



**NETEYE**  
**USER GROUP**  
Cyber Security first!

# Elastic Security

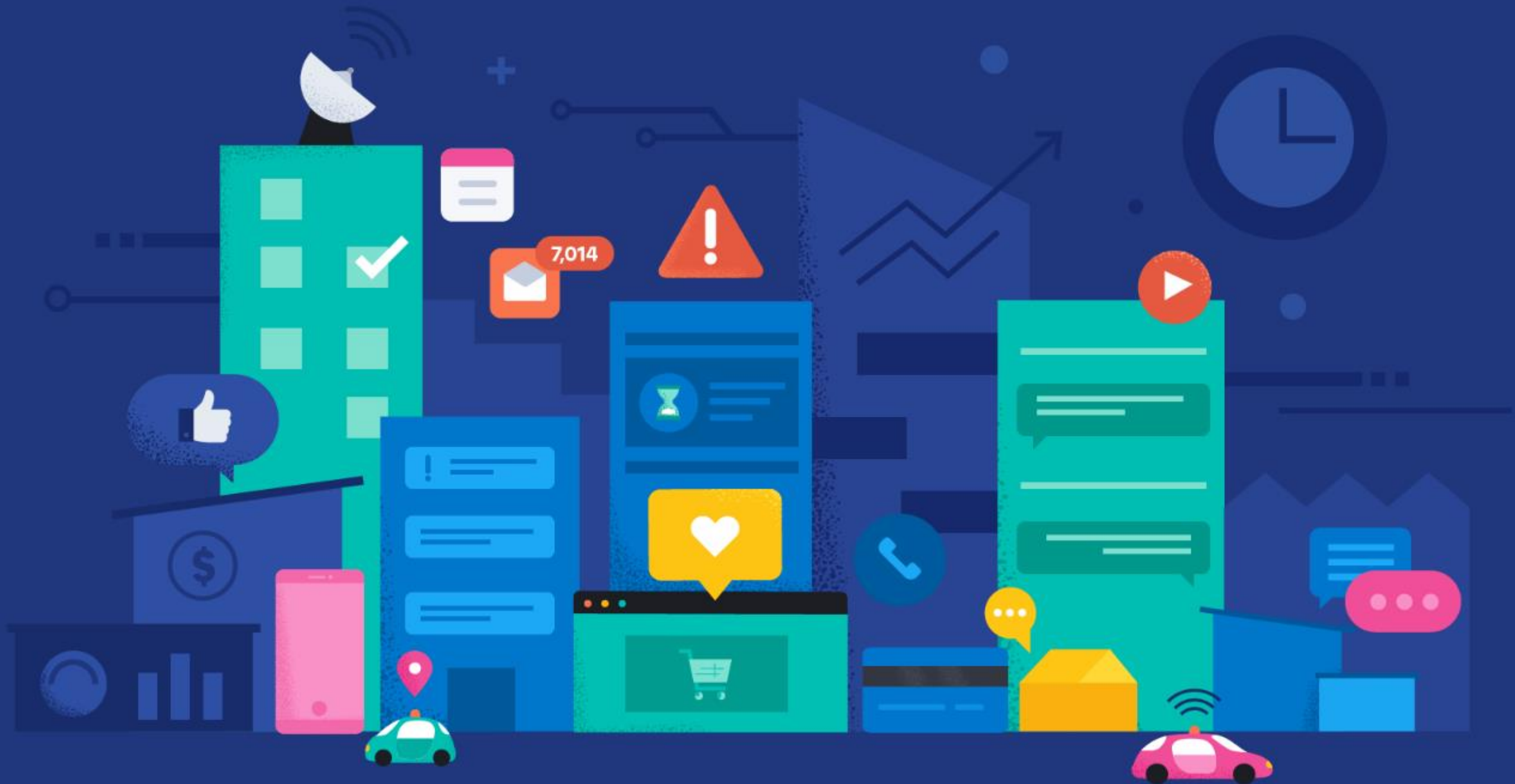
Prevent, detect, and respond at scale

Dimitri Janzen | Director OEM & MSP Sales | CEE

---

September 2022

Today we live in an *always on world*



# A world characterized by real challenges



Content is becoming  
harder to find



Enterprise IT is becoming  
more complex



Cyber threats are becoming  
more sophisticated

Beneath the surface  
all of these challenges are **connected to data**

**480EB**

1 EB = 1000 PB = 1,000,000 TB

Data produced  
daily by 2025

Conventional solutions  
*just don't work* anymore

## WHAT YOU NEED

Visibility

Any + all data

Analytics

ML / anomalies

Protection

Easily pivot

Response

Automate tasks

## WHAT CONVENTIONAL SOLUTIONS DELIVER

Doesn't scale

Insufficient context

Takes too long

Mundane tasks only

# Security teams need **a better way**



## Prevent attacks

- Known and unknown
- Pre-execution ransomware
- MITRE TTPs, advanced threats



## Detect accurately

- Minimal false-positives
- Rich entity context
- Coupled with critical business context



