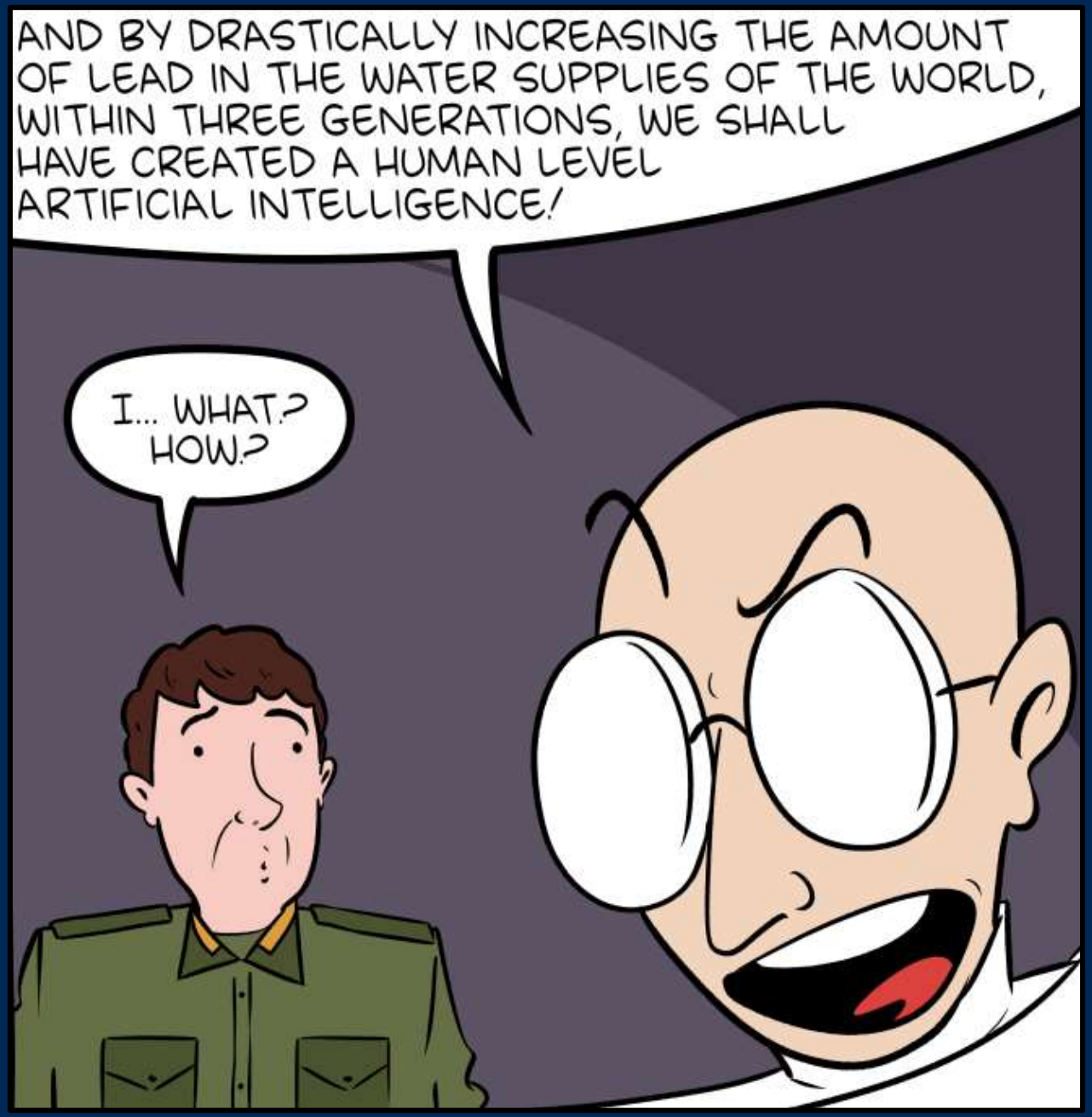
The State of Artificial Intelligence in Security and Risk Management

Jeremy D'Hoinne
@jeremydhoinne

Gartner®



Used with permission from Zach Weinersmith smbc-comics.com

Any AI can be made "human level" by lowering all human intelligence.

Key Areas Where New Algorithms Can Improve Enterprise's Security Posture

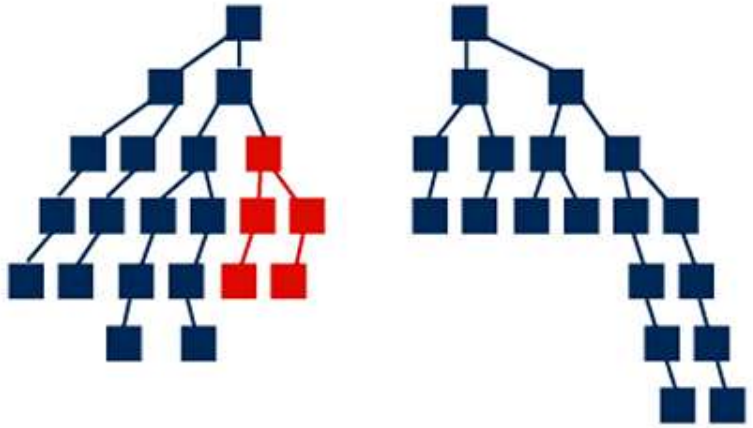
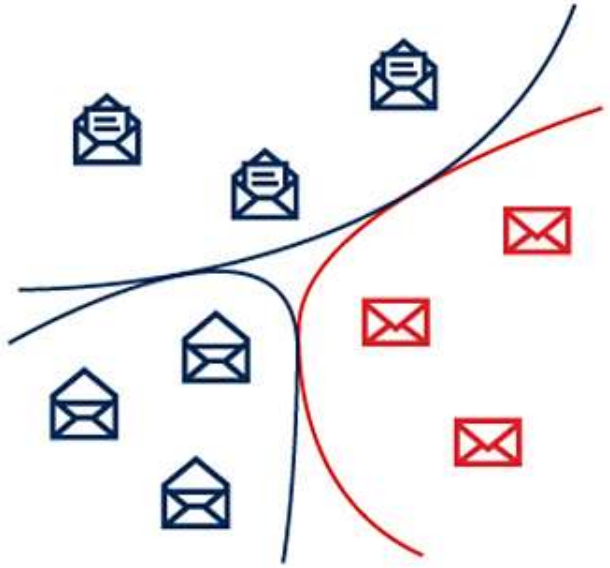
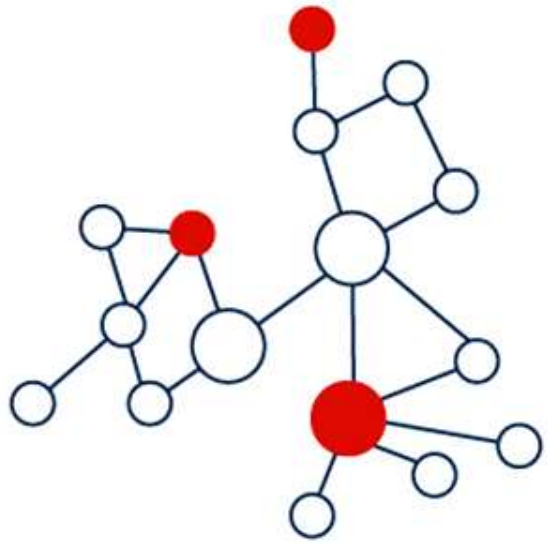
1. Infrastructure Protection
2. Identity and Access Management
3. Risk Management
4. Application and Data Security
5. Security Operations

