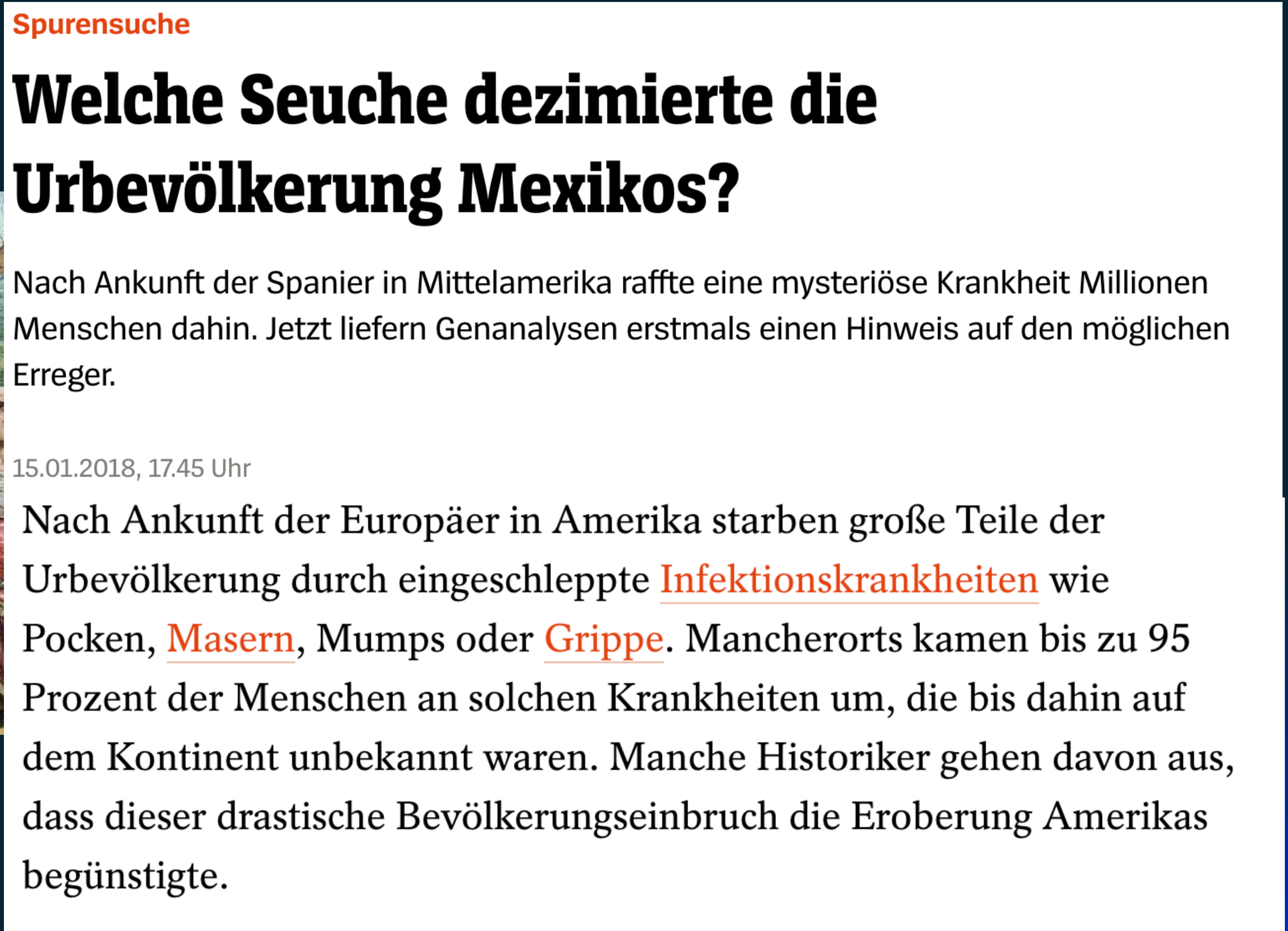
deep instinct

Vorbeugen statt heilen – wie neuronale Netze Unternehmen sicherer machen

The conques



Spurensuche

Welche Seuche dezimierte die Urbevölkerung Mexikos?

Nach Ankunft der Spanier in Mittelamerika raffte eine mysteriöse Krankheit Millionen Menschen dahin. Jetzt liefern Genanalysen erstmals einen Hinweis auf den möglichen Erreger.

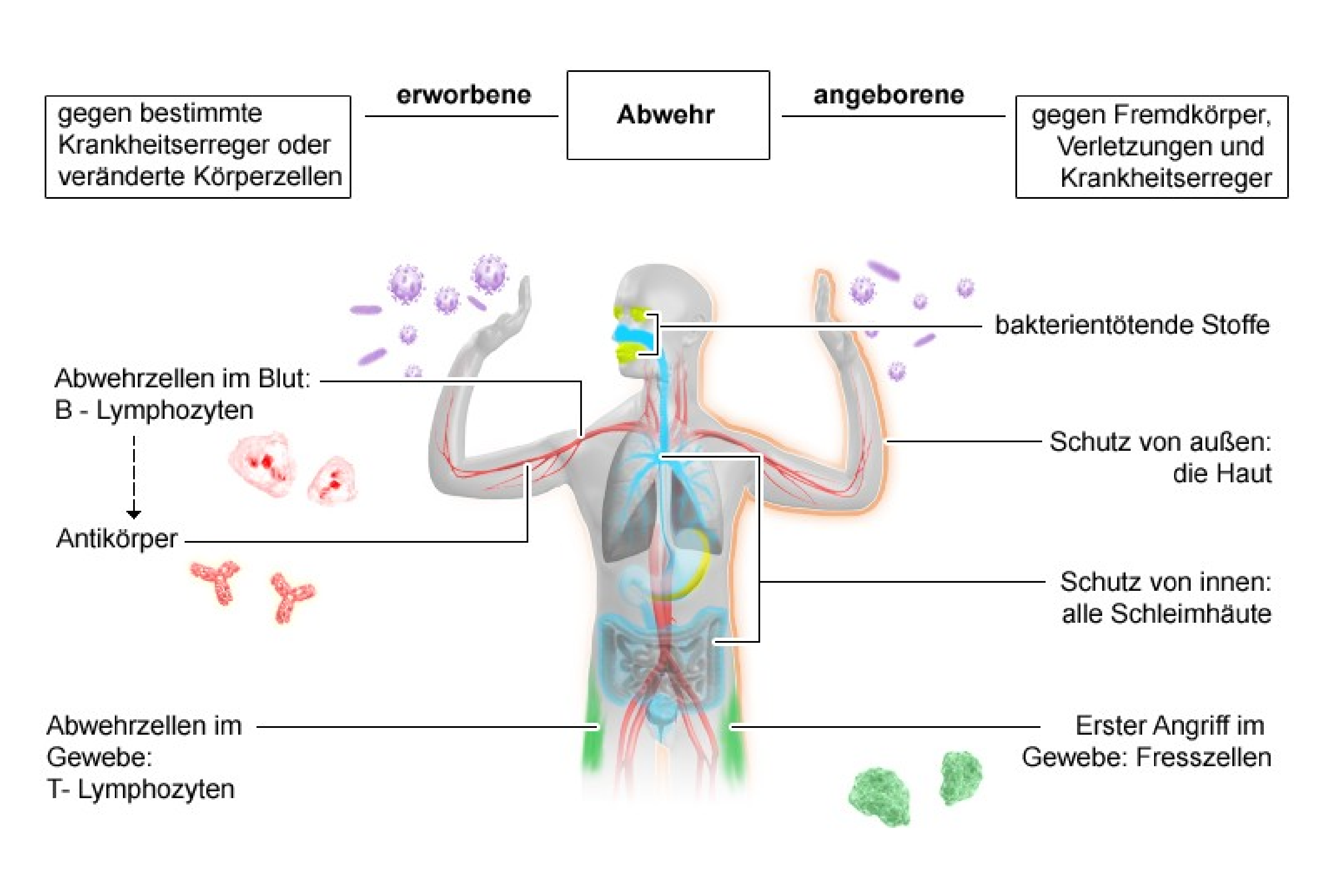
15.01.2018, 17.45 Uhr

Nach Ankunft der Europäer in Amerika starben große Teile der Urbevölkerung durch eingeschleppte Infektionskrankheiten wie Pocken, Masern, Mumps oder Grippe. Mancherorts kamen bis zu 95 Prozent der Menschen an solchen Krankheiten um, die bis dahin auf dem Kontinent unbekannt waren. Manche Historiker gehen davon aus, dass dieser drastische Bevölkerungseinbruch die Eroberung Amerikas begünstigte.

