Acronis

#CyberFit

Cyber Defense in the AI Era

Opportunities and Challenges Ahead

Candid Wüest


Artificial
Intelligence
is Everywhere

DeepFakes – Video/Audio/Image

- BEC/CEO fraud with fake voice/video calls
  - Realtime DeepFake or pre-generated sequences
- DeepFake as-a-service offers e.g. for KYC bypass
- Synthetic Identities for social media & industrial espionage


Forbes

FORBES > INNOVATION > CYBERSECURITY

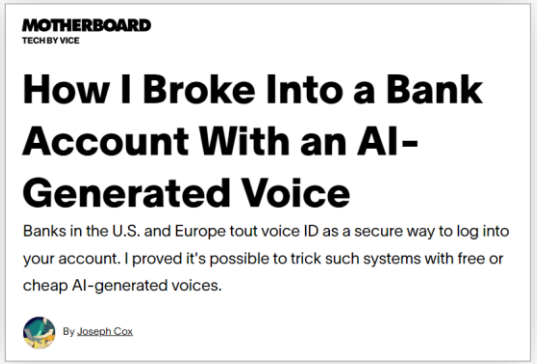
EDITORS' PICK

Fraudsters Cloned Company Director's Voice In $35 Million Bank Heist, Police Find

Thomas Brewster Forbes Staff

Associate editor at Forbes, covering cybercrime, privacy, security and surveillance.

Oct 14, 2021, 07:01am EDT


MOTHERBOARD

TECH BY VICE

How I Broke Into a Bank Account With an AI-Generated Voice

Banks in the U.S. and Europe tout voice ID as a secure way to log into your account. I proved it's possible to trick such systems with free or cheap AI-generated voices.

By Joseph Cox

AI malware is not the same as AI malware

Difficult to know if an attack was created with AI

AI powered Threat

e.g. fully autonomous malware which contains an AI model and adapts itself.

Probability: ○○○○○
Impact: ●●●●○

AI generated Threat

e.g. malware script created by ChatGPT that does not contain any LLM parts.

Probability: ●●●○○
Impact: ●○○○○

AI supported Threat

e.g. phishing email mass sender script created by GenAI, which personalizes data via LinkedIn.

