

Elastic Financial Analyst Day 2022

September 19, 2022

Forward-looking statements and non-GAAP disclaimer

This presentation and the accompanying oral presentation contain forward-looking statements that involve substantial risk and uncertainties, which include, but are not limited to, our future results of operations and financial position, including our expected financial results for the fiscal fiscal quarter ending October 31, 2022 and the fiscal years ending April 30, 2023, April 30, 2024 and April 30, 2025; financial targets; business strategy; plans and objectives for future operations; our focus on and the growth and adoption of our Elastic Cloud offering; our assessments of the strength of our solutions and products; key product goals; the effectiveness of our go-to-market and growth strategies, assessments of new and existing customers' spending priorities or reasons for selecting our solutions and products; new enhancements to our existing products and services or plans for future products; the expected performance or benefits of our offerings; our customer base, including the needs of our customers and our ability to address these needs; estimates of our potential addressable market and growth opportunities and our ability to address those opportunities; and our expectations regarding revenue mix, our ability to grow our business, the drivers of growth and the benefits of our investments. Actual outcomes and results may differ materially from those contemplated by these forward-looking statements due to uncertainties, risks, and changes in circumstances, including but not limited to those related to: our future financial performance, including our expectations regarding our revenue, cost of revenue, gross profit or gross margin, operating expenses (which include changes in sales and marketing, research and development and general and administrative expenses), and our ability to achieve and maintain future profitability; our ability to continue to deliver and improve our offerings and develop new offerings; customer acceptance and purchase of our new and existing offerings and the expansion and adoption of our Elastic Cloud offerings; our inability to realize value from investments in the business; our ability to maintain and expand our user and customer base; the impact of the COVID-19 pandemic and variants on the macroeconomic environment, on our business, operations, hiring and financial results, and on businesses and spending priorities of our customers and partners; the impact of our licensing model on the use and adoption of our software; the impact of our pricing model strategies on our business; the impact of foreign currency exchange rate and interest rate fluctuations on our results; our international expansion strategy; our operating results and cash flows; the sufficiency of our capital resources; our ability to successfully execute our go-to-market strategy and expand in new and existing markets, and our ability to forecast customer retention and expansion; and general market, political, economic and business conditions.

Additional risks and uncertainties that could cause actual outcomes and results to differ materially are included in our filings with the Securities and Exchange Commission (the “SEC”), including the quarterly report on Form 10-Q for the quarter ended July 31, 2022 and other subsequent reports filed with the SEC. SEC filings are available on the Investor Relations section of Elastic’s website at ir.elastic.co and the SEC’s website at www.sec.gov. Elastic assumes no obligation to, and does not currently intend to, update any such forward-looking statements, except as required by law.

In addition to GAAP financial information, this presentation and the accompanying oral presentation include certain non-GAAP financial measures. See the Appendix for a reconciliation of all historical non-GAAP financial measures to their nearest GAAP equivalent.

Elastic Investor Day 2022



Ash Kulkarni
CEO



Shay Banon
Co-Founder & CTO



Janesh Moorjani
CFO & COO



Michael Cremen
Chief Sales Officer



Rick Laner
Chief Customer Officer



Steve Kearns
VP
Elastic Platform



Sajai Krishnan
GM
Elastic Observability



Santosh Krishnan
GM
Elastic Security



Matt Riley
GM
Elastic Enterprise Search



Nikolay Beliov
VP
Investor Relations

elastic

Agenda

Topic	Presenter	Time
Elastic Business Strategy	Ash Kulkarni	1:00pm PT
Elastic Search Platform	Shay Banon with GMs & Product Leads	1:30pm PT
Break		3:00pm PT
Accelerating GTM	Michael Cremen	3:15pm PT
Customer Panel	Rick Laner	3:45pm PT
Journey to $2B with Profitable Growth	Janesh Moorjani	4:15pm PT
Q&A with Elastic Leadership		4:45pm PT
Reception and Demos		5:15pm PT

elastic

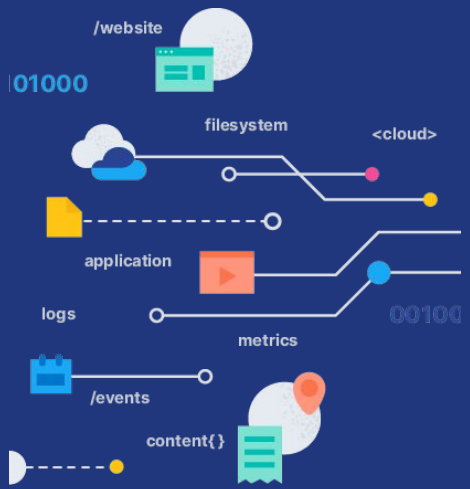
Elastic Business Strategy

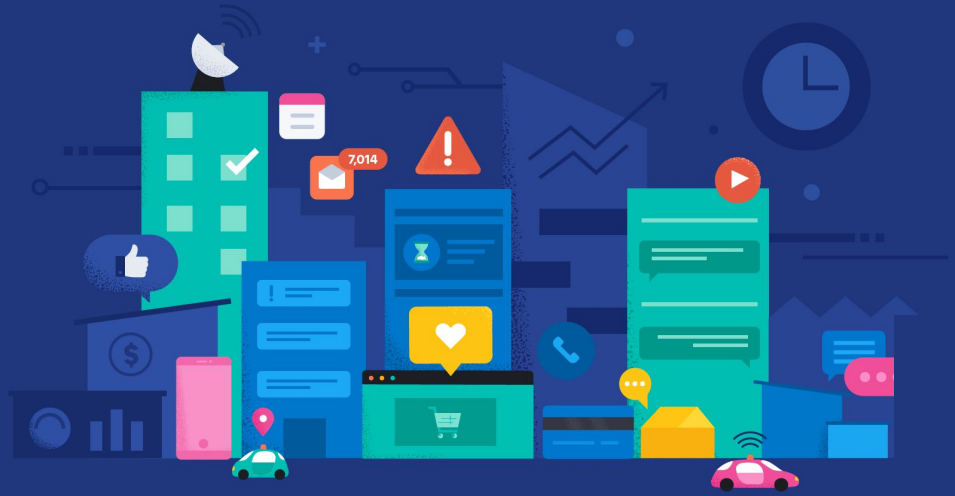


Ash Kulkarni
CEO

elastic

We live in a world of
exponential data growth & **increasing complexity**





Increasing User Expectations

Digital Transformation

Cloud Migration

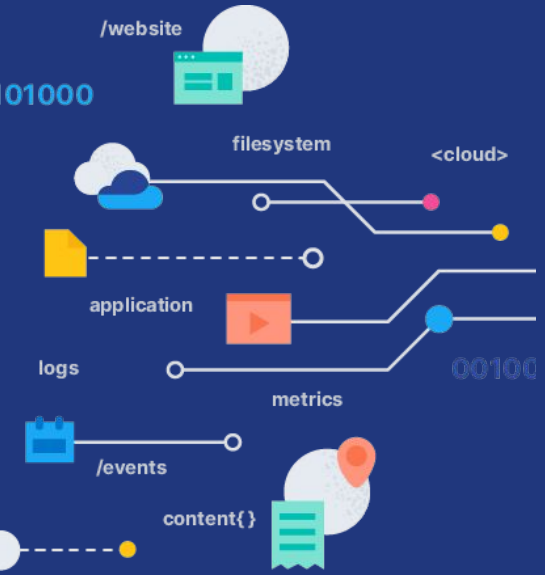
Unstructured Data

Semi-structured Data

Structured Data

6

Organizations need to



Visualize and Explore

Search and Analyze

Ingest Everything

Public cloud

Hybrid

On-premises



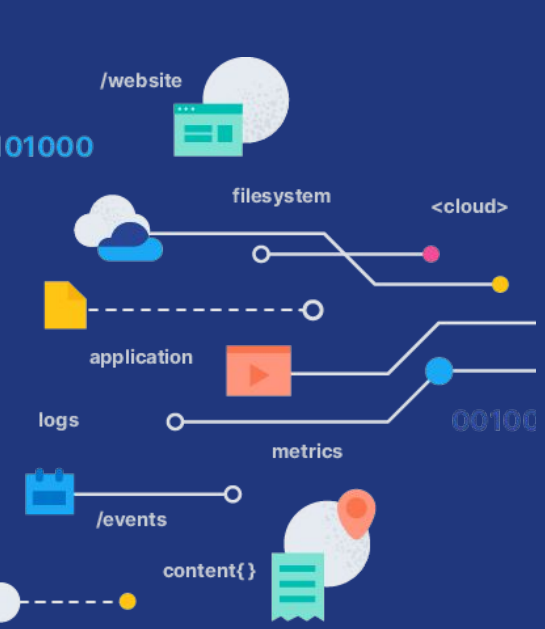
elastic

3 Search-Powered Solutions



elastic

Elastic Search Platform



Observability

Security

Enterprise Search

Kibana
Visualize and Explore

Elasticsearch
Search and Analyze

Integrations
Ingest Everything

Public cloud

Hybrid

On-premises



elastic

Key differentiators of the **Elastic Search Platform**



Powered by
search technology



Delivered in
one platform



Designed with
open architecture

elastic

Powered by **search technology**

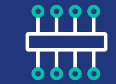
Speed	Real-time (milliseconds)
Scale	Petabyte scale
Relevance	ML, vector search
Insight	Analytics and visualization

elastic

Delivered in **one platform**



Simple getting started experience
across solutions



Unified end-to-end workflows
for all three solutions



Single resource-based pricing model
and consumption billing for all three solutions



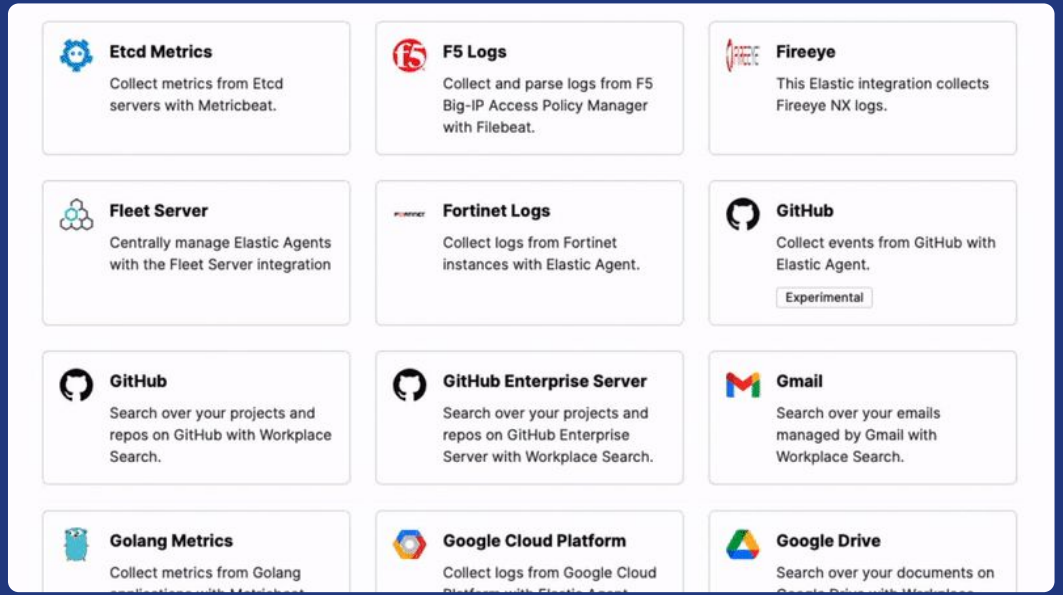
Effortlessly correlate and reuse data
across use cases and solutions in a single data store

elastic

Designed with an **open architecture**

- A robust community with 12 years of history
- 200+ pre-built connectors
- A rich ecosystem of partners

  (Hyperscalers, GSIs, MSSPs, Technology Partners)



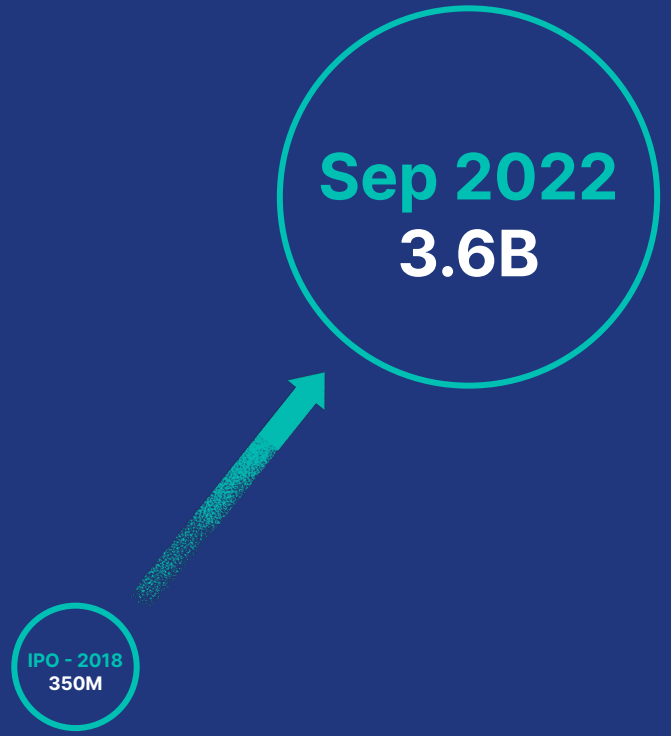
elastic

Built on a **ubiquitous foundation**

3.6B+ **Downloads**

103K+ GitHub Stars

183K+ Pull Requests



* GitHub stars, and PRs across Elasticsearch, Kibana, Logstash, and Beats

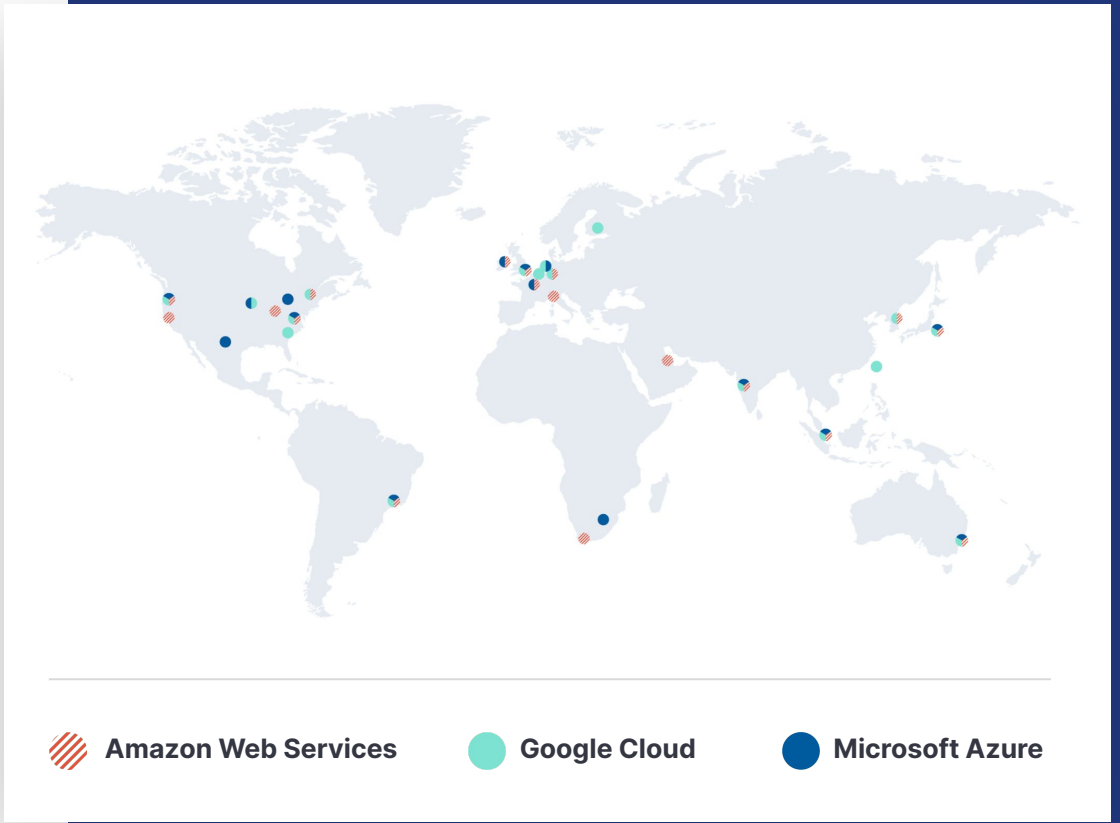
elastic

Available **wherever our customers are**

Public cloud | Hybrid | On-premises

53 regions globally

6B search requests per day



aws Google Cloud Microsoft Azure

Alibaba Cloud Tencent Cloud

15

WHY CUSTOMERS CHOOSE

Elastic Observability



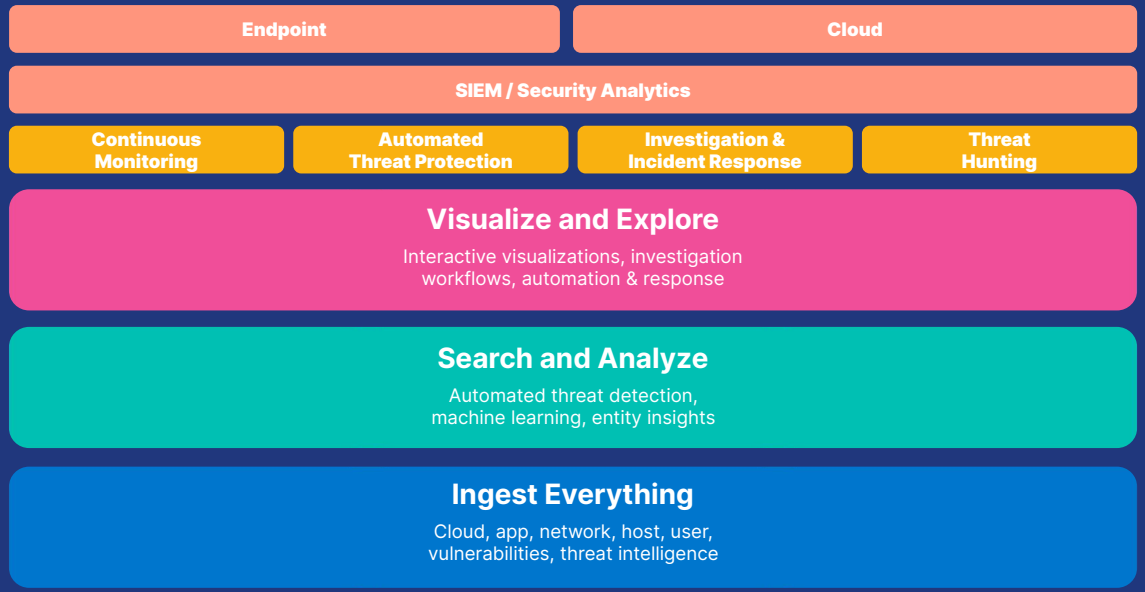
ZURICH

+ More than 40 on-prem and cloud applications to observe
+ Chose Elastic for the ability to analyze and explore terabytes of unstructured data in real time
+ Now they can find root-causes, and resolve any issue or outage in minutes instead of days

elastic

WHY CUSTOMERS CHOOSE

Elastic Security



orange™ Business Services

+ Over 1,000 pieces of internal network equipment and multiple security data silos

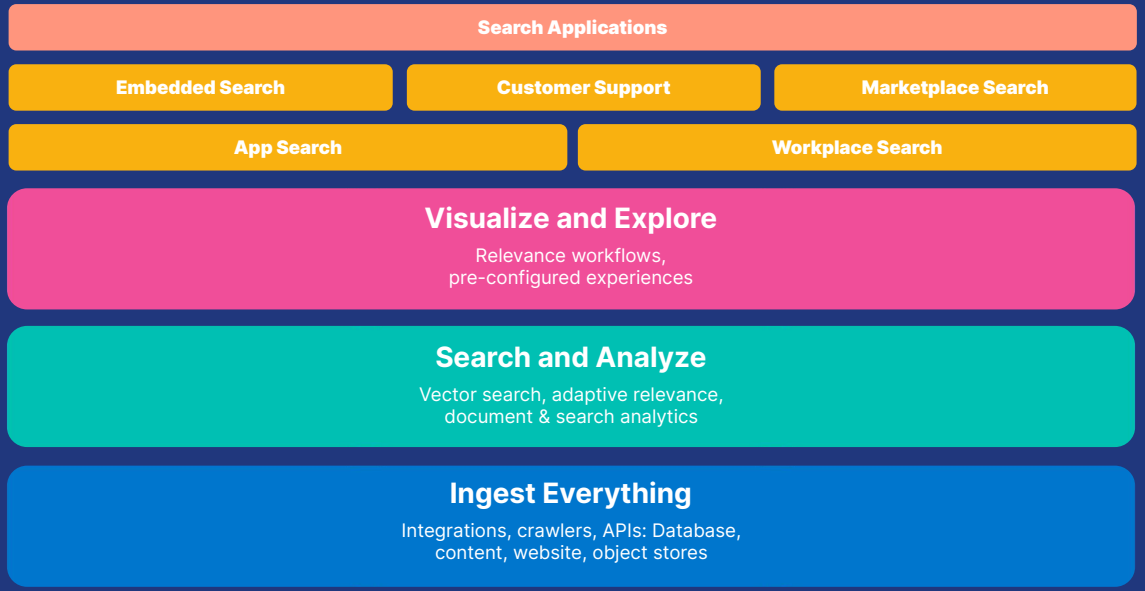
+ Chose Elastic for the ability to ingest all their security data, standardize it, and automatically detect threats

+ Now they can concentrate all their security workflows into a single solution - reducing MTTX

elastic

WHY CUSTOMERS CHOOSE

Elastic Enterprise Search

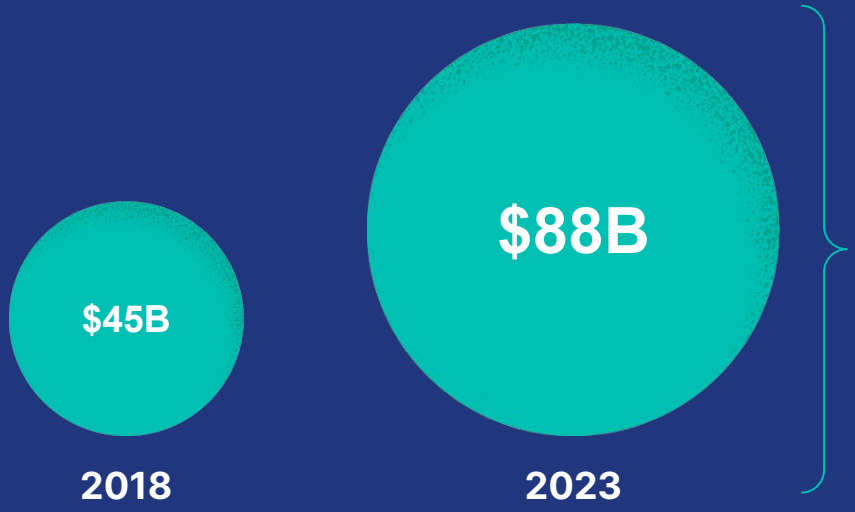


BMW

+ Customers worldwide searching across millions of unique permutations of car configurations
+ Chose Elastic for the ability to deliver a centralized, searchable repository, tailored to different sales channels, markets, and audiences
+ Now they can drive increased revenue across the globe

elastic

Our total addressable market





Significant expansion from organic growth & expanding into new markets

Source for 2023 TAM: IDC Semiannual Software Tracker - Final Historical 2021 | H2; IDC Semiannual Security Products Tracker - Final Historical 2021 | H2
Search consists of Intelligent Knowledge Discovery and portions of Digital Commerce, Customer Service Applications, Text & Audio AI, and others
Observability consists of IT Operations Management and portions of IT Automation and Configuration Management and others
Security consists of Modern Endpoint Security, SIEM, Server Security, and Tier-2 SOC Analytics / Cloud Native XDR
Elastic Platform consists of portions of Database management systems, End-User Query/Reporting/Analysis, and others

elastic

Elastic's growth vectors



As new customers adopt Elastic



As customer data volume grows



As customers adopt more use cases



As customers adopt more solutions

Almost 400 customers >$100K ACV with 2+ solutions



As customers adopt the cloud

39% of revenue via Cloud, Q1 FY23



As customers adopt higher subscription tiers

Enterprise tier is the fastest growing tier for Cloud customers

elastic

Go to Market Strategy

Bottom Up

Community

Cloud Marketplaces

Onboarding



Top Down

Instrumentation

Expansion

Customer Buying Journey

elastic

Elastic Security

1 **Land with:** SIEM

Elastic Observability

Land with: Log analytics 1



Our Go to Market Strategy: Land

1 **Land with:** Search applications

Elastic Enterprise Search

elastic

22

Our Go to Market Strategy: Expand within

Elastic Security

1

2

Expand within:
+ Endpoint
+ Cloud
+ XDR

Elastic Observability

1

2

Expand within:
+ APM
+ Infrastructure
+ Digital exp
(RUM + synth)



2

1

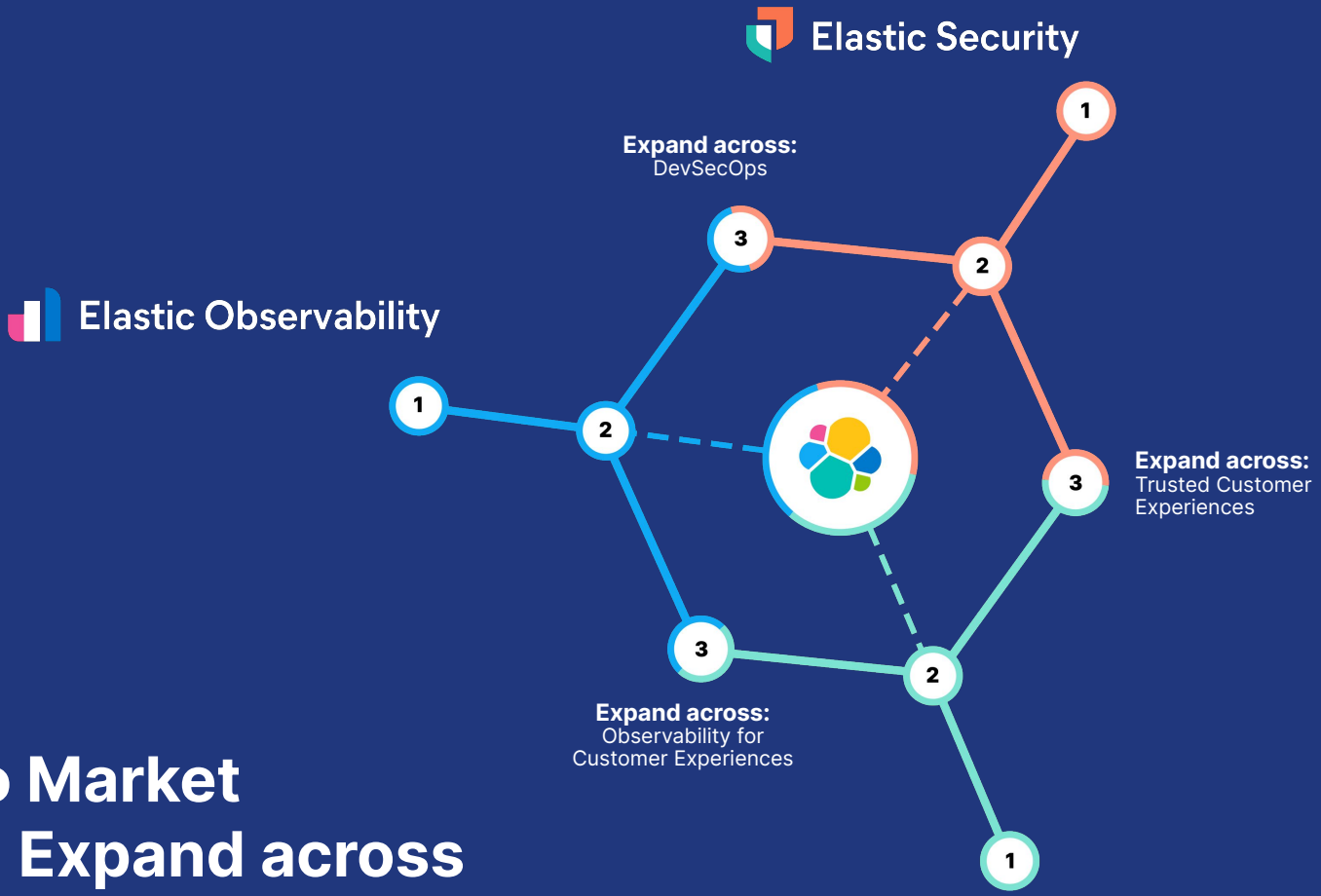
Expand within:
+ eCommerce
+ Workplace search
+ Customer support