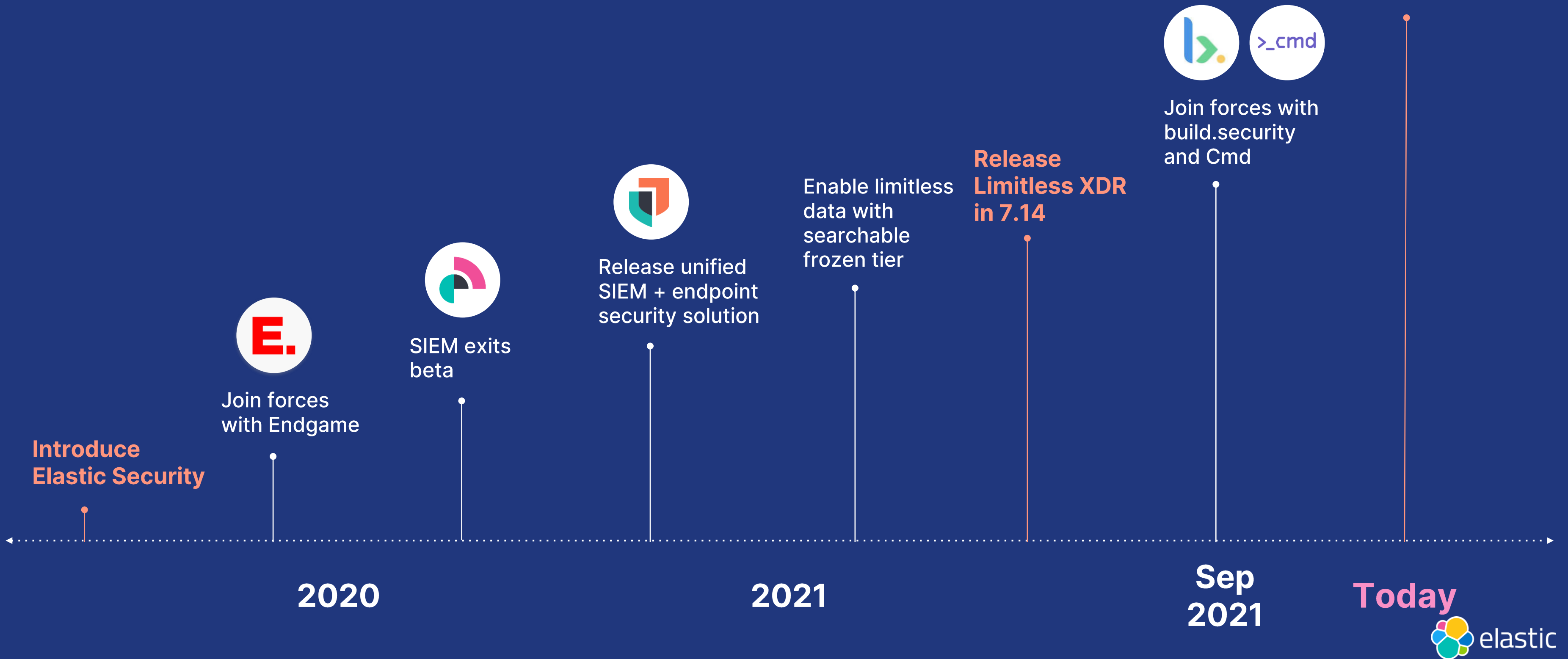
## Respond rapidly

- Ad-hoc correlation
- Seamless context gathering
- Remote response actions



# Elastic Security Extends to Cloud

**Released Cloud Security!**  
Expand cloud security capabilities





# Meet the Elastic Search Platform





# BEST PLATFORM FOR Security



**Search** enables real-time, holistic visibility for all SecOps



**Search** reduces dwell times to minimize or avoid damage



**Search** facilitates real-time detection and protection from endpoints to the data center



For continuous monitoring, automated threat protection, investigation & response, & threat hunting

## Prevent & Collect

### Pre-execution prevention

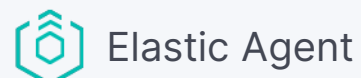
- Ransomware & malware prevention via ML & MBR
- Memory threat protection

### Post-execution prevention

- Ransomware protection via behaviors & canary files
- Malicious behavior protection

### Collection

- Kernel-level host activity collection
- Network activity analysis



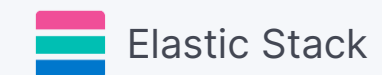
## Detect

- Detections built and tested by Elastic researchers and community: use cases, rules, ML models
- Advanced analytics, interactive visualizations, root-cause analysis
- Hunting and alert triage workflows
- Insights, context, and guidance embedded throughout UI
- Threat intelligence integrations
- Fast and scalable search platform, open data schema, on-prem to multi-cloud



## Respond

- Investigation & response workflows
- Alert actions: email, Slack, SOAR & ticketing platforms
- Case connectors: IBM, JIRA, ServiceNow, Swimlane
- Simple custom connections



- Host inspection via osquery
- Remote response actions



# Elastic Security Labs is **on your team**

- Research global threat landscape and advanced threat tradecraft
- Augment infosec teams with expertise in specialized disciplines
- Build and test automated protections to stop threats at scale
- Lower the analyst learning curve with triage and investigation guides
- Contribute to the global security community by sharing findings