https://www.tagesspiegel.de/wissen/kolumbus-4046653.html

https://www.spiegel.de/wissenschaft/mensch/mexiko-welche-seuche-dezimierte-die-urbevoelkerung-a-1187998.html

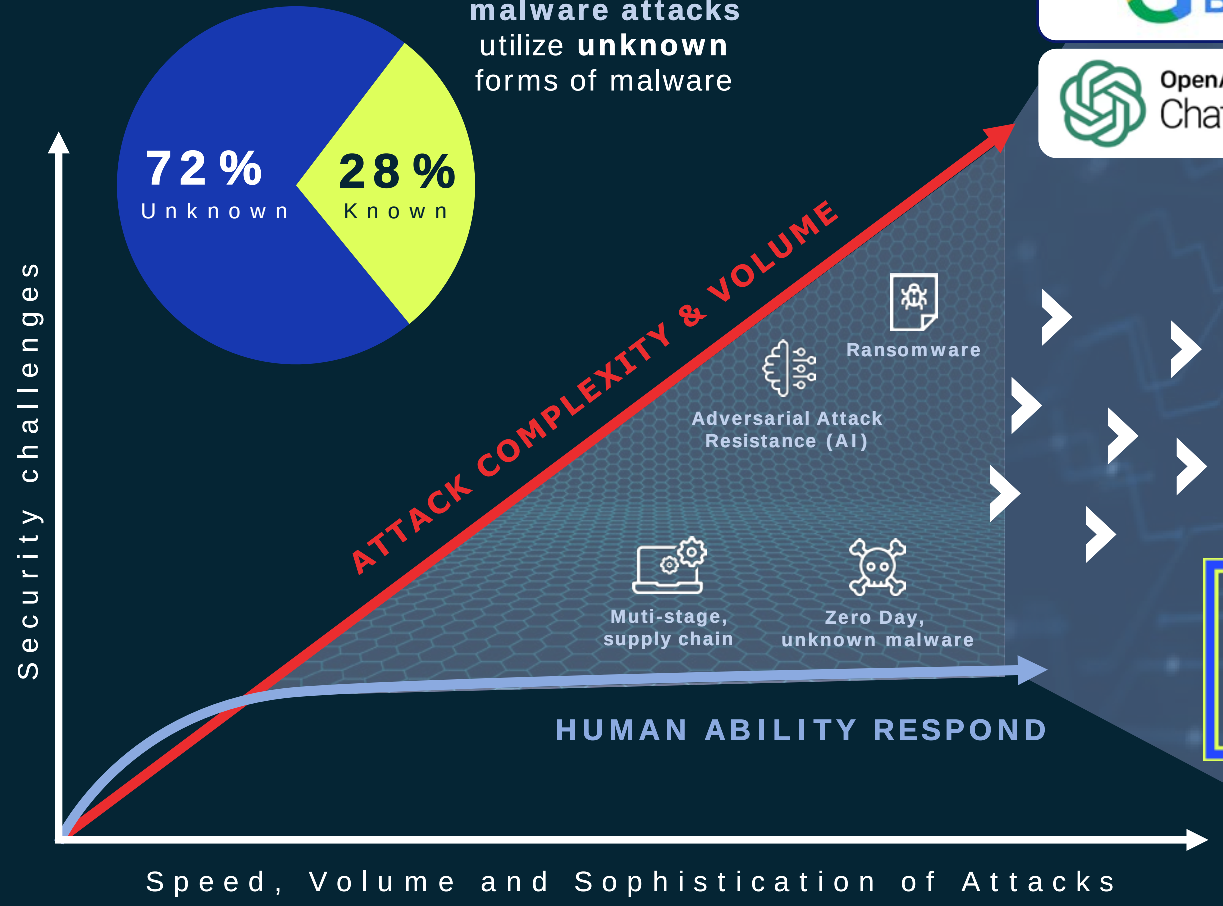
The innate and adaptive immune systems


erworbene
Abwehr
angeborene
gegen bestimmte Krankheitserreger oder veränderte Körperzellen
gegen Fremdkörper, Verletzungen und Krankheitserreger
bakterientötende Stoffe
Abwehrzellen im Blut: B - Lymphozyten
Antikörper
Schutz von außen: die Haut
Schutz von innen: alle Schleimhäute
Abwehrzellen im Gewebe: T- Lymphozyten
Erster Angriff im Gewebe: Fresszellen

https://www.gesundheitsinformation.de/das-angeborene-und-das-erworbene-immunsystem.html

Who wants to conquer us today; unknown AI-generated Threats

72% of **malware attacks** utilize **unknown** forms of malware



Bard

OpenAI ChatGPT4.0

AI Mutating Malware

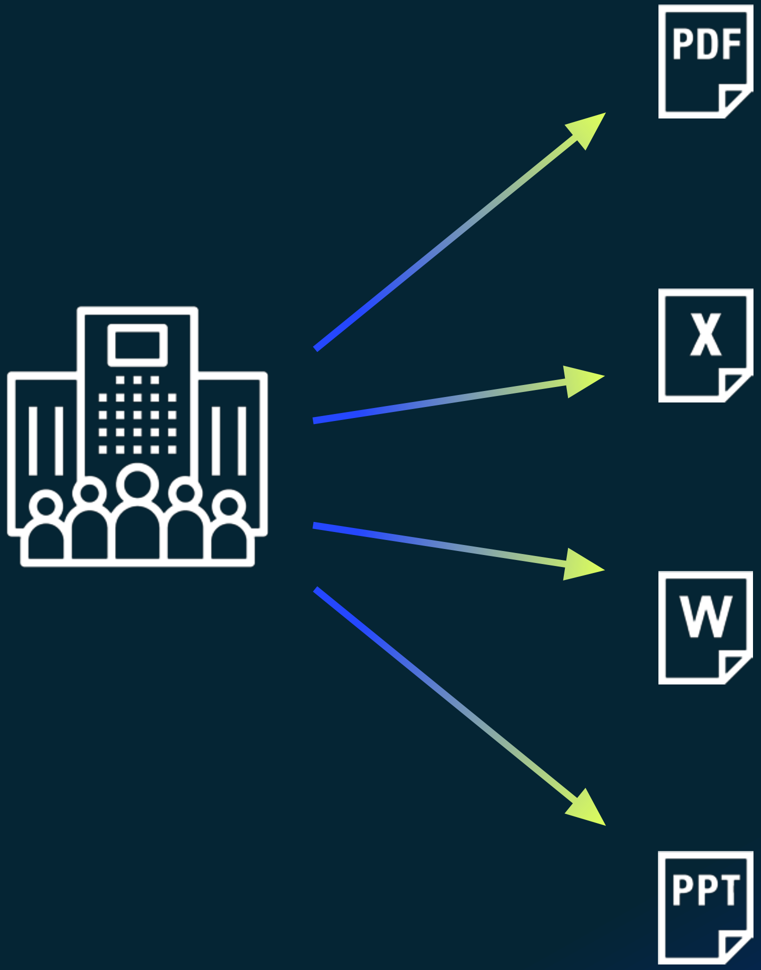
Unknown Malware as the norm

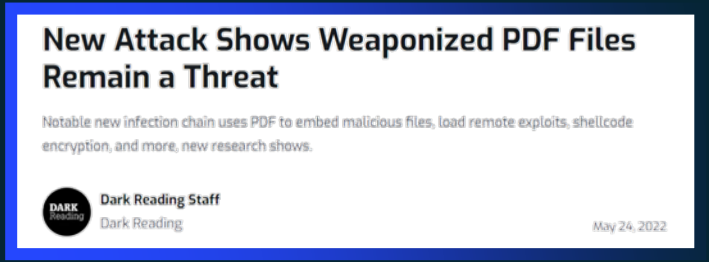
Zero Day → **Zero Hour** → **Zero Minute**