Elastic Enterprise Search

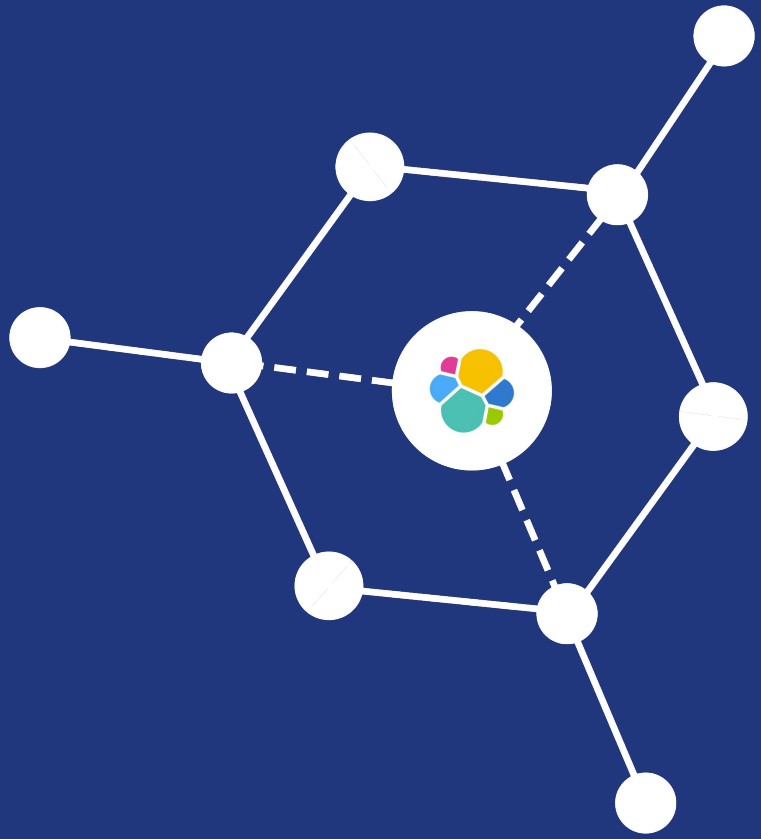
elastic

23

Our Go to Market Strategy: Expand across



24



Emirates NBD

elastic

25

Elastic Observability

1. Started with Log Analytics



Emirates NBD

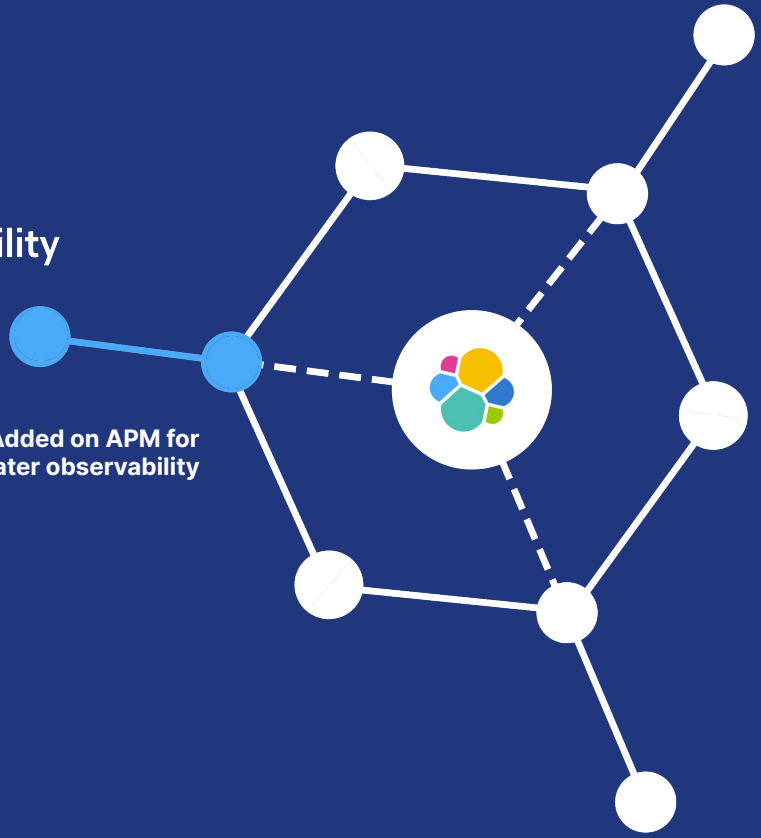
elastic

26

Elastic Observability

1. Started with Log Analytics

2. Added on APM for greater observability



Emirates NBD

elastic

27

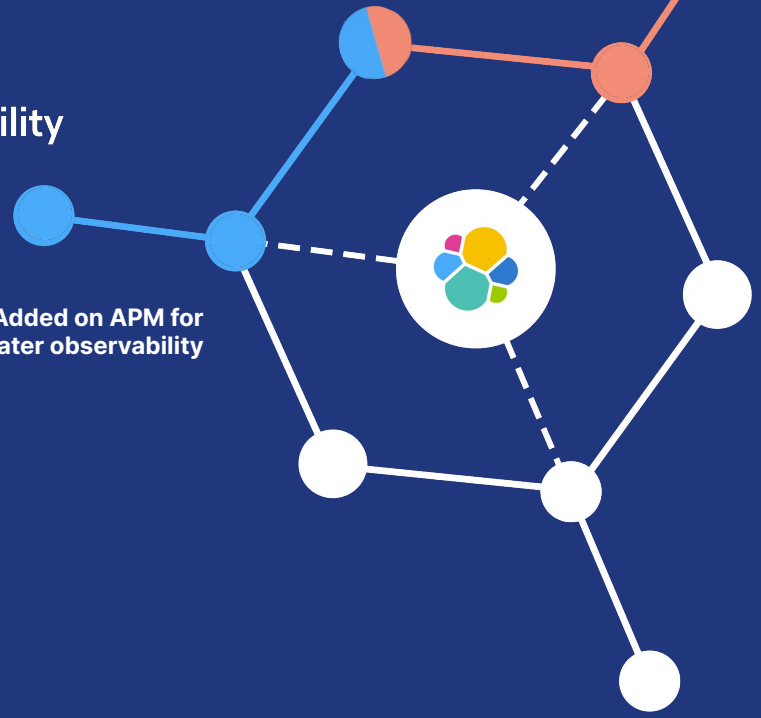
Elastic Security

3. Expanded to protect their entire digital ecosystem w/ SIEM

Elastic Observability

1. Started with Log Analytics

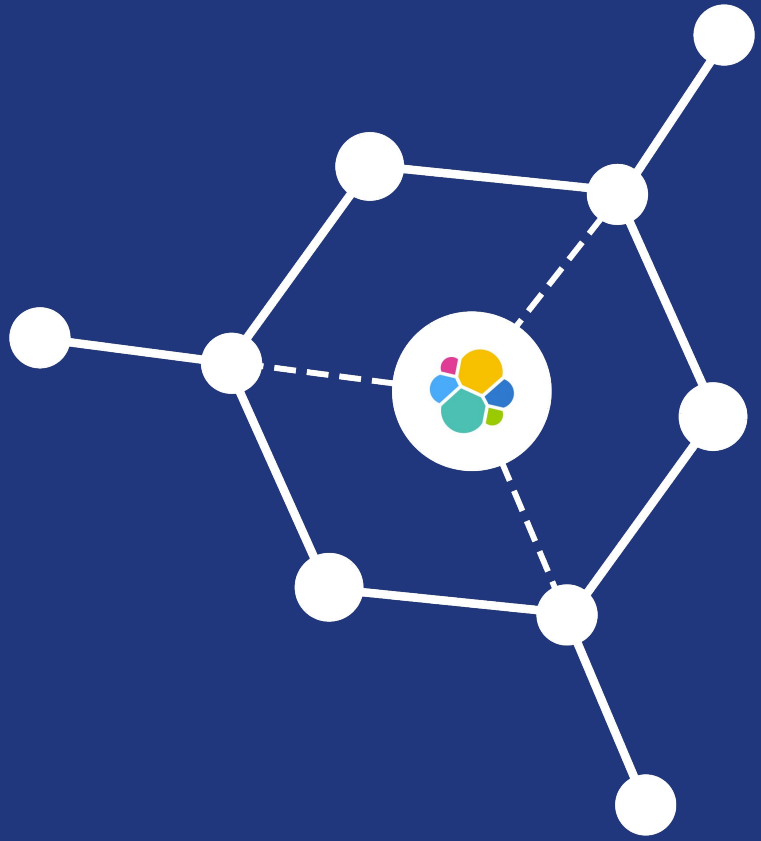
2. Added on APM for greater observability



Emirates NBD

elastic

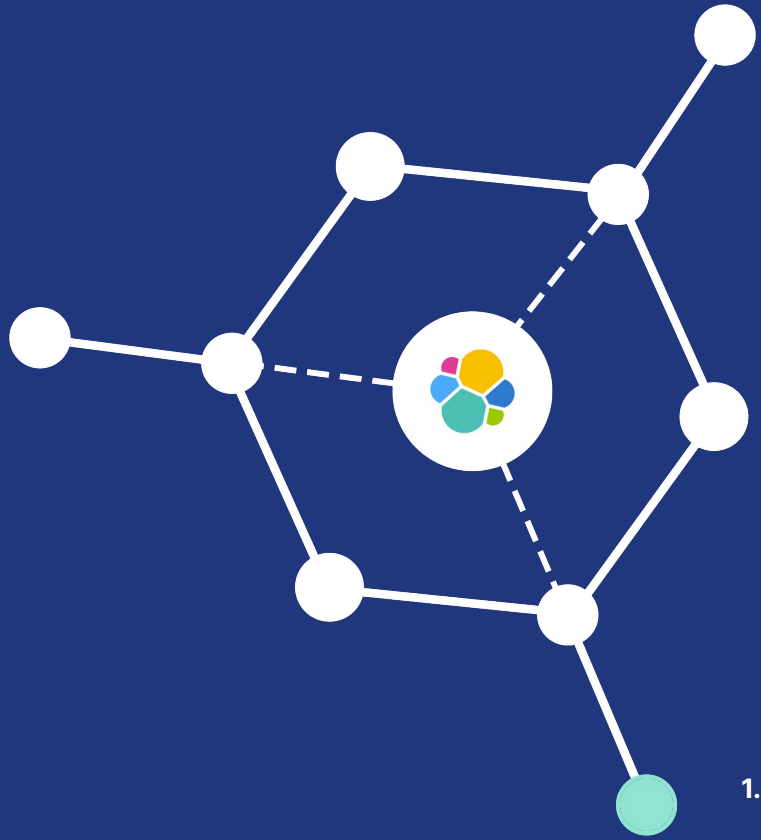
28



Booking.com

elastic

29



Booking.com

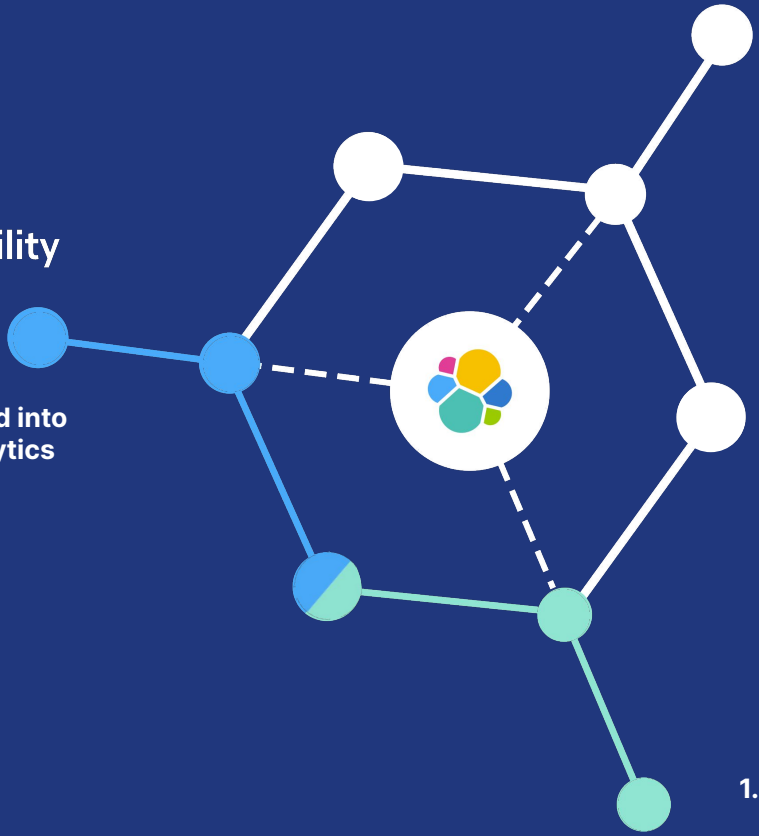
1. Start with search

Elastic Enterprise Search

elastic

30

Elastic Observability

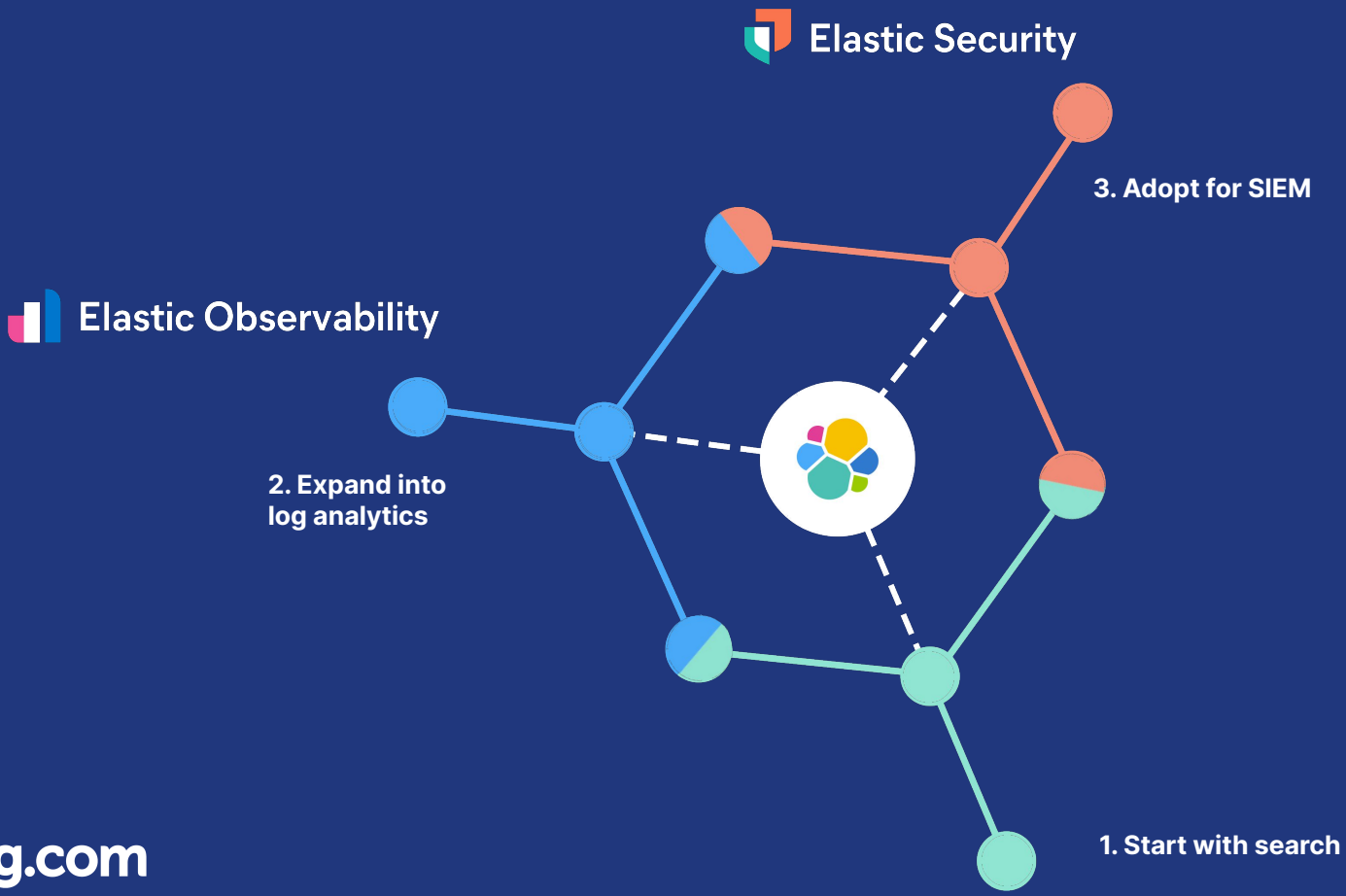


Booking.com

Elastic Enterprise Search

elastic

31



Booking.com

Elastic Enterprise Search

elastic

32

Building a generational company

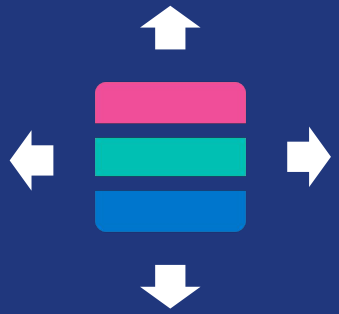


Durable growth

Cement leadership in log analytics, SIEM, and search applications

Support customer shift to Cloud

Expand into new solutions leveraging the platform



Competitive moat

The power of search across unstructured data

Leverage from building in one platform

Open architecture



Profitable growth

Efficient bottom up adoption

Frictionless marketplace adoption

Enterprise focus

Efficient R&D on one platform

elastic

Elastic Search Platform



Shay Banon

Co-Founder & Chief Technology Officer

elastic

Accelerating Elastic through the platform



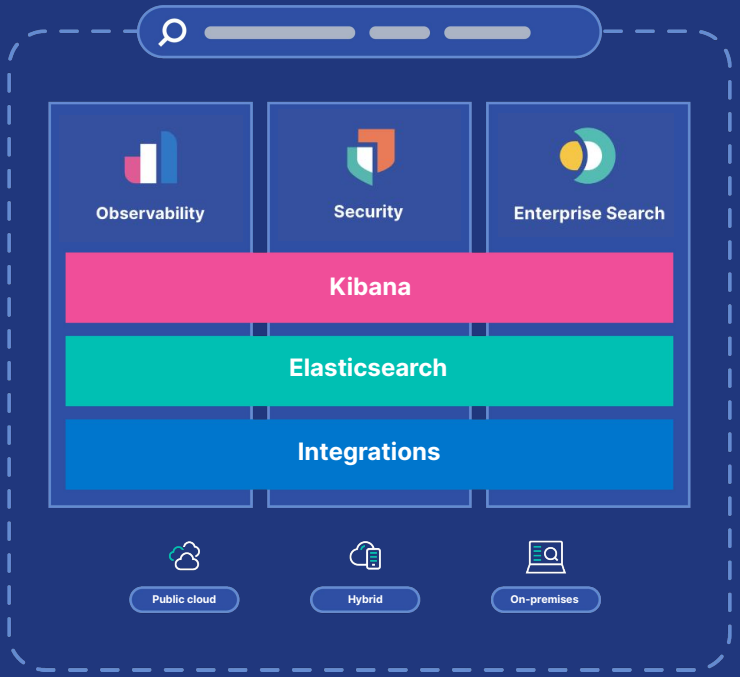
- Director to Vice President
- 20 years in Search & Analytics
- 8 years at Elastic