One solution  
for all of your  
security use cases



Extended detection and response

Continuous  
monitoring

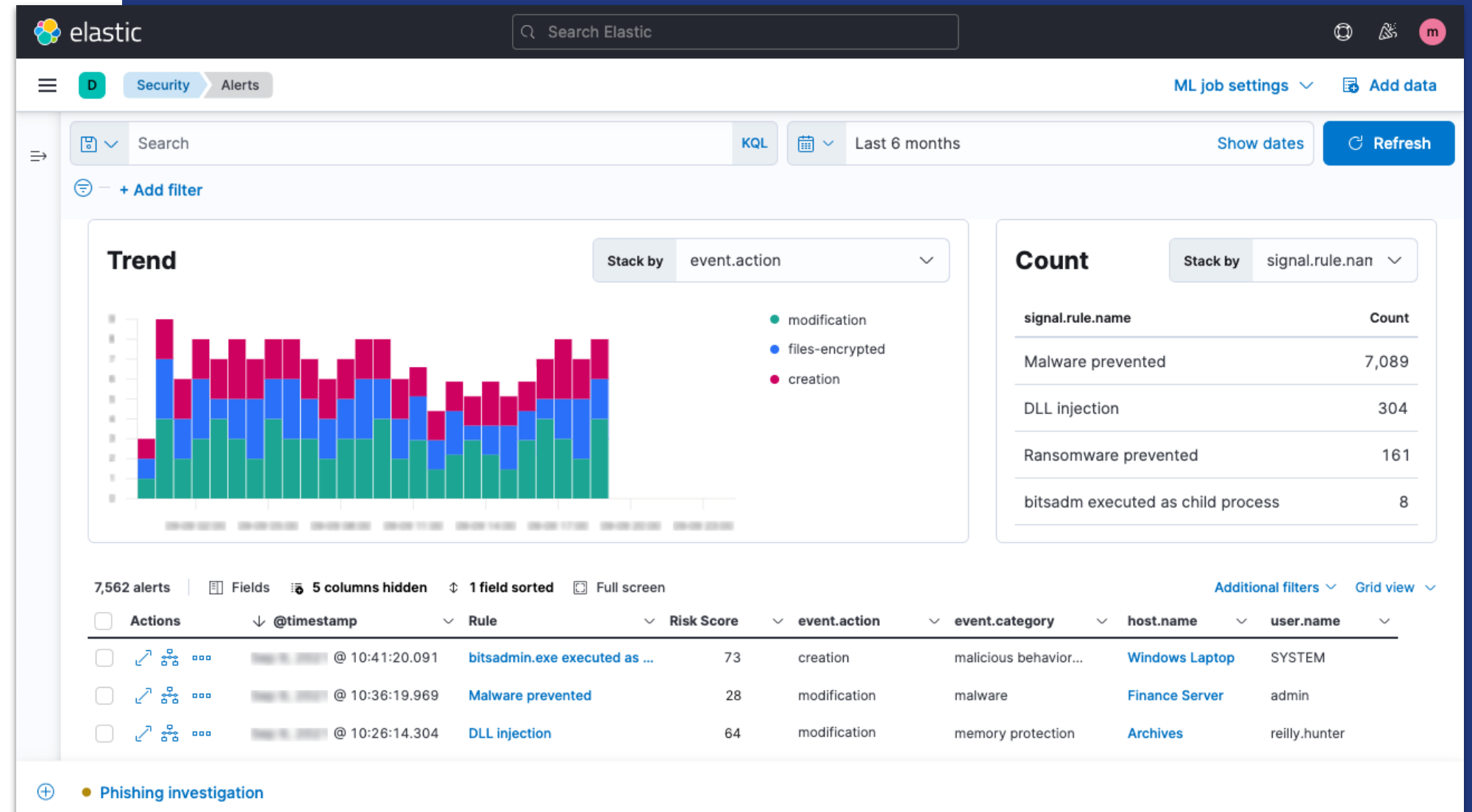
Automated threat  
protection

Investigation &  
Response

Threat hunting

# Continuous monitoring

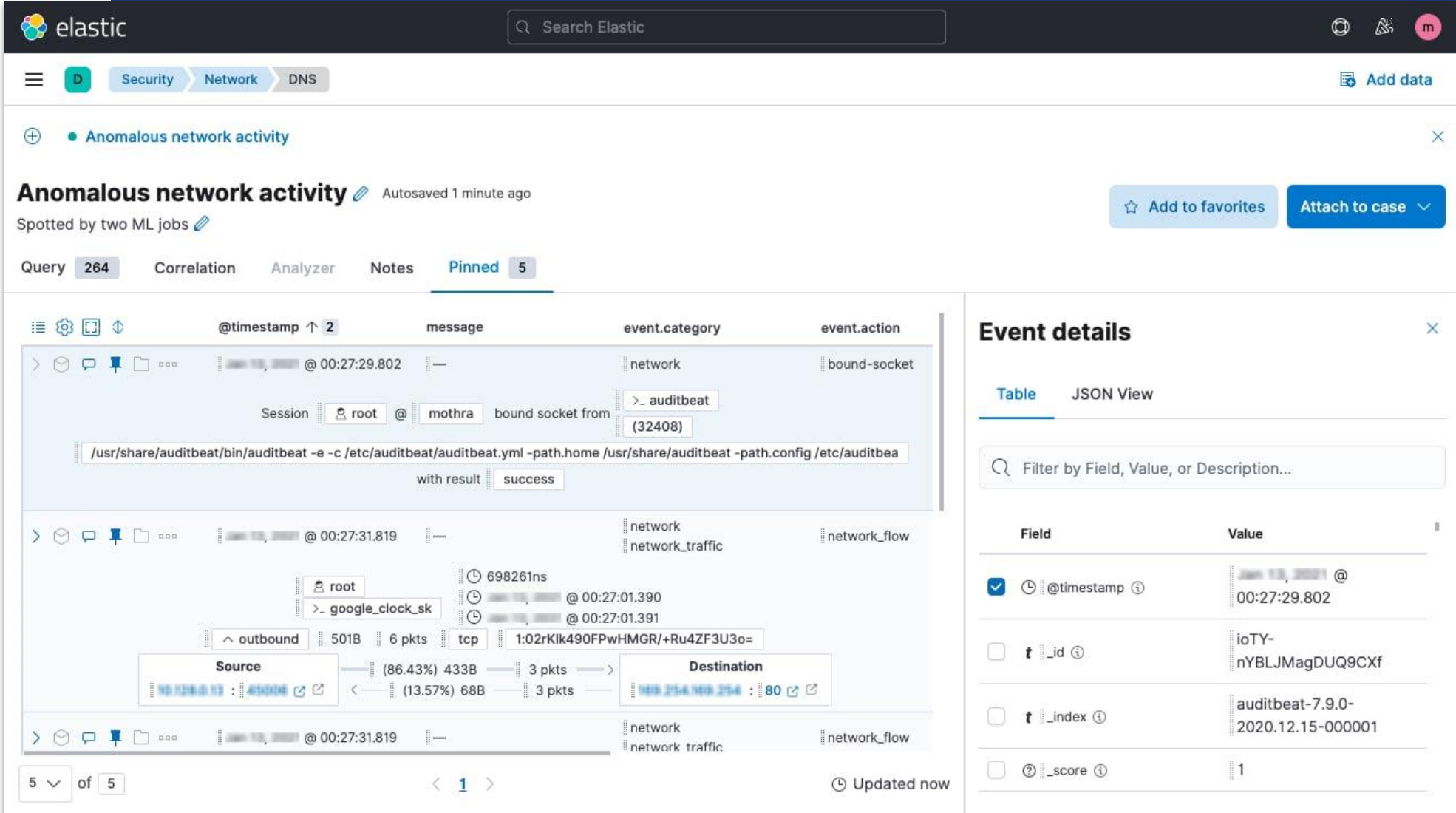
- Gain visibility across your enterprise
- Gather information of any kind — cloud, user, network, you name it
- Explore all of your data on tailored graphs and dashboards





# Threat hunting

- Leverage petabytes of data, enriched with threat intel
- Glean insights with advanced analytics
- Uncover threats you expected — and others you didn't