1a

Infrastructure Protection — *Prevent: Threat Detection*

Gartner

Machine Learning for Threat Detection

Malware	Spam	Phishing
		
Classification Static and dynamic analysis	**Classification** Content and header	**Social Graph** Links — server and sender IPs

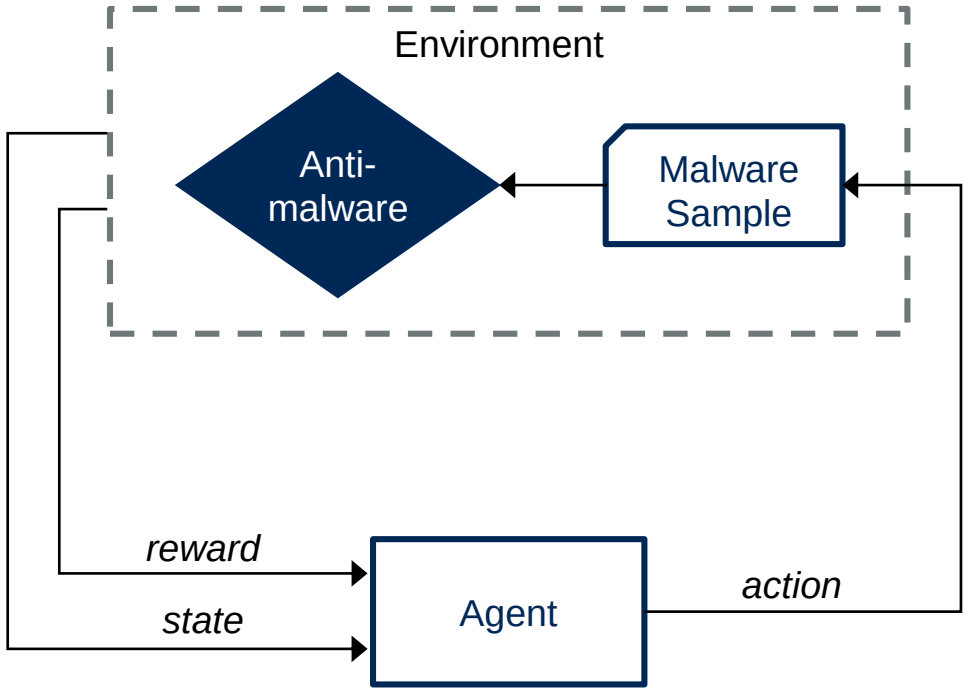
Source: Gartner
ID: 466678_C

Gartner

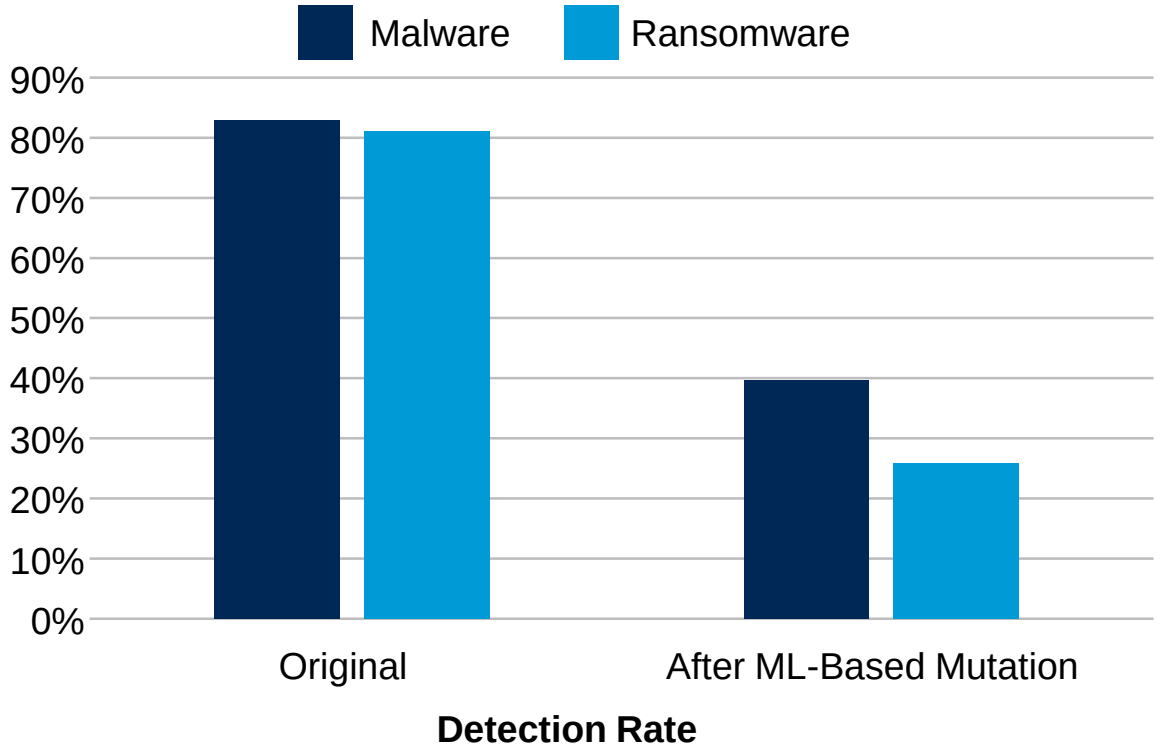
Sometimes You're the Cat and Sometimes You're the Mouse: Attackers Like "AI" Too