Steve Kearns
VP Platform Product Management

DataGravity BASIS TECHNOLOGY BBN TECHNOLOGIES EMD LEXIGEN

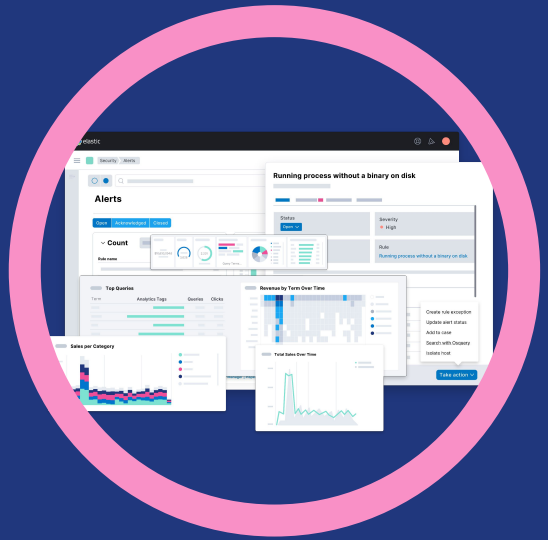
elastic

One data analytics platform for search-powered solutions

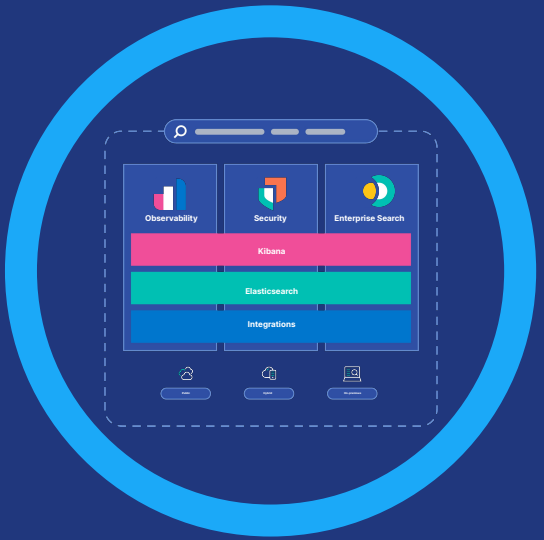


elastic

One platform to buy, maintain, and manage







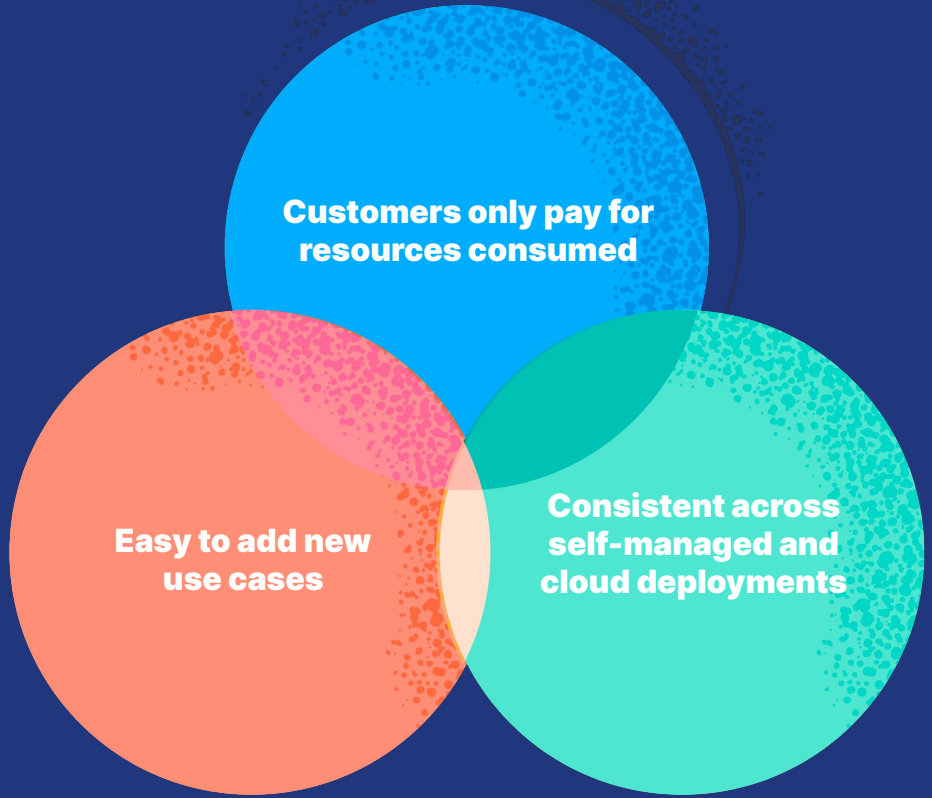
No edge of the map

Tool consolidation

Operational efficiencies

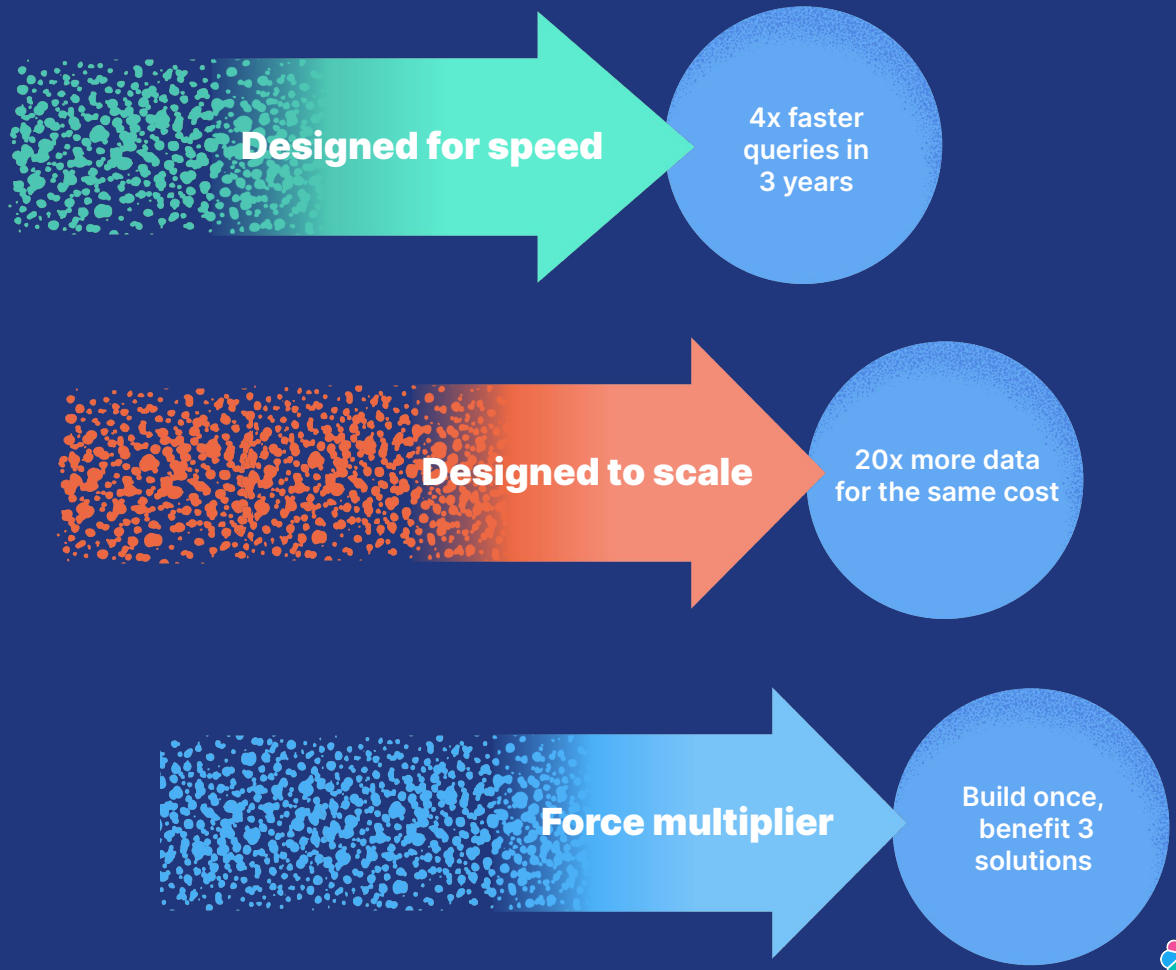
elastic

Pricing model encourages expansion



elastic

Drive Efficiency

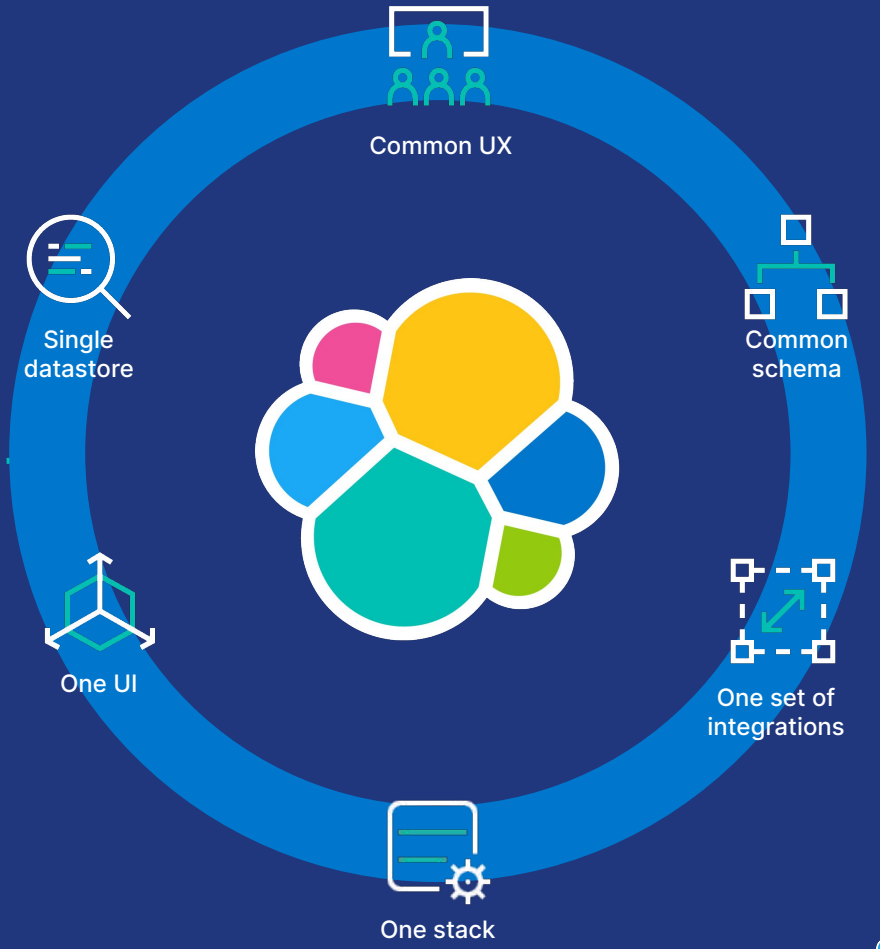


elastic

Drive Consistency

Elastic

Customers

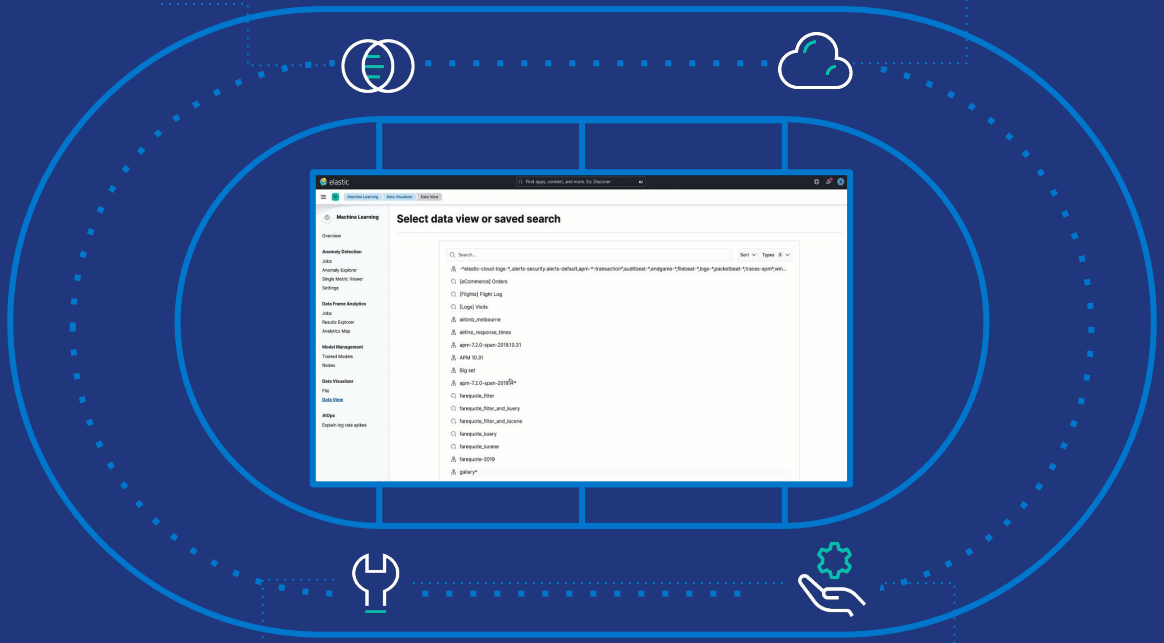


elastic

Innovate Faster

Features developed once

Simplified in Elastic Cloud



Accelerated solution development

Easy to develop new use cases

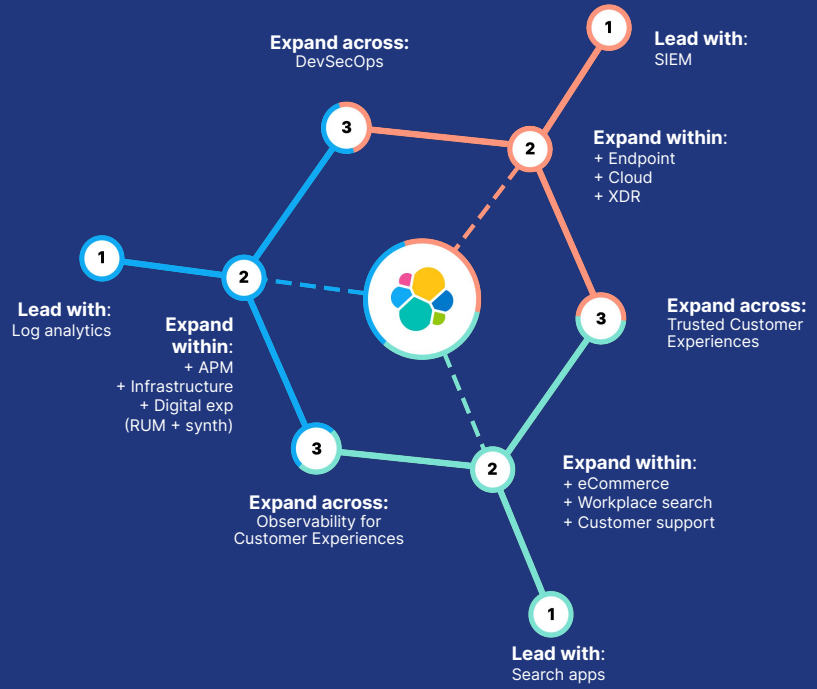
elastic

Enabling Elastic Solutions to Grow Faster

Adding a use case is as simple as adding another data source

Shorter sales cycle, faster expansion

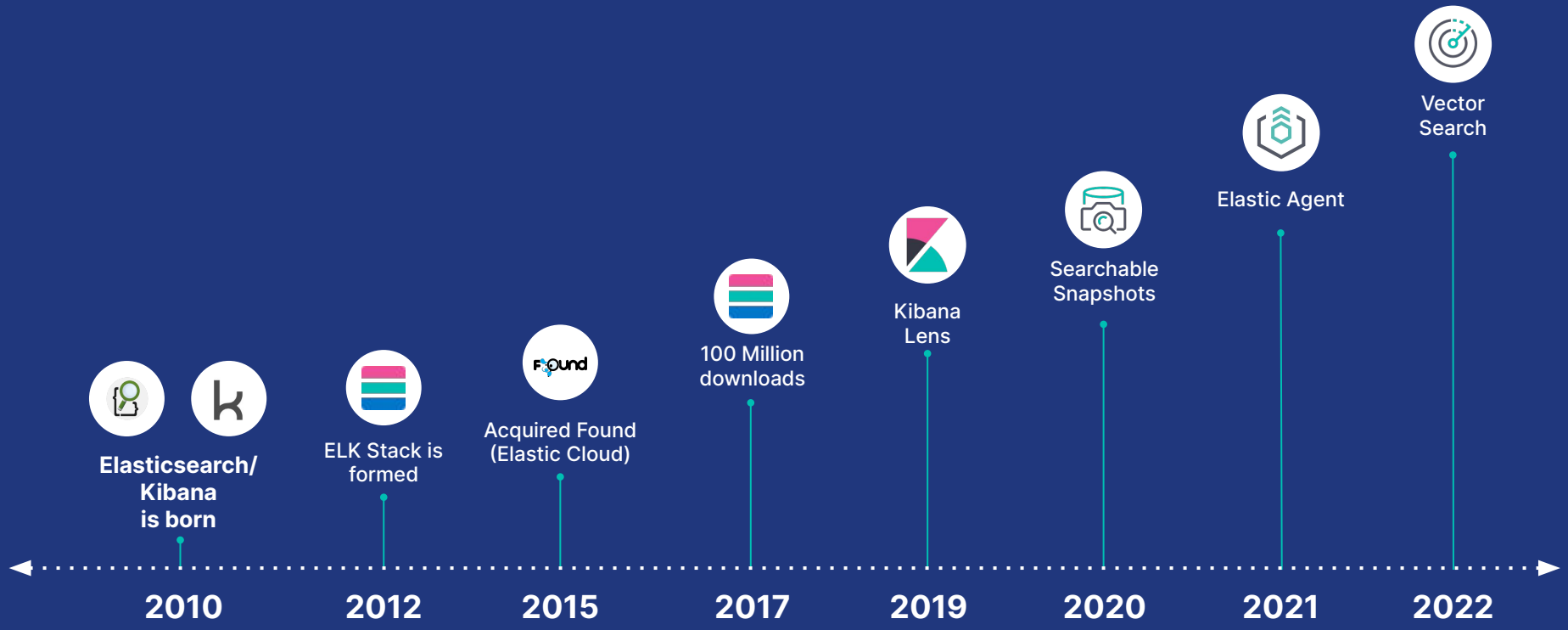
Stickiness



elastic

42

Continuous Innovations in the platform



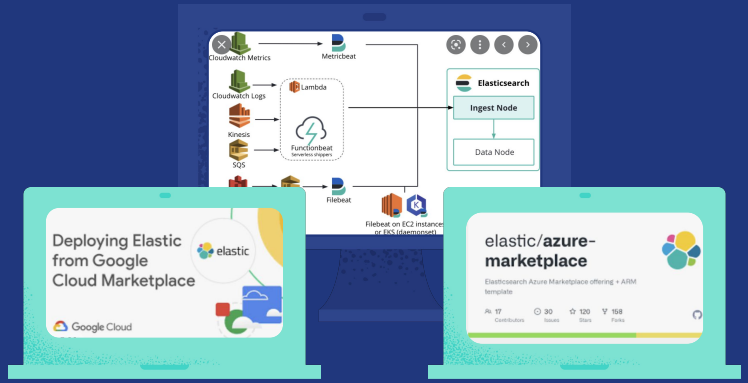
elastic

43

Cloud first, hybrid ready

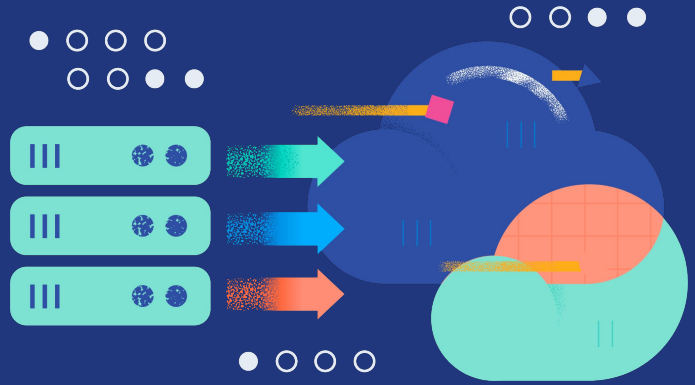
3 clicks to deployment

User experience targeted to specific ecosystem



Easy to adopt Elastic Cloud

Search across on-prem & Elastic Cloud



elastic

44

Doubling down on time series metrics



> 70% Storage efficiency for time series metrics

Protection from security threats, deeper insights

Combining structured metrics with unstructured logs and traces

elastic

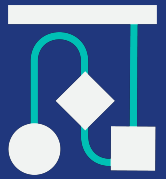
Enabling more powerful data analytics



Powerful queries that even novice analysts can write



Faster analysis of complex security & observability issues



New query execution engine enables joins & transforms

elastic

Leaning into Cloud for even more scale and speed, and reduced TCO



Searchable Snapshots
Decouple storage and compute to lower TCO



Evolved Searchable Snapshots
Decouple services like search and index from storage for flexibility



Elasticsearch On-Demand
Independently scale each service for increased speed and cost efficiency



Stateless Elasticsearch:
Lower TCO with flexibility

elastic

Summary



elastic

Elastic Observability



Sajai Krishnan
General Manager, Observability

- **5 months at Elastic**
- **GM Wavefront Observability at VMware**
- **17 years GM/CEO**
- **Partner Booz Allen & Hamilton**

vmware aws NetApp Booz | Allen | Hamilton

elastic

Cloud, containers, microservices, mobile are creating exploding system dynamism and complexity, requiring new approaches to observability



Doubling developer productivity





Elastic unified observability monitors 400 services

- Easily correlate app and infra performance across AWS services (Kinesis, Lambda, ECS, Fargate etc.)
- Accolade owns the data
- Track business impact (e.g. patient wait time)

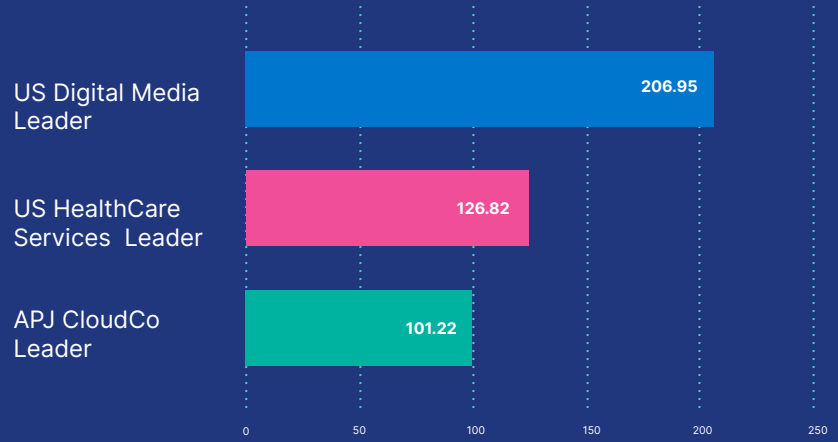


”With Elastic, we are now able to cross-compare data, like logs or metrics with application traces. This was previously impossible when the data was isolated in different platforms. It's transforming our organization and making the lives of our developers so much easier.”

Positive Elastic APM Momentum

- **31% of all observability clusters in Elastic Cloud now have APM**
- A US mutual fund co. is **monitoring over 1800 services** with Elastic APM
- A leading US healthcare services provider only has at-scale APM (no logs); looking to consolidate logs
- A large cable co. had logs, then just "11 mins to add Java tracing for a production application"

Top 3 APM customers with 100 - 200 TBs of APM data



ML is set to trigger notifications when there are unusual spikes or ebbs in customer transactions. *Before adopting Elastic observability across 100s of applications "we might not have known until the end of a day that there was a problem with the ATM machine."*

– Ali Rey, Vice President of Cloud and Data Platforms, Emirates NBD

Observability is business critical …even in uncertain times

Observability is essential

Increasing cloud & container adoption

- Increasing Scale, Dynamism

Increasing customer interest

"Tool-zoo" consolidation + cloud transformation initiative

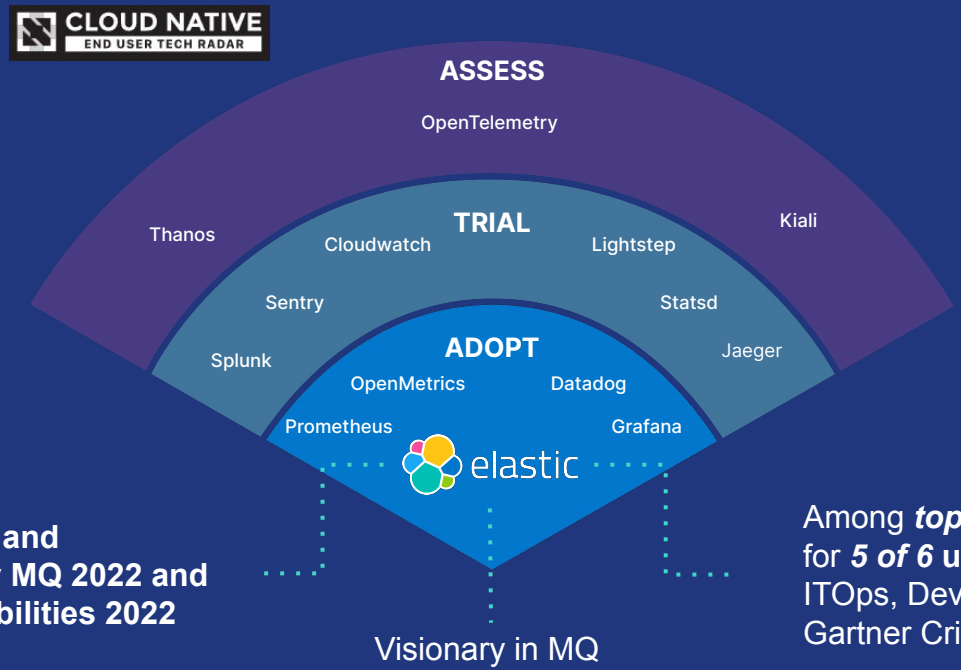
Ongoing customer conversation on consolidation, across various verticals:

- Mobile, Telco, Cable
- Finance, healthcare
- Gaming, SaaS

53

Elastic : Broad adoption/familiarity, at scale

3.6B+ downloads of ELK; a widely adopted solution for modernization



Gartner APM and Observability MQ 2022 and Critical Capabilities 2022

Visionary in MQ

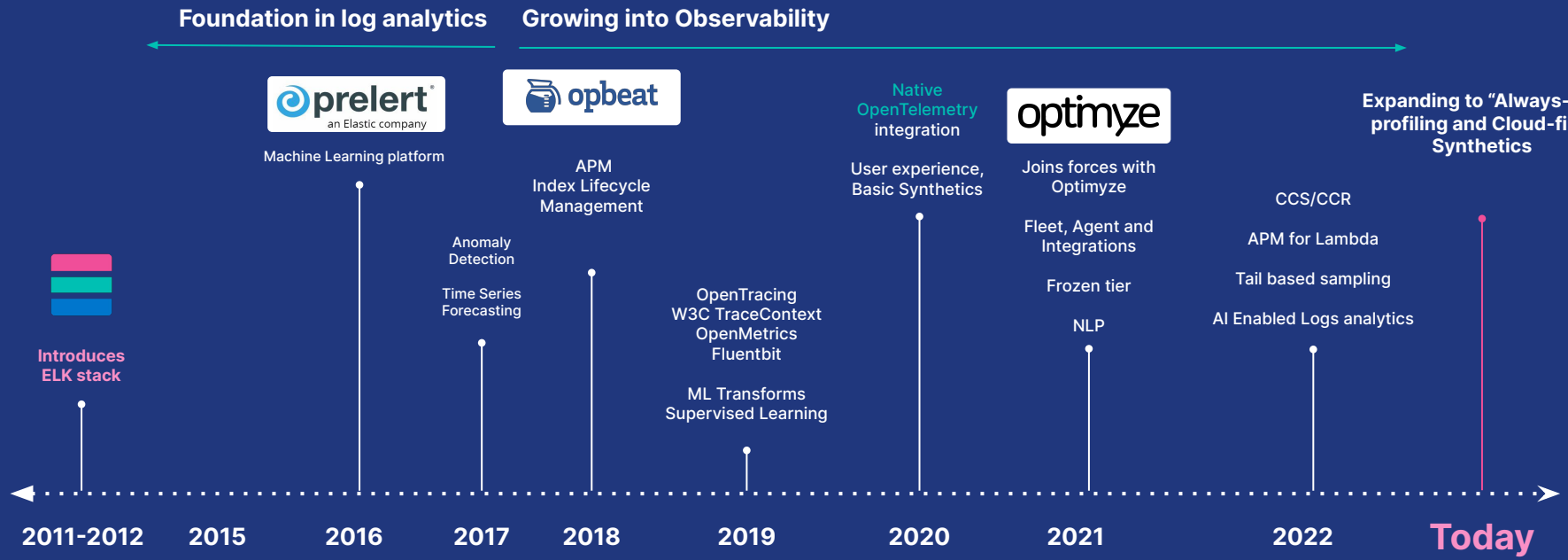
Among ***top 3 vendors***, for ***5 of 6*** **use-cases** across ITOps, DevOps and SecOps in Gartner Critical Capabilities 2022

CNCF End-user Analysis https://radar.cncf.io/

54

100% integrated observability

Full-stack, open and extensible

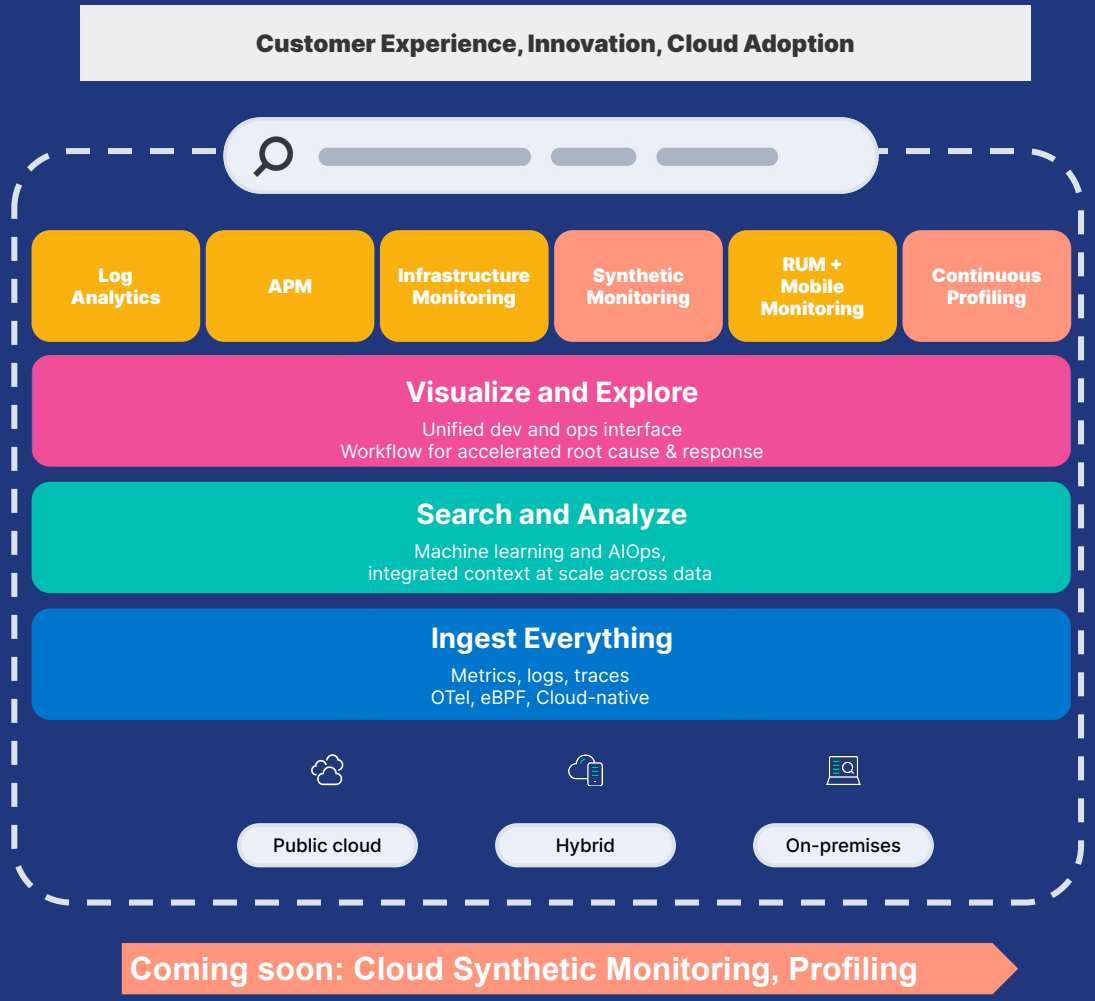


elastic

55

Full-stack, multi-cloud, comprehensive, performant, economical, intelligent

Elastic Observability

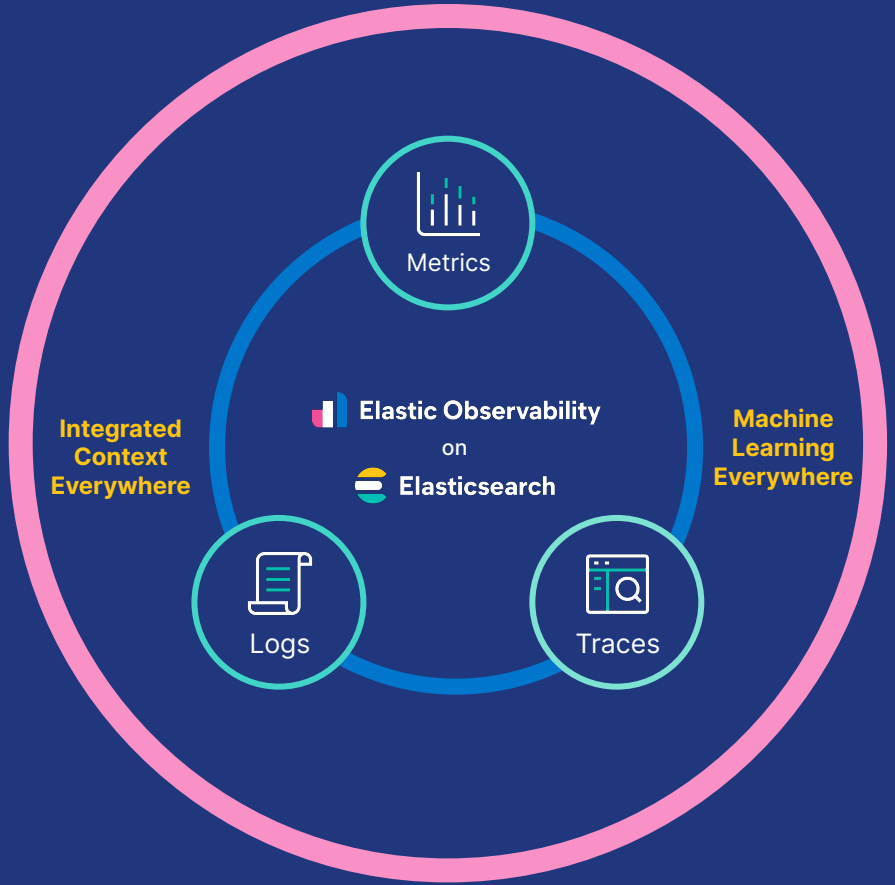


Elastic advantage - One platform, single store

High cardinality, dimensionality data at scale

(keep **ALL** your data)

- **Unlimited Logging**
  no rehydration required, always indexed
- **Unlimited Tracing**
  no time limitations, no default sampling
- **Unlimited Metrics**
  no time limitations



Powerful ML & Analytics

- Anomaly detection across all telemetry
- Out-of-the box & customizable ML
- Sophisticated supervised and unsupervised ML models
- Ad-hoc analytics - understand “unknown unknowns”

elastic

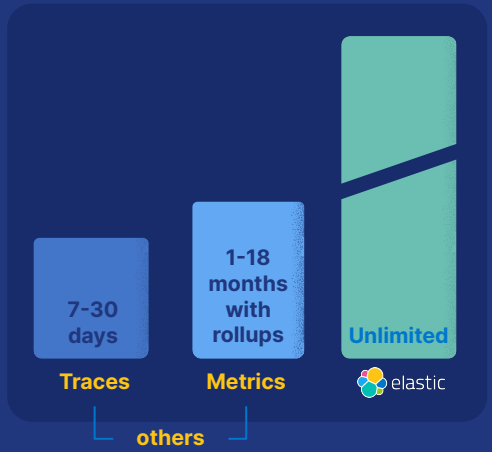
57

Elastic log analytics : A solid foundation for building upon

Enterprise logs are ubiquitous, have a large footprint, and are difficult to replace



Elastic's least expensive tier, beats other **log** vendors' top tier performance handily



Metrics vendors reflect architectural constraints for integrated multi-signal observability



APM vendors have multiple challenges:

- Reluctant adoptees of OpenTelemetry / open standards
- ~15%* penetration covering customer's mission-critical applications
- PB-scale observability requiring new back-ends

**APM penetration, based on company estimates*

elastic 58

Why we win

OBSERVABILITY CAPABILITIES



Industry **leader for log analytics** - scale, performance, TCO



Integrated observability: Full-stack, multi+hybrid cloud



Open: **Best-in-class OpenTelemetry** support

PLATFORM CAPABILITIES



ML "everywhere" - actionable insights across use-cases



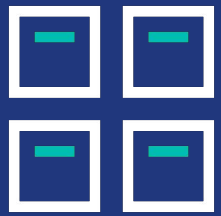
Deploy and adopt all capabilities at scale with seamless **consumption billing**



Enduring economics: tiered storage, on-prem + cloud, cross-cluster search, observability + security

59

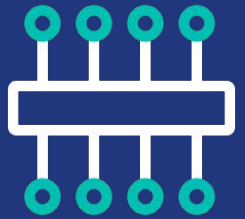
FY23 Elastic Observability investments



"Always on, continuous profiling"
Profile everything, all the time, zero instrumentation, 1% overhead



Cloud Synthetic Monitoring
Cloud- and developer-first synthetic monitoring



Differentiated AIops leveraging single integrated store & unified observability, underlying ML

Cloud Synthetic Monitoring Beta

- **270+** beta customers
- **17% of 8.3+** observability clusters

60



Demo

elastic

61

acmefinancial

Search for tickers, documents, news, learning resources, support, and more

Cassandra B.

My assets

View portfolio →

Sept 19th 2022 2:45 EST

$250,901.22 ▲ 4.1%

$10,521.42



Markets & holdings

Filter

Holdings | Recommended based on your holdings

SHOP	Shopify	$42.45	+23.4%
SQ	Square	$66.38	-8.9%
SNAP	Snap Inc.	$11.30	+1.5%
AAPL	Apple	$155.65	-4.5%
TWTR	Twitter	$38.60	+8.9%
TSLA	Tesla	$269.32	-12.2%

6 of 22 See all →

AcmeInsight℠ market intelligence

Bringing the information relevant to you, from around the globe, in real-time

Because you invest heavily **in social commerce companies**

Updated 45 seconds ago



Published September 19, 2022
Online commerce has seen its biggest year yet and shows no sign of slowing down, according to Retailers United



Published July 22, 2022
Micro-financing startup Klo is getting ready for monster hit on Wall Street

Because you recently searched **for pharmaceutical stocks**

Updated 3 minutes ago



Published September 12, 2022
DrugInc's recent legal woes represent a unique opportunity for long position, according to F.H.W. Smith



Published August 5, 2022
With COVID-19 out of the re are vaccines manufacturer for growth?

Trending for individuals with a similar investment profile

Updated 6 hours ago



Published September 2, 2022
Growth stocks are in technical oversell territory. What does that mean for the average investor?