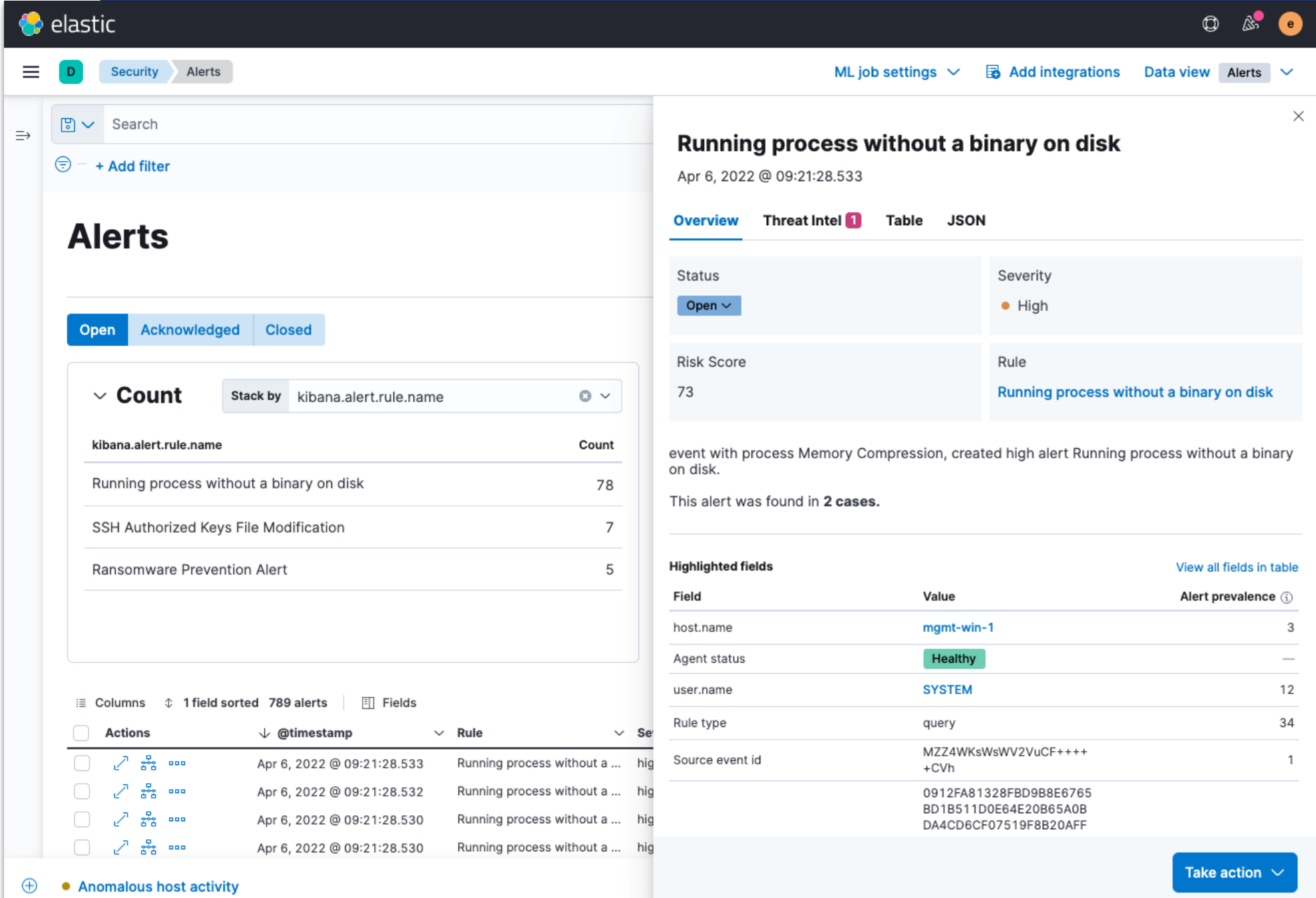


The screenshot displays the Elastic Security interface. At the top, there's a search bar and navigation tabs for Security, Network, and DNS. A breadcrumb trail shows the current view: Anomalous network activity. Below this, the main content area shows a list of events. The first event is highlighted, showing a session for 'root' on 'mothra' with a 'bound socket from' action. The event details panel on the right shows a table with fields like @timestamp, \_id, \_index, and \_score, with their corresponding values.

Field	Value
<input checked="" type="checkbox"/> @timestamp	2020-12-15T00:27:29.802Z
<input type="checkbox"/> _id	ioTY-nYBLJMagDUQ9CXf
<input type="checkbox"/> _index	auditbeat-7.9.0-2020.12.15-000001
<input type="checkbox"/> _score	1

# Automated threat protection

- Thwart complex attacks with ML and behavior analytics
- Block malware and ransomware on every endpoint
- Advance SecOps maturity to stop threats at scale