43%

of all malware downloads are **Malicious Office Documents***

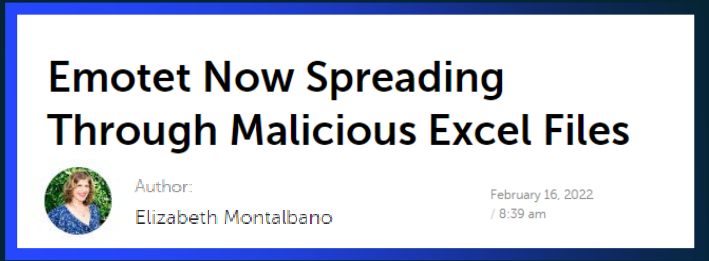
File Uploads and Downloads: Increased Malware Risk



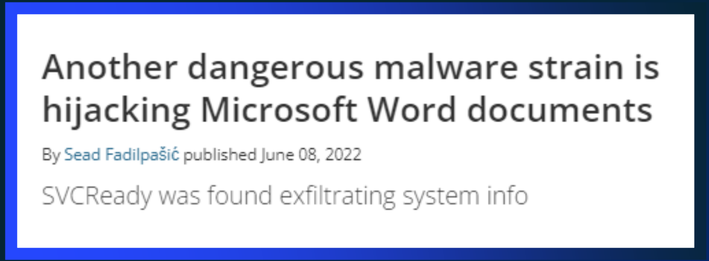

New Attack Shows Weaponized PDF Files Remain a Threat

Notable new infection chain uses PDF to embed malicious files, load remote exploits, shellcode encryption, and more, new research shows.