Using reinforcement learning to evade machine learning based malware detection:

Markov Decision Process Formulation of the Malware Evasion Reinforcement Learning Problem



Malware Detection Rate (VirusTotal)



Source: "Learning to Evade Static PE Machine Learning Malware Models via Reinforcement Learning," arXiv

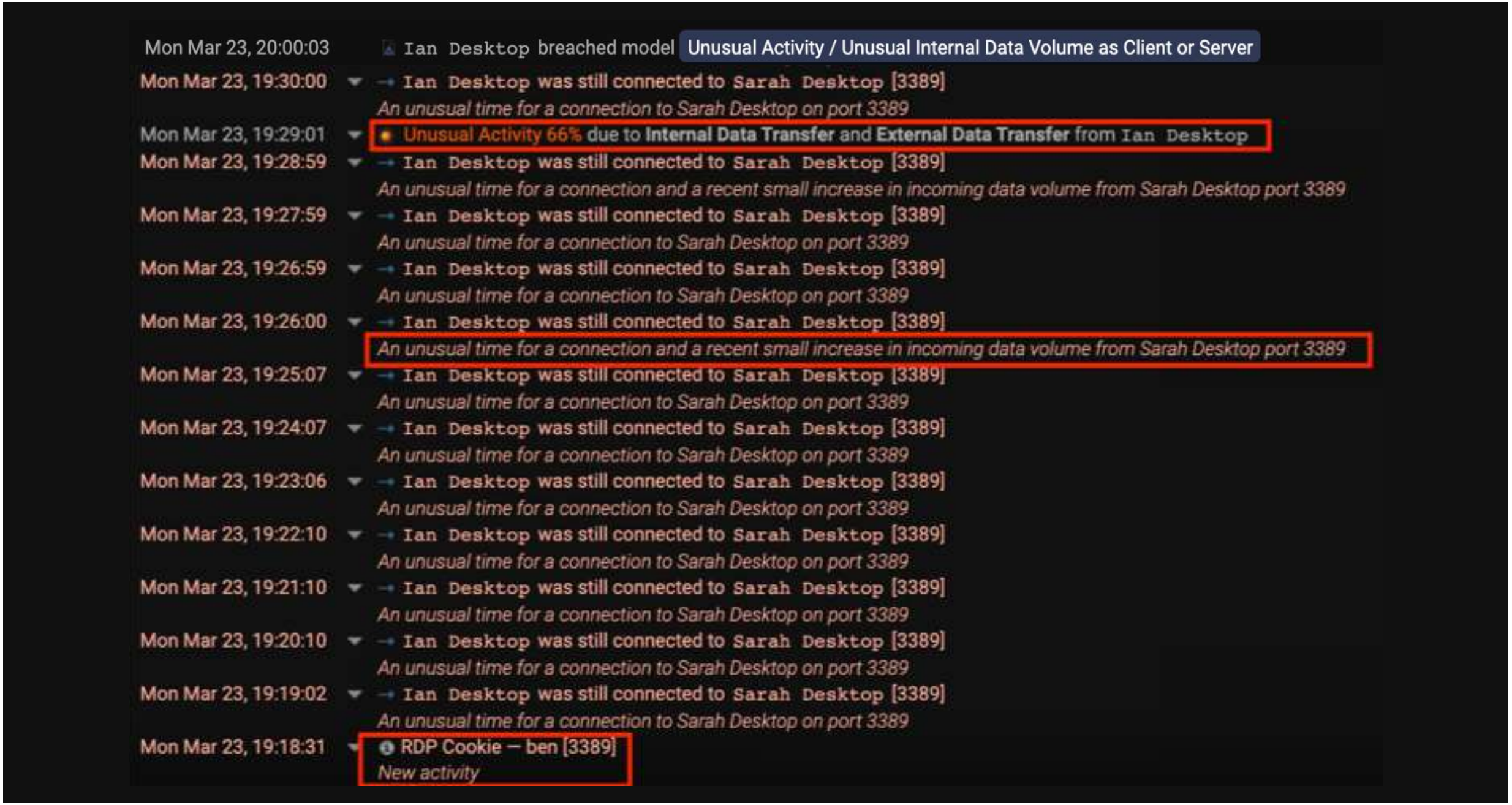
Gartner

1b

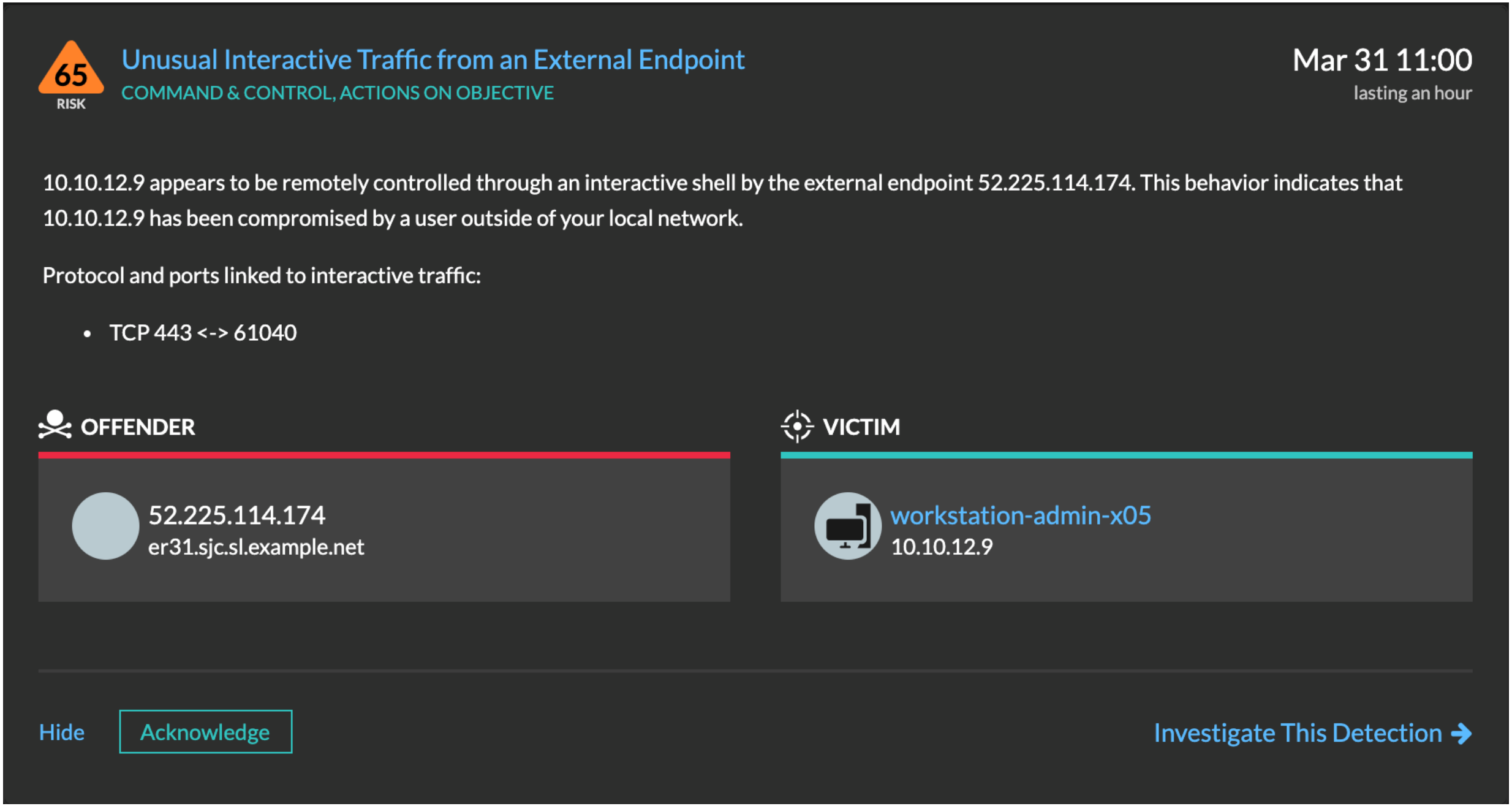
Infrastructure Protection — *Detect: Behavioral Analysis*

Gartner

Sample Detection Leveraging Machine Learning



Source: Darktrace



Source: ExtraHop

Geographically Unusual Remote Access i-Ode8d37876cfcd3e4

Status	Open
ID	1453
Description	Device has been accessed from a remote host in a country that doesn't normally access the local network. For example, a local