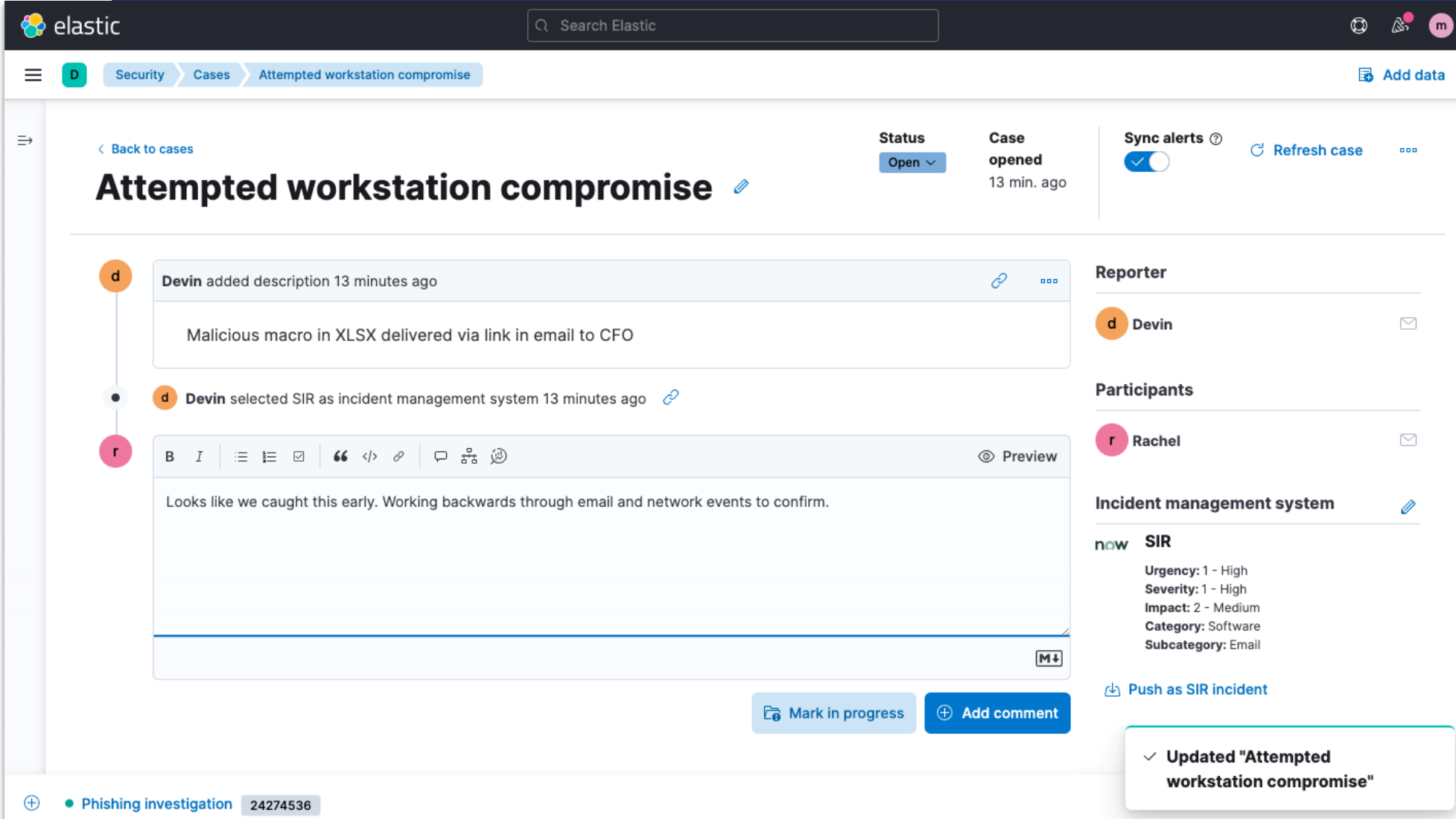
The screenshot displays the Elastic Security Alerts interface. The main view shows a table of alerts with columns for 'kibana.alert.rule.name' and 'Count'. The 'Running process without a binary on disk' rule has a count of 78. Below the table, there are options for 'Actions', '@timestamp', and 'Rule'. A detailed view of the 'Running process without a binary on disk' alert is shown on the right, including its status (Open), severity (High), risk score (73), and rule name. The detailed view also includes a table of highlighted fields with their values and alert prevalence.

