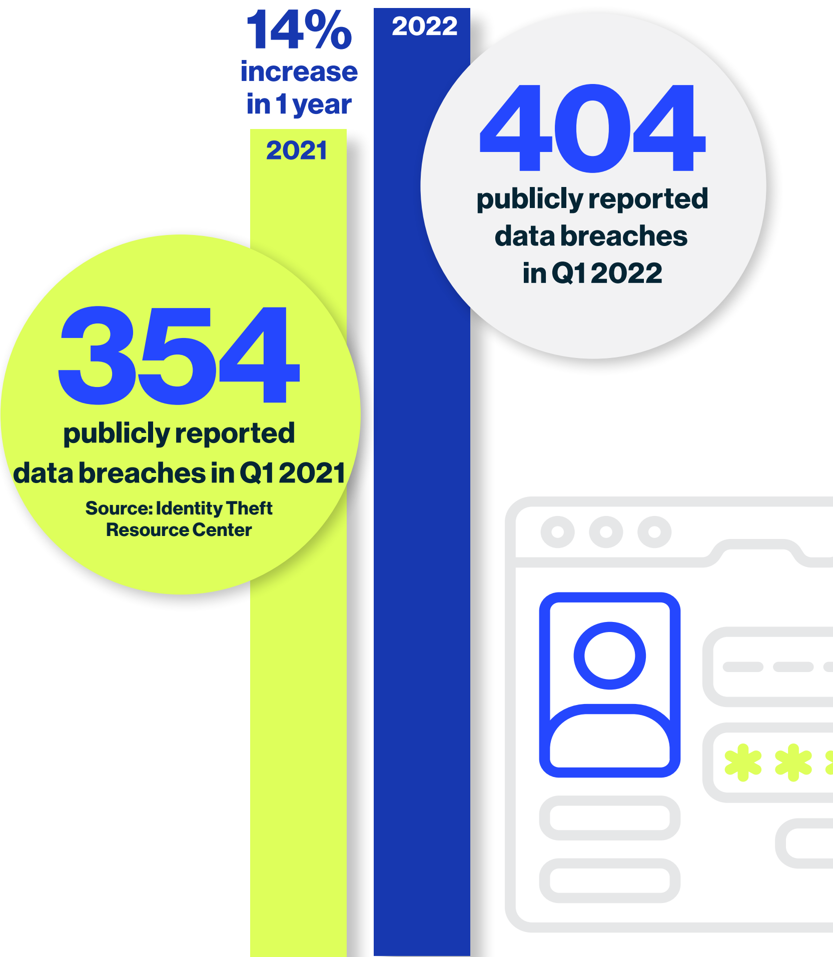
Beyond costs, a cyberattack can cause irreparable damage to a company's brand, share price, and day-to-day operations. According to a recent Deloitte **survey**, 32% of respondents cited operational disruption as the biggest impact of a cyber incident or breach. Other repercussions cited by companies include intellectual property theft (22%), a drop in share price (19%), reputational loss (17%), and a loss of customer trust (17%).

Given these significant risks, organizations simply can't afford to accept the status quo on protecting digital assets. "If we are to ever get ahead of our adversaries, the world needs to change the mindset from detection to one of prevention," says Caspi. "Organizations need to change the way they perform security and combat hackers."



INCREASING NUMBER OF DATA BREACHES IN THE UNITED STATES

If the first quarter of the past two calendar years is any indication, the rate of data breaches will keep increasing year over year.