server accepting an SSH connection from a foreign source would trigger this alert. This alert uses the Remote Access observation and may indicate misuse or a compromised device.

Source: Cisco Stealthwatch

Suspicious Remote Desktop

Lateral Movement

Assign Share Investigate in Cognito Recall

Unusual keyboards for this network used with server 192.168.12.11

Mar 29th 2020 18:47
RDP Client Token: andyb
RDP Clientname: hacktool
Product ID: xyz

Unusual keyboard layout: Serbian (Cyrillic) - 3098

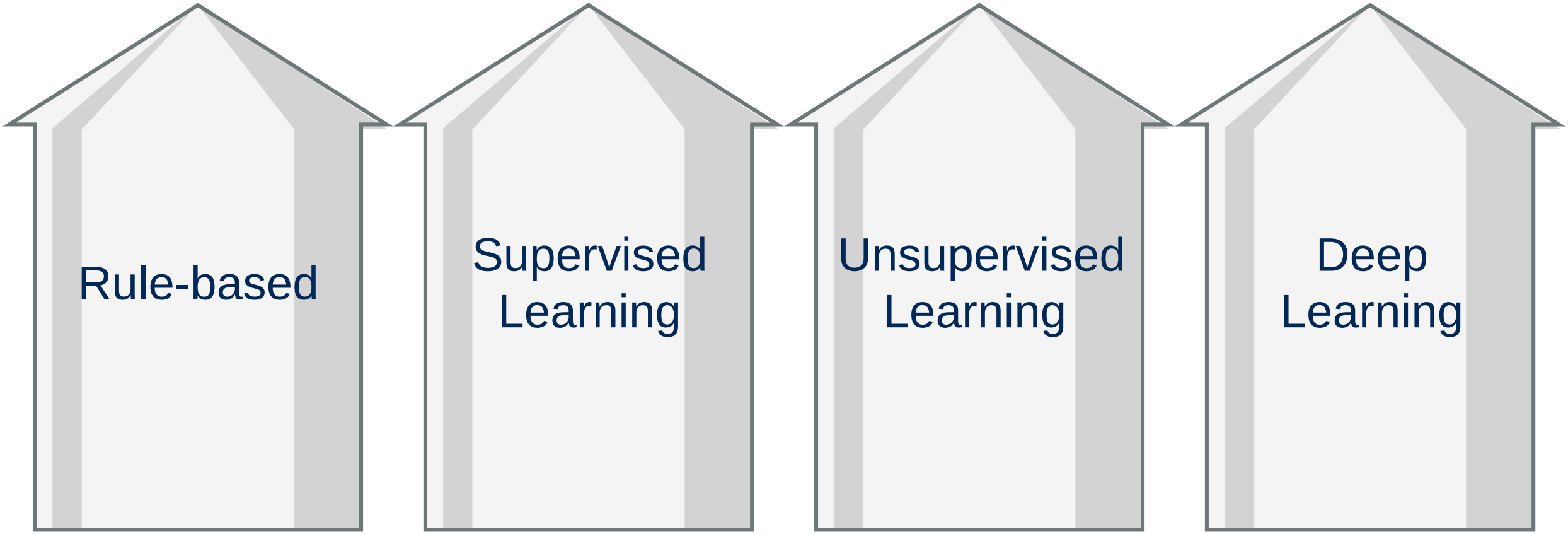
Normal keyboard layouts for this network between: Mar 29th 2020 - Mar 29th 2020 18:47

Hebrew - 1037	Finnish - 1035	US - 1033
French - 1036	Spanish - 1034	

Source: Vectra

“99% of the value we see today comes from supervised learning.”