Field	Value	Alert prevalence
host.name	mgmt-win-1	3
Agent status	Healthy	—
user.name	SYSTEM	12
Rule type	query	34
Source event id	MZZ4WksWsWV2VuCF+++++CVh	1
	0912FA81328FBD9B8E6765BD1B511D0E64E20B65A0BDA4CD6CF07519F8B20AFF	














# Investigation and response

- Expose unfolding attacks by correlating diverse data
- Seamlessly access vital context
- Respond rapidly with case management and powerful automations

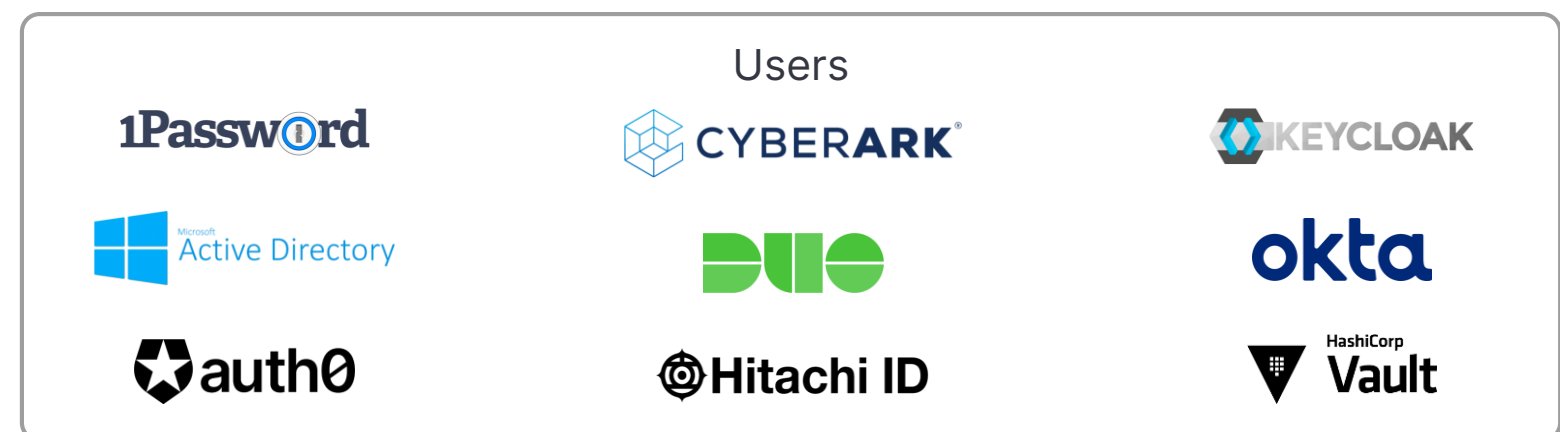
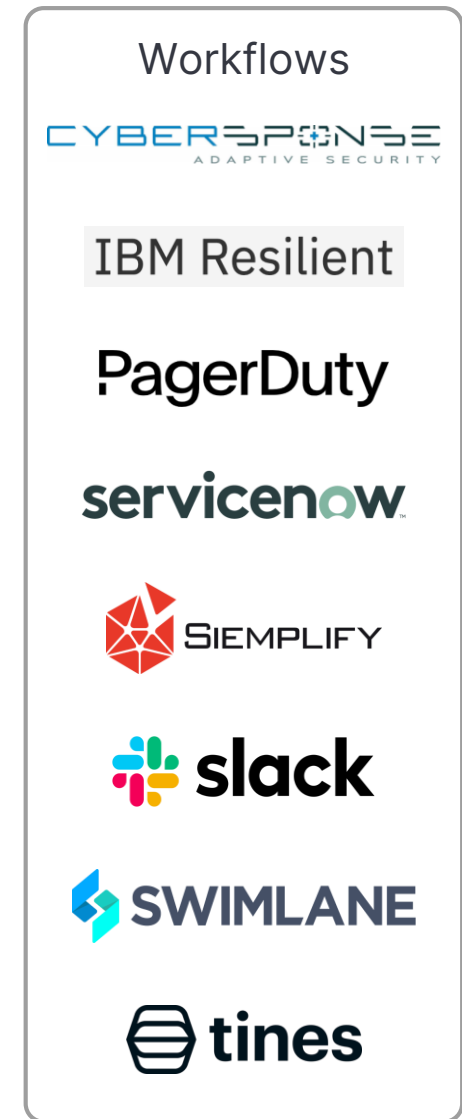