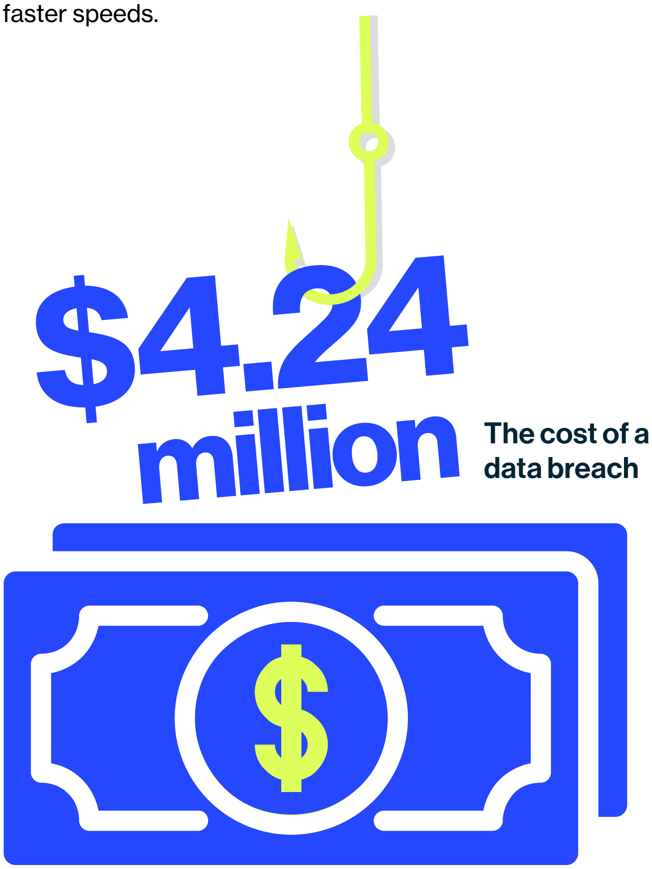


Source: Identity Theft Resource Center

Deep learning can be the difference

Up until now, many cybersecurity experts have viewed machine learning as the most innovative approach to safeguarding digital assets. But deep learning is ideally suited to change the way we prevent cybersecurity attacks. Any machine learning tool can be understood, and theoretically reverse engineered to introduce a bias or vulnerability that will weaken its defenses against an attack. Bad actors can also use their own machine learning algorithms to pollute a defensive solution with false data sets.

Fortunately, deep learning addresses the limitations of machine learning by circumventing the need for highly skilled and experienced data scientists to manually feed a solution data sets. Rather, a deep learning model, specifically developed for cybersecurity, can absorb and process vast volumes of raw data to fully train the system. These neural networks become autonomous, once trained, and do not require constant human intervention. This combination of a raw data–based learning methodology and larger data sets means that deep learning is eventually able to accurately identify much more complex patterns than machine learning, at far faster speeds.



$4.24 million The cost of a data breach

Source: Cost of a Data Breach Report 2021 by IBM and the Ponemon Institute

Deep learning in enterprise applications

Because deep learning technology is effective at automating tasks normally performed by humans, enterprise applications are plentiful and increasingly commonplace. A 2021 global survey of 500 CTOs conducted by STX Next found that 20.7% of CTOs have implemented deep learning technologies into their stacks.

COMMON ENTERPRISE USE CASES

Natural language processing. This technology fuels bots, virtual assistants, translators, and text applications like auto-correct and sentiment analysis. Most of us interact with this technology every day with such tasks as filtering e-mail and searching websites and the internet.

Anomaly detection. This application of deep learning is important and widespread across industries. It's used to detect fraudulent transactions, to identify faults in manufacturing systems, to detect intrusions into network infrastructures, and to assist in interpreting medical imaging, to name just a few use cases.

Computer vision. Image and pattern recognition technologies offer a broad swath of applications across industries. In manufacturing, for example, they can help detect product defects on an assembly line. They can review static or real-time images and video for classification or labeling, or identify modified images or deepfakes. Other applications include image and video review to identify customer or employee theft; to ensure safety measures are followed by employees, such as hand washing in restaurants, or the use of hard hats on construction sites; and even to facilitate remote preventative maintenance in industries like wind farming.

These applications represent just the tip of the iceberg for potential deep learning use cases in enterprise. According to recent market research, the "global deep learning market was valued at $2.99 billion in 2021 and is expected to reach $68.70 billion by 2029." The main drivers identified include rising trends toward digitization, increase in cyberattacks, and increasing integrations with advanced technologies.

"Deep learning outshines any deny list, heuristic-based, or standard machine learning approach," says Mirel Sehic, vice president and general manager for Honeywell Building Technologies (HBT), a multinational corporation and provider of aerospace, performance materials, and safety and productivity technologies. "The time it takes for a deep learning–based approach to detect a specific threat is much quicker than any of those elements combined."

