2023 Global Threat Trends: An Elastic Security Perspective

elastic

Search. Observe. Protect.

whoami

- Sr Security Architect, Consultant
- Elastic Global Security Specialists Group
- Architect and Builder of Security Operations Capability
- Lover of everything security (...and yes, I have other hobbies too!)

Marvin Ngoma

[“CISSP”, “GSOM”, “Msc”]

eMail **marvin**@elastic.co

slack **@marvin.ngoma** on **elasticstack.slack.com** (Public community slack)

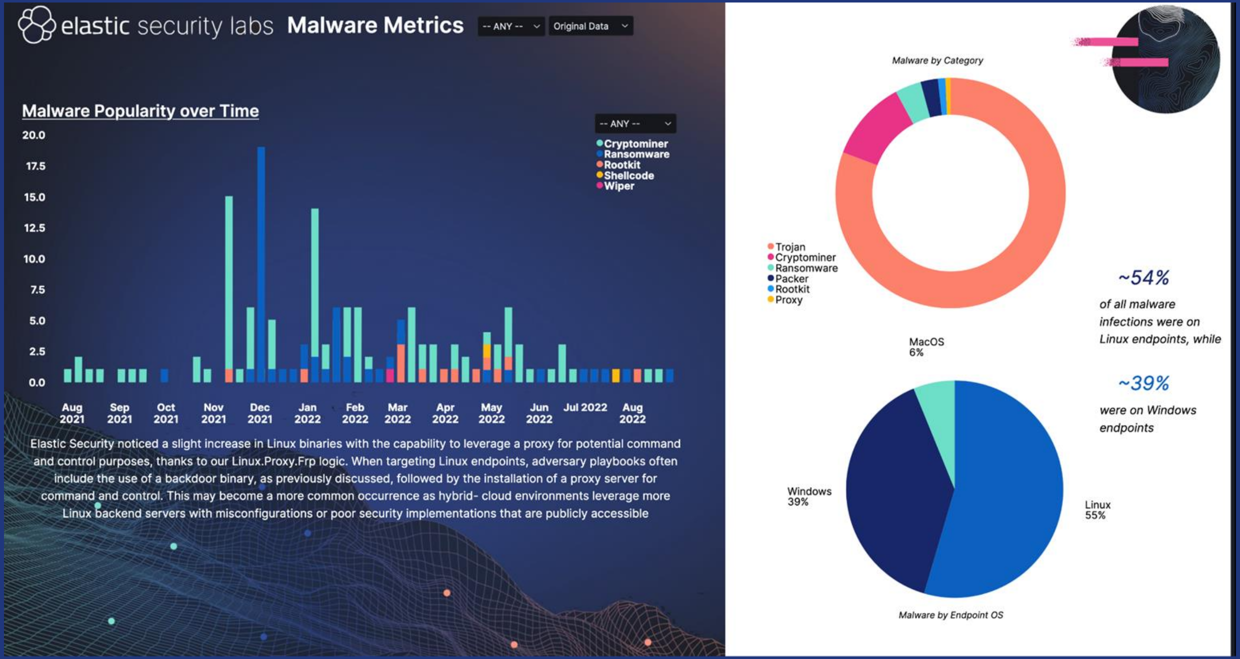
LinkedIn Marvin Ngoma
https://www.linkedin.com/in/tyolani

Outline

- **Elastic Global Threat Report**
  - What are we seeing in 2023 so far?
  - Why does the report matter?
  - How Elastic Security leverages the report
- **Elastic Security Overview**
  - What problems are we solving?
  - Augmentation of SIEM, Endpoint Security & Cloud Security

Elastic Global Threat Report

- **A summary of**
  - threat trends,
  - forecasts, and
  - recommendations
- **Based on analyzing millions of telemetry events shared by users around the world.**



Elastic Security noticed a slight increase in Linux binaries with the capability to leverage a proxy for potential command and control purposes, thanks to our Linux.Proxy.Frp logic. When targeting Linux endpoints, adversary playbooks often include the use of a backdoor binary, as previously discussed, followed by the installation of a proxy server for command and control. This may become a more common occurrence as hybrid- cloud environments leverage more Linux backend servers with misconfigurations or poor security implementations that are publicly accessible

~54%

of all malware infections were on Linux endpoints, while

~39%

were on Windows endpoints

elastic

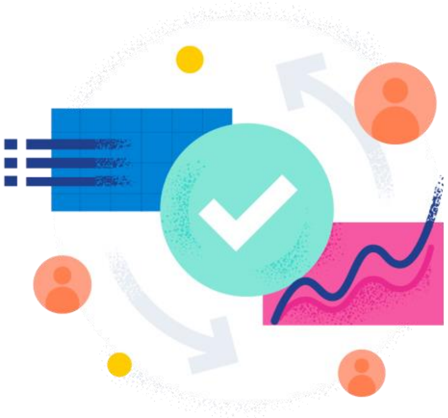
So far in 2023...

- 25% increase in Ransomware
- Significant increase in malware on Linux
  - Huge concern, especially with the advent of cloud computing
- Trojans and in-memory attacks increasing
  - Driven by AV evasion objective
  - Impairing defenses
  - This includes use of LOL/GTF BINs

Why does this matter?

- **Trends**
  - Help focus on relevant prevention and detection capability
- **Forecasts**
  - Understanding adversary traits and objectives
  - Proactiveness in threat hunting
- **Recommendations**
  - Early prevent and detect capability
  - Quick address of zero-day threats
  - Threat intel?

How Elastic Security leverages the report?



