

# **Vorbeugen statt heilen – wie neuronale Netze Unternehmen sicherer machen**



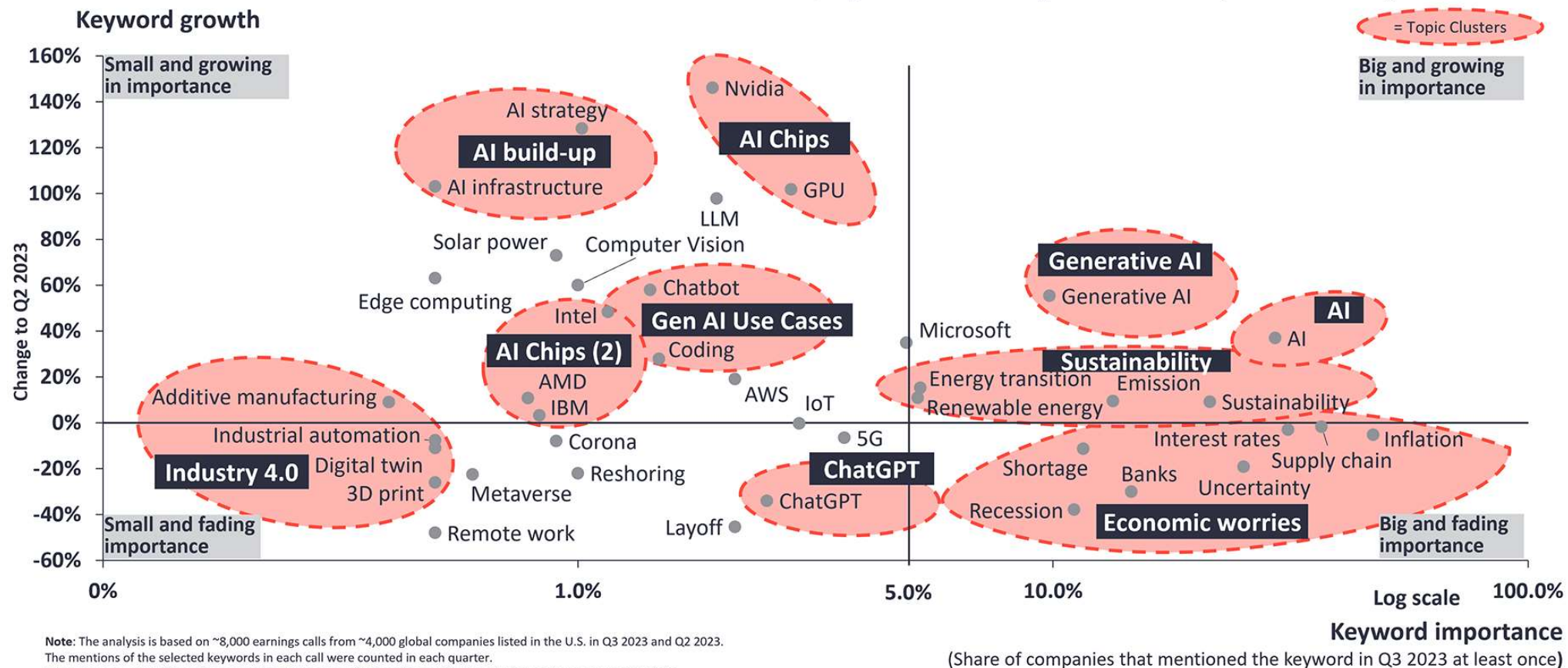
# Generative AI is transforming the world



**Generative AI**

# What is generative AI?

## What CEOs talked about in Q3/2023 (vs. Q2/2023)





# 75% of CEOs acknowledge advanced generative AI as the gateway to success – IBM Study 2023





# The Dark Side of Generative AI





# Generative AI – the next tactical Cyber Weapon

TECHNOLOGY EXECUTIVE COUNCIL

## The generative AI companies

PUBLISHED WED, AUG 2 2023•10:34 AM



Susan Caminiti  
@SUSANCAMINITI

FORBES > INNOVATION

# Generative AI Is The Next Tactical Cyber Weapon For Threat Actors



Yuen Pin Yeap Forbes Councils Member

Forbes Technology Council

COUNCIL POST | Membership (Fee-Based)