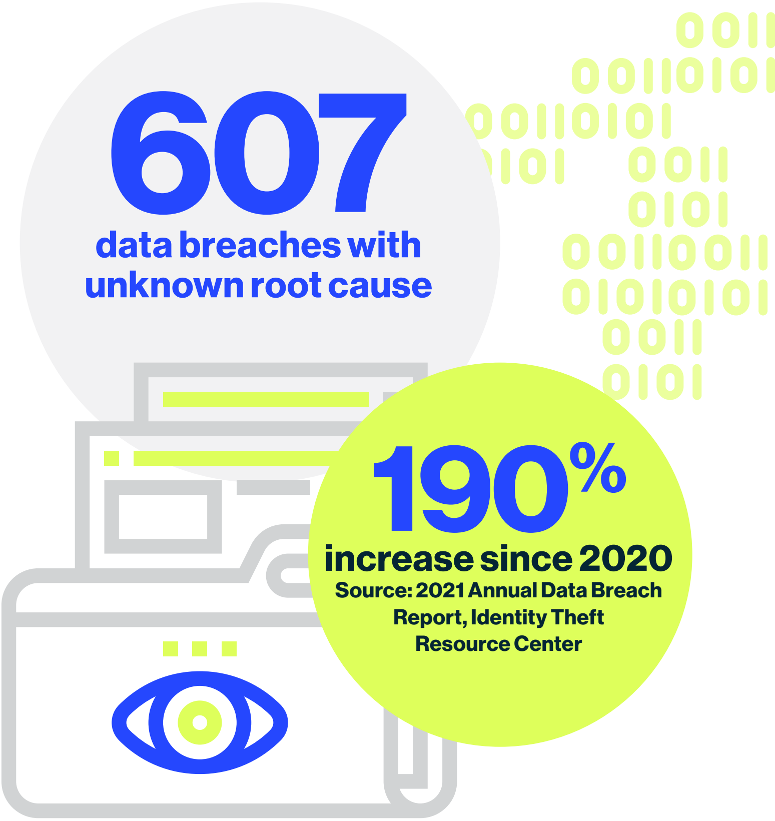
Another advantage of deep learning is its ability to predict the threat of adversarial AI. Adversarial machine learning is a technique that tricks AI models by feeding them deceptive data. Essentially, adversaries intentionally exploit the way traditional machine learning–based solutions work by finding a bias that will bypass their detection capabilities and deceive them into accepting malicious files as benign. However, because a deep learning network doesn't rely on feature engineering, it's more challenging for threat actors to create malware that can understand and exploit how the system works.

What's more, a deep learning model can be deployed on any endpoint using negligible processing resources. Other technological advantages of deep learning include a substantially higher accuracy rate in identifying malware and other fileless threats and a much lower false-positive rate. And because deep learning is agnostic to file types, it can be applied to any file format, even to any operating system, without requiring substantial modifications or adaptations.

"Machine learning relies heavily on a manual tasking where you have to extrapolate and manually direct features to teach machine learning algorithm models," says Sehic. "However, an unsupervised deep learning model can be bombarded with copious amounts of data and, if properly and purposefully built, it will sort through it all" to proactively predict and detect cybersecurity attacks.

Bottom-line gains possible

In addition to its technological prowess, deep learning also offers significant business benefits and cost savings. "It's not possible to directly feed raw data into a machine learning model," says Caspi. As a result, he says, "cybersecurity teams must analyze the data and determine its most important features and properties." The problem with this scenario, he says, is that hiring and retaining the necessary talent to perform feature extraction can be both costly and challenging, especially in today's tight labor market.



607

data breaches with unknown root cause

190%

increase since 2020

Source: 2021 Annual Data Breach Report, Identity Theft Resource Center

Conversely, the "low-touch aspect" of deep learning makes it particularly appealing to resource-strapped organizations, says Sehic. "You don't need to have eyeballs on the screen or a highly skilled cybersecurity professional combing through a bunch of data," he says. Rather, deep learning "as it relates to improved cybersecurity threat detection, is all about the ability to detect novel and new threats with very minimal human interaction while not requiring constant updates to that specific model. When you combine these factors with deep learning's low false-positive rate, it's unparalleled in the industry."