Expert Research with Elastic Security Labs

- Open threat research and malware analysis e.g. SPECTRALVIPER, r77 rootkit, Lobshot malware, XWORM and AGENTTESLA, SUDDENICON, SiestaGraph, ICEDID
- Out-of-the-box, constantly updated threat detection rules (~820)
- Out-of-the-box adaptable unsupervised machine learning models (65+)
- Curated security artifacts for malware, ransomware, memory, and more

https://www.elastic.co/security-labs/

So what does Elastic Security offer today?

The Elastic Security Solution

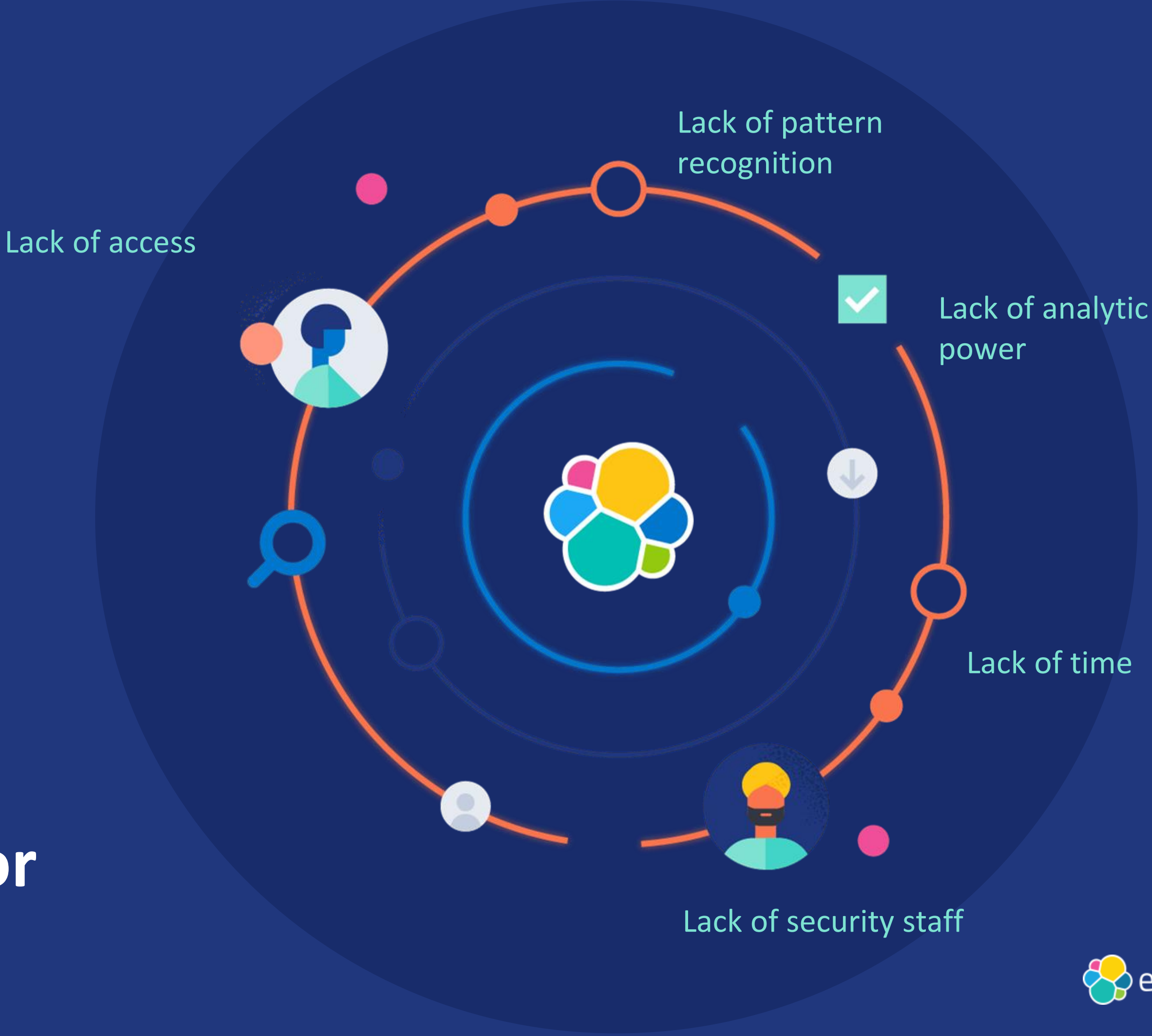