Published September 19, 2022
16 strategies for diversifying declining portfolio without skipping on the upside

My order history

Last month | YTD | Custom | Filter orders

	ASSET	DATE	STATUS	VOLUME	UNIT PRICE	PROCEEDS	GAINS
	SHOP:NYSE	9/19/2022	In progress	1,000	USD42.90	USD4,290.00	USD3,440.12
✓	SHOP:NYSE	9/18/2022	Executed	2,000	USD41.40	USD8,280.00	(USD425.45)
●	SHOP:NYSE	9/16/2022	On hold	1,000	USD38.10	-	-
✓	DIS:NYSE	9/10/2022	Executed	2,000	USD128.90	USD257,800.00	USD38,440.12
✗	DIS:NYSE	9/10/2022	Cancelled	200	USD120.45	-	-
✗	DIS:NYSE	9/10/2022	Cancelled	150	USD112.23	-	-
✗	DIS:NYSE	9/10/2022	Cancelled	10	USD109.67	-	-
✓	SQ:NYSE	9/07/2022	Executed	2,000	USD41.40	USD8,280.00	(USD425.45)
✓	SQ:NYSE	9/05/2022	Executed	1,000	USD42.90	USD4,290.00	USD3,440.12
✓	SQ:NYSE	9/01/2022	Executed	1,000	USD42.90	USD4,290.00	USD3,440.12

10 of 25,234 See all →

Recommended reads from Acme's Investment Education Center

Based on your activity and portfolio



Options trading and covered calls with Acme℠ →

Because you recently searched for covered calls



Strategic portfolio rebalancing for retirement →

Because your portfolio distribution skews heavily towards short-term gains



Working with an Acme℠ Wealth Assitant →

Because your order history suggests we can support your needs

SPX500	DJ30	NSDQ100	EURUSD	USDJPY	VIX	RUT	XOI	CADUSD	MXNUSD
4781.38	25780.01	11628.70	1.0426⁶	135.22⁹	25.47	1809.23	1642.98	1.2326⁶	0.05002⁹
+0.66%	+0.31%	+1.06%	-0.54%	-0.31%	+11.46%	+0.31%	+1.06%	-0.54%	-0.31%

Need Help

Ask your question

elastic

62

Elastic Observability



Onboard

Getting business and operational data into Elastic Observability

Insights

Automatically get more out of your observability data and take actions

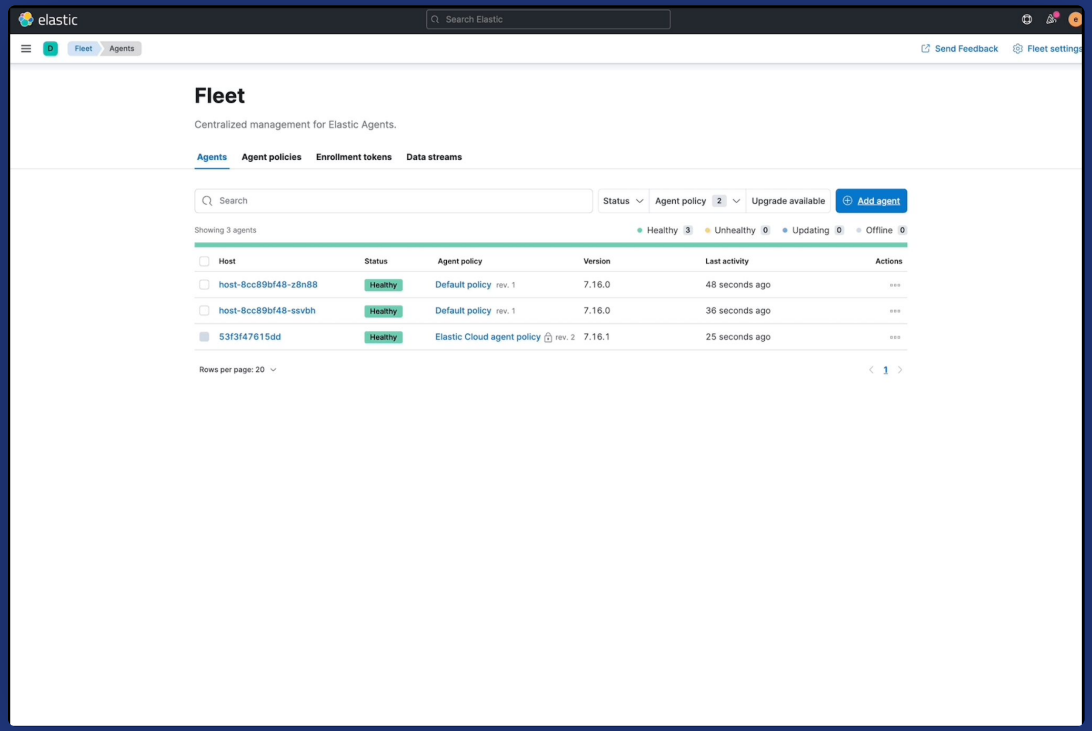
Grow and Expand

Expand Observability as the business scales

elastic

63

Elastic Observability data onboarding



Single unified Agent for telemetry, forwarding data and protection

Centrally managed

Standardized with **Open Telemetry**

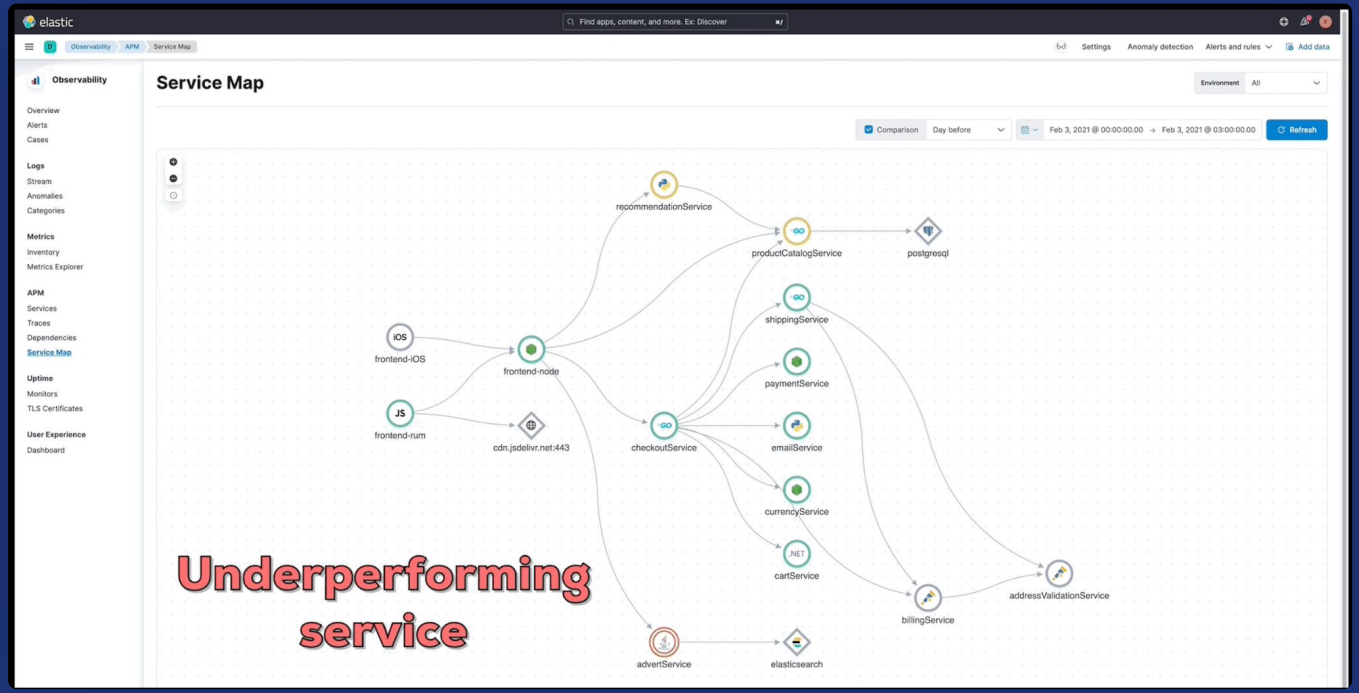
200+ ready-built integrations

Enabled with **a single click**

elastic

64

Elastic Observability guided root cause analysis



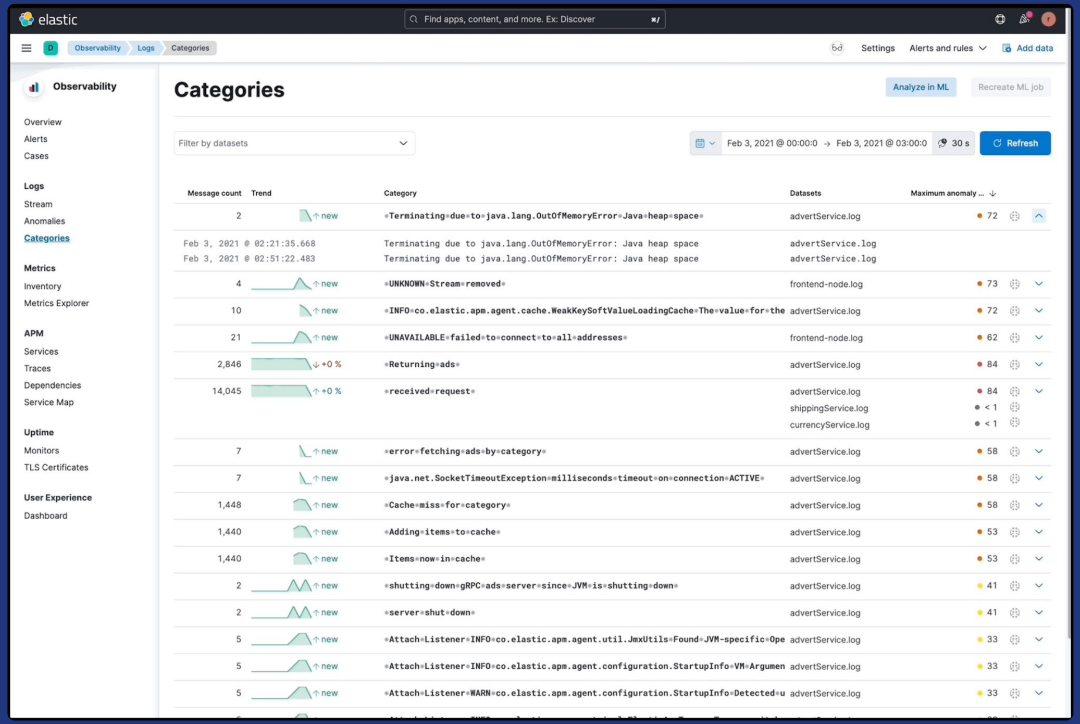
Correlate Traces, Logs, Metrics **for better resolution**

Machine learning as a core driver of the root case analysis workflow

elastic

65

Logs: Unstructured at scale, with speed



Collect **unstructured** and structured logs

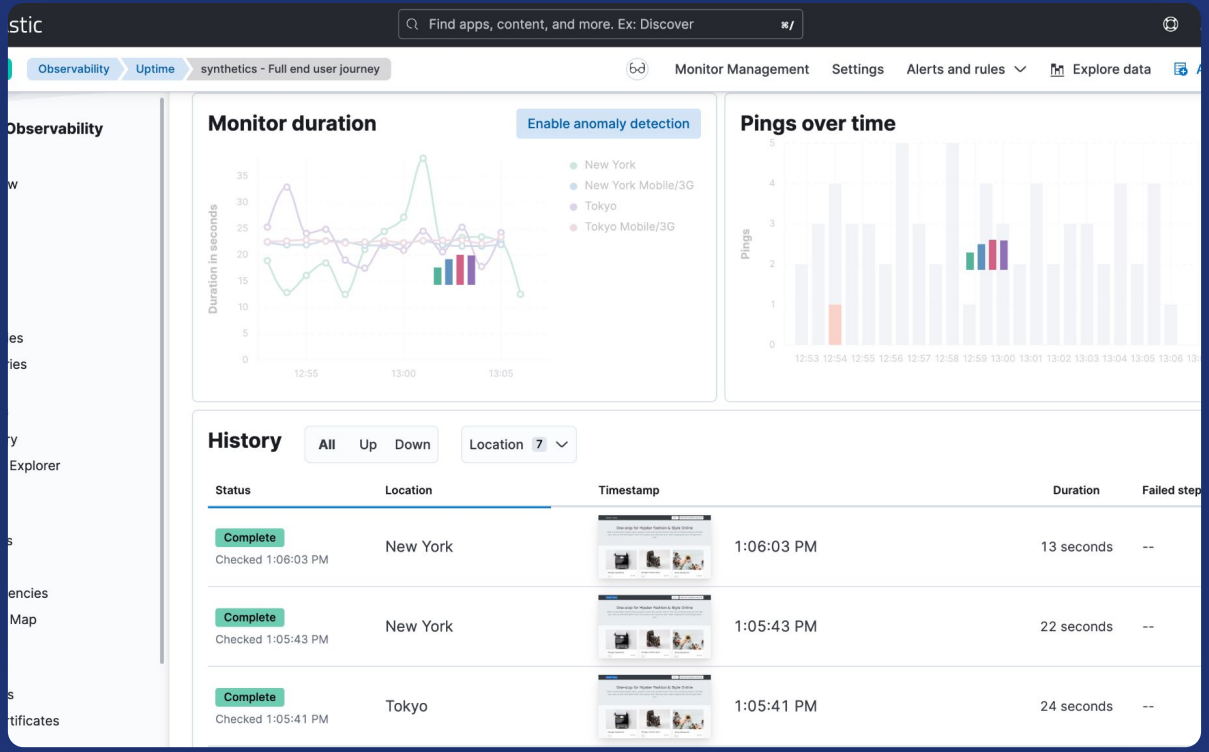
Stream, categorize, analyze logs

Reduce investigation time with a single pane of glass

elastic

66

Unified Observability from the user to the kernel



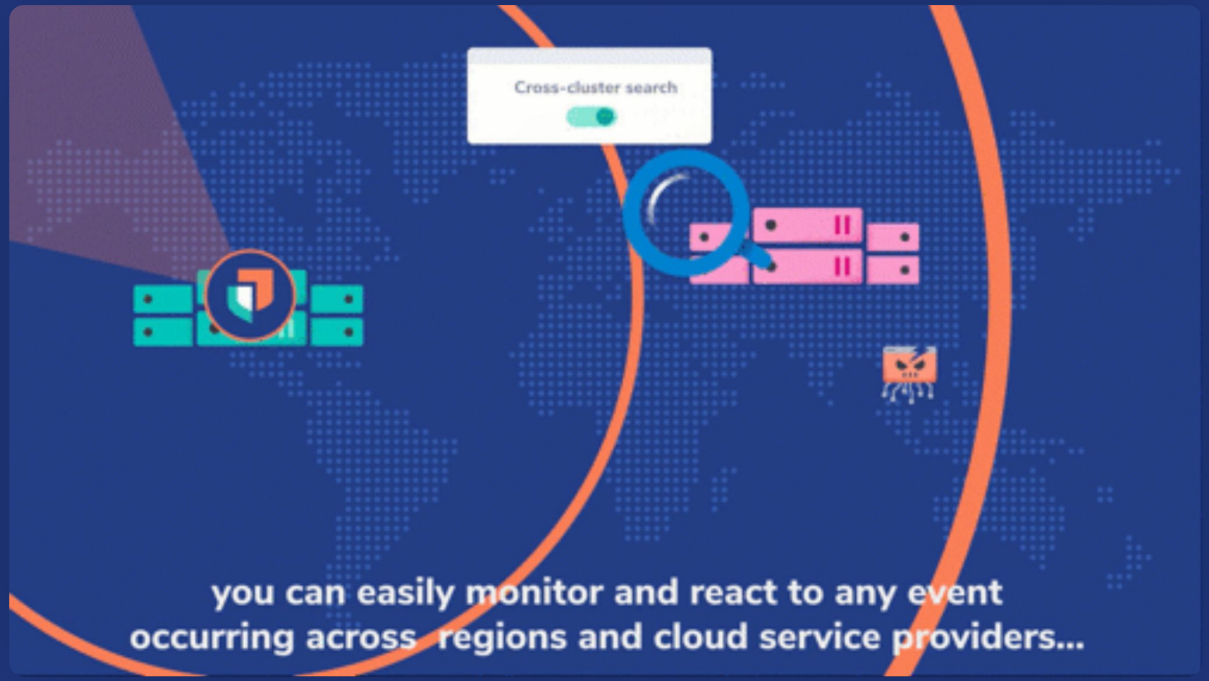
Availability monitoring,
from the highest
to the lowest level of the
stack

User experience analysis
with Synthetic Monitoring

elastic

67

Federated observability - Deploy anywhere, observe everything



Across **Elastic Cloud, private cloud, and on-premises -** in any combination

Decentralized observability, with **first pane** experience

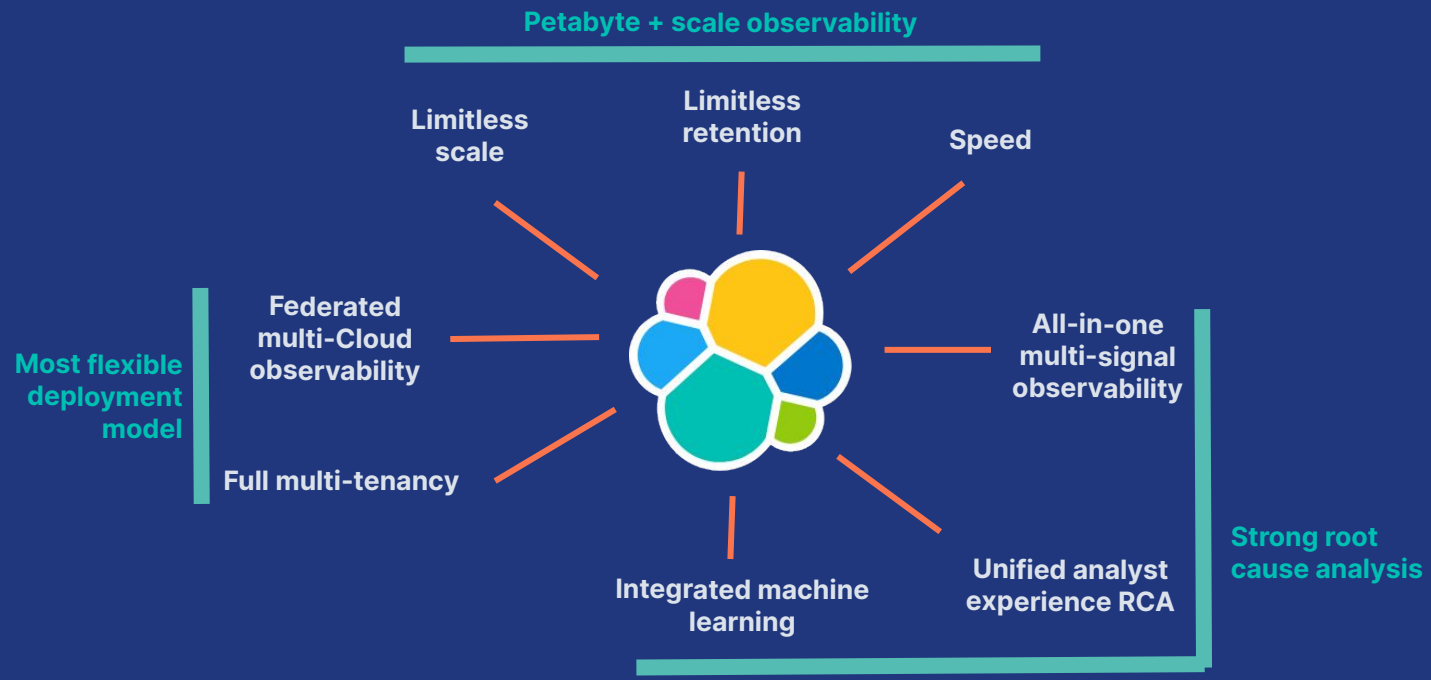
Replication at every level, data loss prevention

elastic

68

Unique dimensions of Elastic Observability

Keeping total cost of ownership under control



elastic

69

Elastic Security



Santosh Krishnan
General Manager, Security

- CEO of Cmd prior to acquisition
- 20+ years of product leadership
- 7+ years in Cybersecurity
- 1 year at Elastic

>_cmd lookout Akamai Lucent Technologies Bell Labs Innovations

elastic

Beneath the surface,
modern security challenges
are all connected to data



Expand security data visibility & coverage

with Elastic Security

- Increased security related log collection from **500 GB** per month to over **10 TB** per month
- Reduced response times for security incidents by **30%**

“Protecting OLX mission-critical data with Elastic Security gives us and our customers the confidence that we can enhance and expand our network of local trading platforms in a secure environment.”

-OLX Security Team

elastic aws

Vision: Modernize security operations with the power of data



Expand visibility into threat surface



Detect and prevent threats in real time



Reduce time to response and protection

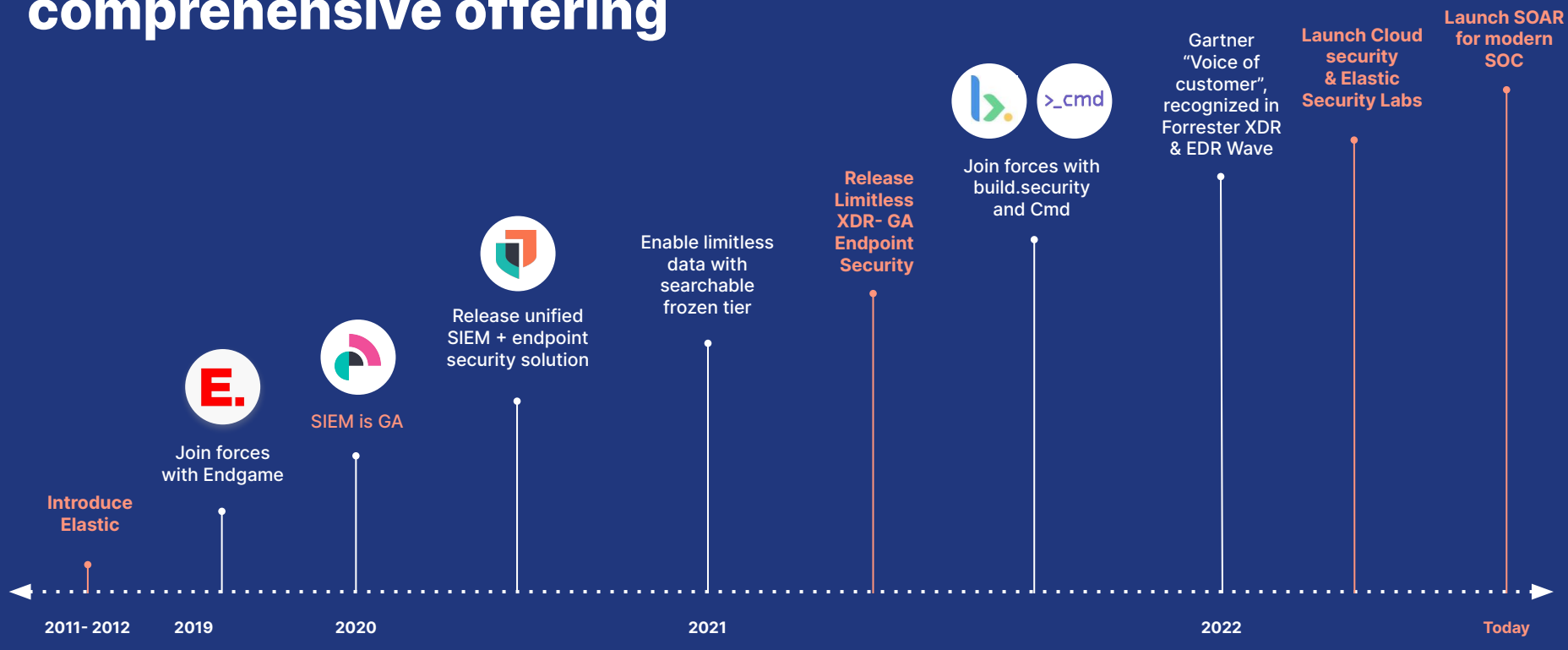


Integrate security tooling into a consolidated offering



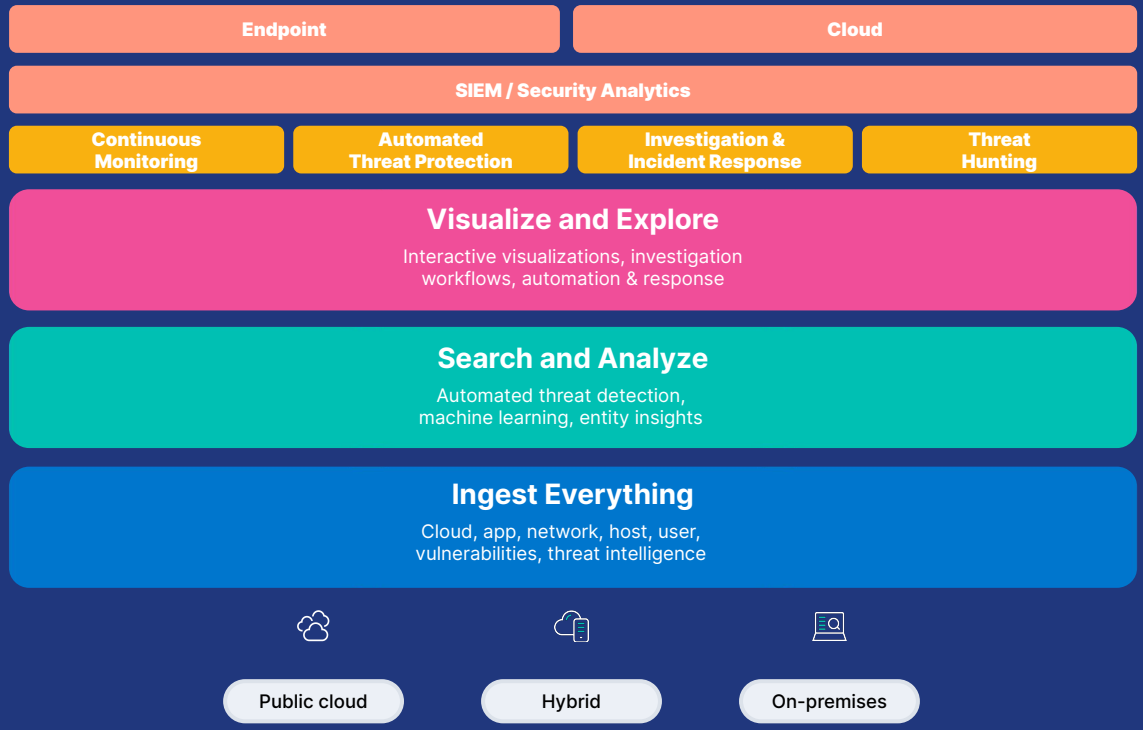
Ready for hybrid and multi-cloud environments

From analytics to a comprehensive offering



74

Elastic Security



elastic

75

Market Tailwinds and Where We Win



Replace legacy **SIEM** with an analytics-based next-generation product



Future-proof EDR with **eXtended Detection and Response (XDR)**



Consolidate fragmented tools with unified **cloud security**

Bell

OAK RIDGE National Laboratory

Emirates NBD

orange™

citadel group
TECHNOLOGY + EDUCATION

elastic

76

Elastic Security
by the numbers

69%

Decreases impact of threats by 69%, with 90% customer satisfaction
(Annual Value Study)

10x

Over 10x faster at lower cost
(Forrester TEI)

25%

~25% of ACV in FY22

#5

Top 5 in market share, top 3 in growth
(IDC Worldwide SIEM Market Shares, 2021)

77

Why we win

SECURITY CAPABILITIES



Open & integrated

Consolidated use cases, rich integrations



Native protections

OOTB detections powered by ML models and threat research



Automated insights

Insights driven investigate workflows and incident response

PLATFORM CAPABILITIES



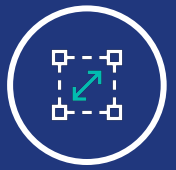
One platform

Security and Observability, hybrid and multi-cloud



Data management

Efficient storage, high-speed search and analytics



Start small, scale up

Flexible licensing model

78

FY23 Elastic Security investments

Response actions

- Remediation center
- File and process operations
- Integrated and native SOAR

CWP & CSPM

- CWP for cloud-native workloads, containers, and hosted Kubernetes
- CSPM across native and hosted K8s

Endpoint | **Cloud**

SIEM

Threat intelligence management

- New tools to integrate and manage threat intelligence feeds
- Investigate/hunt, search, validate threat intel

Entity analytics

- Host and user risk score
- Expanded User and Entity Behavior Analytics (UEBA)



Demo

80

Elastic Security



Search, Detect, Investigate

Detecting the most complex threats, powered by search

Automation, Prevention and Remediation

Expand into automation and prevention with actions and Elastic Agent

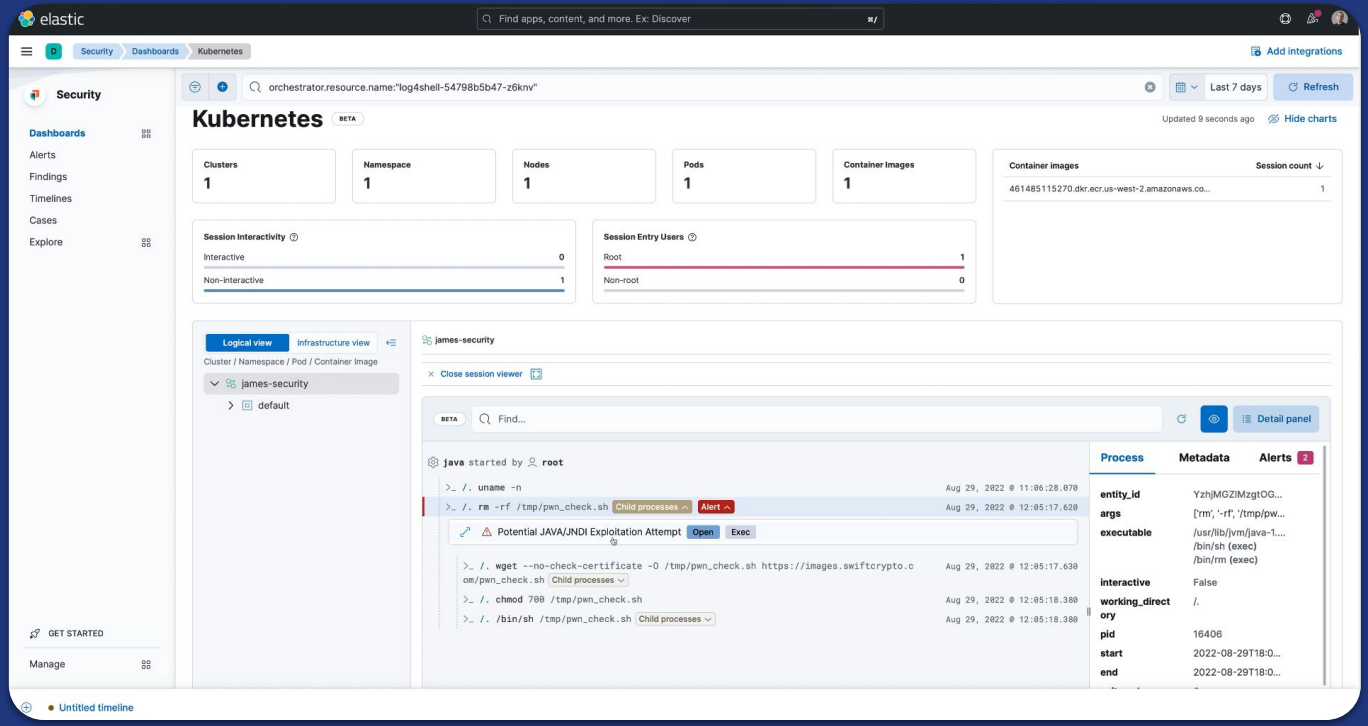
Open and transparent

Arm organizations with tools, knowledge and confidence to tackle the skills shortage and lower risk

elastic

81

Dedicated views: Multiple teams, one platform



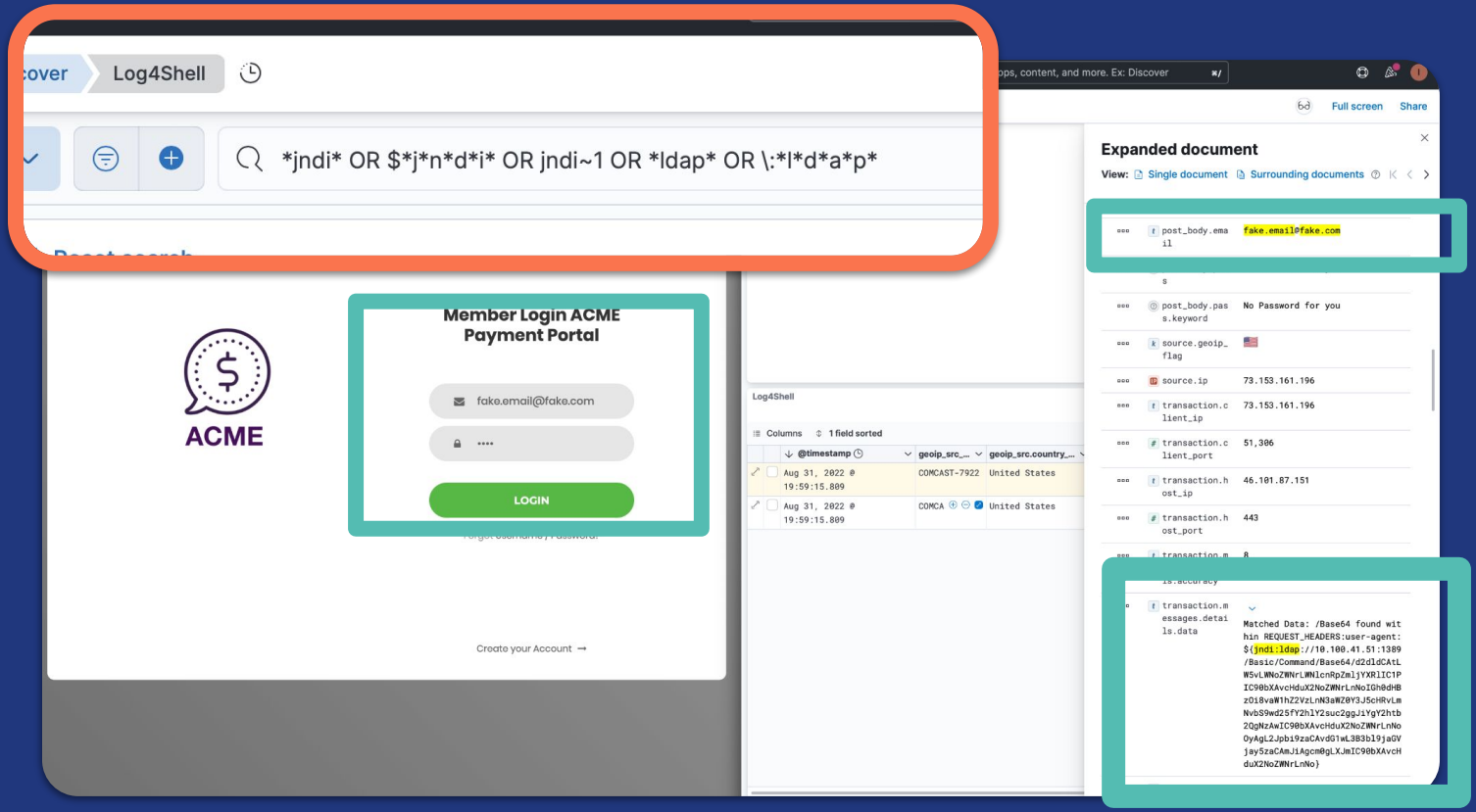
Pivot between solutions with a single click