Investing in people, best practices, and partners

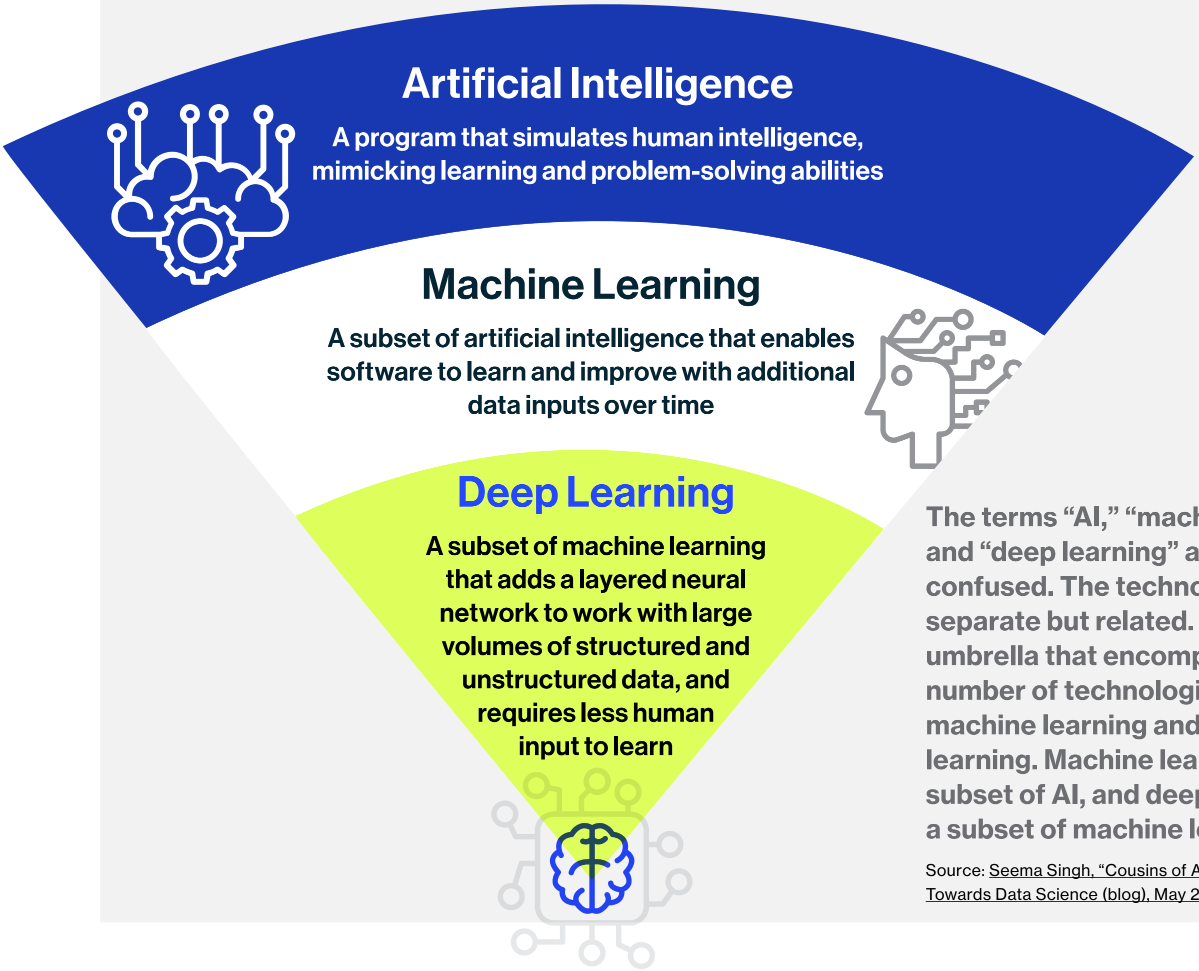
Despite significant business benefits, there are some important measures organizations must take before fully embracing deep learning. For starters, Caspi says it's critical that cybersecurity teams carefully consider the quantity and quality of their training data. That's because the better the training data, the better a deep learning model will perform.