The screenshot displays the Elastic Security interface for a case titled "Attempted workstation compromise". The interface includes a search bar at the top, navigation tabs for "Security", "Cases", and "Attempted workstation compromise", and a "Search Elastic" input field. The case details show a status of "Open", a case opened 13 minutes ago, and a "Sync alerts" toggle. The main content area features a timeline of events: "Devin added description 13 minutes ago" with the text "Malicious macro in XLSX delivered via link in email to CFO", and "Devin selected SIR as incident management system 13 minutes ago". A rich text editor below shows a comment: "Looks like we caught this early. Working backwards through email and network events to confirm." The right sidebar lists the reporter "Devin", participants "Rachel", and the incident management system "SIR" with details: Urgency: 1 - High, Severity: 1 - High, Impact: 2 - Medium, Category: Software, Subcategory: Email. A "Push as SIR incident" button is also visible. At the bottom, a notification states "Updated 'Attempted workstation compromise'".

# A trusted solution across industries and geographies

TECHNOLOGY	FINANCE	TELCO	CONSUMER	HEALTHCARE	PUBLIC SECTOR	AUTOMOTIVE / TRANSPORTATION	RETAIL
							
							
							
							
							

# Integrations with **technology partners** you trust



# The Elastic Security Difference



## Open & integrated

Flexible data ingest and community support, with no vendor lock-in



## Native protections

Reduce mean time-to-protection with built-in prevention, detection and response



## Analyst workflows

Simplify deployment and management with a single stack and integrated workflows



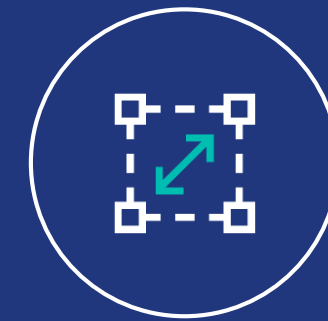
## Contextual insights

Investigate and hunt with a limitless data store powered by market-leading search



## Security + Observability

Secure the endpoint and cloud applications, or address customer experience, from a single interface



## Start small, scale up

Start simple and go big with predictable and flexible licensing

**Don't take**  
— just our —  
**word for it**



## Named a Peer Insights Customer Choice for SIEM by Gartner

Overall rating of 4.6 out of 5 in 2021 Gartner Peer Insights *Voice of the Customer* report for SIEM

Recommended by 98% of SIEM customers (highest in the industry)

<https://www.elastic.co/blog/elastic-security-recognized-customers-choice-gartner-peer-insights-report>

### ★★★★★ User Rating

“The solution provides fast and accurate insight across all the different apps and systems. With the built-in functionality, correlating events across the environment is really easy and together with the rest of the stack our SOC can continuously monitor, investigate, and respond in an intuitive and fast flow.”

— Technical Lead Security Monitoring in the Services industry

### ★★★★★ User Rating

“Displaced a number of legacy SIEM products, being able to provide longer retention and a higher ingest rate.”

— IT Security Manager in the manufacturing industry

### ★★★★★ User Rating

"You can't beat the speed and price. Great experience especially with how fast new features are being released. The search speed is incredible that no other product can compete with. Easy to scale and easy to have 100% availability due to distributed architecture.”