Use the **same agent** to collect data, regardless of the source

Check for compliance, and **take preventative action**

82

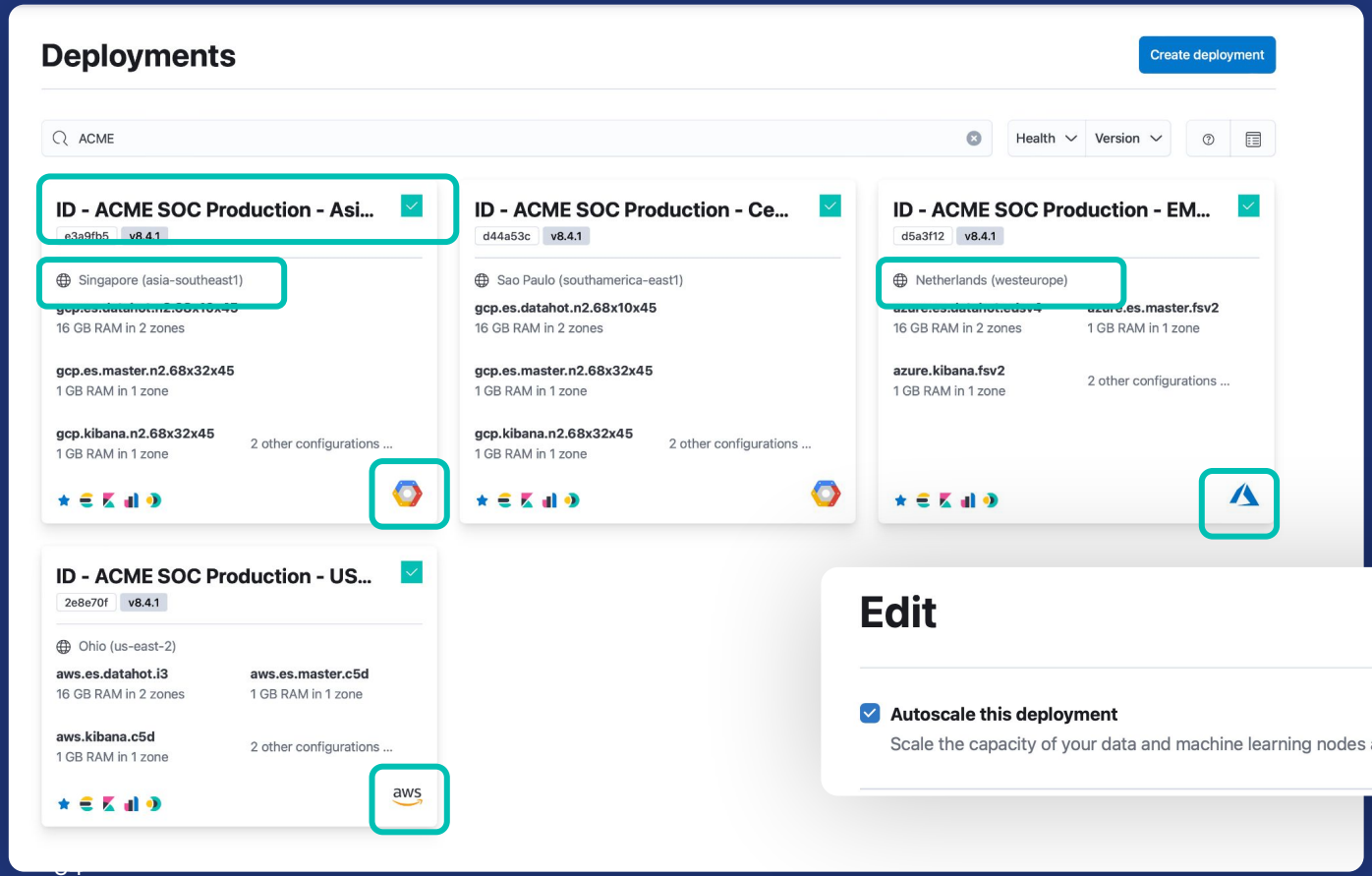
Complex searches over unstructured data, with ease



elastic

83

Cross Cluster Search and Autoscaling

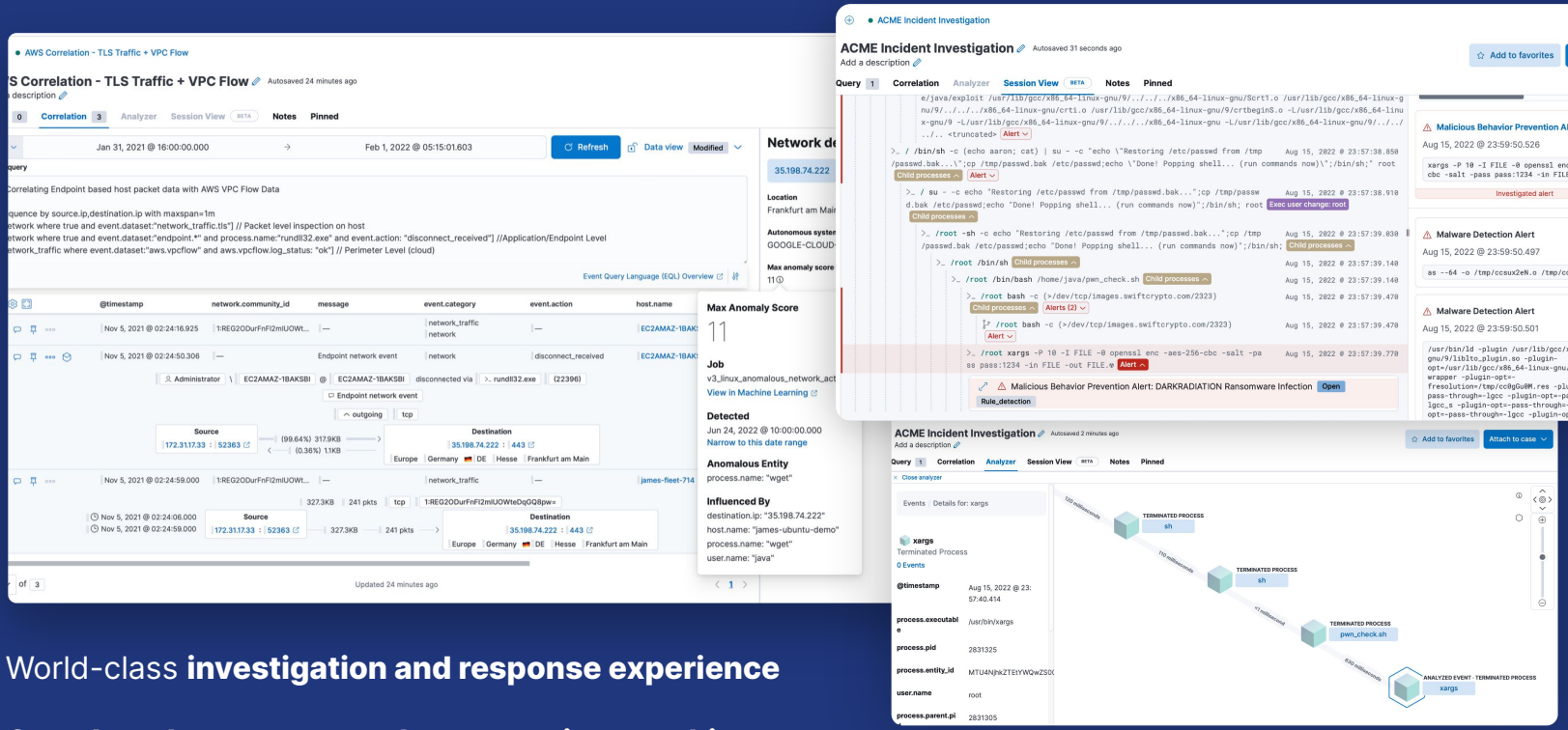


Deploy in any cloud provider, in the region of choice

Significant cost savings in data egress

Deployments scale, as and when needed

Timeline: One unified investigative interface



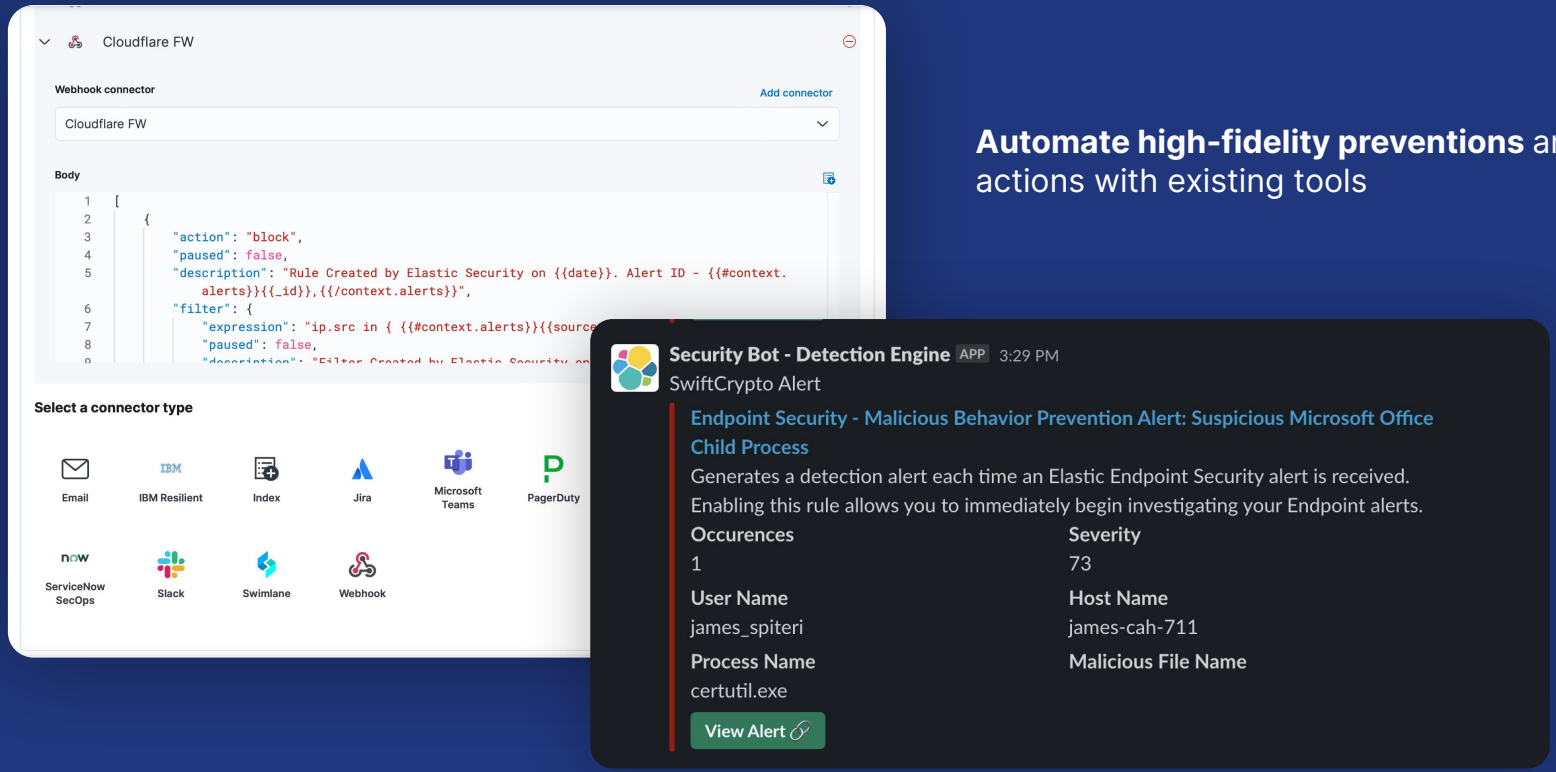
World-class **investigation and response experience**

Correlate data sources, take notes, view machine learning anomalies and much more

elastic

85

Detection Actions: Security automation for the Enterprise

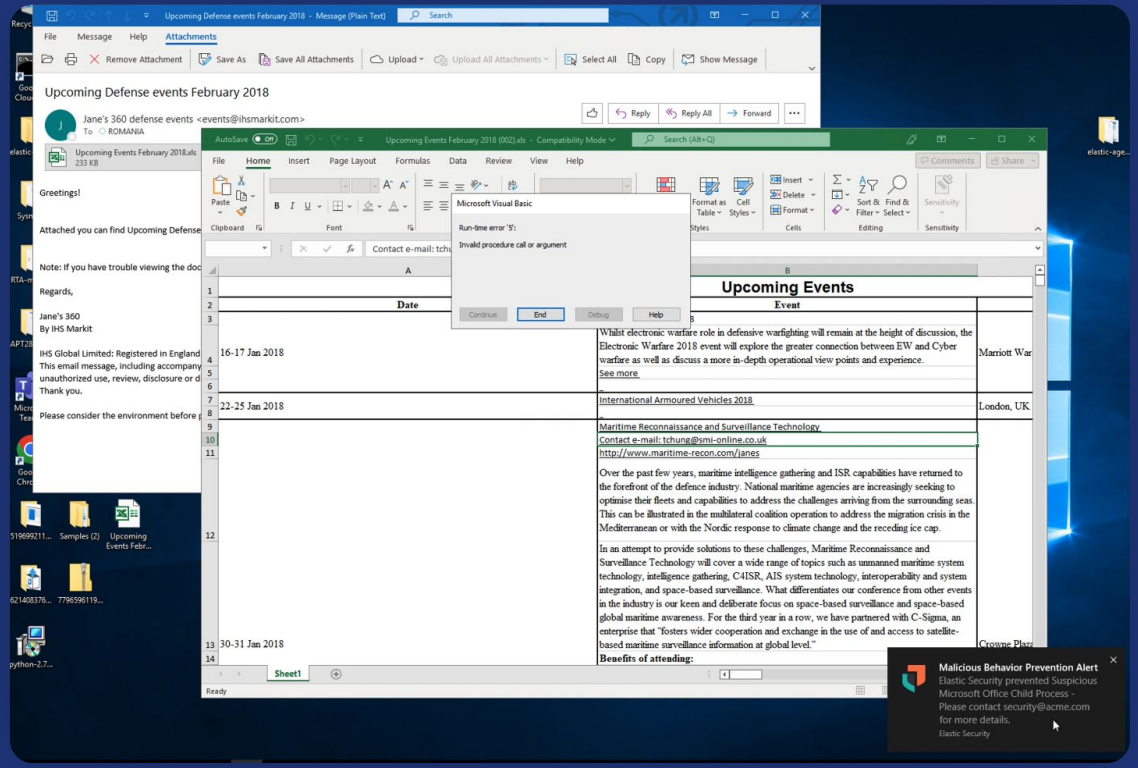


Automate high-fidelity preventions and actions with existing tools

elastic

86

Attack prevention:
Protect users and customer data, on any device



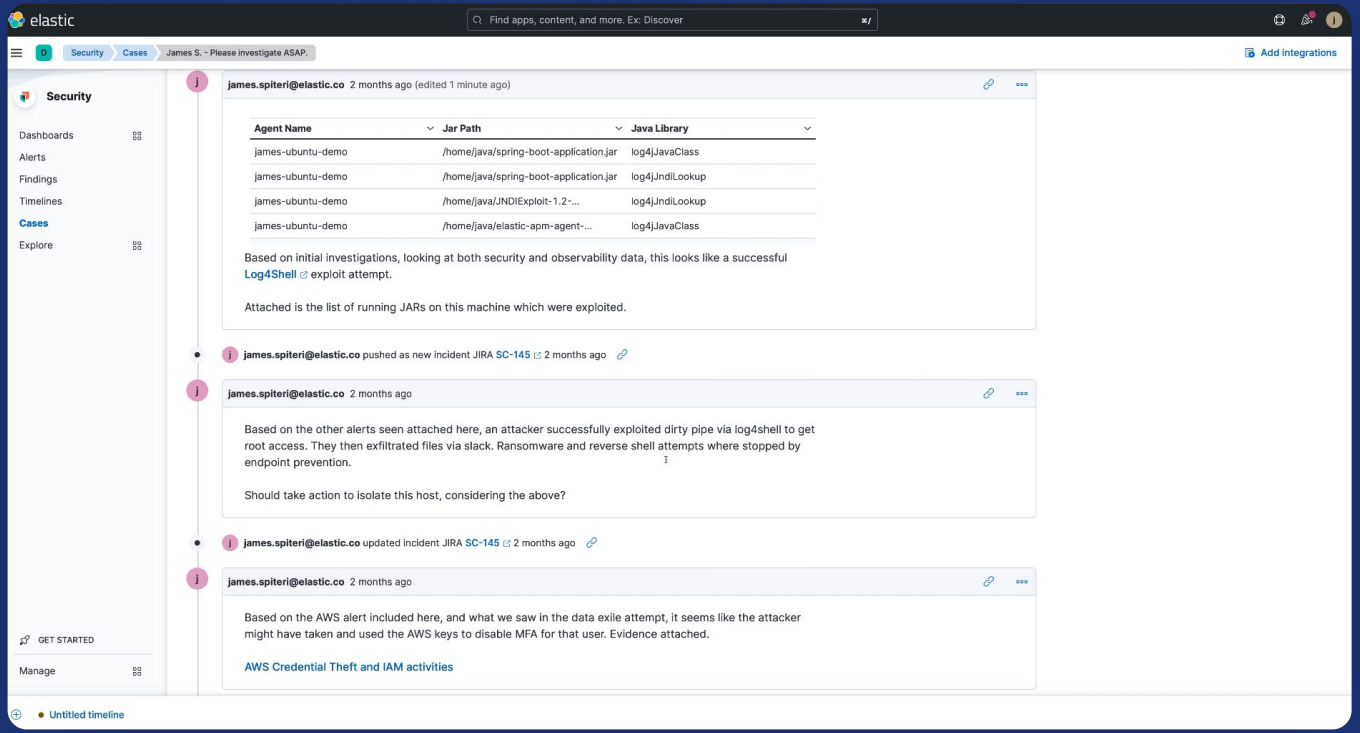
Prevent attacks on any device, **without having to worry about license quotas**

Run Elastic Agent **whenever and wherever** you need it

elastic

87

Case Management

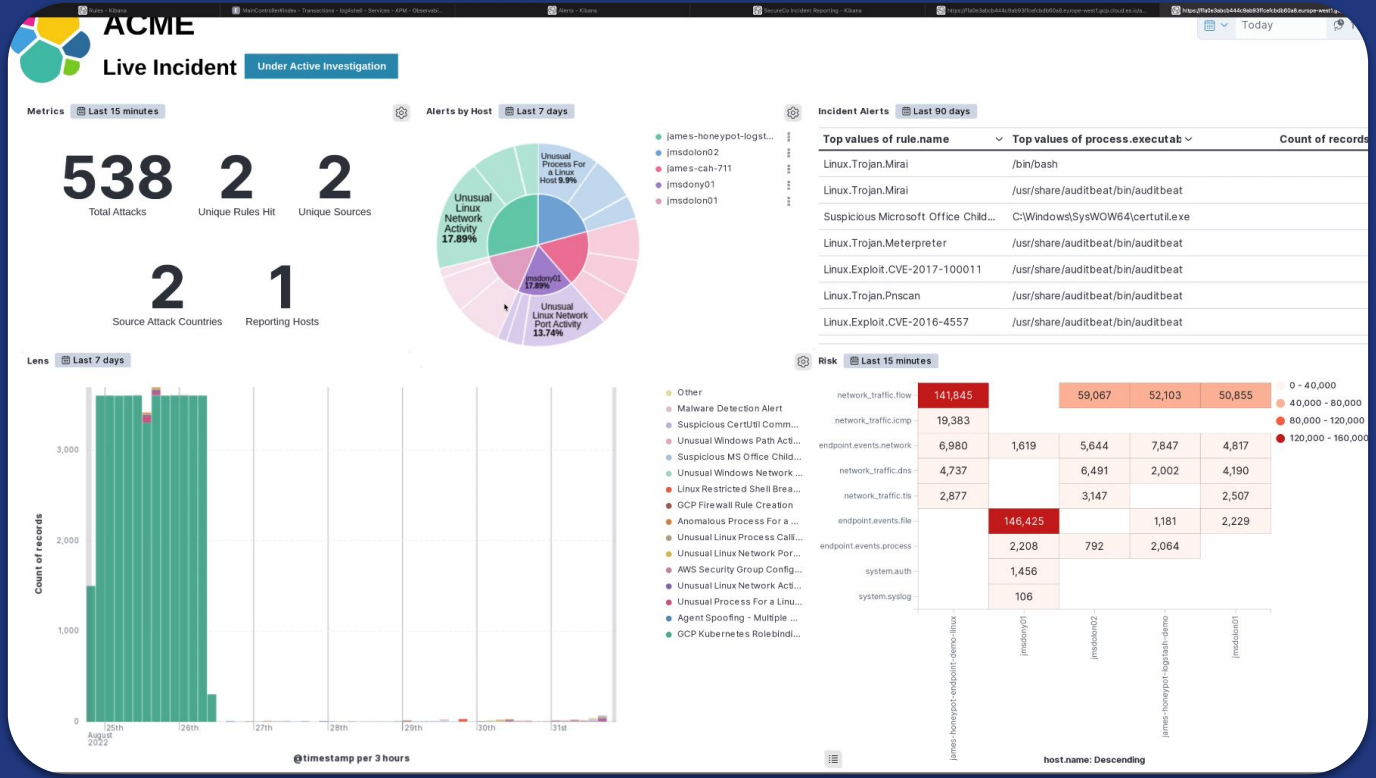


Keep track of ongoing incidents **in the most collaborative way possible**

Integrate with **any existing ticketing systems**

88

Canvas: Executive Reporting, and more



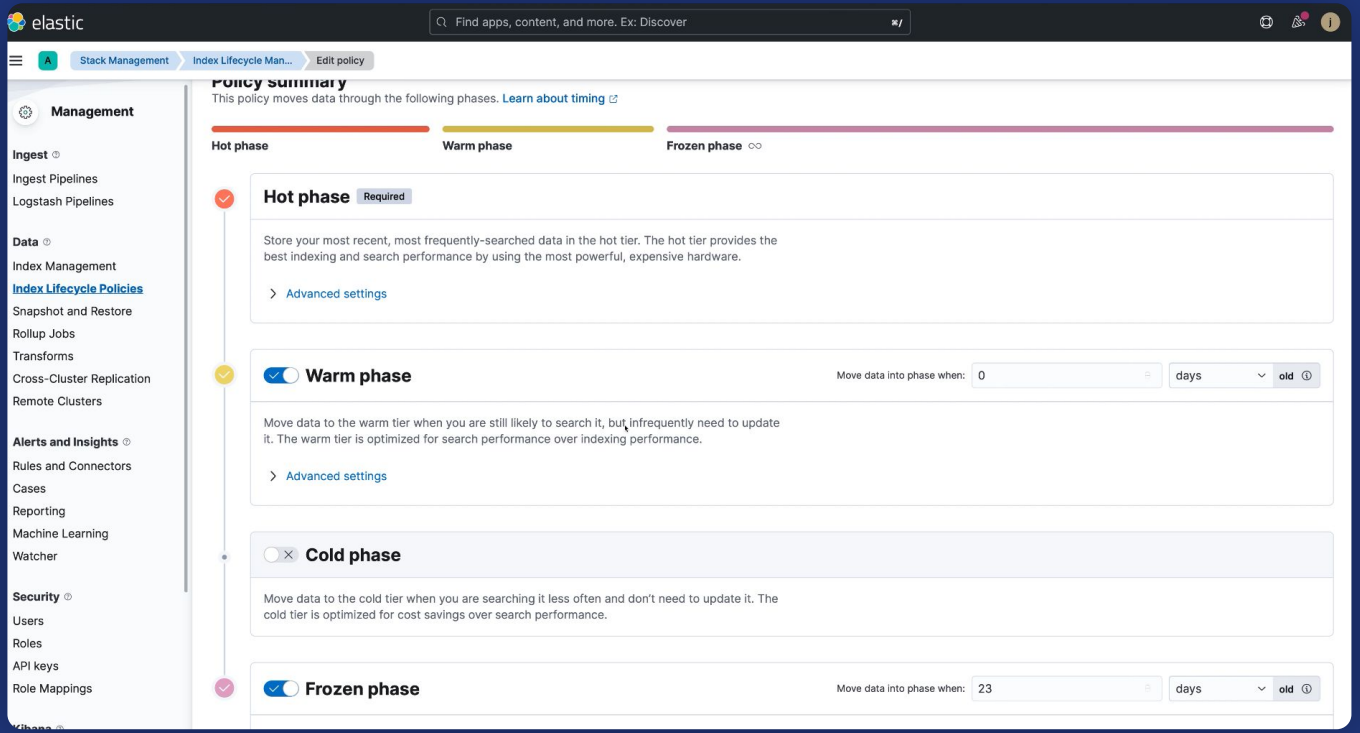
Executive-level reports with ease

Real-time view, or export at the click of a button

elastic

89

Data Lifecycle Management



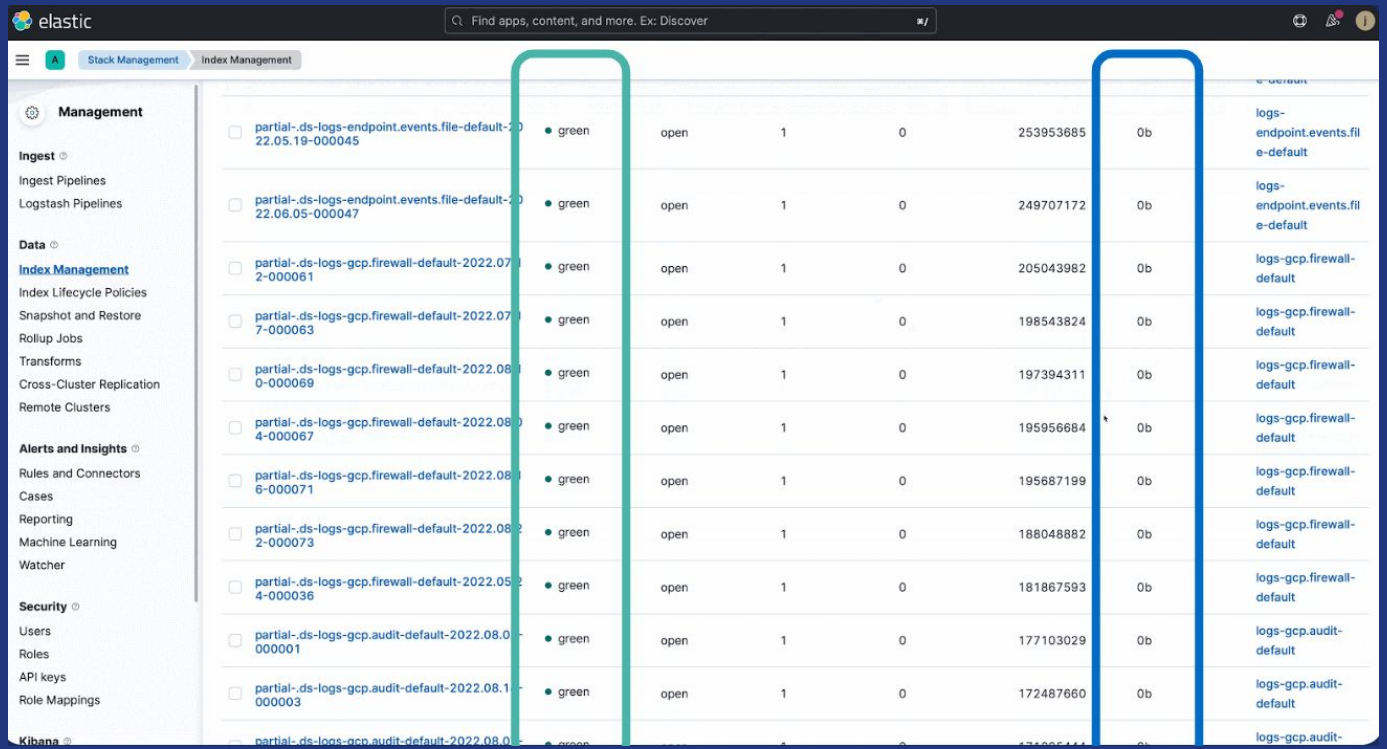
Data lifecycle functionality promotes **extended or perpetual retention**