Modern Security Operations Platform

elastic

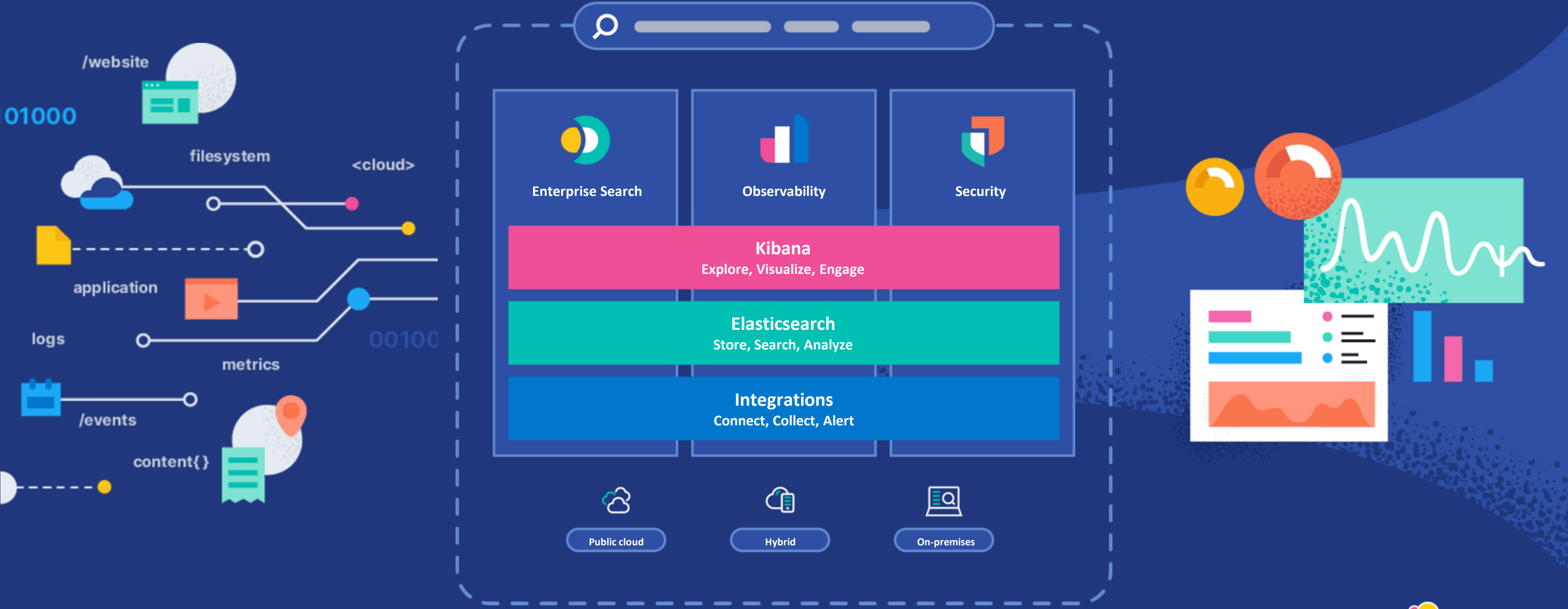
> “
>
> **Protect the world’s data from attack**

Elastic Security Mission Statement

Data is the common denominator



The Elastic Search Platform



Enterprise Search

Observability

Security

Kibana
Explore, Visualize, Engage

Elasticsearch
Store, Search, Analyze

Integrations
Connect, Collect, Alert

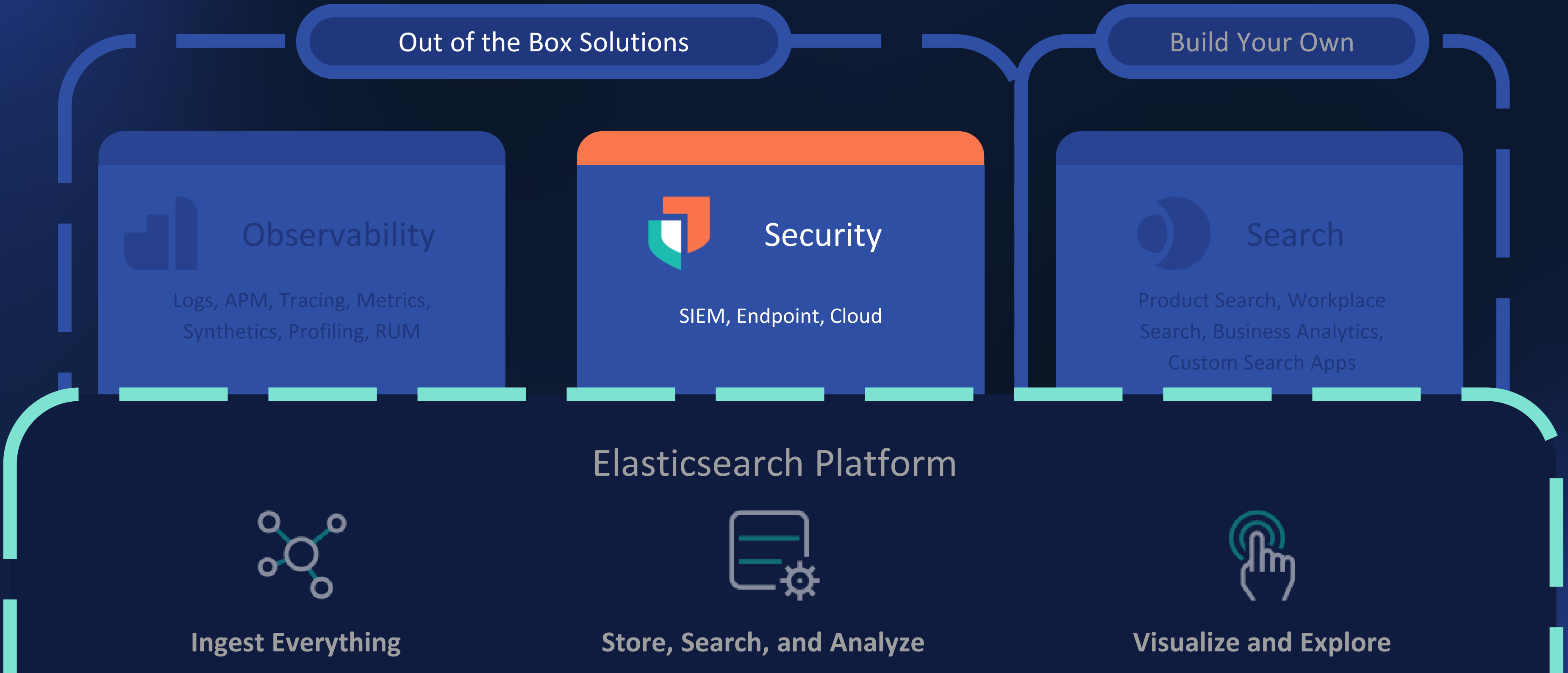
Public cloud

Hybrid

On-premises

Elastic Security

Unified SIEM, endpoint detection & response, and cloud security in a single solution