Another way to make the most of deep learning is to use it with other technologies, such as natural language processing and dynamic network analysis. Doing so can dramatically increase protection and prevention capabilities. Building a best-of-class cyber-defense system with a focus on real-time prevention using deep learning can ensure the rapid detection of increasingly complex attack vectors and components.

Even the most powerful cybersecurity defense toolkit, however, requires skilled IT professionals at the helm. “People as a whole are the linchpin to a good security architecture and security practice,” says Sehic of Honeywell. “For us, it really starts with having the right team on board to focus on operational technology challenges across critical infrastructure environments.”

> “Deep learning outshines any deny list, heuristic-based, or machine-learning approach.”
>
> **Mirel Sehic, head of cybersecurity at Honeywell**

AI vs. machine learning vs. deep learning



Artificial Intelligence

A program that simulates human intelligence, mimicking learning and problem-solving abilities

Machine Learning

A subset of artificial intelligence that enables software to learn and improve with additional data inputs over time

Deep Learning

A subset of machine learning that adds a layered neural network to work with large volumes of structured and unstructured data, and requires less human input to learn

The terms “AI,” “machine learning,” and “deep learning” are often confused. The technologies are separate but related. AI is a broad umbrella that encompasses a number of technologies, including machine learning and deep learning. Machine learning is a subset of AI, and deep learning is a subset of machine learning.

Source: Seema Singh, “Cousins of Artificial Intelligence,” Towards Data Science (blog), May 27, 2018

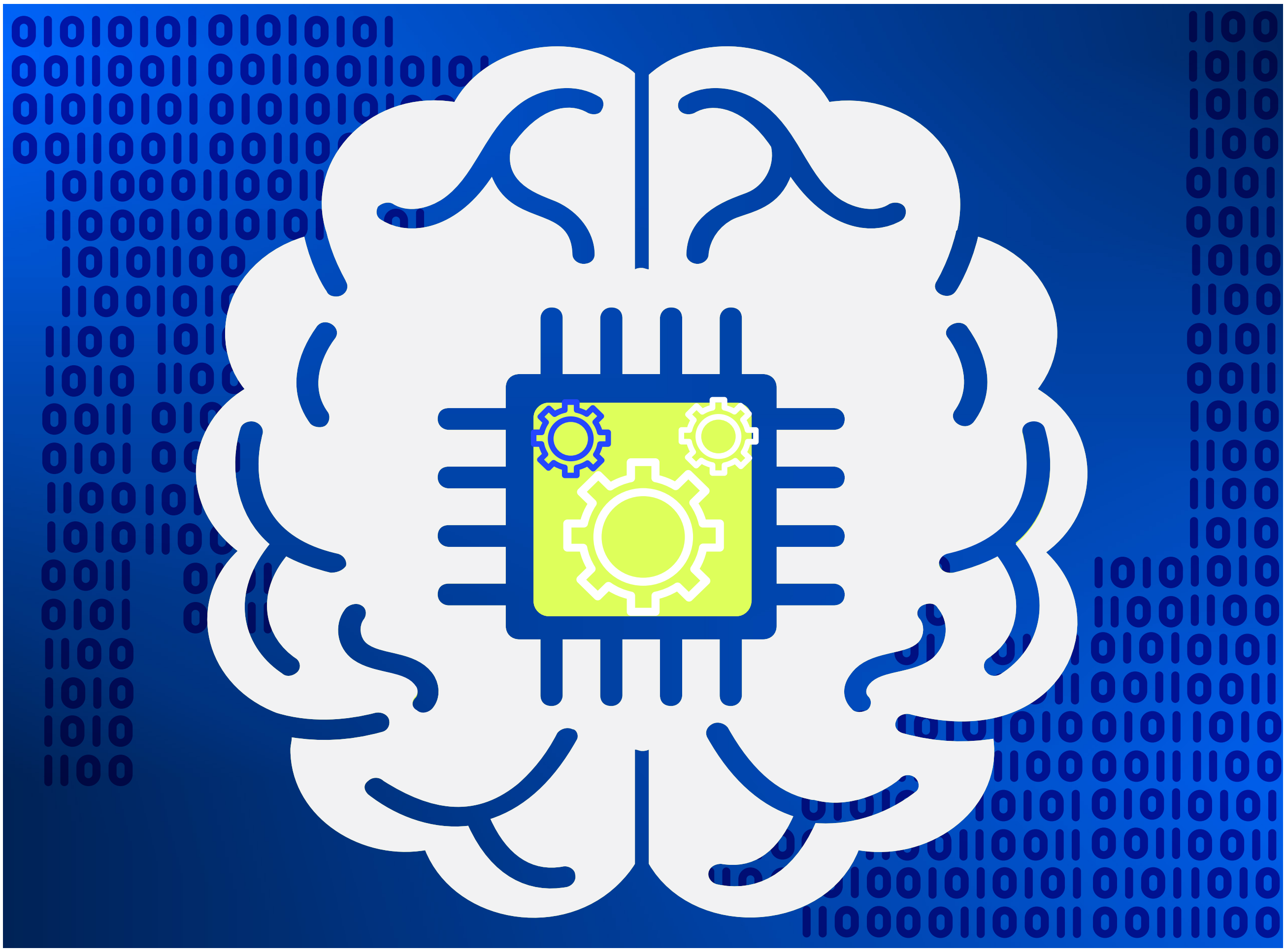
For this reason, Sehic says organizations must take the time to continuously educate those working on cybersecurity and the introduction of deep learning systems, as well as raise cybersecurity awareness among employees in non-security roles. Educational initiatives include helping employees recognize the potential impact of an attack on an organization's financial well-being, the increasing prevalence of cybersecurity threats, and the countermeasures and best practices that can keep systems safe from ill-intentioned actors.