Change data retention policies **on the fly, with ease**

elastic

90

Searchable Snapshot View



Search and look back across all data, **with no change to the analyst experience**

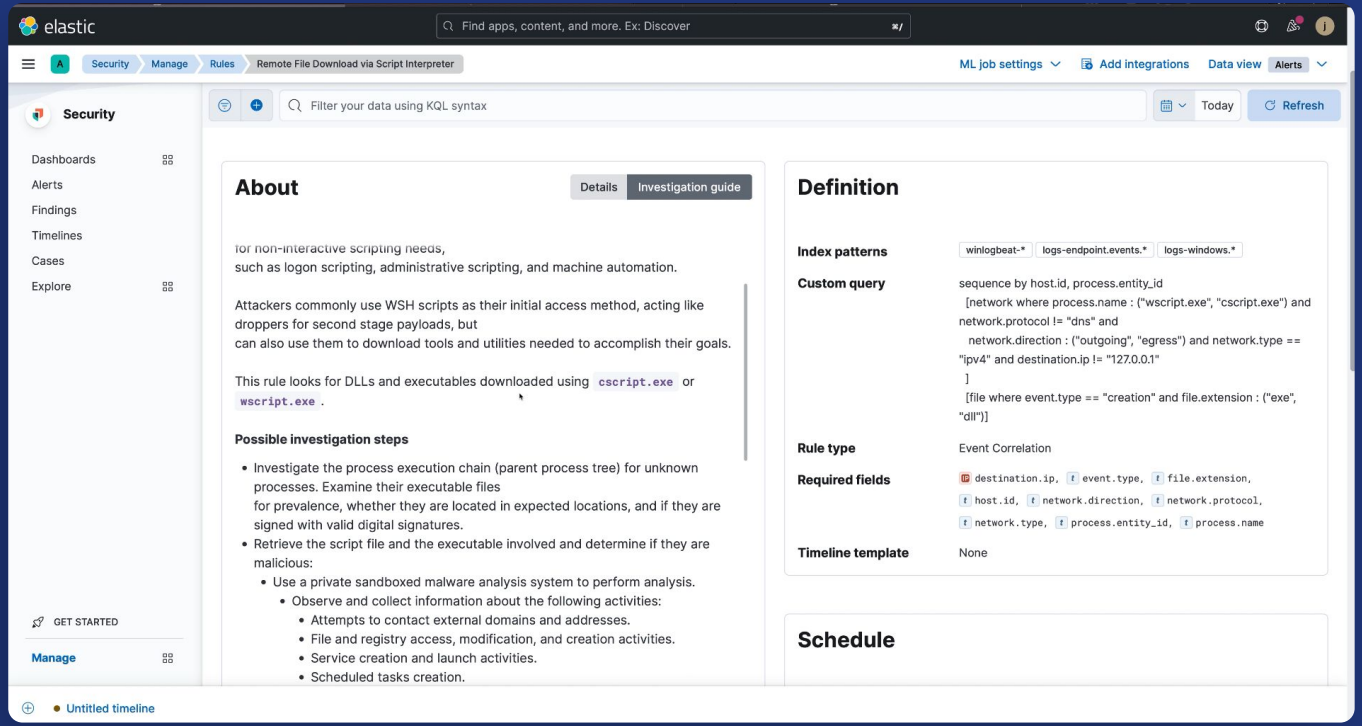
Save in infrastructure and storage costs, or costly data retrieval expenses

When the next supply chain attack hits, checking if you're vulnerable is just a search away

elastic

91

Detections and Investigation Guides

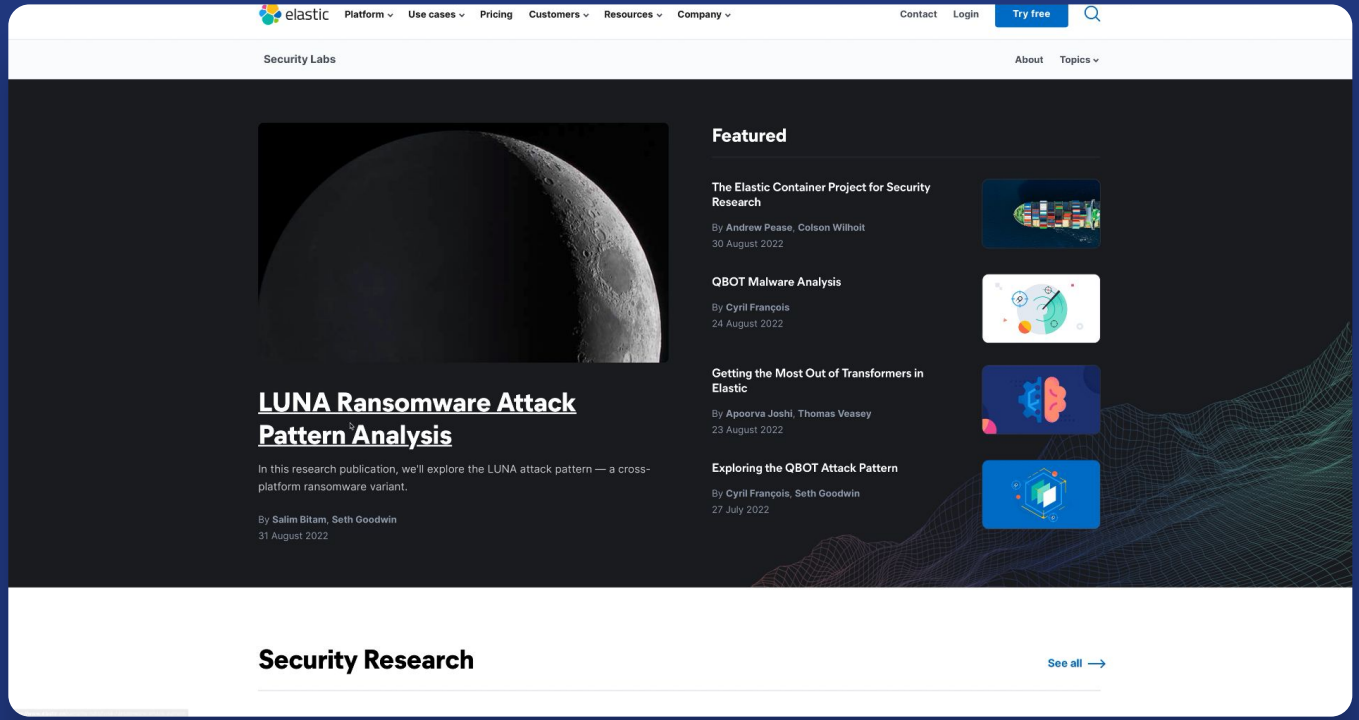


Elastic helps with the cyber skills shortage by **providing 100's of prebuilt detection rules and investigation guides**

Giving teams all the help they need, **right from the same console**

92

Elastic Security Labs



Teams can **leverage research articles and malware analysis** via Elastic Security Labs

93

README.md

Protections Artifacts

Elastic Security prevents ransomware and malware, detects
free and open, ready for every endpoint.

Protections-Artifacts is the home of our detection logic (rule
believe that being open and transparent is critical for the suc
interested in additional background.

Directory

Below you will find the artifacts we have opened in this repos

Folder	Description
`behavior/`	EQL based malicious behavior rules
`yara/`	Yara rules for malware protection

Questions? Problems? Sugg

If you would like you to provide feedback or contribute to this
artifact's readme and open an issue using one of the provide
because this repository is automatically generated.

You can also reach us in our Slack Workspace or in the Secu

License

Copyright Elasticsearch B.V. and/or licensed to Elasticsearch
Licensed under the Elastic License 2.0; you may not use the

Contributors must sign a Contributor License Agreement be

README.md

python 3.8+ | Unit Tests passing | chat #security-detection-rules | ATT&

Detection Rules

Detection Rules is the home for rules used by Elastic Security. This
testing, validation, and release of rules for Elastic Security's Detect

This repository was first announced on Elastic's blog post, Elastic
additional content, see the accompanying webinar, Elastic Security

Table of Contents

- Detection Rules
  - Table of Contents
  - Overview of this repository
  - Getting started
  - How to contribute
  - Licensing
  - Questions? Problems? Suggestions?

Overview of this repository

Detection Rules contains more than just static rule files. This repos
integrating with the Detection Engine in Kibana.

folder	
`detection_rules/`	Python module for rule parsing, va
`detection_rules/etc/`	Miscellaneous files, such as ECS
`kibana/`	Python library for handling the AP
`kql/`	Python library for parsing and vali
`rta/`	Red Team Automation code used
`rules/`	Root directory where rules are sto
`tests/`	Python code for unit testing rules

Getting started

README.md

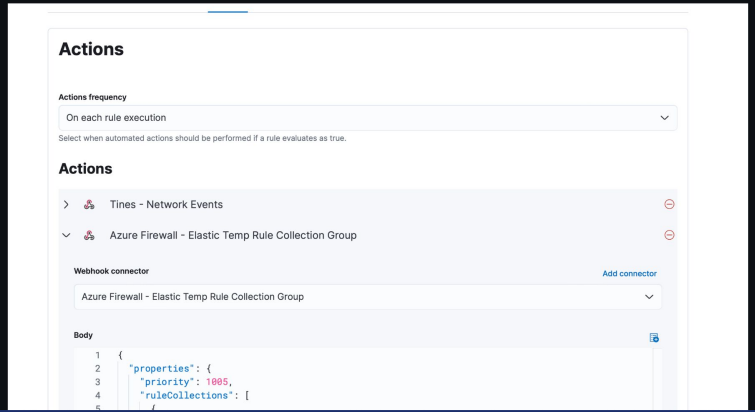
Security Action Examples

This repository contains a few examples of webhook actions that can be added to rules within Elastic Security. Each subdirectory contains the following files:

- A JSON file containing the action content. Please feel free to change the variables and other content as you see fit.
- A README file with specific instructions for the action connector in question.
- A screenshot of the connector configuration in Kibana's connector management page.
- A screenshot of the expected outcome when an action runs successfully.

Please use these actions with caution, and test appropriately. Do not blindly add an action to a detection rule if you are unsure of what the outcome is, or how it will impact your organization. You should follow any operational procedures you may have in place for any form of automation scenarios.

The screenshot below shows an example of what one of these actions would look like as part of a detection rule configuration:

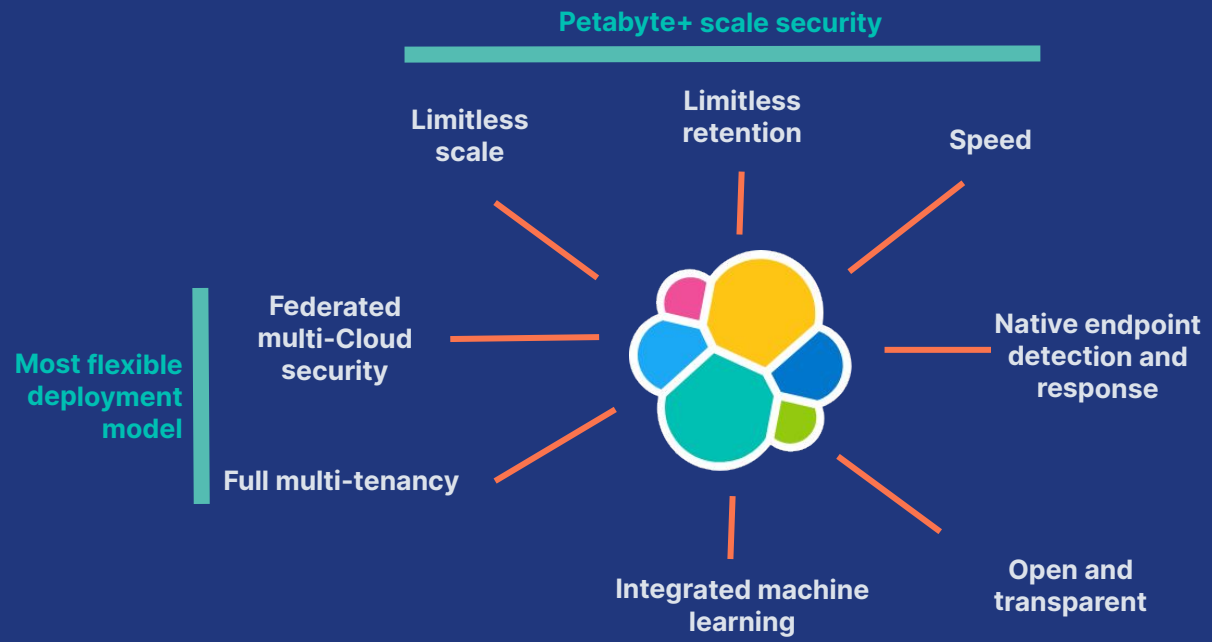


elastic

94

Unique dimensions of Elastic Security

Reducing risk, complexity and cost



elastic

95

Elastic Enterprise Search



Matt Riley
General Manager, Enterprise Search

- **CEO of Swiftype prior to acquisition**
- **12 years in Product Leadership**
- **5 years at Elastic**

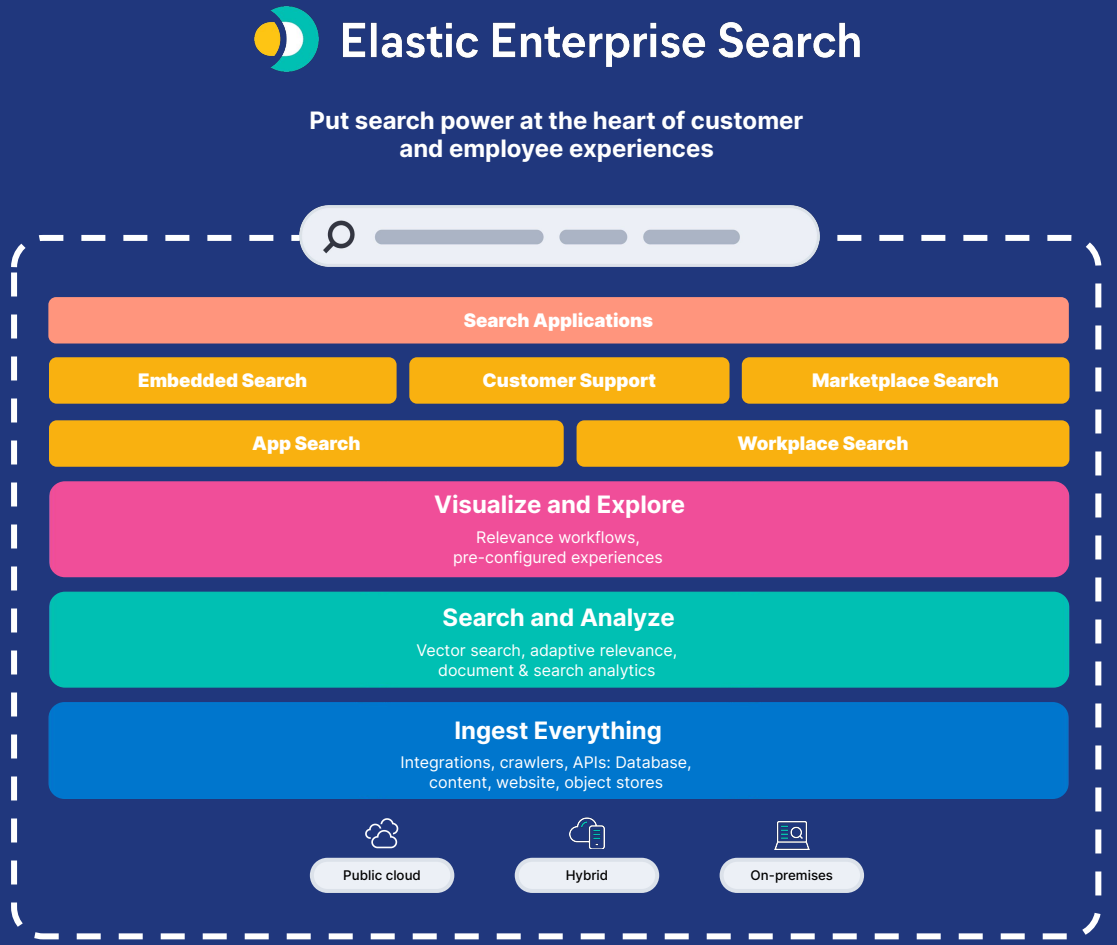
swiftype HomeAway SCRIBD

elastic

Search powers our business

Enterprise Search

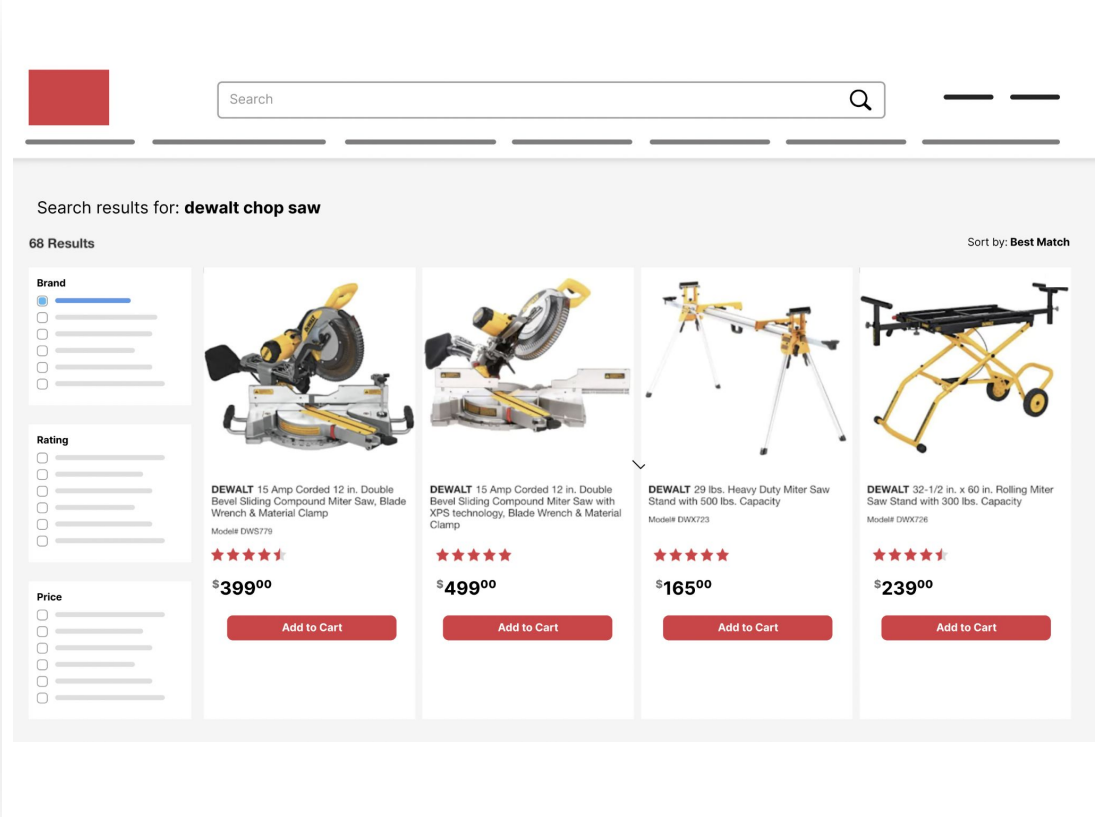
The gold standard for building search applications



98

Leading home supplies retailer

- Consumer-facing Ecommerce Search application for web and mobile
  - Proprietary dense vector models via Machine Learning
  - Nearest Neighbor search at scale
- Quote Center System
- Order Management System
- Several other search-powered applications



99

A leading multinational pharmaceutical corporation

Expediting research with structured and unstructured data searches

Goals:

- Accelerate drug discovery by searching across scientific and experimental data
- Mitigate regulatory risk with validated, real-time answers to auditor questions

Results:

- Ingest large, heterogeneous unstructured data sets, enriched by Machine Learning models
- Deliver relevant search results quickly, analyze and visualize data flexibly
- Significant time savings and reduced effort for employees and scientists

Elastic captures all of these use cases, which propels our business in this market

101

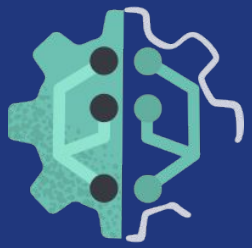
Common fundamental attributes



Unstructured data at scale



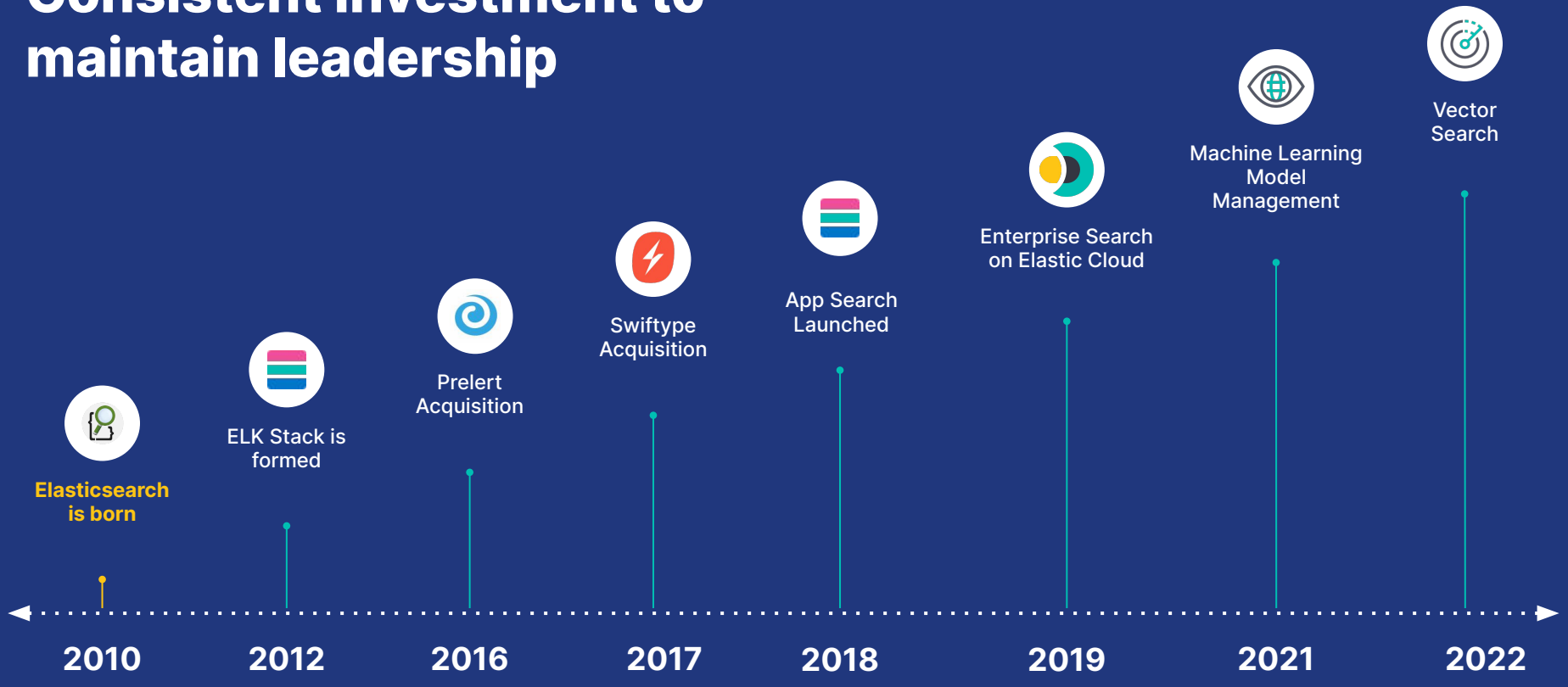
Requires real-time search & discovery



Applications built by developers

102

Consistent investment to maintain leadership























Searching for

- Machine learning to scale
- A better shopping experience
- Faster implementation
- Custom search experiences
- Real time analytics
- Peak user experience

And more…

Key product goals



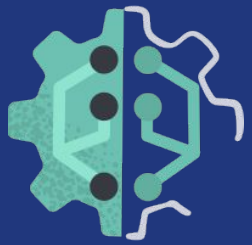
Ease of use

Critical to both developer adoption and Enterprise readiness



Flexibility & power

Driving our ability to capture such a diverse set of use cases



Technology leadership

We create the search capabilities that have defined this market

105

Why we win

SEARCH CAPABILITIES



Established leadership

3.6B+ Downloads

Recognized leader with credibility & widely established footprint in Search



Vibrant ecosystem

183k+ Pull Requests

A passionate community of developers, integrations, & complementary tooling



World-class relevance

Full-text, vector, and hybrid search yields relevant results from vast data sets

PLATFORM CAPABILITIES



One platform

One platform for every search application, in Cloud, on-premises, or hybrid



Operate at scale

Proven speed, scale, and relevance for critical production applications



Flexible pricing & license

Start simple and grow with flexible pricing

FY23 Enterprise Search investments

Continuing to anticipate developer needs



The best, unified platform for developer search applications in the Cloud



Enable increasingly sophisticated use cases, based on emerging technologies, at production scale



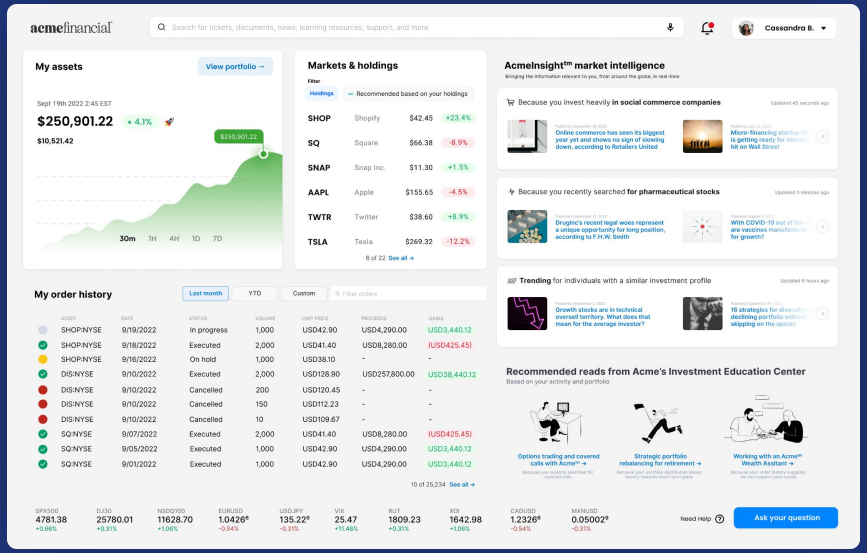
Capture the ever-increasing behavioral analytical data that drive modern search applications



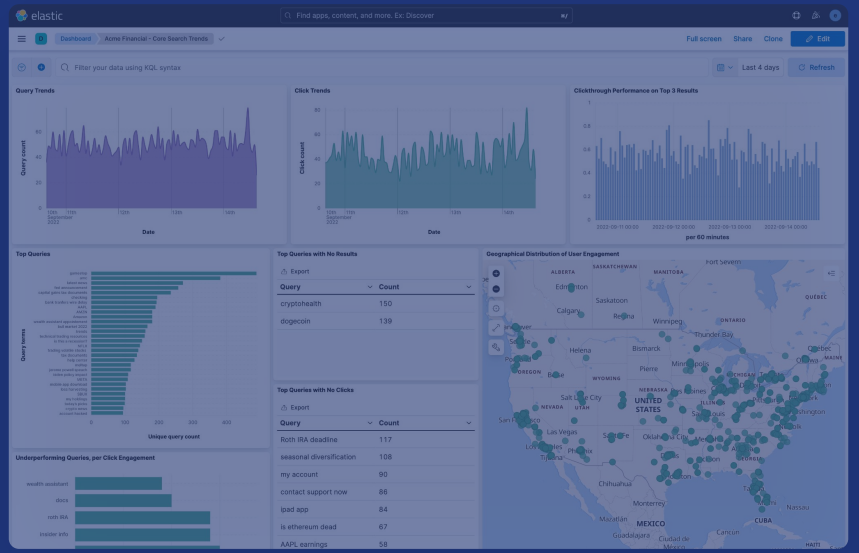
Demo

elastic

108



Delivering search-powered applications



Analyzing behavior and tailoring outcomes

acmefinancial

Search for tickers, documents, news, learning resources, support, and more

Cassandra B.

My assets

View portfolio →

Sept 19th 2022 2:45 EST

$250,901.22 ▲ 4.1%

$10,521.42



Markets & holdings

Filter

Holdings | Recommended based on your holdings

SHOP	Shopify	$42.45	+23.4%
SQ	Square	$66.38	-8.9%
SNAP	Snap Inc.	$11.30	+1.5%
AAPL	Apple	$155.65	-4.5%
TWTR	Twitter	$38.60	+8.9%
TSLA	Tesla	$269.32	-12.2%

6 of 22 See all →

AcmeInsight℠ market intelligence

Bringing the information relevant to you, from around the globe, in real-time

Because you invest heavily **in social commerce companies**

Updated 45 seconds ago



Published September 19, 2022
Online commerce has seen its biggest year yet and shows no sign of slowing down, according to Retailers United



Published July 22, 2022
Micro-financing startup Klo is getting ready for monster hit on Wall Street

Because you recently searched **for pharmaceutical stocks**

Updated 3 minutes ago



Published September 12, 2022
DrugInc's recent legal woes represent a unique opportunity for long position, according to F.H.W. Smith



Published August 3, 2022
With COVID-19 out of the m are vaccines manufacture for growth?