Dark Reading Staff
Dark Reading
May 24, 2022

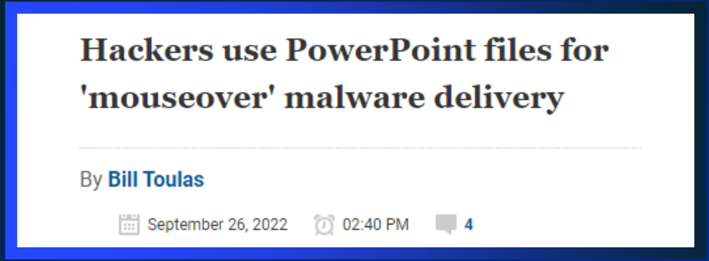

Emotet Now Spreading Through Malicious Excel Files

Author:
Elizabeth Montalbano
February 16, 2022
/ 8:39 am


Another dangerous malware strain is hijacking Microsoft Word documents

By Sead Fadilpašić published June 08, 2022

SVCReady was found exfiltrating system info


Hackers use PowerPoint files for 'mouseover' malware delivery

By Bill Toulas

September 26, 2022 02:40 PM 4

43 %

of all malware downloads are **Malicious Office Documents***

*Source: Atlas VPN 2021

deep instinct

Data Breach – Just the Facts

$9.44M

Average cost of a data breach

$4.54M

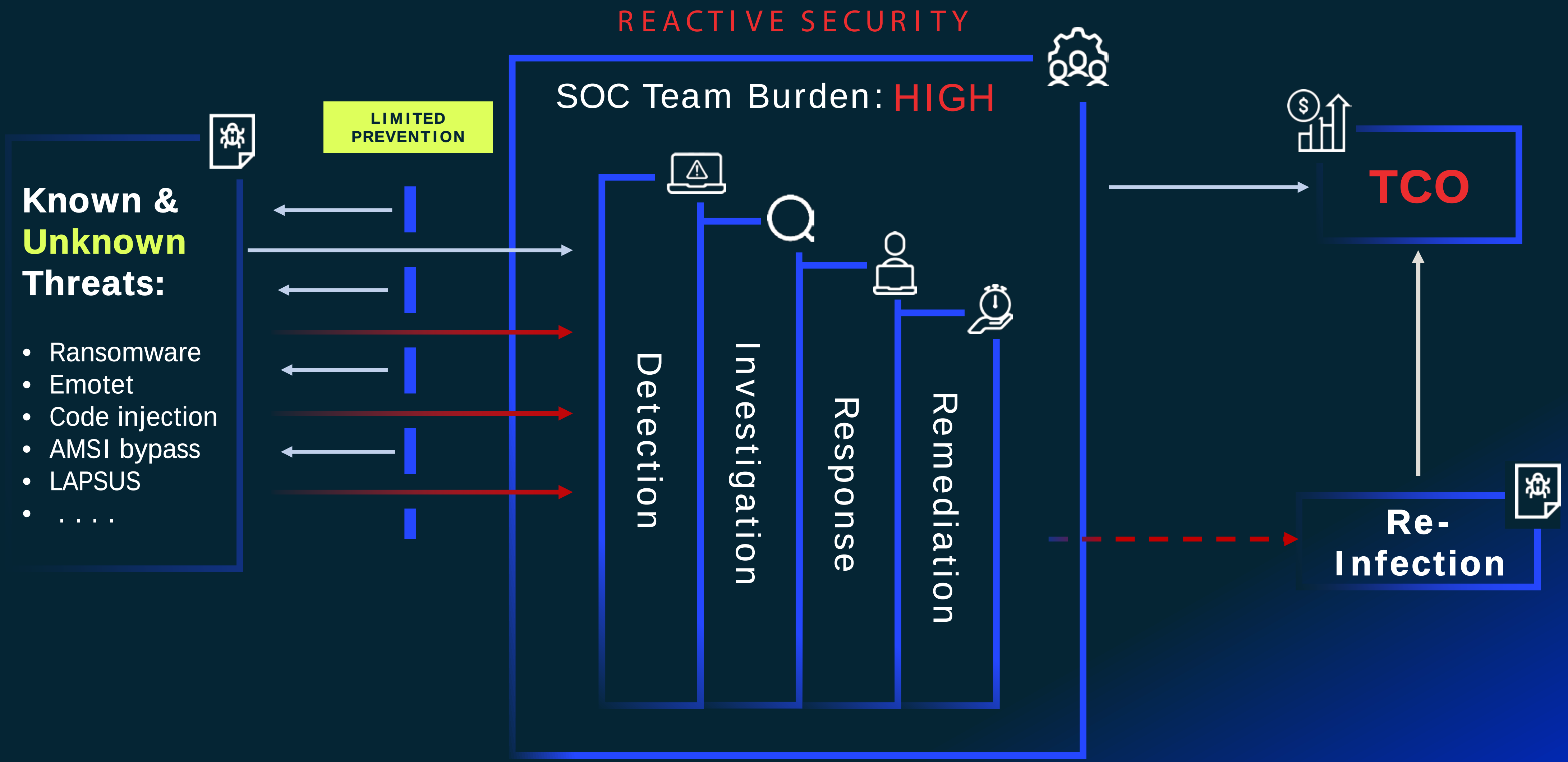
Average cost of a ransomware attack

277 Days

Average to contain a data breach

Source: IBM Security Report 2023

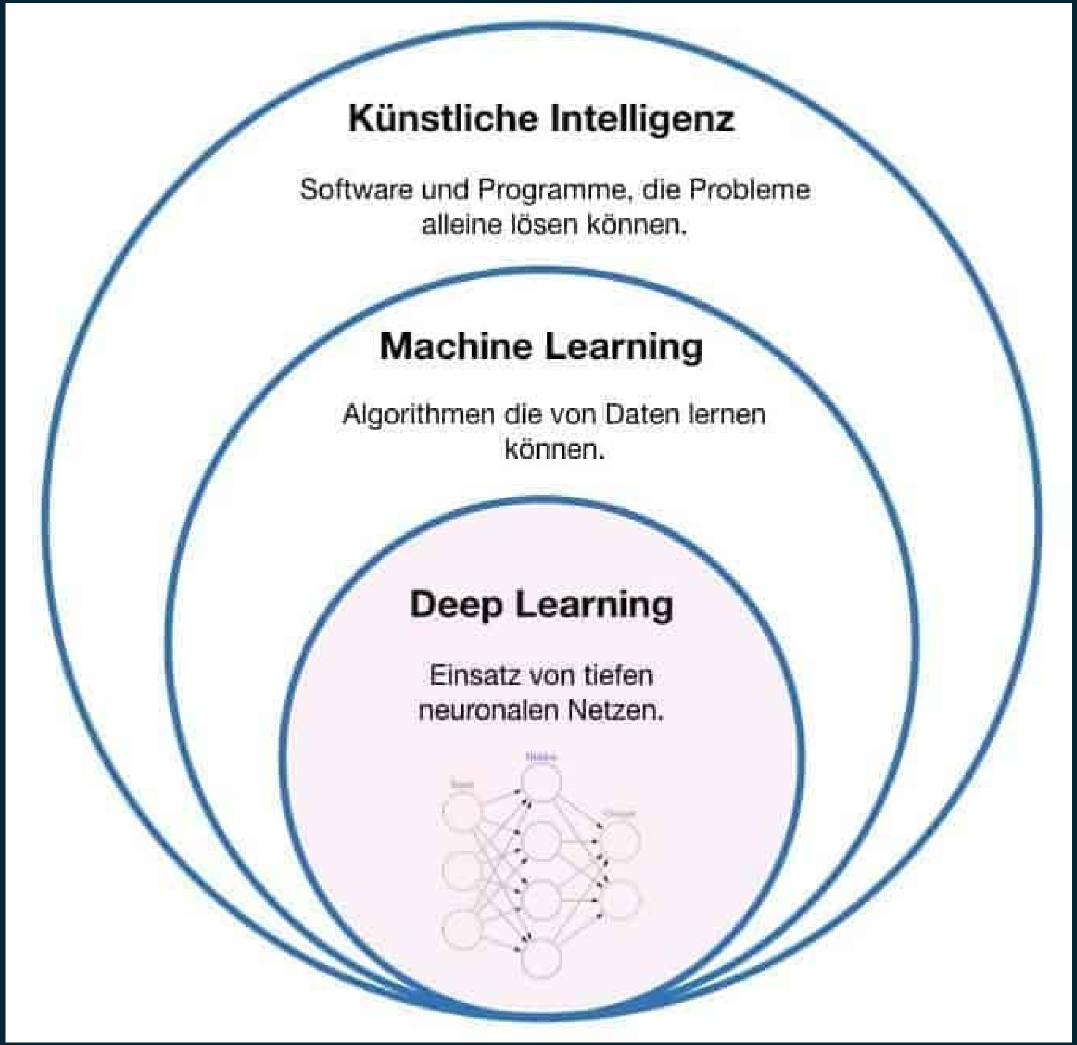
Existing Solutions Assume Breach = Reactive



Known & Unknown Threats:

- Ransomware
- Emotet
- Code injection
- AMSI bypass
- LAPSUS
- ....

How can we apply neural systems



Künstliche Intelligenz

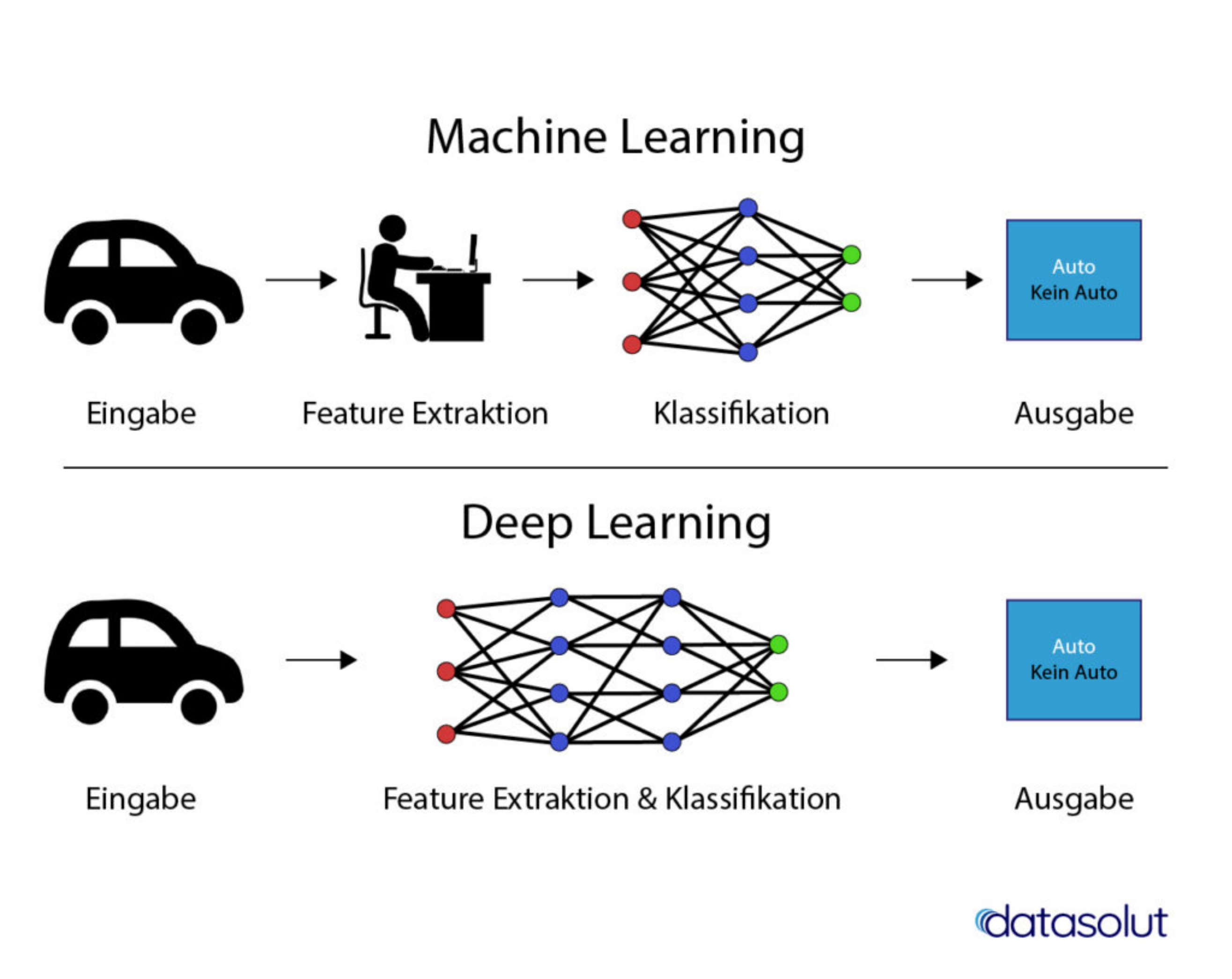
Software und Programme, die Probleme alleine lösen können.

Machine Learning

Algorithmen die von Daten lernen können.

Deep Learning

Einsatz von tiefen neuronalen Netzen.