Oct 16, 2023, 08:00am EDT



# No – but Ransomware is the Terminator for Will Arnett come back?

 Wana Decrypt0r 2.0





**Payment will be raised on**  
5/15/2017 16:32:52

**Time Left**  
02:23:59:49

**Your files will be lost on**  
5/19/2017 16:32:52

**Time Left**  
06:23:59:49

[About bitcoin](#)  
[How to buy bitcoins?](#)  
[Contact Us](#)

### What Happened to My Computer?

Your important files are encrypted. Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

### Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time. You can decrypt some of your files for free. Try now by clicking <Decrypt>. But if you want to decrypt all your files, you need to pay. You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don't pay in 7 days, you won't be able to recover your files forever. We will have free events for users who are so poor that they couldn't pay in 6 months.

### How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>. Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>. And send the correct amount to the address specified in this window. After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Mondays Friday.

 **bitcoin**  
ACCEPTED HERE

**Send \$300 worth of bitcoin to this address:**

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Copy

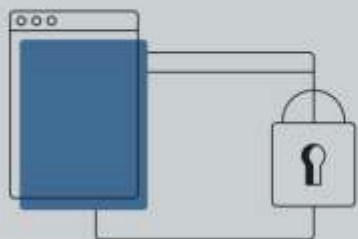
Check Payment

Decrypt

## Ransomware

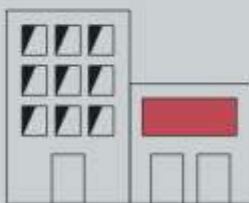
ist weiterhin die größte Bedrohung.

**2** Ransomware-Angriffe auf Kommunalverwaltungen oder kommunale Betriebe wurden durchschnittlich pro Monat bekannt.



**68** erfolgreiche Ransomware-Angriffe auf Unternehmen wurden bekannt.

**15** davon richteten sich gegen IT-Dienstleister.



### Top-3-Bedrohungen je Zielgruppe:

#### Gesellschaft



**Identitätsdiebstahl**  
Sextortion  
Phishing

#### Wirtschaft

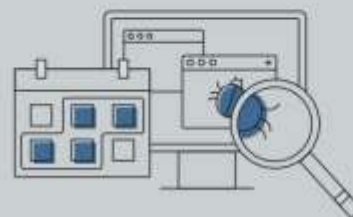


**Ransomware**  
Abhängigkeit innerhalb der IT-Supply-Chain  
Schwachstellen, offene oder falsch konfigurierte Onlineserver

#### Staat und Verwaltung



**Ransomware**  
APT  
Schwachstellen, offene oder falsch konfigurierte Onlineserver

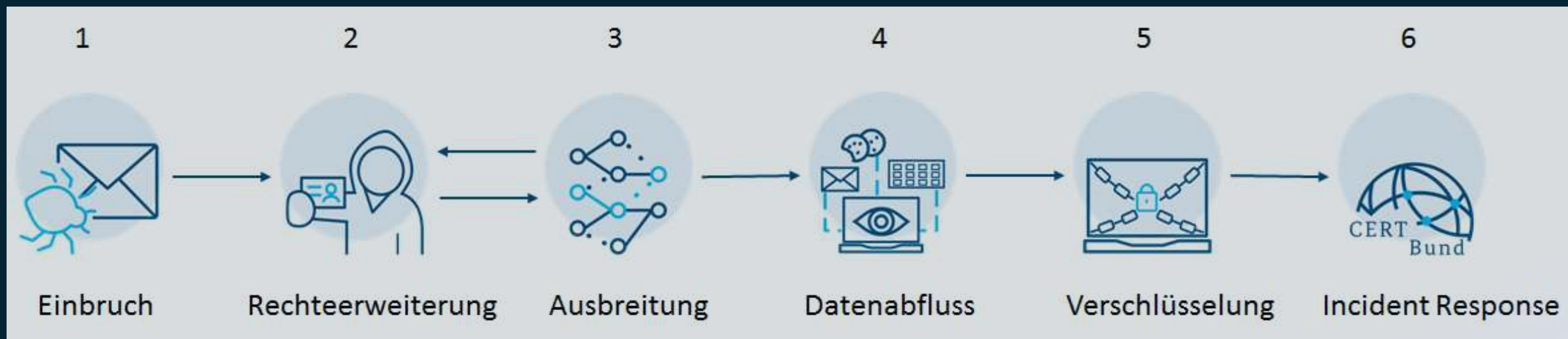


Rund **21.000** infizierte Systeme wurden täglich im Berichtszeitraum erkannt und vom BSI an die deutschen Provider gemeldet.