Trending for individuals with a similar investment profile

Updated 6 hours ago



Published September 2, 2022
Growth stocks are in technical oversell territory. What does that mean for the average investor?



Published September 19, 2022
16 strategies for diversifying declining portfolio without skipping on the upside

My order history

Last month | YTD | Custom | Filter orders

	ASSET	DATE	STATUS	VOLUME	UNIT PRICE	PROCEEDS	GAINS
	SHOP:NYSE	9/19/2022	In progress	1,000	USD42.90	USD4,290.00	USD3,440.12
✓	SHOP:NYSE	9/18/2022	Executed	2,000	USD41.40	USD8,280.00	(USD425.45)
	SHOP:NYSE	9/16/2022	On hold	1,000	USD38.10	-	-
✓	DIS:NYSE	9/10/2022	Executed	2,000	USD128.90	USD257,800.00	USD38,440.12
	DIS:NYSE	9/10/2022	Cancelled	200	USD120.45	-	-
	DIS:NYSE	9/10/2022	Cancelled	150	USD112.23	-	-
	DIS:NYSE	9/10/2022	Cancelled	10	USD109.67	-	-
✓	SQ:NYSE	9/07/2022	Executed	2,000	USD41.40	USD8,280.00	(USD425.45)
✓	SQ:NYSE	9/05/2022	Executed	1,000	USD42.90	USD4,290.00	USD3,440.12
✓	SQ:NYSE	9/01/2022	Executed	1,000	USD42.90	USD4,290.00	USD3,440.12

10 of 25,234 See all →

Recommended reads from Acme's Investment Education Center

Based on your activity and portfolio



Options trading and covered calls with Acme℠ →

Because you recently searched for covered calls



Strategic portfolio rebalancing for retirement →

Because your portfolio distribution skews heavily towards short-term gains



Working with an Acme℠ Wealth Assitant →

Because your order history suggests we can support your needs

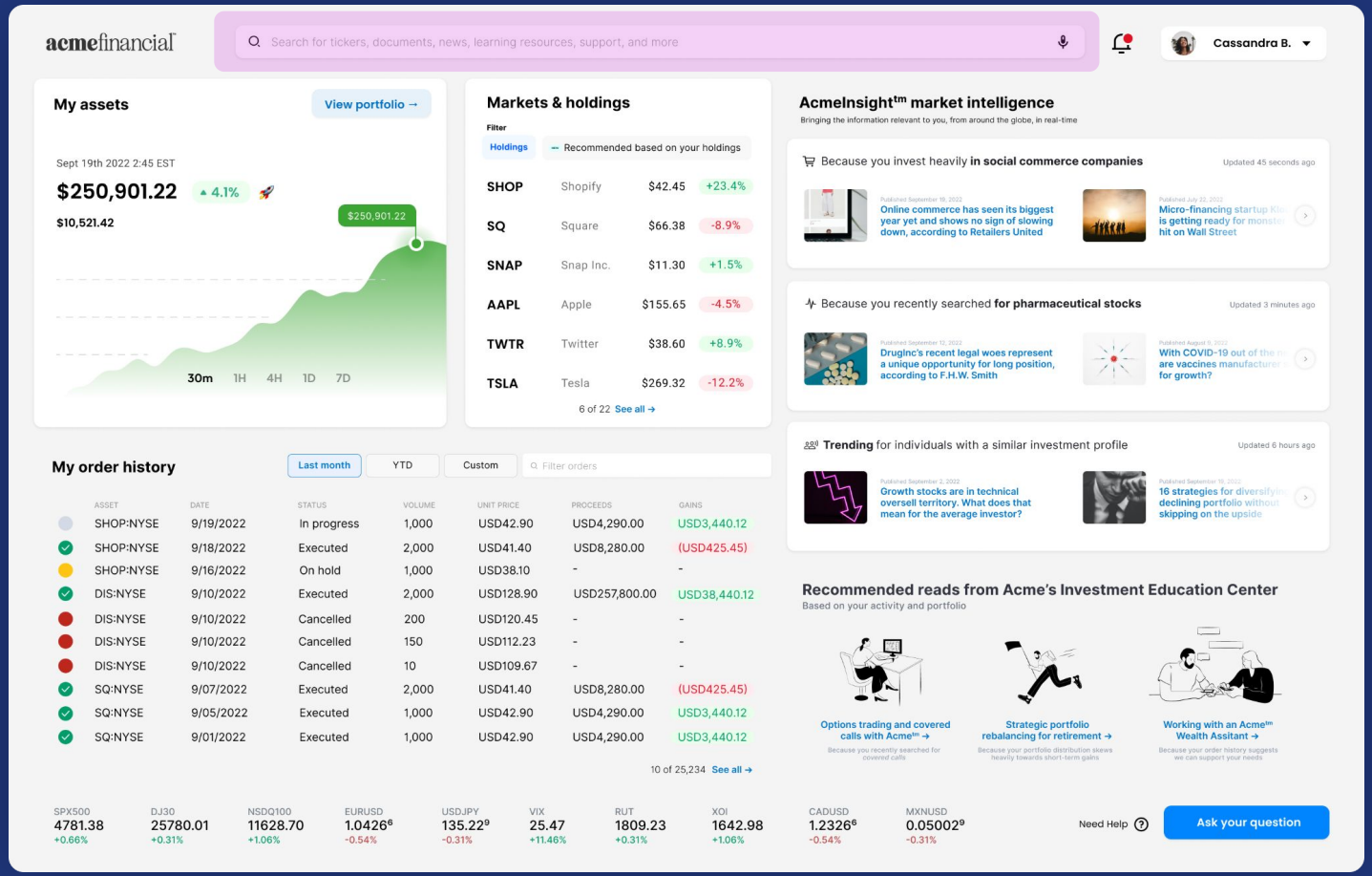
SPX500	DJ30	NSDQ100	EURUSD	USDJPY	VIX	RUT	XOI	CADUSD	MXNUSD
4781.38	25780.01	11628.70	1.0426⁶	135.22⁹	25.47	1809.23	1642.98	1.2326⁶	0.05002⁹
+0.66%	+0.31%	+1.06%	-0.54%	-0.31%	+11.46%	+0.31%	+1.06%	-0.54%	-0.31%

Need Help

Ask your question

elastic

110


acmefinancial
Search for tickers, documents, news, learning resources, support, and more
Cassandra B.
My assets
View portfolio →
Sept 19th 2022 2:45 EST
$250,901.22
4.1%
$10,521.42
$250,901.22
30m 1H 4H 1D 7D
Markets & holdings
Filter
Holdings
Recommended based on your holdings
SHOP Shopify $42.45 +23.4%
SQ Square $66.38 -8.9%
SNAP Snap Inc. $11.30 +1.5%
AAPL Apple $155.65 -4.5%
TWTR Twitter $38.60 +8.9%
TSLA Tesla $269.32 -12.2%
6 of 22 See all →
AcmeInsight™ market intelligence
Bringing the information relevant to you, from around the globe, in real-time
Because you invest heavily in social commerce companies
Updated 45 seconds ago
Online commerce has seen its biggest year yet and shows no sign of slowing down, according to Retailers United
Micro-financing startup Klo is getting ready for monster hit on Wall Street
Because you recently searched for pharmaceutical stocks
Updated 3 minutes ago
DrugInc's recent legal woes represent a unique opportunity for long position, according to F.H.W. Smith
With COVID-19 out of the m are vaccines manufacture for growth?
Trending for individuals with a similar investment profile
Updated 6 hours ago
Growth stocks are in technical oversell territory. What does that mean for the average investor?
16 strategies for diversifyin declining portfolio without skipping on the upside
My order history
Last month
YTD
Custom
Filter orders
ASSET DATE STATUS VOLUME UNIT PRICE PROCEEDS GAINS
SHOP:NYSE 9/19/2022 In progress 1,000 USD42.90 USD4,290.00 USD3,440.12
SHOP:NYSE 9/18/2022 Executed 2,000 USD41.40 USD8,280.00 (USD425.45)
SHOP:NYSE 9/16/2022 On hold 1,000 USD38.10 - -
DIS:NYSE 9/10/2022 Executed 2,000 USD128.90 USD257,800.00 USD38,440.12
DIS:NYSE 9/10/2022 Cancelled 200 USD120.45 - -
DIS:NYSE 9/10/2022 Cancelled 150 USD112.23 - -
DIS:NYSE 9/10/2022 Cancelled 10 USD109.67 - -
SQ:NYSE 9/07/2022 Executed 2,000 USD41.40 USD8,280.00 (USD425.45)
SQ:NYSE 9/05/2022 Executed 1,000 USD42.90 USD4,290.00 USD3,440.12
SQ:NYSE 9/01/2022 Executed 1,000 USD42.90 USD4,290.00 USD3,440.12
10 of 25,234 See all →
Recommended reads from Acme's Investment Education Center
Based on your activity and portfolio
Options trading and covered calls with Acme™ →
Because you recently searched for covered calls
Strategic portfolio rebalancing for retirement →
Because your portfolio distribution skews heavily towards short-term gains
Working with an Acme™ Wealth Assitant →
Because your order history suggests we can support your needs
SPX500 4781.38 +0.66%
DJ30 25780.01 +0.31%
NSDQ100 11628.70 +1.06%
EURUSD 1.0426⁶ -0.54%
USDJPY 135.22⁹ -0.31%
VIX 25.47 +11.46%
RUT 1809.23 +0.31%
XOI 1642.98 +1.06%
CADUSD 1.2326⁶ -0.54%
MXNUSD 0.05002⁹ -0.31%
Need Help
Ask your question

elastic

111

acmefinancial

Search for tickers, documents, news, learning resources, support, and more

Cassandra B.

My assets

View portfolio →

Sept 19th 2022 2:45 EST

$250,901.22 ▲ 4.1%

$10,521.42



Markets & holdings

Filter

Holdings | Recommended based on your holdings

SHOP	Shopify	$42.45	+23.4%
SQ	Square	$66.38	-8.9%
SNAP	Snap Inc.	$11.30	+1.5%
AAPL	Apple	$155.65	-4.5%
TWTR	Twitter	$38.60	+8.9%
TSLA	Tesla	$269.32	-12.2%

6 of 22 See all →

AcmeInsight℠ market intelligence

Bringing the information relevant to you, from around the globe, in real-time

Because you invest heavily **in social commerce companies** — Updated 45 seconds ago



Online commerce has seen its biggest year yet and shows no sign of slowing down, according to Retailers United



Micro-financing startup Klo… is getting ready for monster hit on Wall Street

Because you recently searched **for pharmaceutical stocks** — Updated 3 minutes ago



DruginC's recent legal woes represent a unique opportunity for long position, according to F.H.W. Smith

With COVID-19 out of the m… are vaccines manufacturers… for growth?

Trending for individuals with a similar investment profile — Updated 6 hours ago



Growth stocks are in technical oversell territory. What does that mean for the average investor?



16 strategies for diversifying… declining portfolio without… skipping on the upside

My order history

Last month | YTD | Custom | Filter orders

	ASSET	DATE	STATUS	VOLUME	UNIT PRICE	PROCEEDS	GAINS
	SHOP:NYSE	9/19/2022	In progress	1,000	USD42.90	USD4,290.00	USD3,440.12
✓	SHOP:NYSE	9/18/2022	Executed	2,000	USD41.40	USD8,280.00	(USD425.45)
	SHOP:NYSE	9/16/2022	On hold	1,000	USD38.10	-	-
✓	DIS:NYSE	9/10/2022	Executed	2,000	USD128.90	USD257,800.00	USD38,440.12
	DIS:NYSE	9/10/2022	Cancelled	200	USD120.45	-	-
	DIS:NYSE	9/10/2022	Cancelled	150	USD112.23	-	-
	DIS:NYSE	9/10/2022	Cancelled	10	USD109.67	-	-
✓	SQ:NYSE	9/07/2022	Executed	2,000	USD41.40	USD8,280.00	(USD425.45)
✓	SQ:NYSE	9/05/2022	Executed	1,000	USD42.90	USD4,290.00	USD3,440.12
✓	SQ:NYSE	9/01/2022	Executed	1,000	USD42.90	USD4,290.00	USD3,440.12

10 of 25,234 See all →

Recommended reads from Acme's Investment Education Center

Based on your activity and portfolio



Options trading and covered calls with Acme℠ →

Because you recently searched for covered calls



Strategic portfolio rebalancing for retirement →

Because your portfolio distribution skews heavily towards short-term gains



Working with an Acme℠ Wealth Assitant →

Because your order history suggests we can support your needs

SPX500	DJ30	NSDQ100	EURUSD	USDJPY	VIX	RUT	XOI	CADUSD	MXNUSD
4781.38	25780.01	11628.70	1.0426⁶	135.22⁹	25.47	1809.23	1642.98	1.2326⁶	0.05002⁹
+0.66%	+0.31%	+1.06%	-0.54%	-0.31%	+11.46%	+0.31%	+1.06%	-0.54%	-0.31%

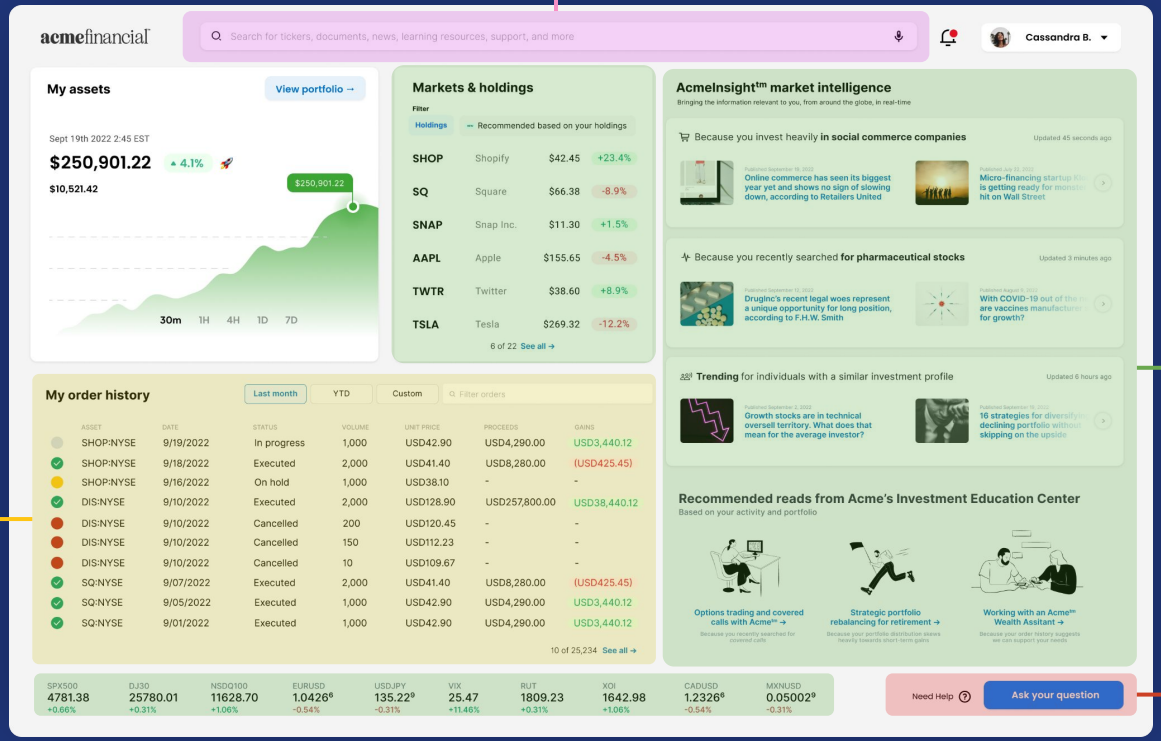
Need Help

Ask your question

elastic

112

Personalized discovery and navigation experience, powered by full-text search



Personalized recommendations, powered by machine learning search

Customer support powered by natural language understanding search

Legacy system offloading, powered by search

elastic

113

nefinancial

Search for tickers, documents, news, learning resources, support, and more

Cassan

covered calls
pharmaceuticals segment performance
SHOP:NYSE

market predictions Q4 2022 Trending
federal reserve meeting notes Trending
1099 form Trending
great resignation Trending

assets

19th 2022 2:45 EST

250,901.22 ▲ 4.1%

521.42

30m 1H 4H 1D 7D

AAPL	Apple	$155.65	-4.5%
TWTR	Twitter	$38.60	+8.9%
TSLA	Tesla	$269.32	-12.2%

6 of 22 See all →

order history

Last month | YTD | Custom | Filter orders

ASSET	DATE	STATUS	VOLUME	UNIT PRICE	PROCEEDS	GAINS
SHOP:NYSE	9/19/2022	In progress	1,000	USD42.90	USD4,290.00	USD3,440.12
SHOP:NYSE	9/18/2022	Executed	2,000	USD41.40	USD8,280.00	(USD425.45)
SHOP:NYSE	9/16/2022	On hold	1,000	USD38.10	-	-
DIS:NYSE	9/10/2022	Executed	2,000	USD128.90	USD257,800.00	USD38,440.12
DIS:NYSE	9/10/2022	Cancelled	200	USD120.45	-	-
DIS:NYSE	9/10/2022	Cancelled	150	USD112.23	-	-

companies Updated



Micro-financing start is getting ready for m hit on Wall Street

Because you recently searched **for pharmaceutical stocks**



Published September 12, 2022
DrugInc's recent legal woes represent a unique opportunity for long position, according to F.H.W. Smith

With COVID-19 out of are vaccines manufac for growth?

Trending for individuals with a similar investment profile



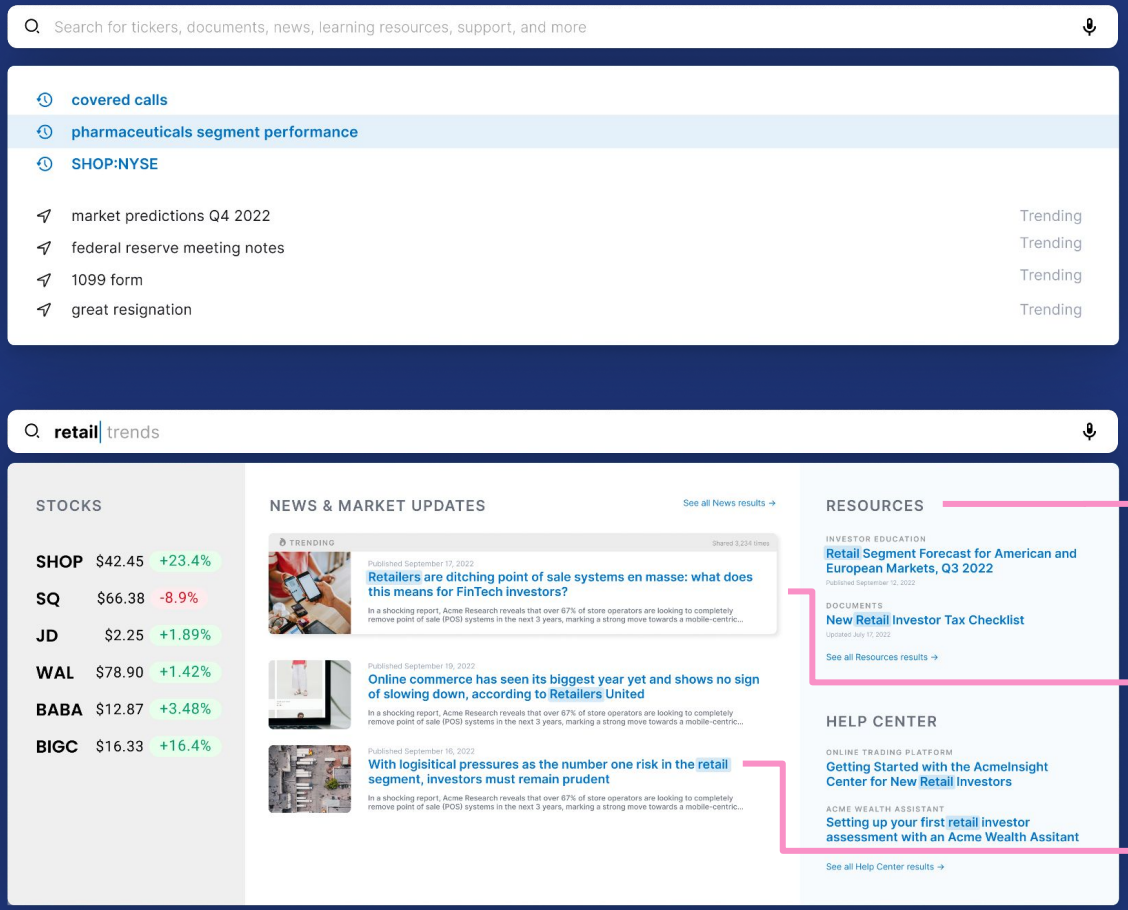
Published September 2, 2022
Growth stocks are in technical oversell territory. What does that mean for the average investor?

16 strategies for div declining portfolio wi skipping on the upsi

Recommended reads from Acme's Investment Education Cen

Based on your activity and portfolio

114



Personalized search history

Locally and globally trending searches, based on user behavior and portfolio

Typo tolerant query suggestions

Relevant results **across multiple data sources**

Adaptive relevance based on trends, recency and other configurable factors

Highlighting, for best-in-class user experience

elastic

115

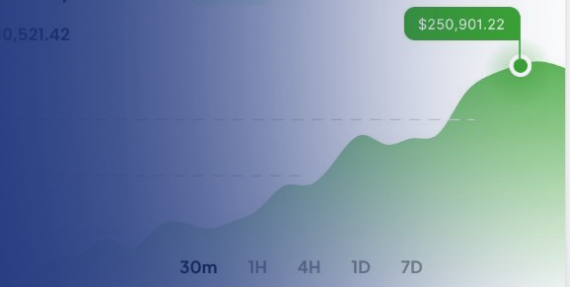
y assets

View portfolio →

pt 19th 2022 2:45 EST

250,901.22 ▲ 4.1%

0,521.42



Markets & holdings

Filter

Holdings | Recommended based on your holdings

SHOP	Shopify	$42.45	+23.4%
SQ	Square	$66.38	-8.9%
SNAP	Snap Inc.	$11.30	+1.5%
AAPL	Apple	$155.65	-4.5%
TWTR	Twitter	$38.60	+8.9%
TSLA	Tesla	$269.32	-12.2%

6 of 22 See all →

AcmeInsight[tm] market intelligence

Bringing the information relevant to you, from around the globe, in real-time

Because you invest heavily **in social commerce companies** — Updated 45 seconds ago



Published September 19, 2022
Online commerce has seen its biggest year yet and shows no sign of slowing down, according to Retailers United



Published July 22, 2022
Micro-financing startup Klo… is getting ready for monster hit on Wall Street

Because you recently searched **for pharmaceutical stocks** — Updated 3 minutes ago



Published September 12, 2022
DrugInc's recent legal woes represent a unique opportunity for long position, according to F.H.W. Smith



Published August 9, 2022
With COVID-19 out of the m… are vaccines manufacturer… for growth?

Trending for individuals with a similar investment profile — Updated 6 hours ago



Published September 2, 2022
Growth stocks are in technical oversell territory. What does that mean for the average investor?



Published September 19, 2022
16 strategies for diversifying a declining portfolio without skipping on the upside

y order history

Last month | YTD | Custom | Filter orders

	DATE	STATUS	VOLUME	UNIT PRICE	PROCEEDS	GAINS
SHOP:NYSE	9/19/2022	In progress	1,000	USD42.90	USD4,290.00	USD3,440.12
SHOP:NYSE	9/18/2022	Executed	2,000	USD41.40	USD8,280.00	(USD425.45)
SHOP:NYSE	9/16/2022	On hold	1,000	USD38.10	-	-
DIS:NYSE	9/10/2022	Executed	2,000	USD128.90	USD257,800.00	USD38,440.12
DIS:NYSE	9/10/2022	Cancelled	200	USD120.45	-	-
NYSE	9/10/2022	Cancelled	150	USD112.23	-	-
NYSE	9/10/2022	Cancelled	10	USD109.67	-	-
	9/07/2022	Executed	2,000	USD41.40	USD8,280.00	(USD425.45)
	9/05/2022	Executed	1,000	USD42.90	USD4,290.00	USD3,440.12
	9/01/2022	Executed	1,000	USD42.90	USD4,290.00	USD3,440.12

10 of 25,234 See all →

Recommended reads from Acme's Investment Education Center

Based on your activity and portfolio



Options trading and covered calls with Acme[tm] →

Because you recently searched for *covered calls*



Strategic portfolio rebalancing for retirement →

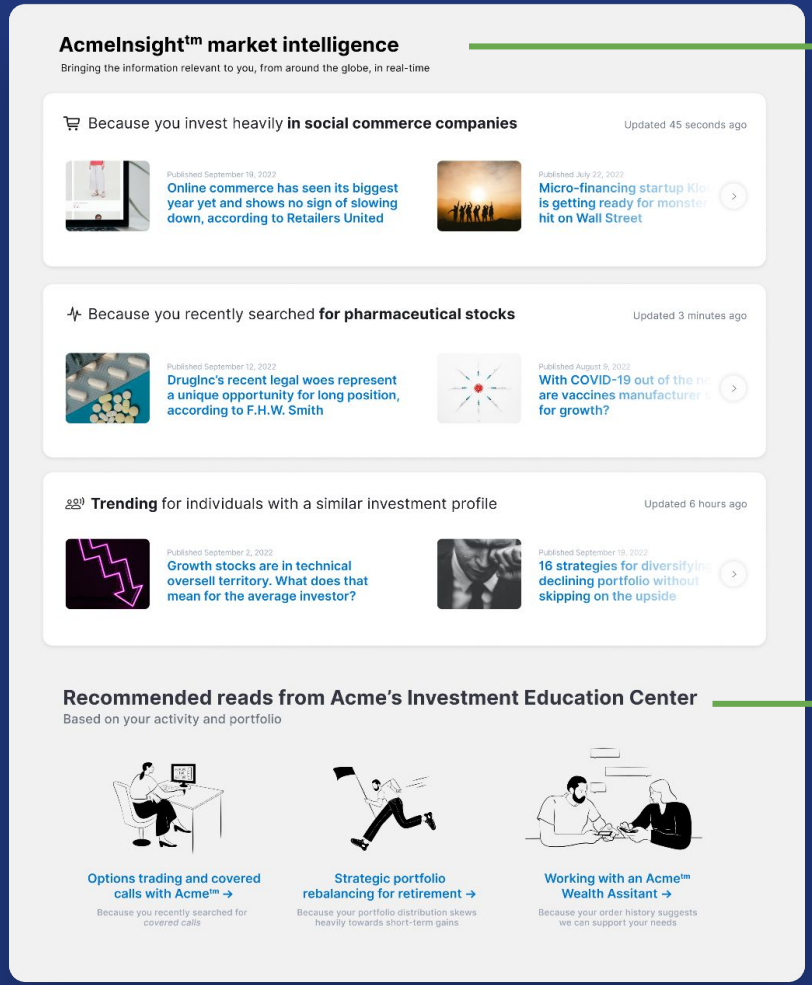
Because your portfolio distribution skews heavily towards short-term gains



Working with an Acme[tm] Wealth Assitant →

Because your order history suggests we can support your needs

116



Personalized recommendations based on user attributes and behavior

Made possible by a **unique combination of native machine learning techniques and vector search algorithms** to create a tailored content experience

Uniquely influenced by **customer behavior and traits data collected and stored directly within Elastic**, with an increasing amount of precision as more information is gathered

elastic

117

AAPL	Apple	$155.65	-4.5%
TWTR	Twitter	$38.60	+8.9%
TSLA	Tesla	$269.32	-12.2%

6 of 22 See all →

Because you recently searched for p



Published September 12, 2022
DrugInc's recent legal woes rep
a unique opportunity for long p
according to F.H.W. Smith

Trending for individuals with a simila



Published September 2, 2022
Growth stocks are in technical
oversell territory. What does th
mean for the average investor?

Month | YTD | Custom | Filter orders

	VOLUME	UNIT PRICE	PROCEEDS	GAINS
progress	1,000	USD42.90	USD4,290.00	USD3,440.12
ecuted	2,000	USD41.40	USD8,280.00	(USD425.45)
hold	1,000	USD38.10	-	-
ecuted	2,000	USD128.90	USD257,800.00	USD38,440.12
ncelled	200	USD120.45	-	-
ncelled	150	USD112.23	-	-
ncelled	10	USD109.67	-	-
ecuted	2,000	USD41.40	USD8,280.00	(USD425.45)
ecuted	1,000	USD42.90	USD4,290.00	USD3,440.12
ecuted	1,000	USD42.90	USD4,290.00	USD3,440.12

10 of 25,234 See all →

Recommended reads from Ac

Based on your activity and portfolio



Options trading and covered calls with Acme℠ →

Because you recently searched for *covered calls*

Str
rebalanc

Because you
heavily t



Mark H. @Acme
Cassandra B.

9/19/2022 2:02PM

Hi! How can I help you today?

Why is my order from 9/16 on hold still? Is it lost? HELP!

On hold orders are generally cleared within 72 hours.