Machine Learning

Eingabe → Feature Extraktion → Klassifikation → Ausgabe

Auto
Kein Auto

Deep Learning

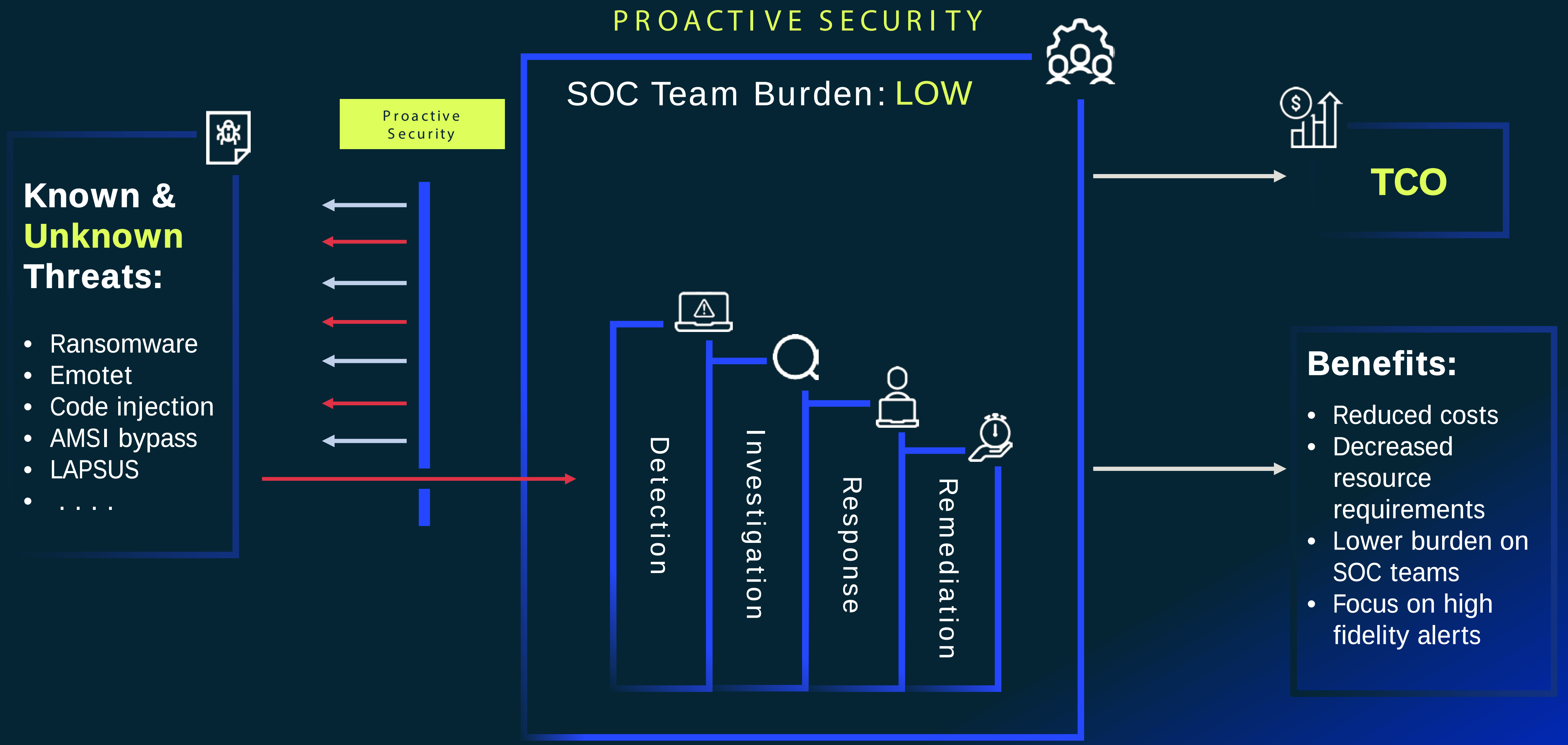
Eingabe → Feature Extraktion & Klassifikation → Ausgabe

Auto
Kein Auto

datasolut

https://datasolut.com/was-ist-deep-learning/

Predictive Prevention = Proactive



PROACTIVE SECURITY

SOC Team Burden: LOW

Proactive Security

Known & Unknown Threats:

- Ransomware
- Emotet
- Code injection
- AMSI bypass
- LAPSUS
- . . . .

TCO

Benefits:

- Reduced costs
- Decreased resource requirements
- Lower burden on SOC teams
- Focus on high fidelity alerts

deep instinct

Fight AI with AI: The Power of Deep Learning

Accuracy

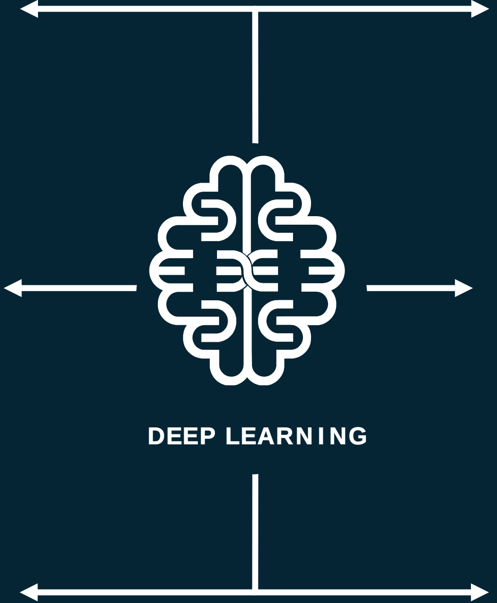
- **Lower false positives**
- **Higher accuracy** of unknown threats
- Automatic **threat classification**

Model Resilience

- **Harder to evade** or reverse engineer
- **Predicts future attacks** without constant updates
- **Operates offline** as effective as online

Data

- **Models** on malicious, benign and anonymized
- **Trains** on **millions of files**



Known Threats

- **Does not require** threat intelligence feeds
- **Not reliant** on heuristics and signatures
- **Avoids** writing to disk first

Unknown Threats

- Moves **beyond basic pattern recognition**
- **Enables prevention** of zero days, fileless, code injection, and PowerShell exploits
- Understands the **DNA of attack** without hash

Autonomous & Intuitive

- **Self-learning**
- **Does not require** human insight
- **Prevents** never-before-seen attacks