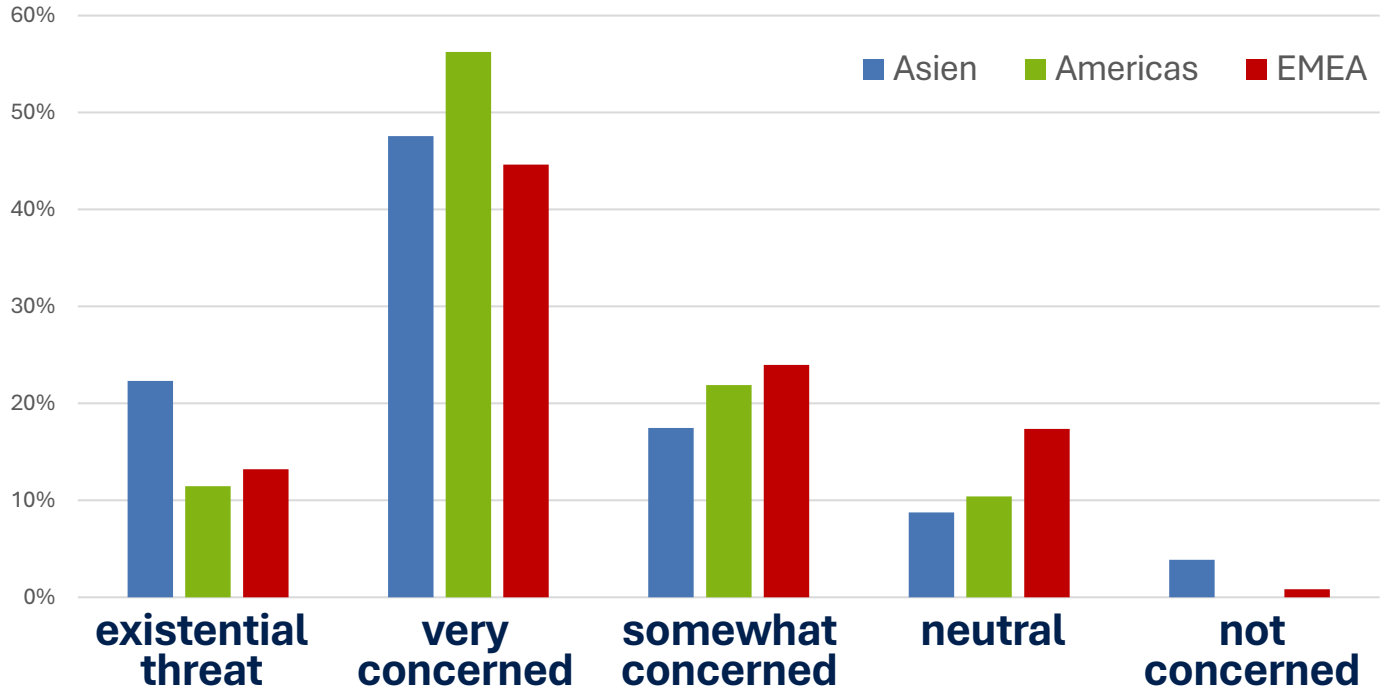
Probability: ●●●●○
Impact: ●●○○○

Threat against the AI

e.g. exploiting classification weights to evade malware detection.

Probability: ●●○○○
Impact: ●●●○○

How concerned are you about cybercriminals using AI to carry out an attack?



Survey Acronis 2023

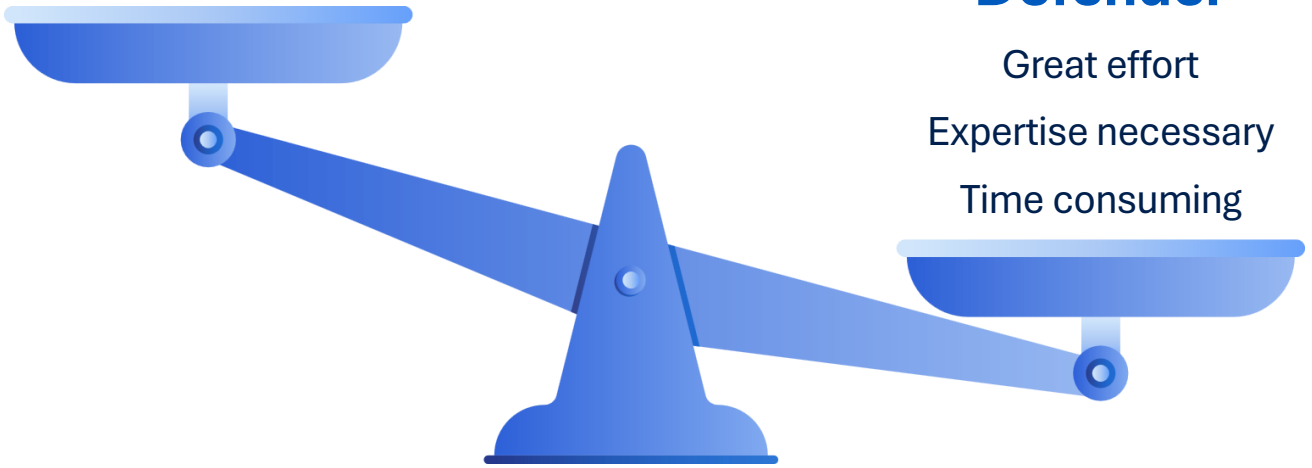
Asymmetric attacks

Attacker

Minimal effort

Little expertise

Fast and scaled



Defender

Great effort

Expertise necessary

Time consuming

Traditional Security Fails

Growing attack surface

- Multiple customers in remote locations
- Mix of on-premises and cloud-based workloads
- Private and public clouds

Security infrastructure gaps

- Multiple security tools deployed for different customers
- Siloed security infrastructure
- Too many alerts overwhelming technicians, and lack of talent

Sophisticated cyberthreats

- Advanced persistent threats (APTs)
- AI-supported attacks, supply chain attacks & zero-day vulnerabilities
- Ransomware generators and ransomware-as-a-service

Common challenges for IT service providers

Specialists

- Many unfilled positions in IT, especially in IT security
- Overburdened IT departments
- More training, courses

Transformation

- Rapid development and constant adjustments
- Cloud computing
- Artificial intelligence
- Automation

IT security and data protection

- Increasing cyberattacks
- Increasing need for robust security solutions
- Stricter data protection regulations

Cost pressure

- Uncertain economic environment
- Optimize costs while increasing efficiency
- Liability risk and legal obligations

Complex IT environments

- Growing number of systems, devices and locations
- Complex updates & patches
- More IT support