— Senior Security Analyst in the communications industry



# Recognized in the Gartner Magic Quadrant for SIEM

## 2021 Gartner Magic Quadrant for Security Information and Event Management (SIEM)

—Kelly Kavanagh, Toby Bussa, John Collins, May 2021

<https://www.elastic.co/campaigns/2021-gartner-magic-quadrant-siem>

This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request. Gartner does not endorse any vendor, product or service depicted in its research publications and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally, and is used herein with permission. All rights reserved.

Figure 1: Magic Quadrant for Security Information and Event Management



Source: Gartner (June 2021)



# THE FORRESTER NEW WAVE™

## Extended Detection And Response (XDR) Providers

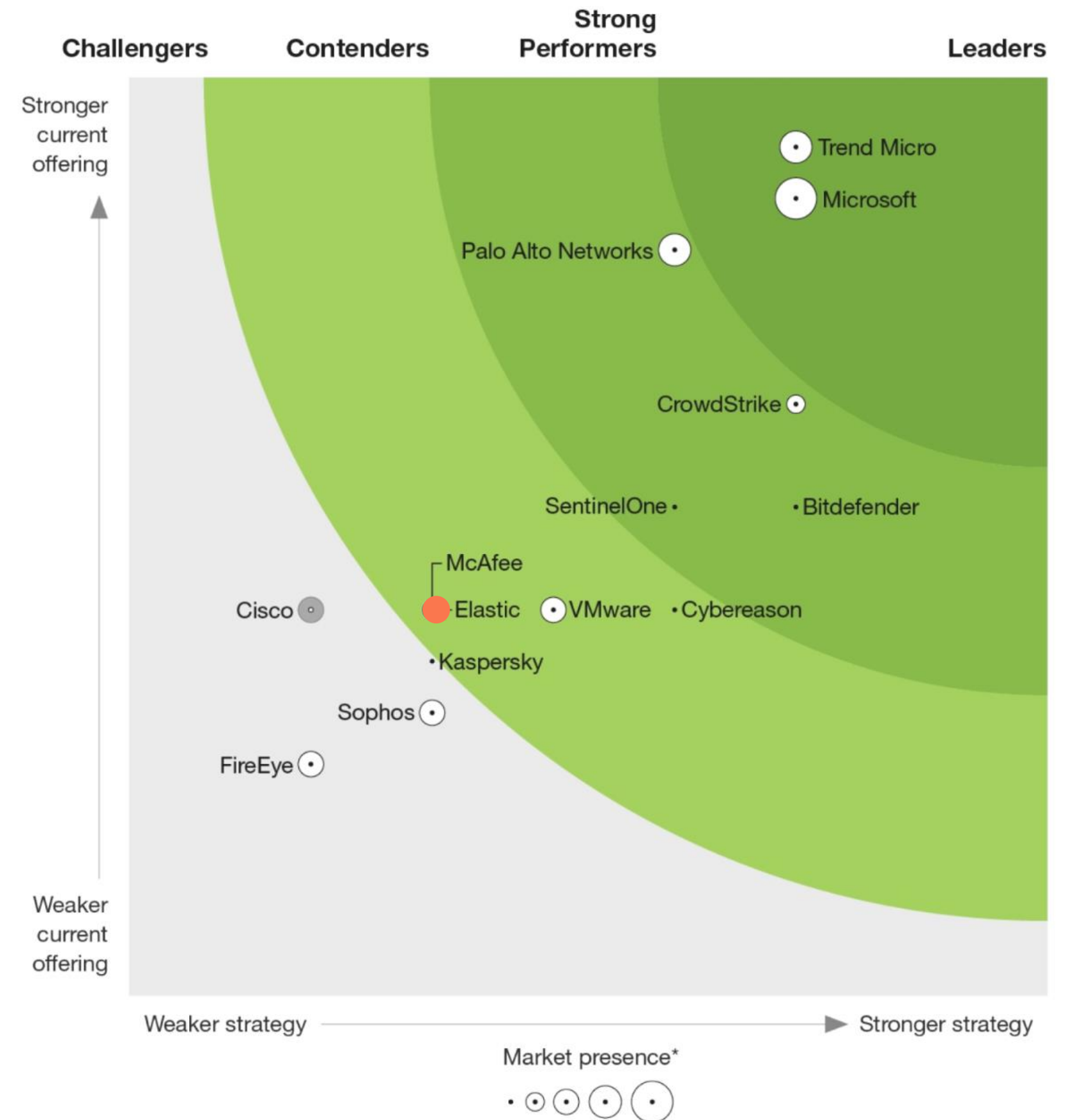
Q4 2021

# Recognized in the Forrester Wave™ for XDR

The Forrester New Wave™: Extended Detection and Response (XDR) Providers

—Allie Mellen, October 2021

<https://www.forrester.com/report/the-forrester-new-wave-tm-extended-detection-and-response-xdr-providers-q4-2021/RES176400>



# Recognized in the Forrester Wave™ for EDR

The Forrester Wave™: Endpoint Detection And Response Providers, Q2 2022

—Allie Mellen, April 2022

<https://www.forrester.com/report/the-forrester-wave-tm-endpoint-detection-and-response-providers-q2-2022/RES176332>

## THE FORRESTER WAVE™

Endpoint Detection And Response Providers

Q2 2022



Thank You