Out of the Box Solutions

Build Your Own

Observability

Logs, APM, Tracing, Metrics, Synthetics, Profiling, RUM

Security

SIEM, Endpoint, Cloud

Search

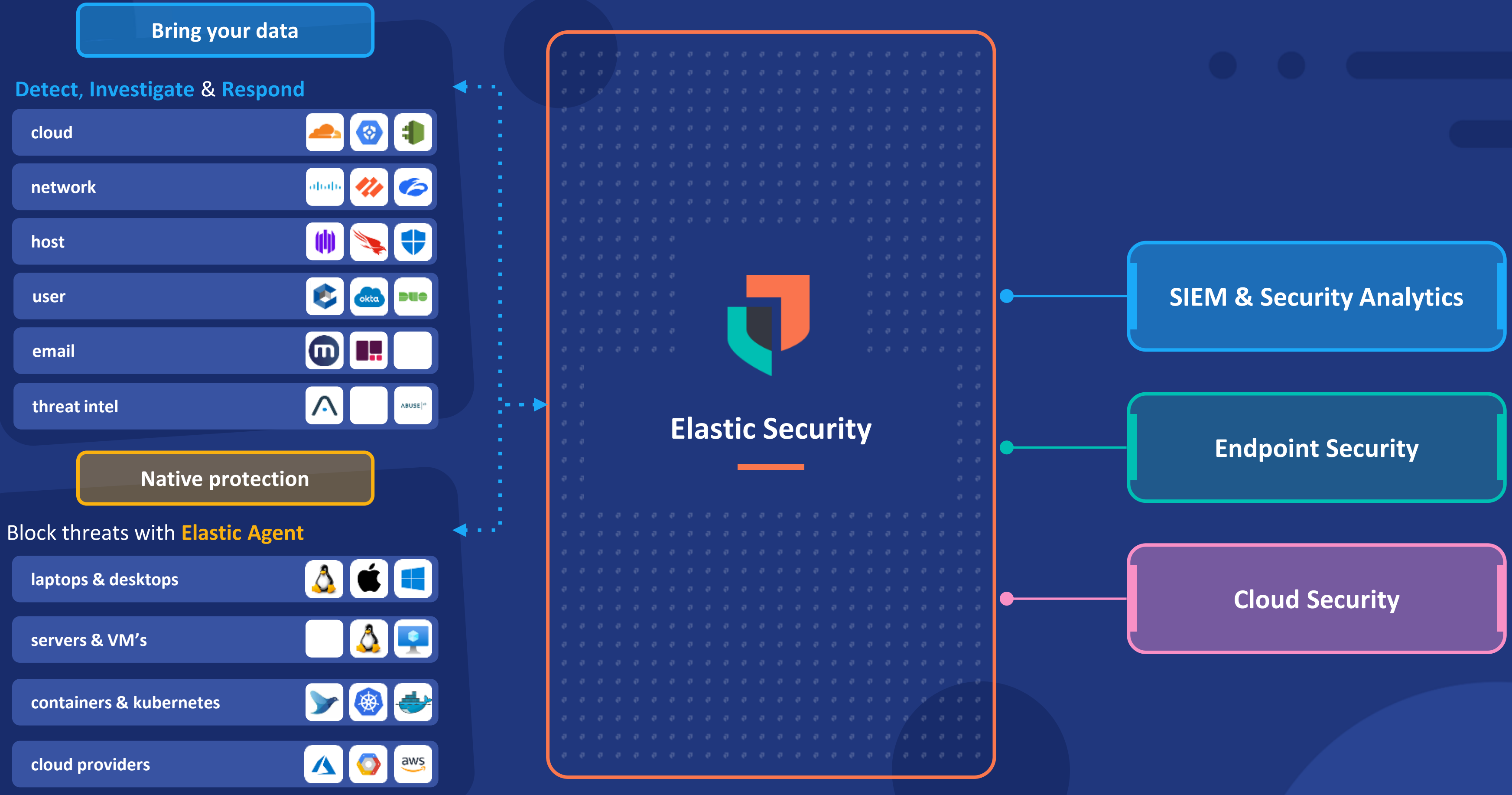
Product Search, Workplace Search, Business Analytics, Custom Search Apps

Elasticsearch Platform

Ingest Everything

Store, Search, and Analyze

Visualize and Explore



Bring your data

Detect, Investigate & Respond

- cloud
- network
- host
- user
- email
- threat intel

Native protection

Block threats with Elastic Agent

- laptops & desktops
- servers & VM's
- containers & kubernetes
- cloud providers

Elastic Security

- SIEM & Security Analytics
- Endpoint Security
- Cloud Security

Powered by Elastic Security Labs - Threat Research

Elastic Security for SIEM

Limitless Data Analysis

- Extensive library of prebuilt data source integrations with Elastic Agent
- Custom ETL via Logstash
- Events, logs, threat intelligence, more
- Normalized to Elastic Common Schema
- Hundreds of prebuilt dashboards
- Data quality & health assessments
- Flexible, cost-effective data retention

Threat Detection

- Flexible detection workflows for searching, correlation, sequences
- Library of ~800 prebuilt rules provide detection engineering expertise
- Optimized SOC workflows for triage, investigation, and case management
- Threat hunting workflows for hypothesis driven hunts