An ever-evolving roster of cybersecurity attacks also requires an ever-evolving arsenal of cybercrime-fighting tools and techniques. Yet, most IT teams lack the time and expertise to constantly vet new vendors and solutions, says Suby of IDC. For this reason, he says, "many organizations partner with a managed service provider, or a managed security service provider, to guide them to the products and technologies they should use. Leveraging these relationships assists in ensuring organizations have the most optimal solutions in place to protect their environment."

A 'new paradigm'

By mimicking the functionality of the human brain, deep learning can recognize suspicious activities that might indicate the presence of bad actors or malware with unmatched speed and accuracy. Doing so helps organizations better anticipate and prevent attacks before they have a chance to tarnish a brand's reputation, erode share price, or lead to revenue losses. That's not to suggest, however, that deep learning alone can combat hackers. Rather, a potent combination of deep learning, seasoned talent, and best practices can provide a distinct competitive advantage in a fast-moving world.

As Sehic explains, "we're moving to this new paradigm where innovative solutions using deep learning come out of the realm of being a 'magical thing' that only very specialized, high-tech people use, to now being available for everyone."



"Deep learning delivers proactive cyber defense" is an executive briefing paper by MIT Technology Review Insights. We would like to thank all participants as well as the sponsor, Deep Instinct. MIT Technology Review Insights has collected and reported on all findings contained in this paper independently, regardless of participation or sponsorship. Laurel Ruma was the editor of this report, and Nicola Crepaldi was the publisher.

About MIT Technology Review Insights

MIT Technology Review Insights is the custom publishing division of MIT Technology Review, the world's longest-running technology magazine, backed by the world's foremost technology institution – producing live events and research on the leading technology and business challenges of the day. Insights conducts qualitative and quantitative research and analysis in the US and abroad and publishes a wide variety of content, including articles, reports, infographics, videos, and podcasts. And through its growing MIT Technology Review Global Insights Panel, Insights has unparalleled access to senior-level executives, innovators, and entrepreneurs worldwide for surveys and in-depth interviews.