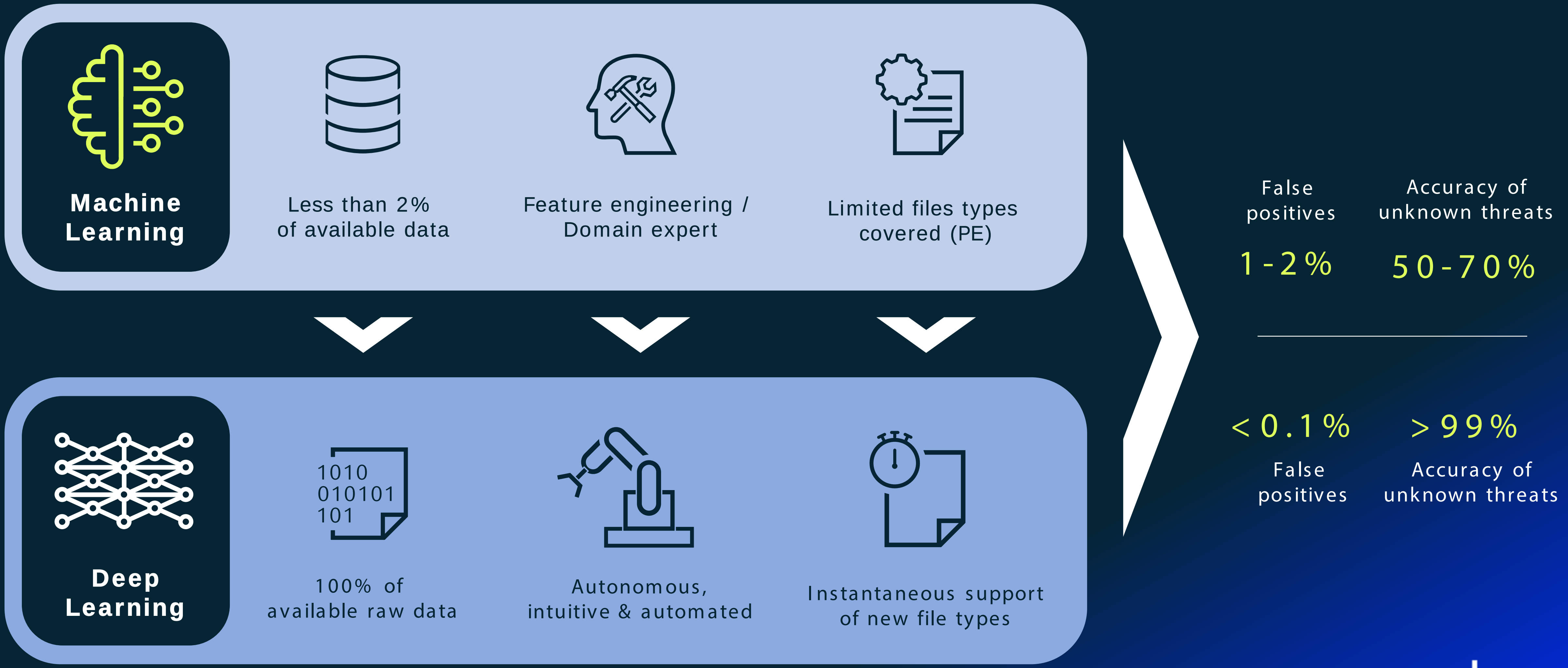
<20ms
Prevention

<0.1%
False positive rate

>99%
Accuracy of unknown threats

deep instinct

Deep Learning Vs. Machine Learning



Machine Learning

Less than 2% of available data

Feature engineering / Domain expert

Limited files types covered (PE)

False positives 1-2%

Accuracy of unknown threats 50-70%

Deep Learning

100% of available raw data

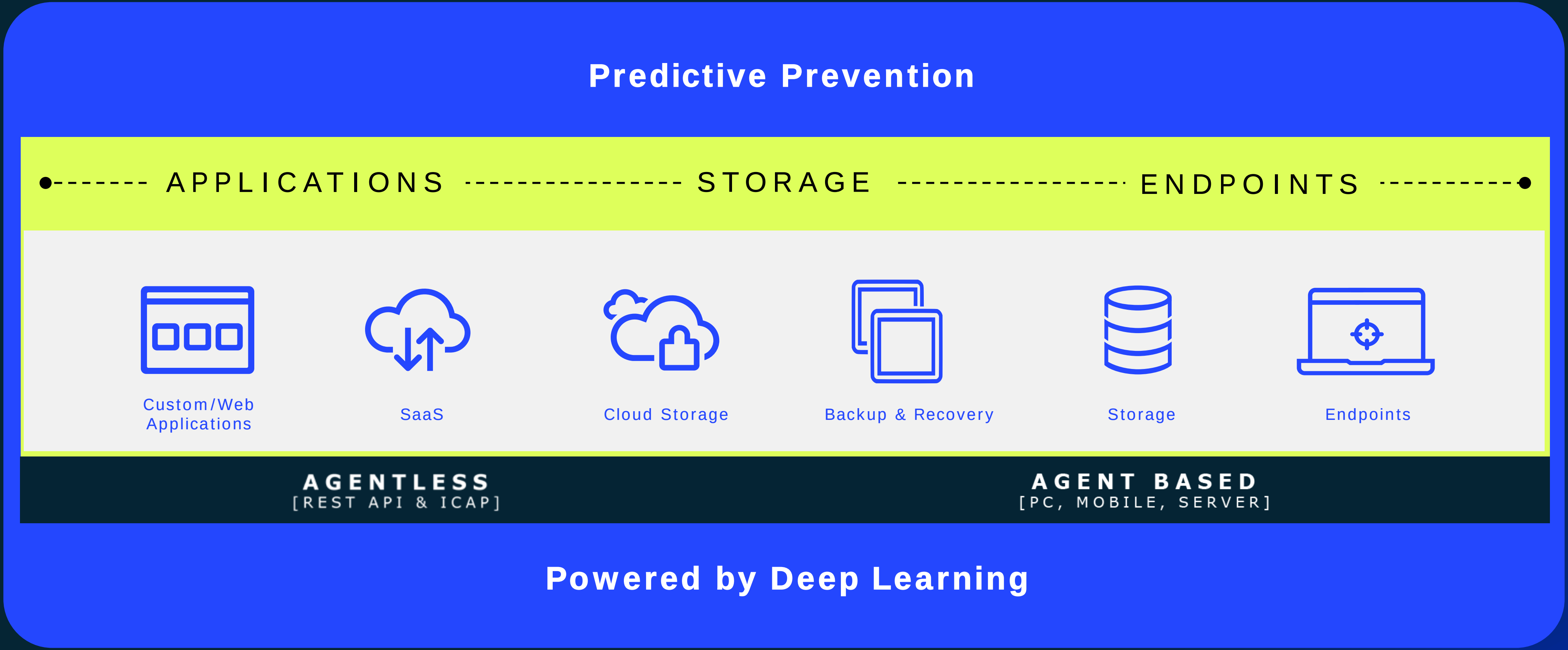
Autonomous, intuitive & automated

Instantaneous support of new file types

<0.1% False positives

>99% Accuracy of unknown threats

Deep Instinct Predictive Prevention Platform



Predictive Prevention

APPLICATIONS — STORAGE — ENDPOINTS

Custom/Web Applications

SaaS

Cloud Storage

Backup & Recovery

Storage

Endpoints

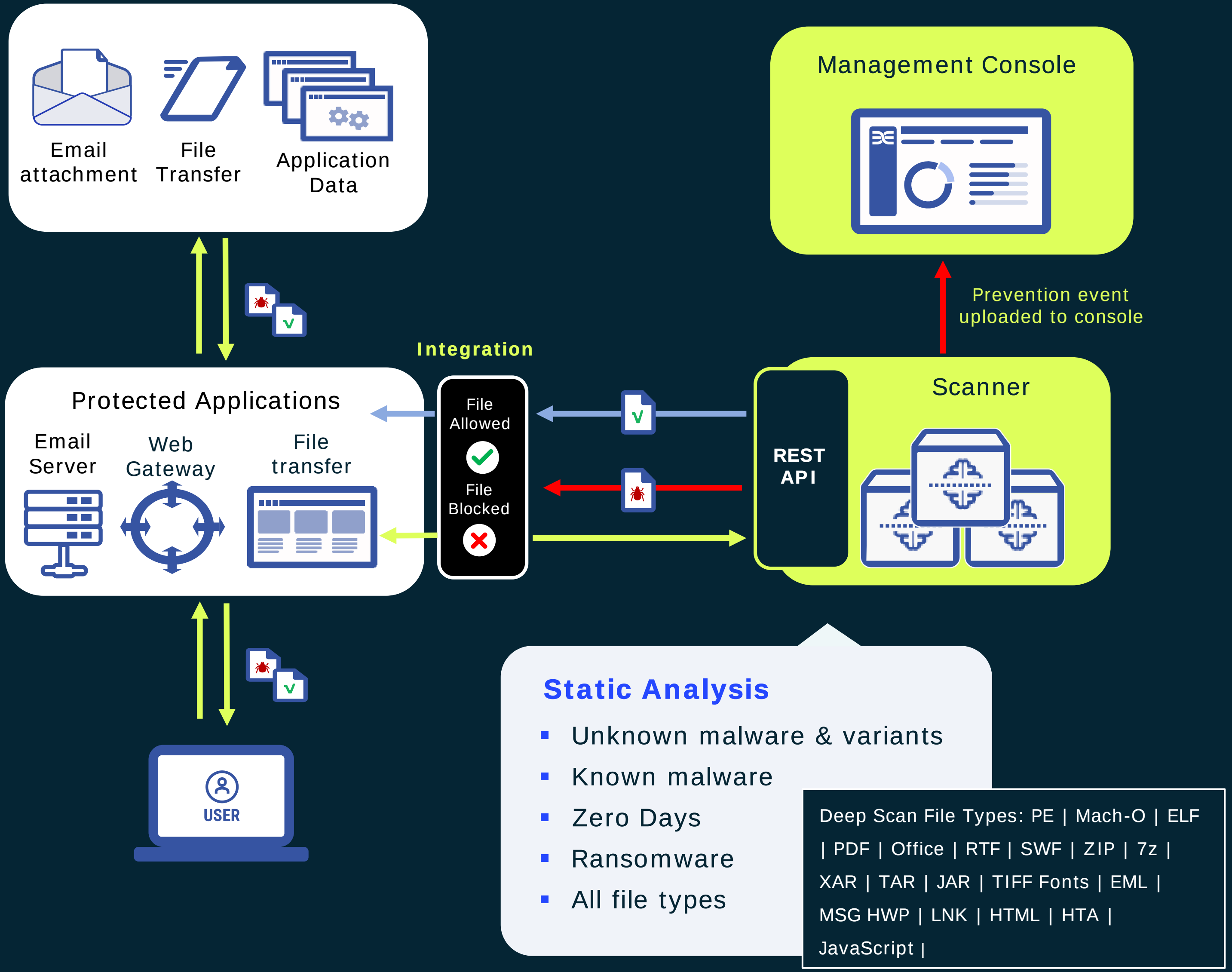
AGENTLESS
[REST API & ICAP]