How AI is changing cyber security

AI-Driven Threat Detection

- Fast AI-Driven Threat Detection
- Find anomalies in the data noise
- Adapt a localized self-learning AI model

Human-AI Collaboration

- Human-AI Collaboration in Security Operations Centers
- Explainability of detections

Automation

- Automating Routine Security Tasks
- Less human errors
- Automate mitigation and respond

Data Visibility

- AI needs to have good input and training data
- Data access challenges
- Solution consolidation

Compliance

- Regulatory and Compliance Implications of AI
- Privacy concerns
- Locked-in to AI models

AI vs. AI

Get your own Terminator

Join the Resistance

Source: Terminator:Tri-Star Pictures

Acronis
Cyber Protect Cloud

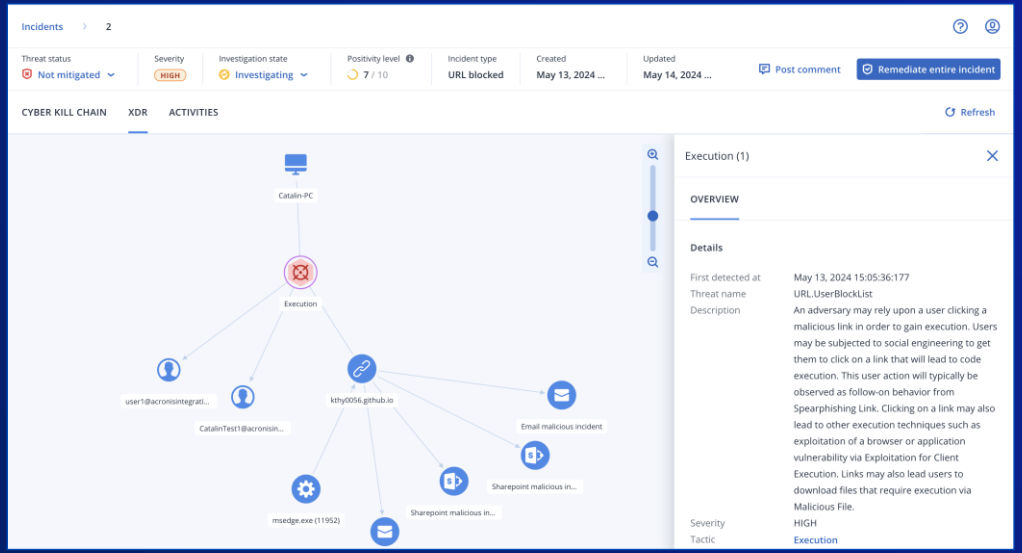
#CyberFit

Comprehensive protection for MSPs in a single solution

1. **Natively integrated, cross-NIST cybersecurity, data protection and endpoint management**

2. **Highly efficient, AI-driven protection for the most vulnerable attack surfaces (EDR and XDR)**

3. **A solution and platform built for MSPs by an MSP-first partner**

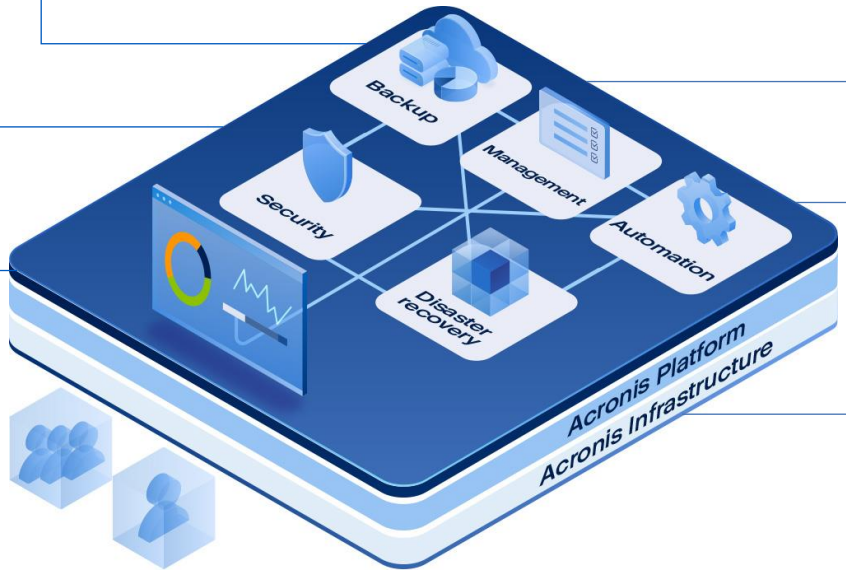


AI / ML in Acronis

Smart backup
Disaster Recovery

Cybersecurity
EPP, EDR & XDR

Support assistant



System health

Smart management

AI copilot

Acronis Delivers the Most Complete Cybersecurity and Data Protection in a Single Solution