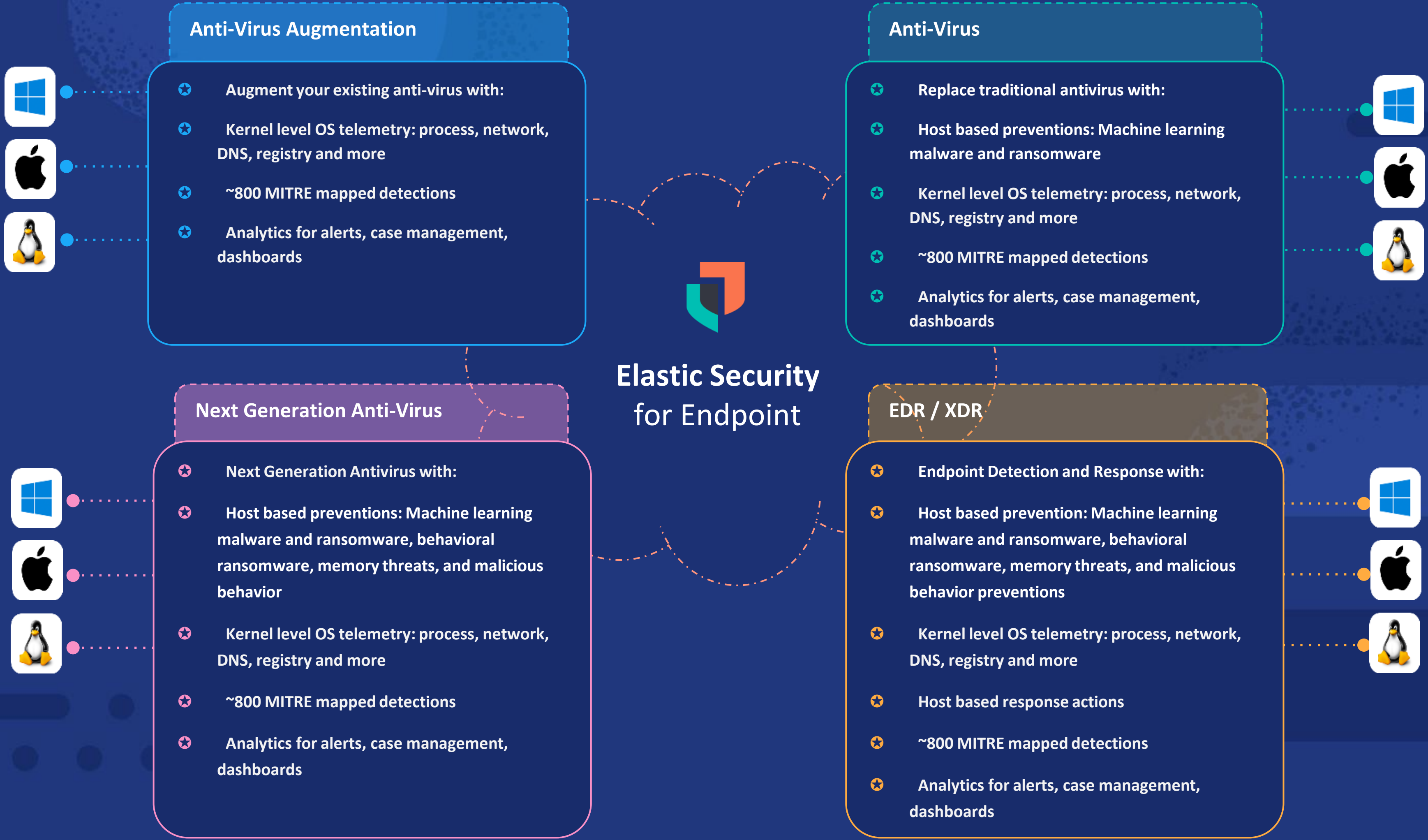
Advanced Entity Analytics

- Highly operationalized machine learning capabilities
- Dozens of prebuilt anomaly detection models
- Risk scores for users, hosts, and other entities
- Unified approach to risk-based alerting

Automation & Remediation

- Automated responses via rule actions
- Interactive investigation guides automate triage and investigation
- Native remediation capabilities when using Elastic Defend (Agent)
- Integrations with 3rd party SOAR tools
- Interactive response console allows hunting, forensics, remediation

elastic



Elastic Security for Endpoint

Anti-Virus Augmentation

- Augment your existing anti-virus with:
- Kernel level OS telemetry: process, network, DNS, registry and more
- ~800 MITRE mapped detections
- Analytics for alerts, case management, dashboards