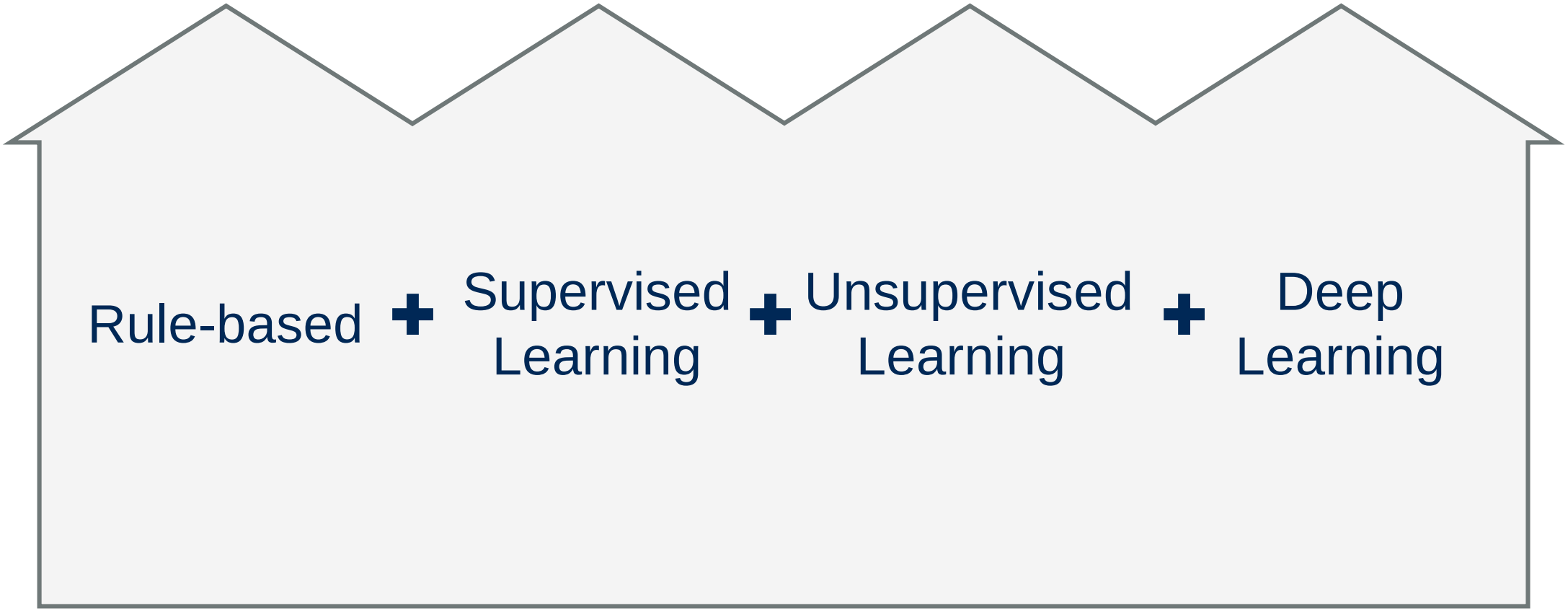
Andrew NG, April 2020



Gartner

“99% of the value we see today comes from supervised learning.”

Andrew NG, April 2020



Gartner

With Machine Learning for Threat Detection, the Details Matter

- **Expect incremental, not transformative results**
- Match the threat detection technology with the threat environment
- Prioritize questions on the scope of ML techniques, rather than the efficacy
- Measure, measure, measure
- Anticipate “ML maintenance” costs
- Combine new techniques with proven ones, don’t replace