Natively integrated

- Complete integrated security stack
- AI and behavior-based detection
- Single agent and a single console and policy for all protection services

Highly efficient

- Low management effort
- Low impact on performance
- Fast technician training and customer onboarding

Built for MSPs and IT departments

- Ease of use
- Mass management for multitenant environments
- Platform for integrating IT tools

Cyber Security

- Endpoint detection and response
- Vulnerability assessment
- Malware resistance
- Email security
- Investigation of incidents
- Protection against ransomware

Data Protection

- Backup
- Disaster Recovery
- Continuous data protection
- Secure cloud storage

Management

- Patch management
- Remote access

Expand with over 200 integrations

Commonly used by MSPs - SIEM, PSA, RMM-Tools

Artificial Intelligence is no match for human stupidity

But hand in hand, they can be more productive

Acronis

Cyber Foundation Program

Share the success of your growing business by helping others

Get your free CSR in a Box training kit

AI-powered integration across NIST

GOVERN

- Provisioning via a single agent and platform
- Centralized policy management
- Role-based management
- Information-rich dashboard
- Flexible reporting

IDENTIFY

- Software and hardware inventory
- Unprotected endpoint discovery
- Content discovery
- Data classification
- Vulnerability assessments

PROTECT

- Security configuration management
- Patch management
- Device control
- Data Loss Prevention
- Security training

DETECT

- AI/ML-based behavioral detection
- Exploit prevention
- Anti-malware and anti-ransomware
- Email security
- URL filtering

RESPOND

- Rapid incident prioritization
- Incident analysis
- Workload remediation with isolation
- Forensic backups
- Remote access for investigation

RECOVER

- Rapid rollback of attacks
- One-click mass recovery
- Self-recovery
- Backup integration
- DR integration

Acronis als Service Provider Partner

Ihr Erfolg ist unser Erfolg!

- **Schnelle Bereitstellung von Diensten** mit einem modularen Ansatz über eine einzige Konsole und einen einzigen Agenten
- Innovation ermöglicht **hochwertige Dienste**, die für Kunden jeder Größe zugänglich sind
- **Kontrolle der TCO** und Vereinfachung von Service-Tiering und -Management mit einer **einzigen, integrierten Plattform**
- **Acronis #CyberFit Partnerprogramm** und Enablement -

1	Agent	Policy	Konsole	Lizenz	Anbieter

Automation and AI / ML for defense

Better detection

- Clear out the background noise automatically — **reduce alert flood**
- Find the **anomalies** in the data set — adapt to new attack patterns
- **Adapt** a localized self-learning AI model to better protect your environment

Better response

- Find the **best mitigation** and respond faster and automatically
- Transfer **expert knowledge** into AI Model — free up experts' time
- Make **more data** available — gather, correlate, enrich, connect and index

Automation

- Facilitate manual tasks
- **Reduce** risks, errors and **complexity**
- **Automatically classify data and systems**

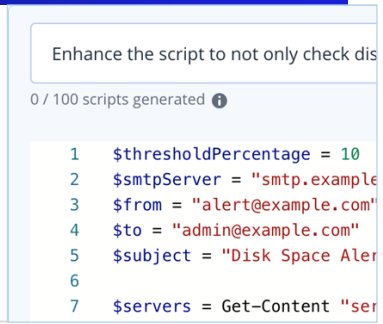
AI-based features

EDR/XDR incident summary

- AI generated incident summary
- Helps to quickly understand the impact of the incident
- Map to MITRE ATT&CK tactics

AI generated scripts & management

- AI-based script generation for PowerShell & Bash for automation
- ML-based monitoring and smart alerting
- Ml-based disk health monitoring
- ML-assisted backup validation



Security AI Copilot

- AI Chatbot to interact with incidents and ask questions
- Find similar incidents
- Explain scripts and impacts
- Guidance on remediation

AI/ML detection

- AI/ML based threat detection
- AI-based event correlation across endpoints
- AI-based prioritization of security incidents across endpoints
- AI-based malicious documents and scripts detection