# Wie verteilt sich Ransomware im Unternehmen



- Bösartige E-Mail
- Ausgenutze (Software) Schwachstellen
- Kompromitierete Zugangsdaten
- Externe File Uploads
- Storage Files

# Wer greift uns überhaupt an?

APT-Gruppe	Bevorzugte Ziele	Bevorzugte Techniken
APT15   VixenPanda   Mirage   Ke3chang	Regierungseinrichtungen   NGOs	<i>Exploits</i> gegen aus dem Internet erreichbare Systeme
APT27   Emissary Panda   LuckyMouse	Energie   Telekommunikation   Pharma	<i>Exploits</i> gegen aus dem Internet erreichbare Systeme
APT28   FancyBear   Sofacy	Regierungseinrichtungen   Militär   Medien   NGOs	<i>Exploits</i> gegen aus dem Internet erreichbare Systeme
APT29   Nobelium   DiplomaticOrbiter	Regierungseinrichtungen	Mails mit Archivdaten als Anhang, die LNK-Dateien enthalten
APT31   JudgementPanda   ZIRCONIUM	Regierungseinrichtungen   NGOs	<i>Exploits</i> gegen aus dem Internet erreichbare Systeme; Bruteforcing
Ghostwriter bzw. Untergruppe UNC1151	Politik   NGOs   Medien	Mails mit Links auf <i>Phishing</i> -Seite
Kimsuky   VelvetChollima	Rüstung   Kanzleien	Word-Dokumente, die makrobehafete Remote Templates nachladen; <i>Social Engineering</i>
Lazarus   SilentChollima	Rüstung   Luftfahrt	Mails mit Archivdaten als Anhang, die trojanisierte Anwendungen enthalten; <i>Social Engineering</i>
MustangPanda (oder VertigoPanda)	Regierungseinrichtungen	Mails mit Archivdaten als Anhang, die LNK-Dateien enthalten
Snake   VenomousBear   Turla	Regierungseinrichtungen   Export	<i>Exploits</i> gegen aus dem Internet erreichbare Systeme
UNC2589	Logistik	Mails mit makrobehafeten Dokumenten im Anhang