Gartner

2

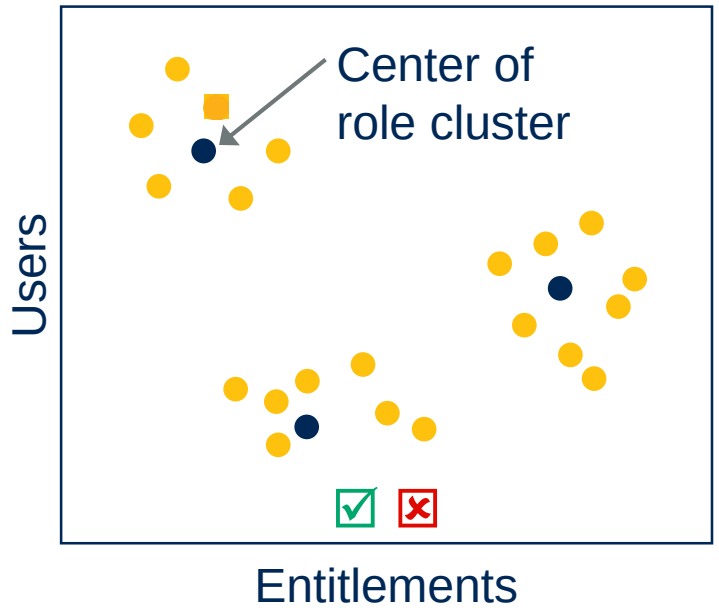
Identity and Access Management

Gartner

IAM Machine Learning Use Cases

Identity Analytics

Governance



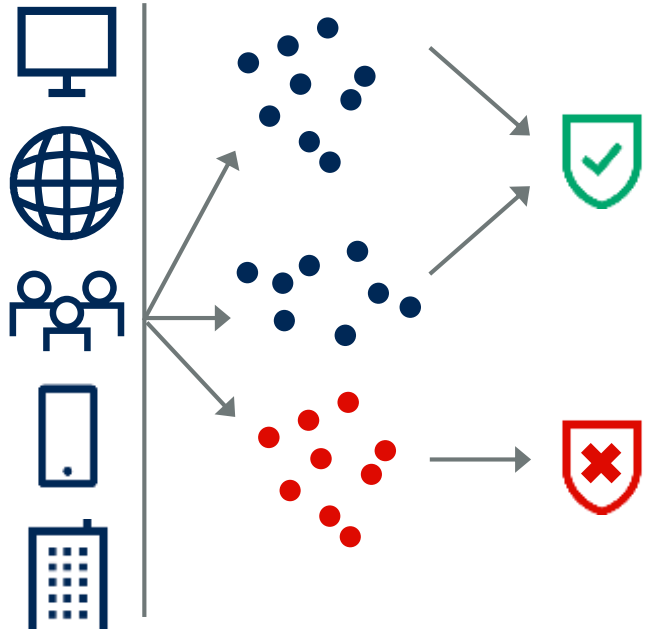
Smart Cluster Analysis

Identity Proofing

Image Recognition

Online Fraud Detection

Behavioral Profiling



Rule-based + (un)supervised
machine learning + deep learning

Gartner

Improve Your Organization's ML Skills Before It Is Necessary

Gartner

	Involvement	Required Understanding
 CISO	• Set expectations • Approve select AI experiments	• AI hype vs. reality • AI maturity for security use
 Technical Advisors	• Recommend select use of AI • Define evaluation metrics	• Architecture impacts • Algorithms (high level)
 Privacy Leaders	• Ensure compliance • Avoid fines	• Data usage • Data flows • Data control
 Security Operations	• Adapt workflows • Measure and report efficacy • Explain “AI results”	• Engine tuning options • Automated decision “logic” • Is ML the best tool or not?