Anti-Virus

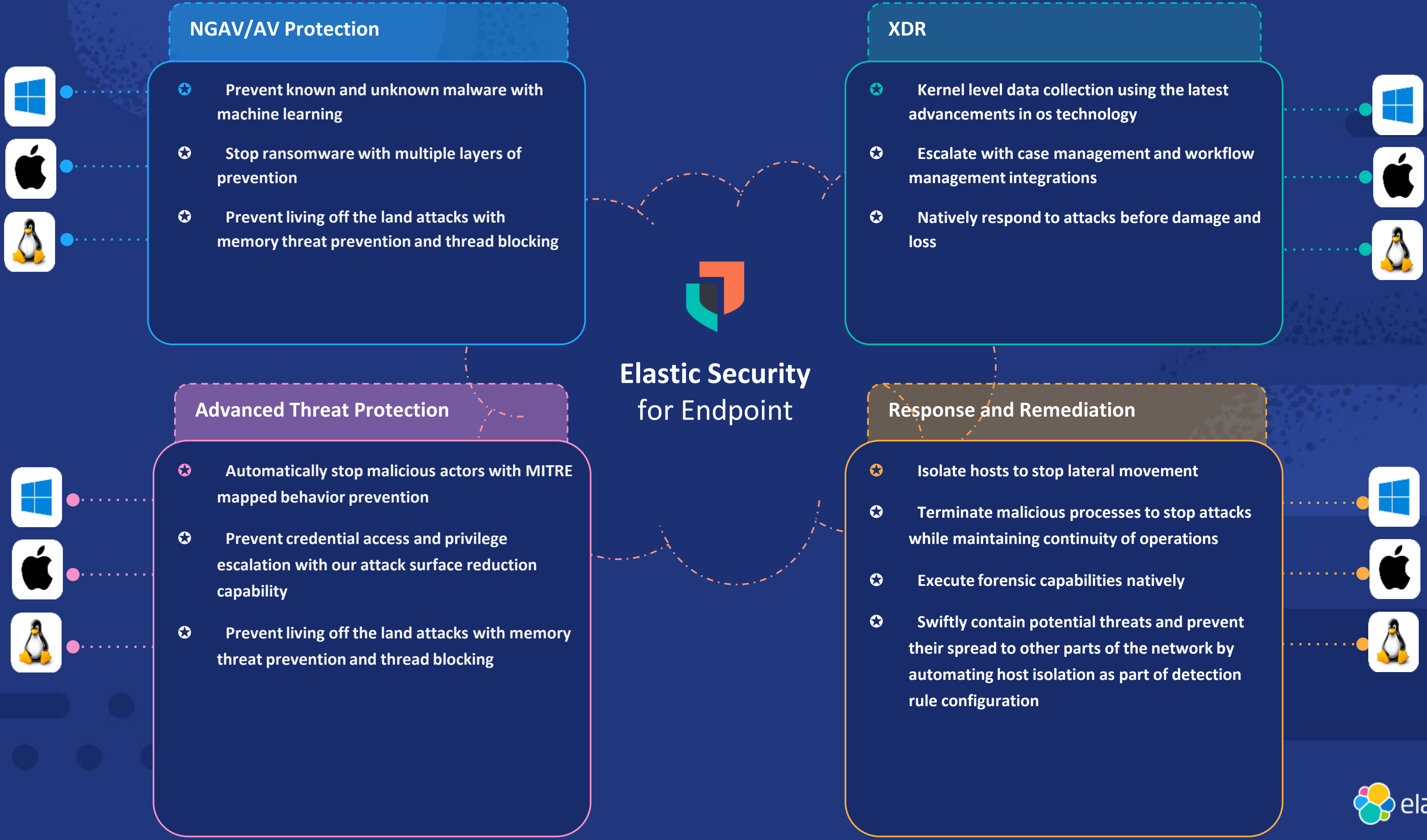
- Replace traditional antivirus with:
- Host based preventions: Machine learning malware and ransomware
- Kernel level OS telemetry: process, network, DNS, registry and more
- ~800 MITRE mapped detections
- Analytics for alerts, case management, dashboards

Next Generation Anti-Virus

- Next Generation Antivirus with:
- Host based preventions: Machine learning malware and ransomware, behavioral ransomware, memory threats, and malicious behavior
- Kernel level OS telemetry: process, network, DNS, registry and more
- ~800 MITRE mapped detections
- Analytics for alerts, case management, dashboards

EDR / XDR

- Endpoint Detection and Response with:
- Host based prevention: Machine learning malware and ransomware, behavioral ransomware, memory threats, and malicious behavior preventions
- Kernel level OS telemetry: process, network, DNS, registry and more
- Host based response actions
- ~800 MITRE mapped detections
- Analytics for alerts, case management, dashboards



Elastic Security for Endpoint

NGAV/AV Protection

- Prevent known and unknown malware with machine learning
- Stop ransomware with multiple layers of prevention
- Prevent living off the land attacks with memory threat prevention and thread blocking

XDR

- Kernel level data collection using the latest advancements in os technology
- Escalate with case management and workflow management integrations
- Natively respond to attacks before damage and loss