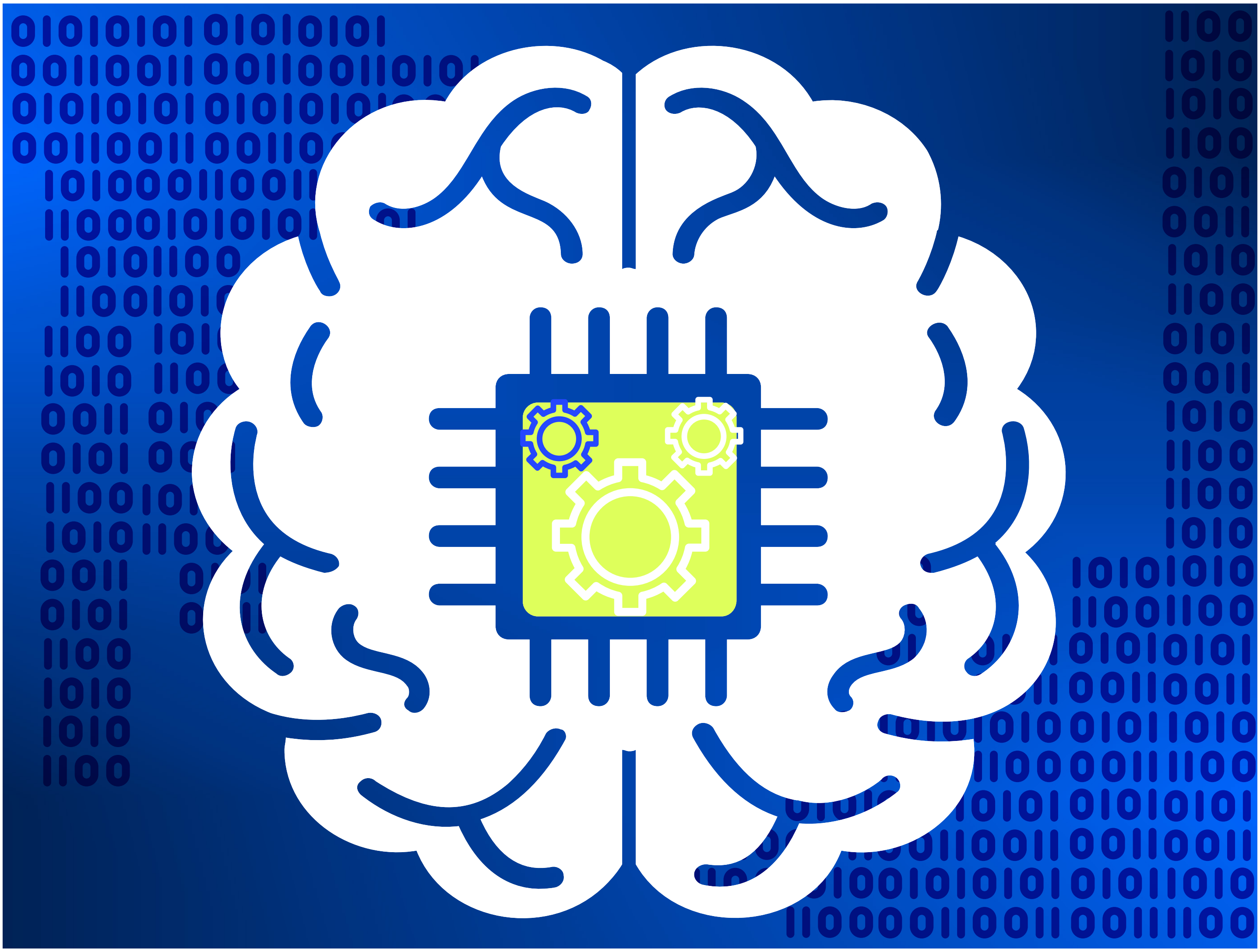
From the sponsor

Deep Instinct takes a prevention-first approach to stopping ransomware and other malware using the world's first and only purpose-built deep learning cybersecurity framework. We predict and prevent known, unknown, and zero-day threats in less than 20 milliseconds, 750 times faster than the fastest ransomware can encrypt. Deep Instinct has more than 99% zero-day accuracy and promises a less than <0.1% false positives rate. The Deep Instinct Prevention Platform is an essential addition to every security stack – providing completed, multi-layered protection against threats across hybrid environments. For more, visit **www.deepinstinct.com**.

deep instinct™

Illustrations
Cover art and spot illustrations created by Chandra Tallman Design LLC, compiled from The Noun Project.

While every effort has been taken to verify the accuracy of this information, MIT Technology Review Insights cannot accept any responsibility or liability for reliance on any person in this report or any of the information, opinions, or conclusions set out in this report.



MIT Technology Review Insights

www.technologyreview.com
@techreview @mit_insights
insights@technologyreview.com