AGENT BASED
[PC, MOBILE, SERVER]

Powered by Deep Learning

Deep Instinct Prevention use Cases

Meet the Attacker Earlier and Ensure Integrity of your applications



Static Analysis

- Unknown malware & variants
- Known malware
- Zero Days
- Ransomware
- All file types

Deep Scan File Types: PE | Mach-O | ELF | PDF | Office | RTF | SWF | ZIP | 7z | XAR | TAR | JAR | TIFF Fonts | EML | MSG HWP | LNK | HTML | HTA | JavaScript |

- **Deploy anywhere** as a container cluster
- **Easily integrate** with REST API
- **No impact** on app performance or user experience with verdict in < 20ms
- **In-Transit File Scanning** on the email gateway integration or any other network hub

Deep Instinct Prevention for Storage

Prevent ransomware and other malware from reaching your on-premise, hybrid cloud or public cloud storage and putting your precious data at risk

Easily integrate with your storage infrastructure

- Dell and NetApp native integration
- AWS S3 cloud storage native integration

Achieve Enterprise scale at low cost

- Less than 20ms file scan time
- Minimum infrastructure costs at maximum scale

Best in class prevention

- Over 99% efficacy
- Less than 0.1% false positives

PURESTORAGE Q1/2024

amazon web services

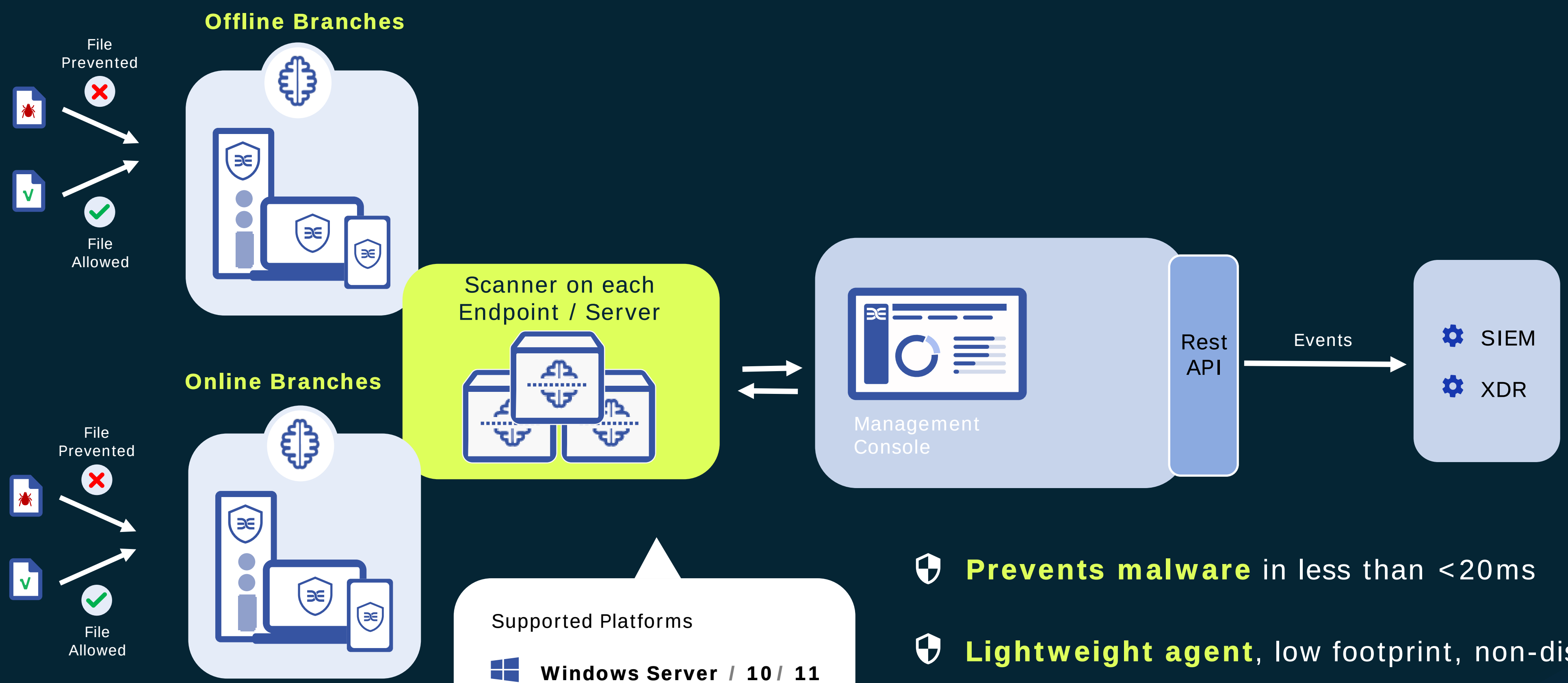
S3

DELL

NetApp

deep instinct

Deep Instinct Prevention for Endpoints & Servers



Supported Platforms

- **Windows Server / 10 / 11**
- **MacOS**
- **Linux**
- **Android**
- **iOS**

- **Prevents malware** in less than <20ms
- **Lightweight agent**, low footprint, non-disruptive
- **Offline functionalities** no updates required. Prevention as good as “online”
- **Supports any scale** when autoscaling and load balancing

deep instinct

Deep Instinct & EDR Solutions

Deep Instinct Prevention is taking a different approach than EDR tools

Prevention

Detection & Remediation

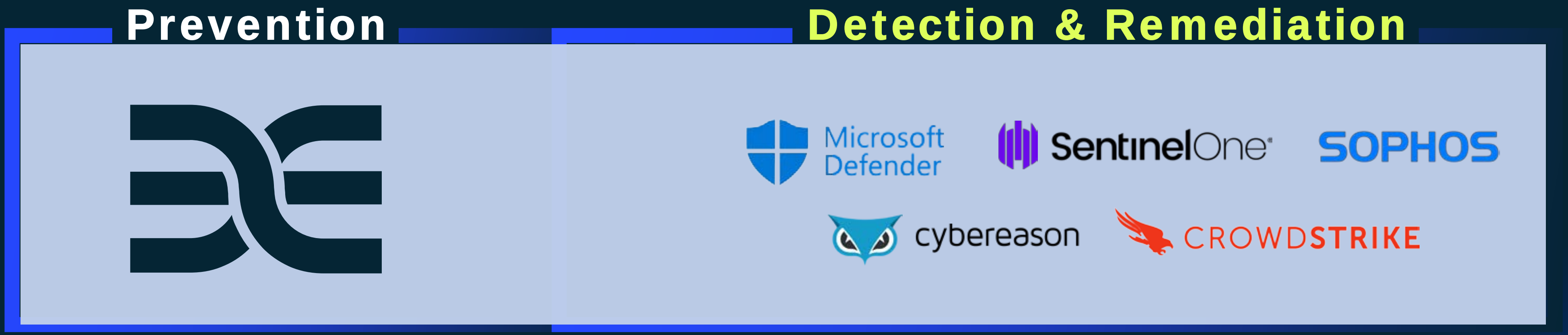
Microsoft Defender
SentinelOne
SOPHOS
cybereason
CROWDSTRIKE