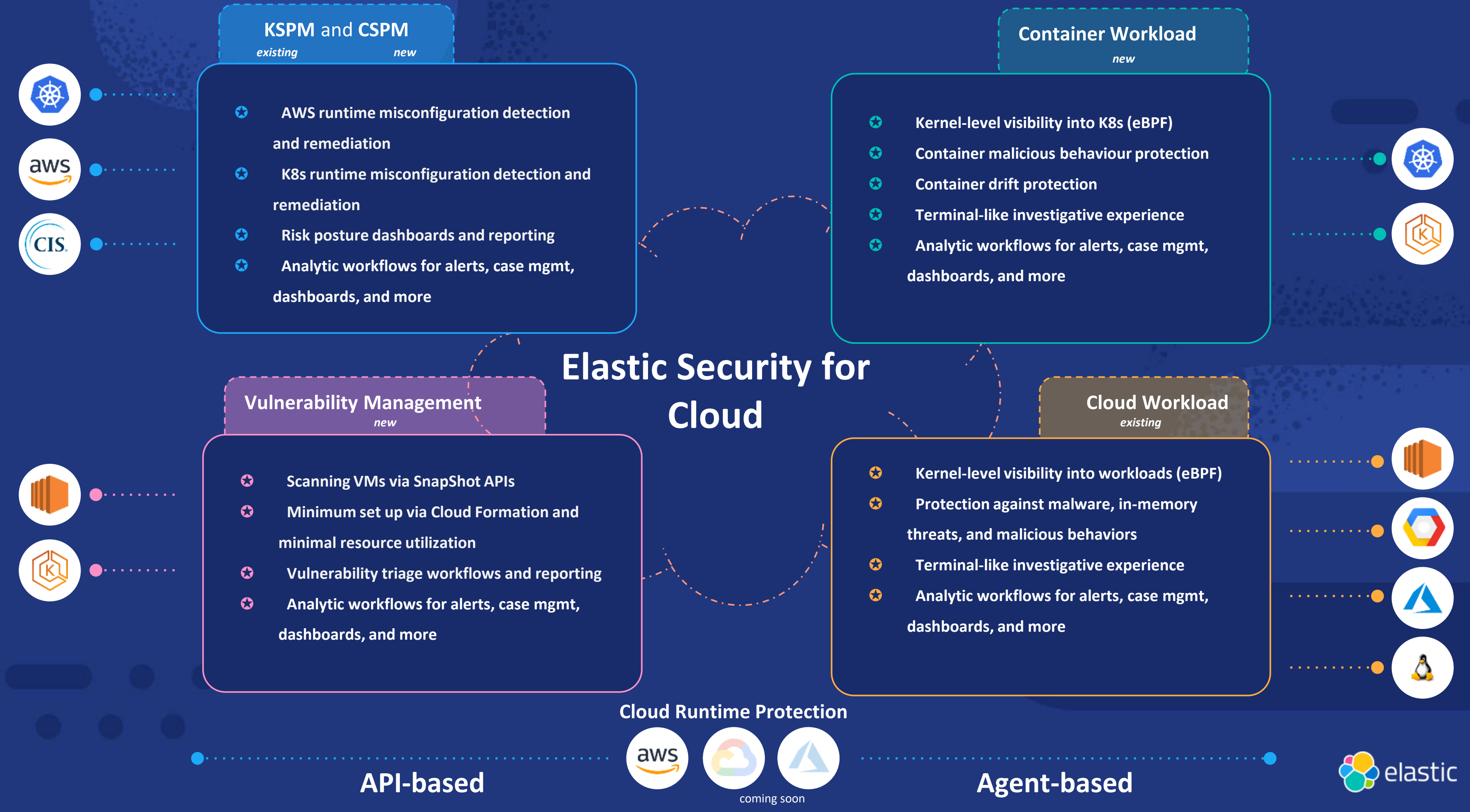
Advanced Threat Protection

- Automatically stop malicious actors with MITRE mapped behavior prevention
- Prevent credential access and privilege escalation with our attack surface reduction capability
- Prevent living off the land attacks with memory threat prevention and thread blocking

Response and Remediation

- Isolate hosts to stop lateral movement
- Terminate malicious processes to stop attacks while maintaining continuity of operations
- Execute forensic capabilities natively
- Swiftly contain potential threats and prevent their spread to other parts of the network by automating host isolation as part of detection rule configuration

elastic



Elastic Security for Cloud

KSPM and CSPM

existing *new*

- AWS runtime misconfiguration detection and remediation
- K8s runtime misconfiguration detection and remediation
- Risk posture dashboards and reporting
- Analytic workflows for alerts, case mgmt, dashboards, and more

Container Workload

new

- Kernel-level visibility into K8s (eBPF)
- Container malicious behaviour protection
- Container drift protection
- Terminal-like investigative experience
- Analytic workflows for alerts, case mgmt, dashboards, and more

Vulnerability Management

new

- Scanning VMs via SnapShot APIs
- Minimum set up via Cloud Formation and minimal resource utilization
- Vulnerability triage workflows and reporting
- Analytic workflows for alerts, case mgmt, dashboards, and more

Cloud Workload

existing

- Kernel-level visibility into workloads (eBPF)
- Protection against malware, in-memory threats, and malicious behaviors
- Terminal-like investigative experience
- Analytic workflows for alerts, case mgmt, dashboards, and more

Cloud Runtime Protection

coming soon

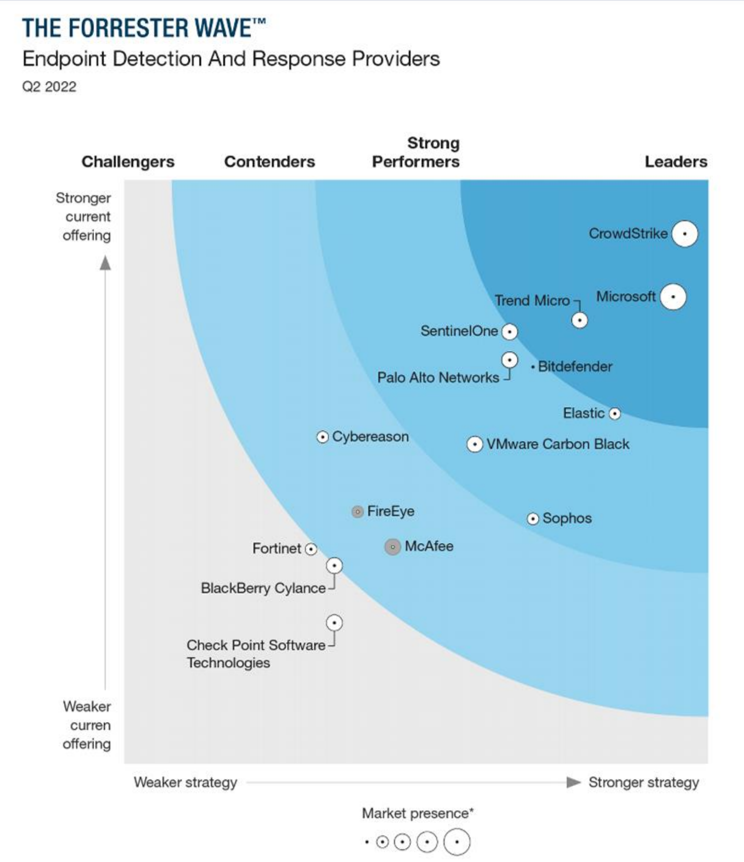
API-based

Agent-based

elastic

Elastic named a Strong Performer in The Forrester Wave for EDR Providers, Q2 2022