Source: Gartner
ID: 466678_C

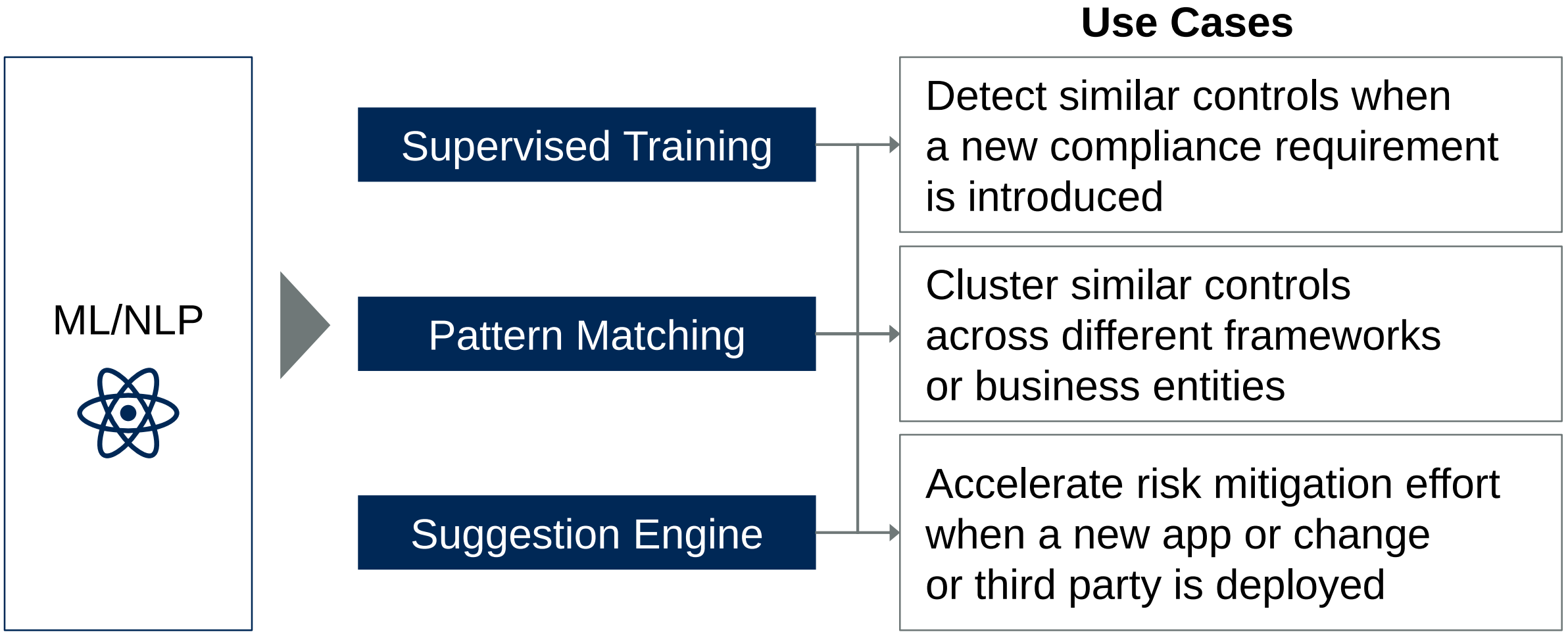
Gartner

3

Risk Management

Gartner

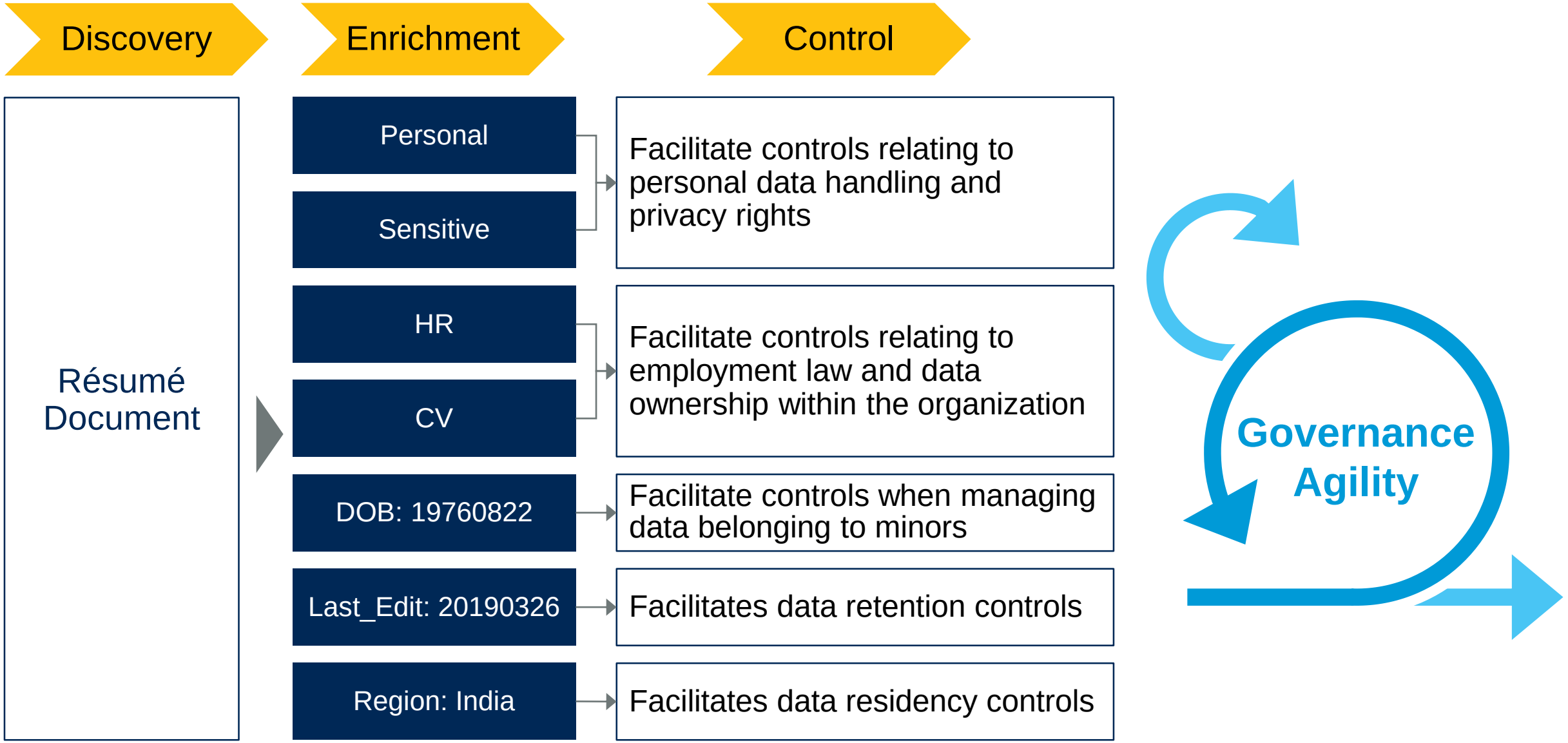
Emerging Risk Management Use Cases by Applying ML/NLP



Better Identifying Privacy Risks

Using techniques such as ML, computer vision and NLP to automate both static and dynamic tagging, ultimately to delivery governance agility.

Gartner



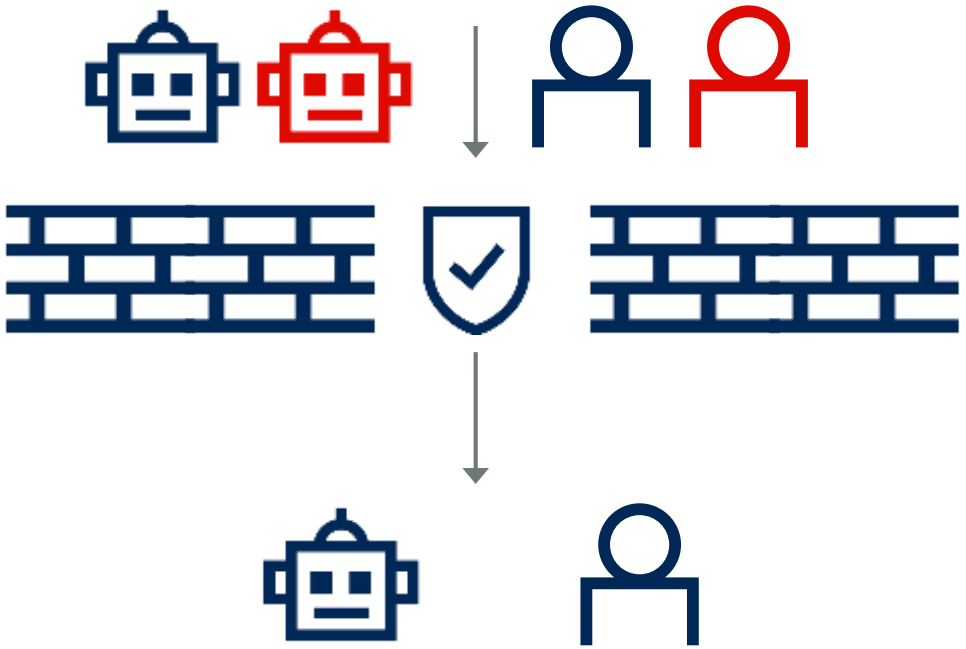
4

Application and Data Security

Gartner

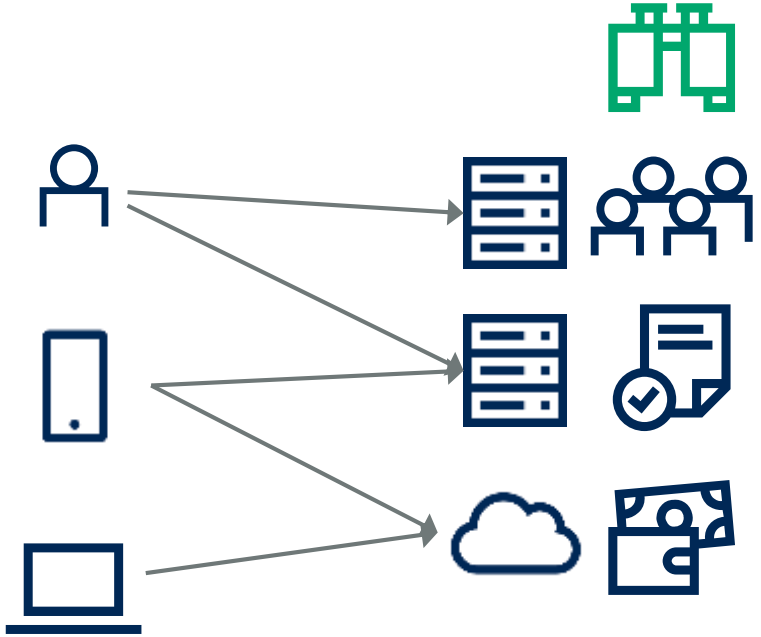
Machine Learning's Maturity Varies With Use Cases

Bot Detection



Behavioral analysis complements reputation, rule and fingerprinting.