Prevention first	Prevention	Detection first
Accurately prevents >99% threats	Efficacy	Low detection rates for unknown & documents
Low FPs rate	Accuracy	Noisy, creates alert fatigue
Autonomous & Fast	Speed	Cloud Dependent
Proactive Deep Learning	Technology	Reactive Machine Learning

Deep Instinct & EDR Solutions

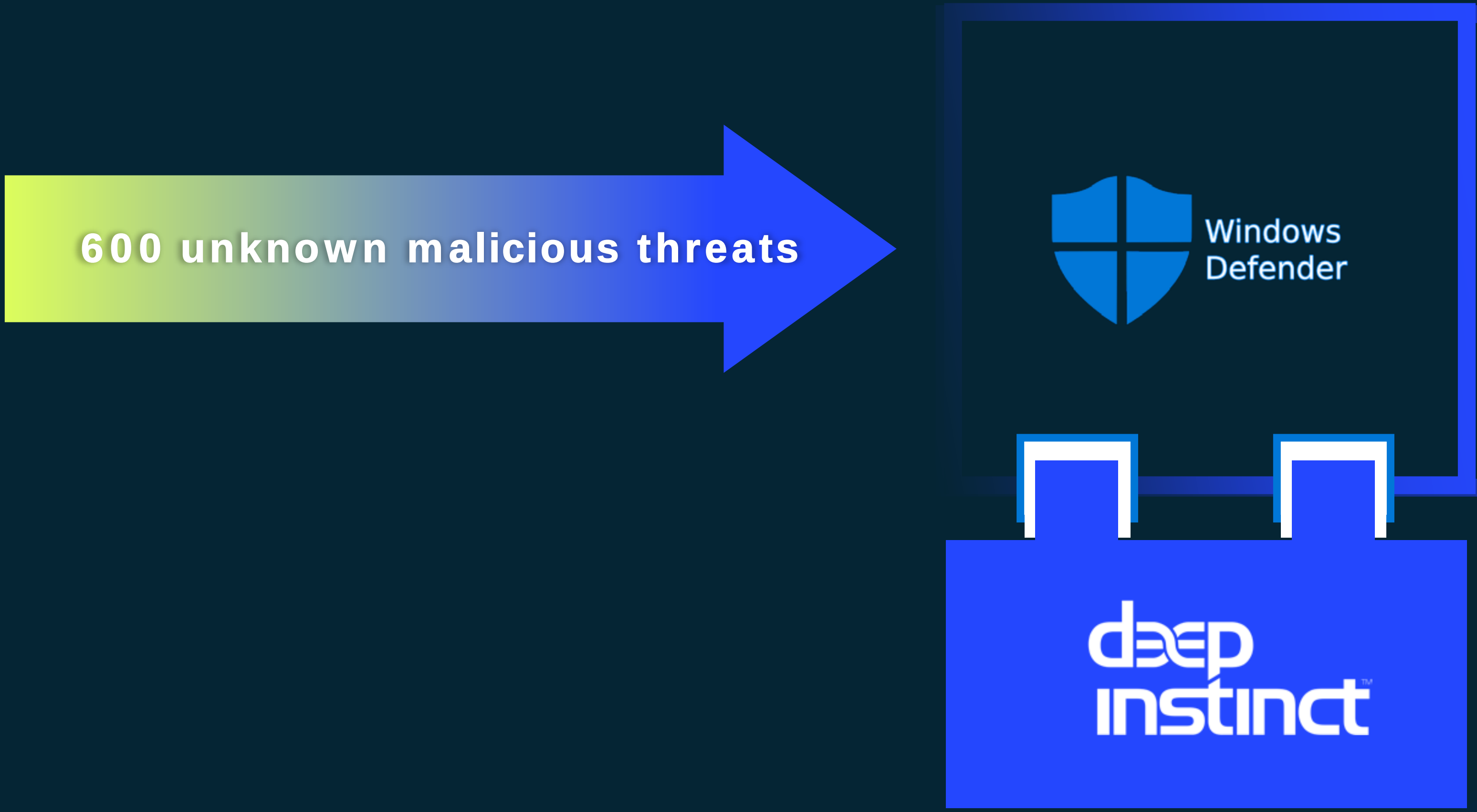
Integrate Deep Instinct Prevention with Microsoft Defender for Endpoints (and other EDRs) to enhance your prevention capabilities and close the security gap

Deep Instinct non disruptive, lightweight agent can run side by side with any EDR solution and prevent attacks



- Prevent unknown and known threats
- Reduce the risk of ransomware and unknown attacks
- Respond to threats faster & improve ROI
- Reduce number of alerts and optimize security operations

Fortune 500 Case Study:
Deep Instinct Enhances Windows Defender



- 25% missed detection (offline)
- 80% missed office and pdf files (offline)
- 10% missed detection (online)
- 40% missed office and pdf files (online)

- Preventing detections Defender misses Competitors miss
- 0% missed detection (online or offline)
- <0.1% false positive rate, lower TCO.

***Malicious threats:**
40% Ransomware, 40% Portable Executables, 10% PDF, 10% Office
June 2023

The Solution - Deep Instinct Prevention

Layer of prevention for greater efficiency, lower risk and lower TCO

EFFICACY

- >99% prevention of unknown threats
- <0.1% false positive rate
- <20ms prevention

PREVENTION

- Prevention before malware executes
- Protects against adversarial AI attacks
- Layered prevention against complex attacks

OPERABILITY

- Lowers TCO and Increased ROI of the entire security stack
- Increases analyst productivity and efficiency to fight threats
- Can augment any EDR solution and integrates with any SIEM/XDR

Powered by Deep Learning

Deep Instinct: A Business Overview

Founded in 2015

Headquartered in NYC and TLV. Offices in London and Tokyo

Deep Learning Framework Protected by 5 Granted Patents

Global Customer Base / +3300 End Customers

SEIKO
TANIUM
DICKEY'S BARBECUE PIT
Equity Trustees
T-Systems
THE 20
Honeywell THE POWER OF CONNECTED
Suncoast Credit Union
Elara Caring
box
UNION PACIFIC
citi
BARCLAYS

Strategic and Financial Investors

BlackRock
chrysalis investments
untitled. INVESTMENTS
PayPal
SAMSUNG VENTURE INVESTMENT
JUPITER ASSET MANAGEMENT
Unbound
MILLENNIUM
COATUE
LG

Industry Recognition

Forbes

Ranked by Forbes among the "Top 13 Companies that uses Deep Learning in the World"

Gartner Magic Quadrant

CYBER SECURITY EXCELLENCE AWARDS WINNER 2021

Endpoint Protection

2021 FORTRESS CYBER SECURITY AWARD

Endpoint Detection

SE Labs AAA APR-JUN 2021 ENTERPRISE ENDPOINT PROTECTION

2021 GLOBEE AWARDS GRAND WINNER CYBER SECURITY GLOBAL EXCELLENCE AWARDS

AI ARTIFICIAL INTELLIGENCE EXCELLENCE AWARD 2022

THE CHANNEL CO. CRN SECURITY 100 2022

MITRE ENGENUITY ATT&CK EVALUATIONS Enterprise WIZARD SPIDER & SANDWORM PARTICIPANT 2022

MITRE ENGENUITY A Foundation for Public Good

2021 WINNER Deep Neural Network BIG AWARDS FOR BUSINESS 2021

deep instinct

Vielen Dank für Ihre Aufmerksamkeit

Sebastian Bach, M.Sc.
Regional Sales Manager

Sebastian.Bach@deepinstinct.com
+49 163 7875 114