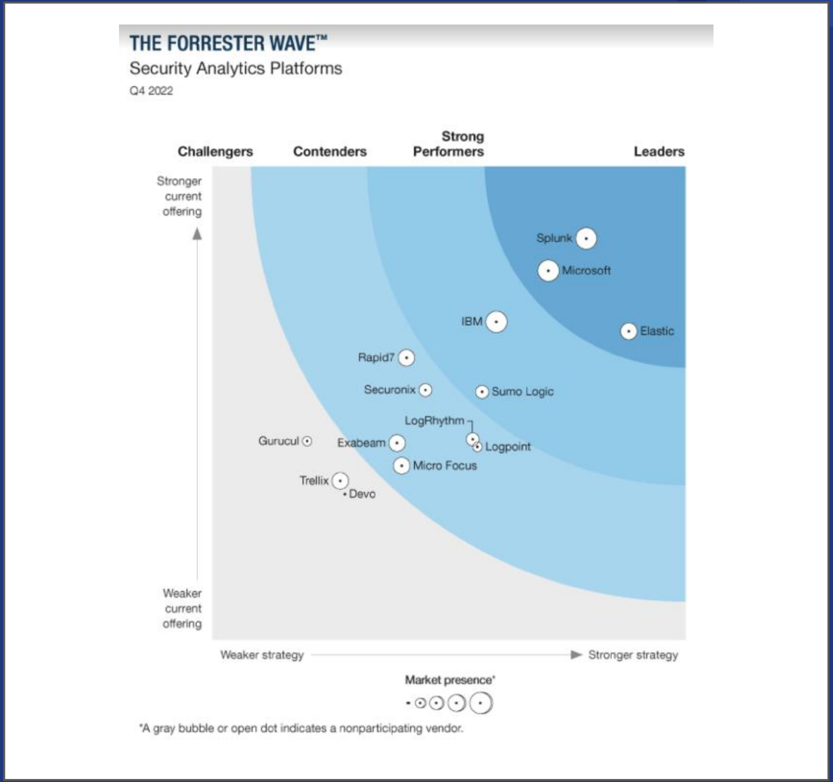
- Elastic envisions security as a data problem and prioritizes features that enable customers to use that data as they see fit.
- It has nurtured an online community so that security teams can crowdsource expertise, which customer references find valuable.


THE FORRESTER WAVE™
Endpoint Detection And Response Providers
Q2 2022

The Forrester Wave™ is copyrighted by Forrester Research, Inc. Forrester and Forrester Wave™ are trademarks of Forrester Research, Inc. The Forrester New Wave™ is a graphical representation of Forrester's call on a market. Forrester does not endorse any vendor, product, or service depicted in the Forrester Wave™. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change.

Elastic named a Leader in **The Forrester Wave™ Security Analytics Platforms Q4 2022**

- *“Elastic provides incredible flexibility and visualizations in an open offering.”*
- *“Reference customers value the flexibility on pricing and subsequent cost savings that Elastic provides.”*
- *“Elastic Security best suits clients comfortable with security engineering looking for an extremely customizable product.”*



THE FORRESTER WAVE™
Security Analytics Platforms
Q4 2022

*A gray bubble or open dot indicates a nonparticipating vendor.

FORRESTER®

WAVE LEADER 2022

Security Analytics Platforms

The Forrester Wave™ is copyrighted by Forrester Research, Inc. Forrester and Forrester Wave™ are trademarks of Forrester Research, Inc. The Forrester New Wave™ is a graphical representation of Forrester’s call on a market. Forrester does not endorse any vendor, product, or service depicted in the Forrester Wave™. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change.

elastic

Elastic Security is for everyone

NetApp
BRI
U.S. AIR FORCE
Walmart
ECOLAB
EzeCastle INTEGRATION
Emirates NBD
MASERGY
WILEY
Martin's Point Health Care
Insane FORENSICS
OLX GROUP
UC DAVIS UNIVERSITY OF CALIFORNIA
CALGARY CATHOLIC SCHOOL DISTRICT
VITAS Healthcare
SMARTER CITY SOLUTIONS Integrated (for) Life
PSCU
UNIVERSITY OF NEVADA RENO OMNIA PRO PATRIA 1874
OAK RIDGE National Laboratory
OmniSOC
TALOS
SoftBank
SL SALT LAKE COUNTY
wepay a CHASE company
TDS
Bell
ECS
misi
bit SOUTH DAKOTA BUREAU OF INFORMATION AND TELECOMMUNICATIONS
personal CAPITAL

Questions & Feedback

Thank You!!

elastic

How can you learn more about Elastic Security

- See the power of prevention at ohmymalware.com
- Try Elastic Security for yourself at cloud.elastic.co
- Download our Global Threat Report at elastic.co/security-labs
- Speak to your local Elastic expert or partner