Data Security



Started with data discovery and categorization. Growing use for DLP.

Gartner

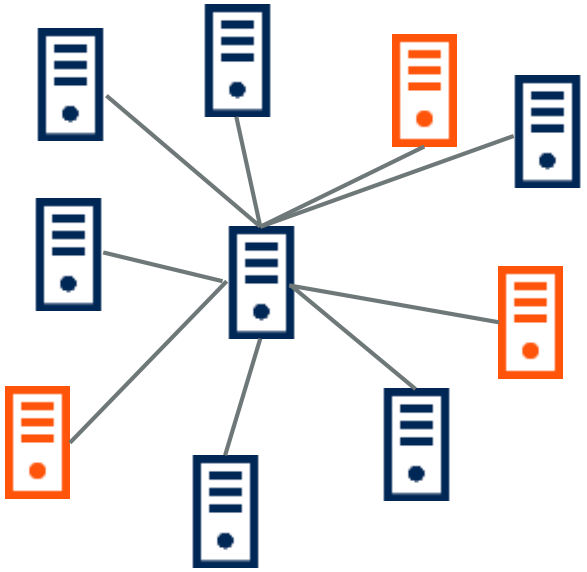
5

Security Operations — *Respond*

Gartner

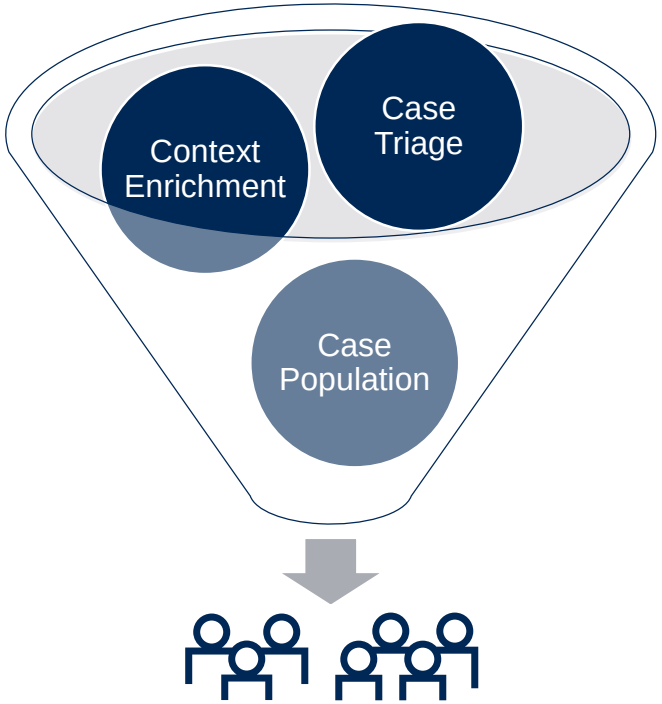
Security Operation Automation

Asset Discovery



Policy Automation

Orchestration



- The value of automation stops where accountability begins.
- Good solutions enable continuous learning and incremental changes.

Optimizing Costs With AI

- Don’t buy AI. Purchase complementary techniques with measurable results against your higher risk threat vectors.
- Do competitive Proof of Concept once you have the outcome-driven metrics ready.
- Favor short-term (one year) subscriptions.
- Focus on people and process before the tool. AI won’t replace staff.

Wrapping Up

Gartner

State of AI Across Security Leaders
Key Initiatives

Infrastructure Protection	• Threat detection (malware, spam, phishing, …) • Anomaly detection (network, endpoint, …)
Identity and Access Management	• Identity analytics (governance, identity proofing) • Online fraud detection
Risk Management	• Compliance • Privacy risks
Application and Data Security	• Bot mitigation • Data discovery and categorization
Security Operations	• Asset discovery • Policy automation • Security orchestration

Recommendations

- Embrace AI in security for uses where there is no shortage of high-quality training data.
- Use machine learning as a complementary technique.
- Set technology as staff augmentation, not replacement.
- Choose metrics before you start evaluating.
- Test (on your data), test (to solve your problems), test (against others).

Action Plan for CISOs

Monday Morning:

- *Review* existing use of machine learning in security and risk management
- *Survey* your team about promising uses of machine learning

Next 90 Days:

- *Measure* more reliably with consistent metrics for each use case
- *Prioritize* areas for machine learning experiments

Next 12 Months:

- *Experiment* machine learning as a feature, where you can evaluate efficacy
- *Standardize* framework for evaluating new algorithms

Recommended Gartner Research

- **5 Areas Where AI Will Turbocharge Privacy Readiness**
  Bart Willemsen (G00380045)
- **Practical Privacy — Discovery Automation of Privacy Risk**
  Nader Henein and Marc-Antoine Meunier (G00376386)
- **Market Guide for User and Entity Behavior Analytics**
  Gorka Sadowski, Jonathan Care and Others (G00361156)

For information, please contact your Gartner representative.

Gartner

Recommended Gartner Research — IAM

- **Modernizing IAM Architecture With Machine Learning**
  Mary Ruddy (G00386813)
- **Transform User Authentication With a CARTA Approach to Identity Corroboration**
  Ant Allan and Jonathan Care (G00345217)
- **How to Select a Machine Learning Vendor for Fraud Detection in Online Retail**
  Akif Khan and Jonathan Care (G00382774)