Tabelle 1: Für Deutschland relevante APT-Gruppen  
Quelle: BSI



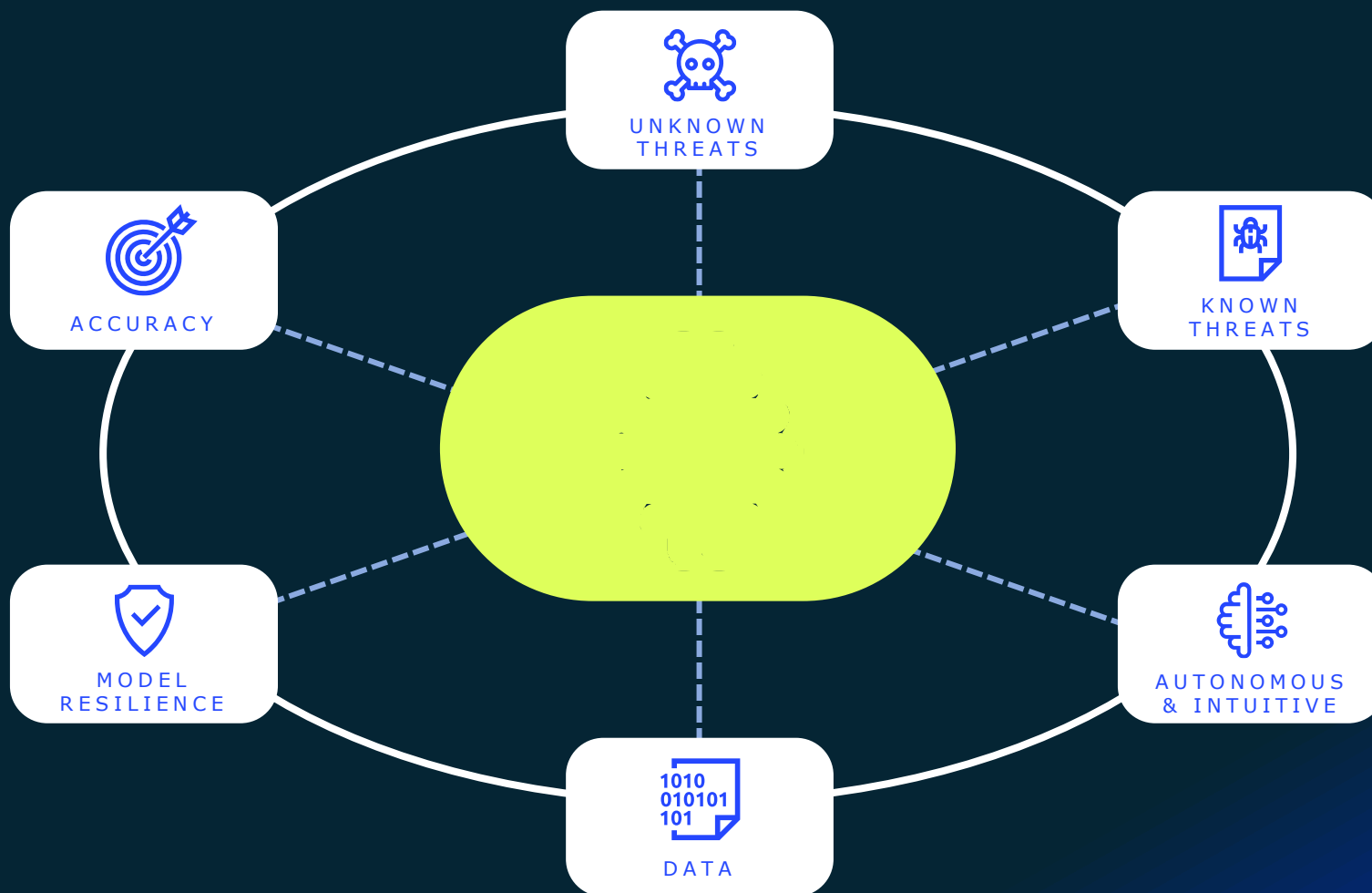
# Deep Learning





# Say Hello to Predictive Prevention

Powered by Deep Learning



**>99%**

**Prevention**

Accuracy of  
unknown threats



**<0.1%**

False  
positive rate




**<20ms**


Prevention




# Deep Learning Vs. Machine Learning




**Machine Learning**



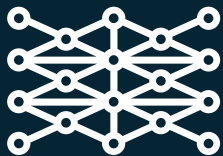
Less than 2% of available data




Feature engineering / Domain expert



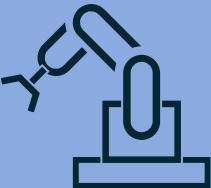
Limited files types covered (PE)




**Deep Learning**



100% of available raw data



Autonomous, intuitive & automated



Instantaneous support of new file types



False positives  
**1-2%**

Accuracy of unknown threats  
**50-70%**

**<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

# Unmatched Efficacy Powered by Deep Learning

	deep instinct	Competitor #1	deep instinct	Competitor # 2	deep instinct	Competitor # 3
Scanned	726	726	867	867	649	649
Prevented	725	466	867	541	642	574
Missed	1	260	0	326	7	75
Efficacy	99.8%	64.1%	100%	62.4%	99%	88.4%

# 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

20

Honeywell  
THE POWER OF CONNECTED

Suncoast  
Credit Union

Elara Caring

box



citi

BARCLAYS

## Strategic and Financial Investors

BlackRock

chrysalis  
investments

untitled.  
INVESTMENTS

PayPal

SAMSUNG  
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



Endpoint  
Protection



Endpoint  
Detection





# **Vielen Dank für Ihre Aufmerksamkeit**

**Sebastian Bach, M.Sc.  
Regional Sales Manager**

**[Sebastian.Bach@deepinstinct.com](mailto:Sebastian.Bach@deepinstinct.com)  
+49 163 7875 114**