Here are a few links to review:

Guide: **Reviewing a pending/held order →**

Forum: **List of On Hold scenarios with actions →**

Document: **Filing an On Hold Complaint →**

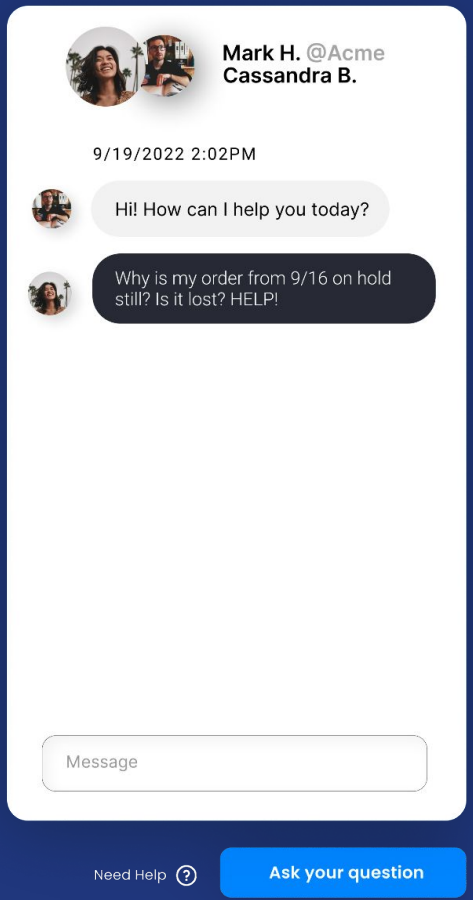
Message

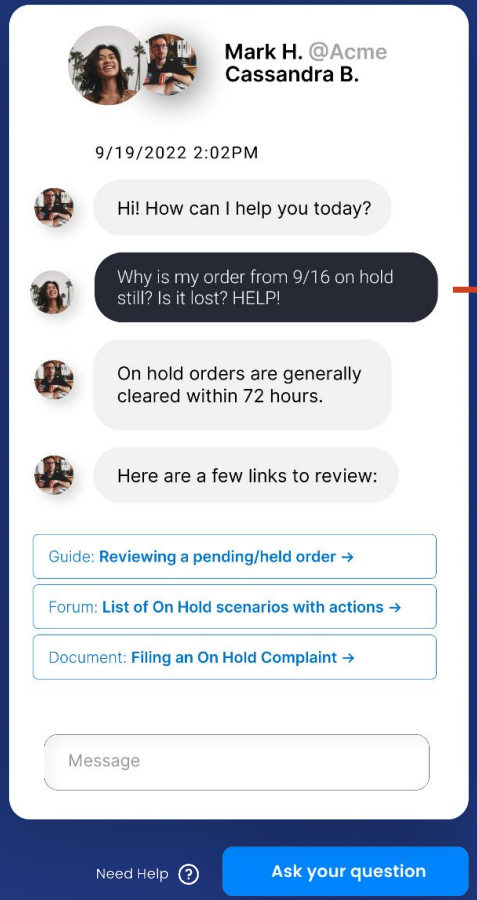
EURUSD	USDJPY	VIX	RUT	XOI	CADUSD	MXNUSD
1.0[illegible]^{6}	135.22^{9}	25.47	1809.23	1642.98	1.2326^{6}	0.05002^{9}
-0.54%	-0.31%	+11.46%	+0.31%	+1.06%	-0.54%	-0.31%

Need Help

Ask your question

118





Automate first-touch and instantly engage with customers, while mitigating support costs

Natural language understanding enabling human, conversational expression of intent in a variety of contexts

Question answering capabilities powered by unique combination of native machine learning techniques and vector search algorithms, from one or multiple data sources

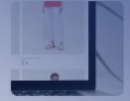
elastic

119



SQ	Square	$66.38	-8.9%
SNAP	Snap Inc.	$11.30	+1.5%
AAPL	Apple	$155.65	-4.5%
TWTR	Twitter	$38.60	+8.9%
TSLA	Tesla	$269.32	-12.2%

6 of 22 See all →



Published September 19, 2022
Online commerce has seen its biggest year yet and shows no sign of slowing down, according to Retailers United

Because you recently searched **for pharmaceutic**



Published September 12, 2022
DrugInc's recent legal woes represent a unique opportunity for long position, according to F.H.W. Smith

Trending for individuals with a similar investment



Published September 2, 2022
Growth stocks are in technical oversell territory. What does that mean for the average investor?

My order history

Last month | YTD | Custom | Filter orders

	ASSET	DATE	STATUS	VOLUME	UNIT PRICE	PROCEEDS	GAINS
	SHOP:NYSE	9/19/2022	In progress	1,000	USD42.90	USD4,290.00	USD3,440.12
✓	SHOP:NYSE	9/18/2022	Executed	2,000	USD41.40	USD8,280.00	(USD425.45)
	SHOP:NYSE	9/16/2022	On hold	1,000	USD38.10	-	-
✓	DIS:NYSE	9/10/2022	Executed	2,000	USD128.90	USD257,800.00	USD38,440.12
	DIS:NYSE	9/10/2022	Cancelled	200	USD120.45	-	-
	DIS:NYSE	9/10/2022	Cancelled	150	USD112.23	-	-
	DIS:NYSE	9/10/2022	Cancelled	10	USD109.67	-	-
✓	SQ:NYSE	9/07/2022	Executed	2,000	USD41.40	USD8,280.00	(USD425.45)
✓	SQ:NYSE	9/05/2022	Executed	1,000	USD42.90	USD4,290.00	USD3,440.12
✓	SQ:NYSE	9/01/2022	Executed	1,000	USD42.90	USD4,290.00	USD3,440.12

10 of 25,234 See all →

Recommended reads from Acme's Inve

Based on your activity and portfolio



Options trading and covered calls with Acme℠ →

Because you recently searched for *covered calls*



Strategic portfolio rebalancing for retireme

Because your portfolio distribution heavily towards

120



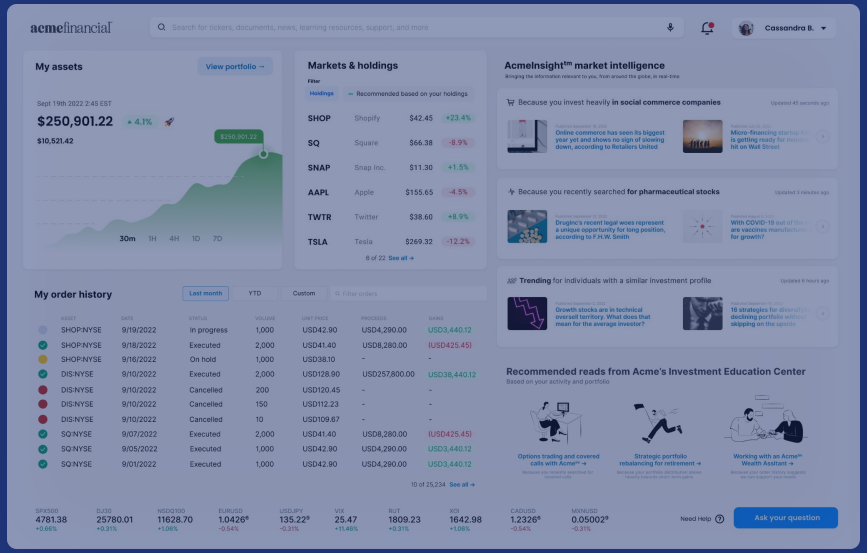
Surface critical information usually stored in systems not generally designed for consumption in end-user applications

Provide users with complete freedom to **analyze and review large amounts of historical data in milliseconds**

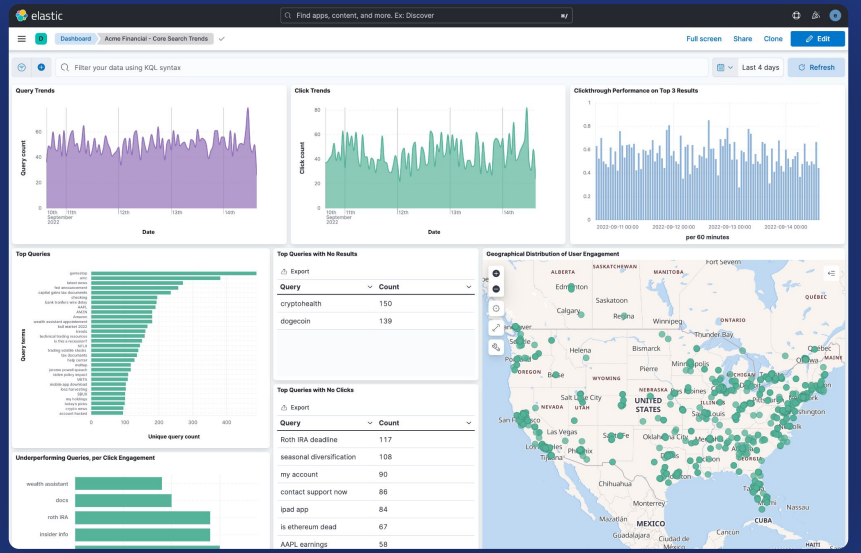
Keep user data safe with tight security controls for sensitive, personal data

elastic

121

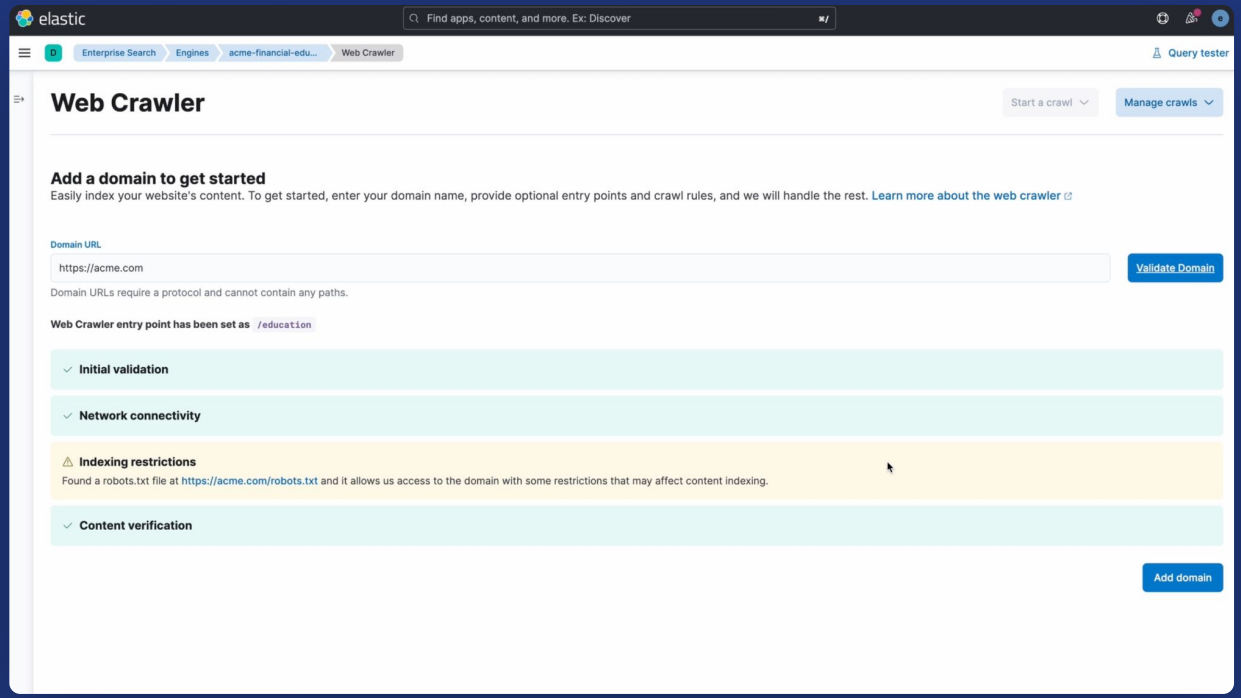


Delivering search-powered applications



Analyzing behavior and tailoring outcomes

122

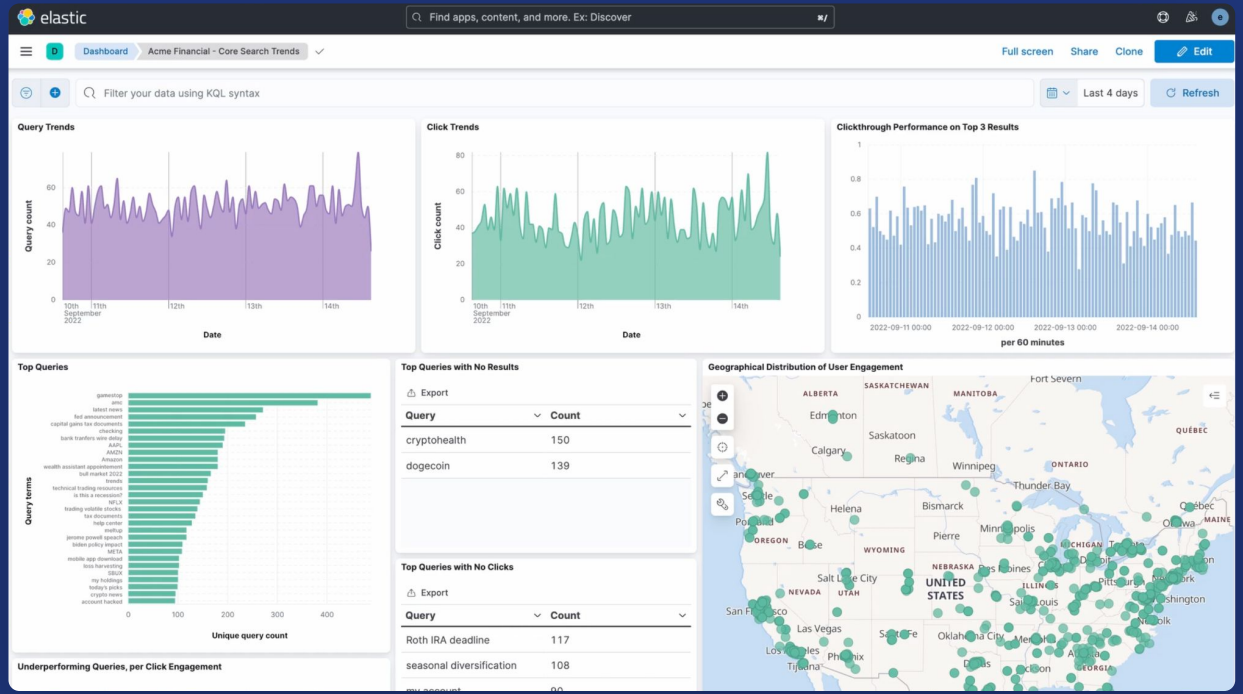


Onboard any data within seconds on Elastic Cloud with broad portfolio of ecosystem integrations to the most adopted enterprise business systems

Continuously scale searchable datasets with a few clicks at any point in time, with no operational downtime

elastic

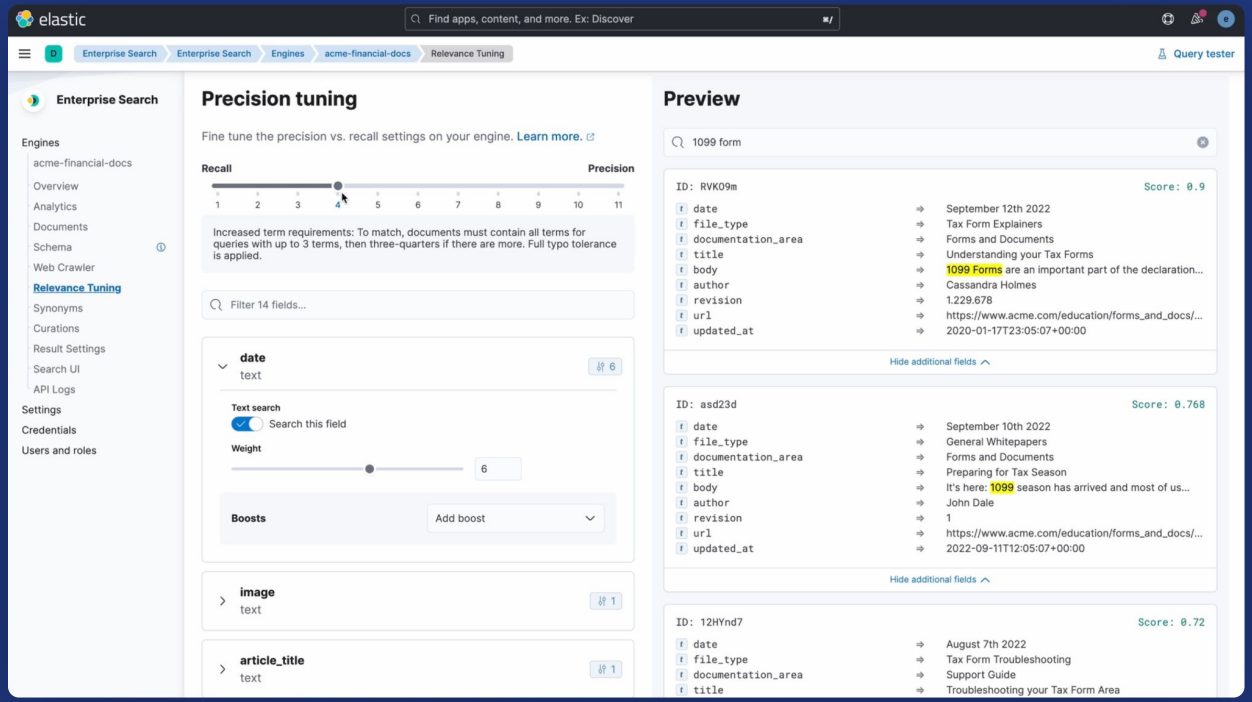
123



User behavior and characteristics automatically captured and stored along with searchable data

Understand and analyze information about users, including search behavior, actions taken, content viewed and more

124

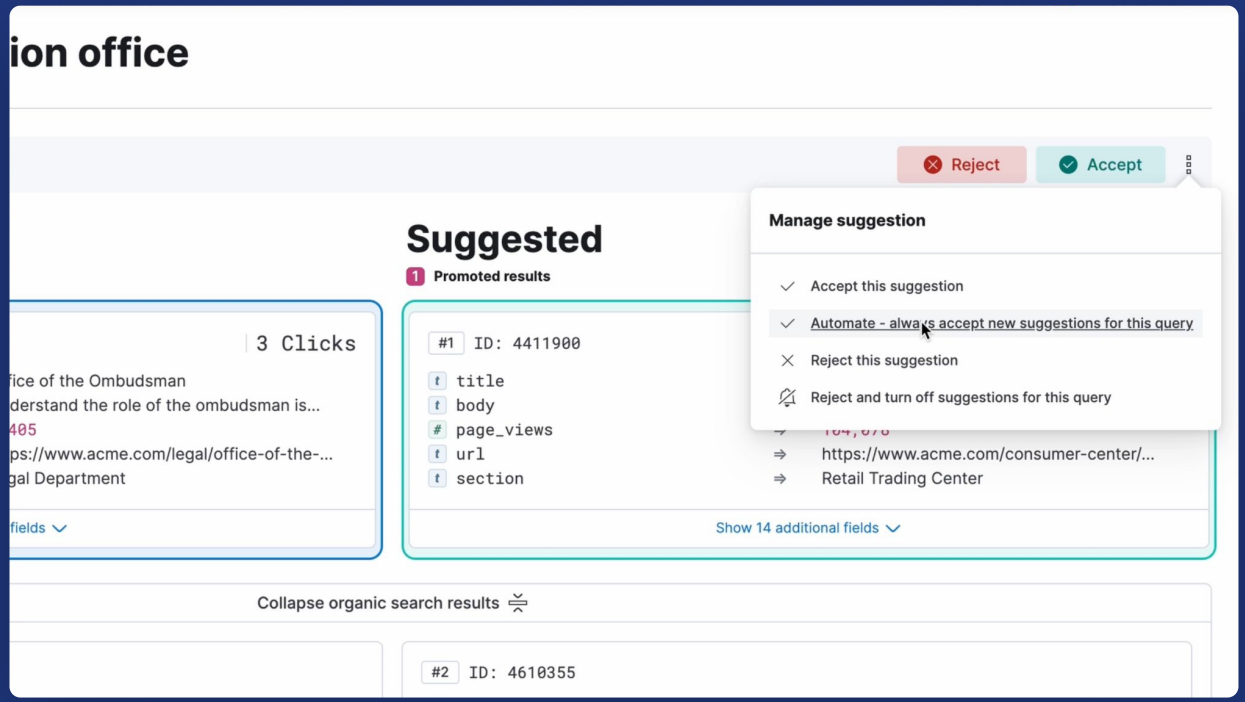


Take immediate action based on user behavior and business objectives and key performance metrics

Automate relevance improvements with intelligent suggestions designed to leverage global and local behavioral trends

elastic

125

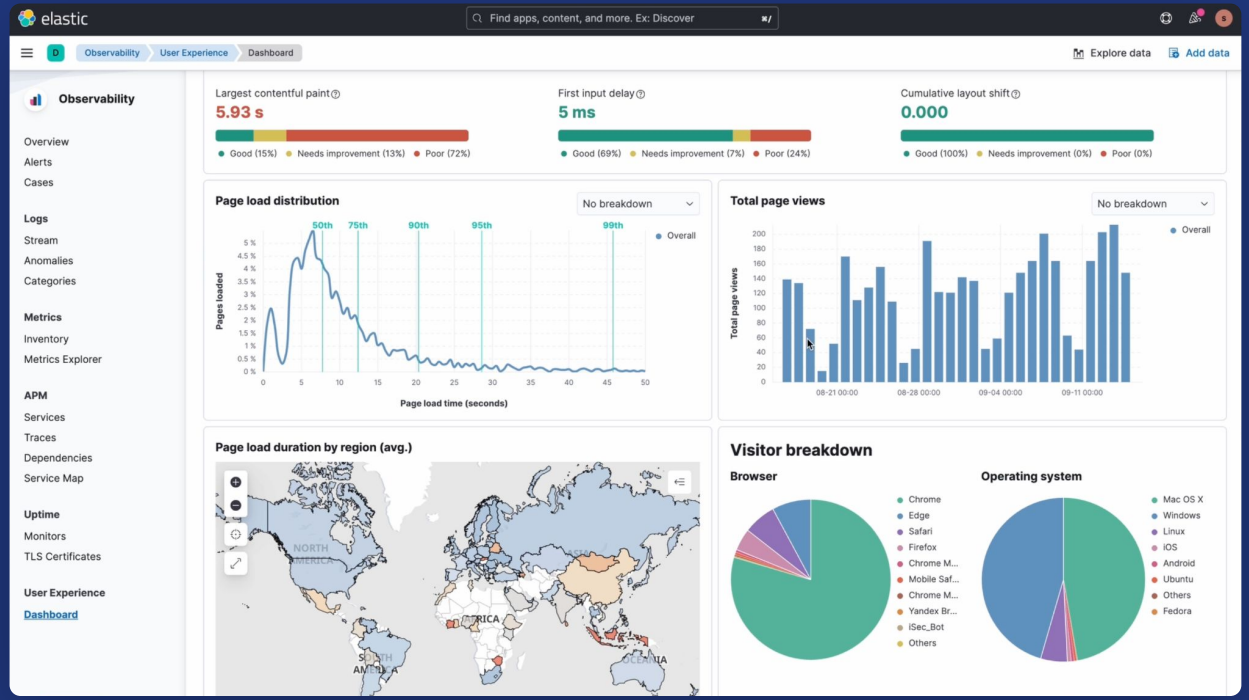


Take immediate action based on user behavior and business objectives and key performance metrics

Automate relevance improvements with intelligent suggestions designed to leverage global and local behavioral trends

elastic

126



Native search experience instrumentation with Elastic Observability, all from a single pane of glass

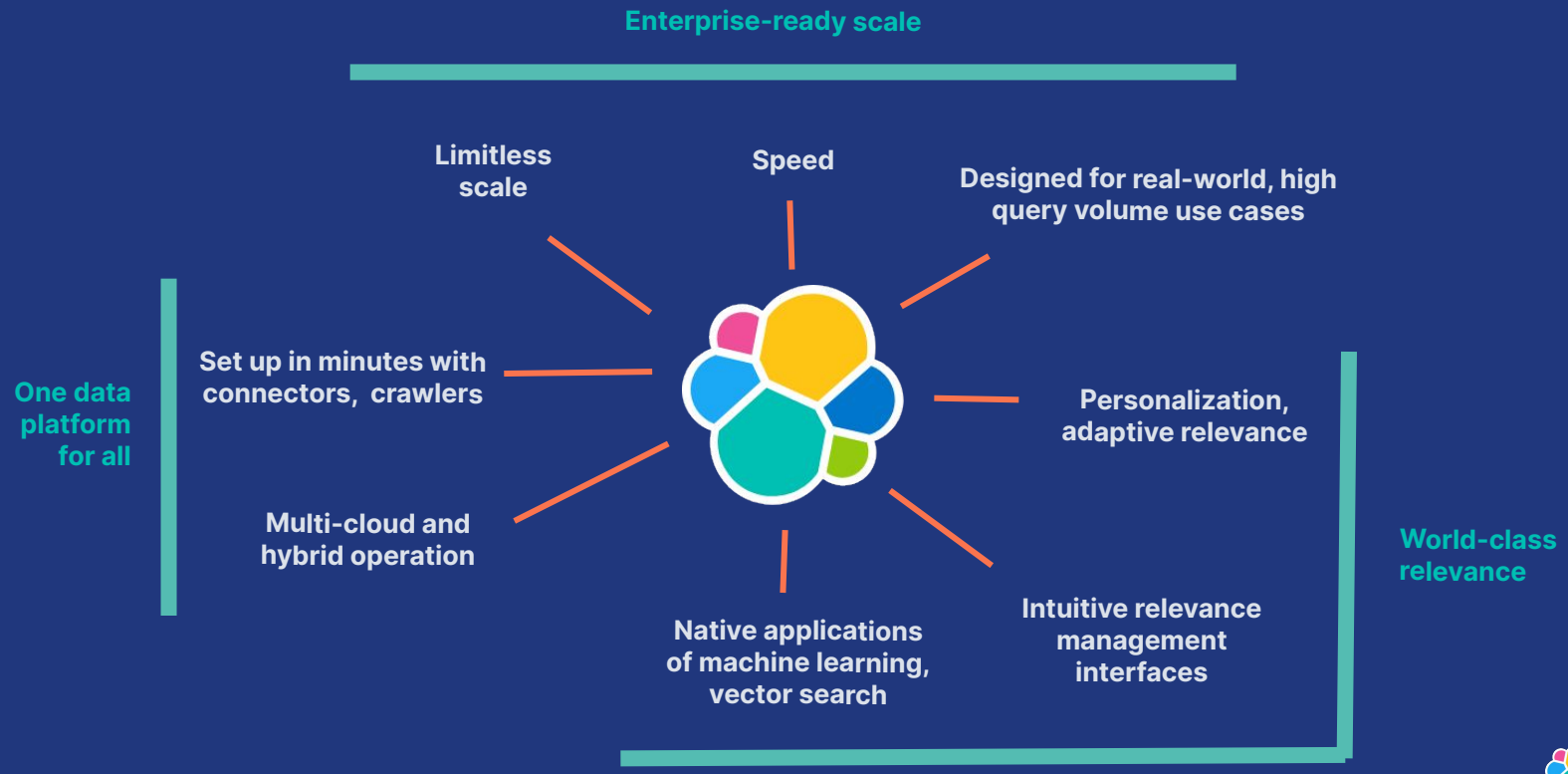
Find bottlenecks or optimization points for the most fine-tuned performance, at any scale

elastic

127

Unique dimensions of Elastic Enterprise Search

Delivering tailored relevance at scale



elastic

128

Accelerating GTM



Michael Cremen

Chief Sales Officer

- **Account Exec** to **Chief Sales Officer**
- **International / Local Experience**
- **20 years in Data**
- **1 year at Elastic**

IBM HITACHI COHESITY VERITAS

elastic

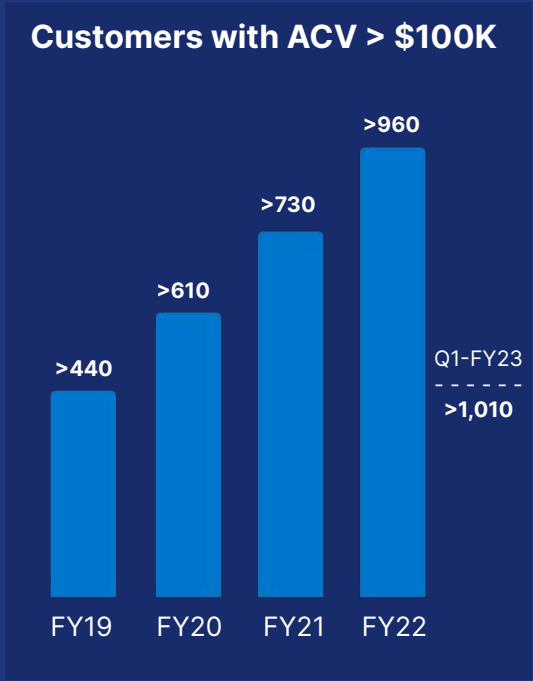
The Elastic Opportunity

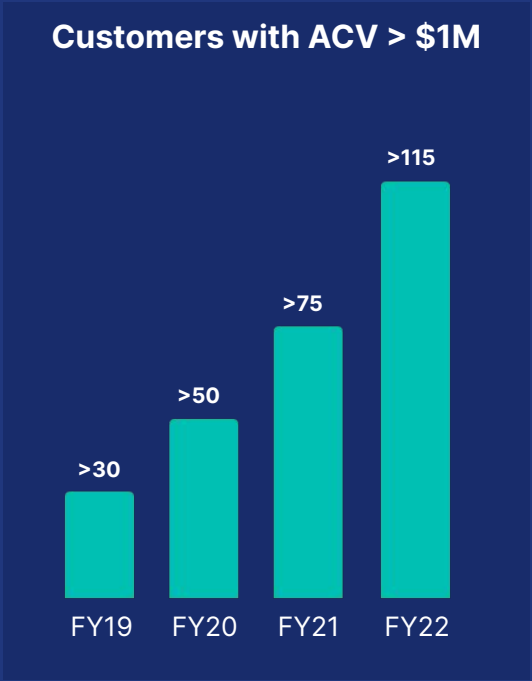
Why I’m Excited About Elastic’s Future

elastic

Market and enterprise traction







elastic

Customers are increasingly choosing Elastic Cloud

Cloud % of **Total Revenue**

FY19	FY20	FY21	FY22
17%	22%	27%	35%

>50% of new logo dollars in Q1FY23

elastic

Why we are Winning



Differentiated Value — One platform, hybrid deployment, one price model



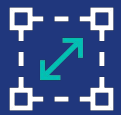
Cloud — Any hyperscaler, monthly or annual contract



Open Heritage — Large Elastic community, bottom up entry point

elastic

Opportunity to Scale GTM



Customer base — Top Down to Expand



Sales force — Growing and evolving sales force



Ecosystem — Who want to do more with us (Hyperscalers, MSPs, MSSPs, GSIs, partners)

elastic

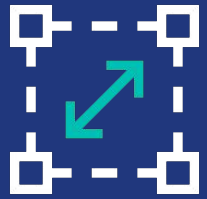
$2B and beyond



Cloud acceleration



Enterprise focus



Expansion across platform

elastic



Cloud Acceleration

Cloud Customer Journey



Go to market



Onboarding customers



Sales motion

elastic



Cloud Acceleration







Ecosystem Leverage



Hyperscaler $150B+*

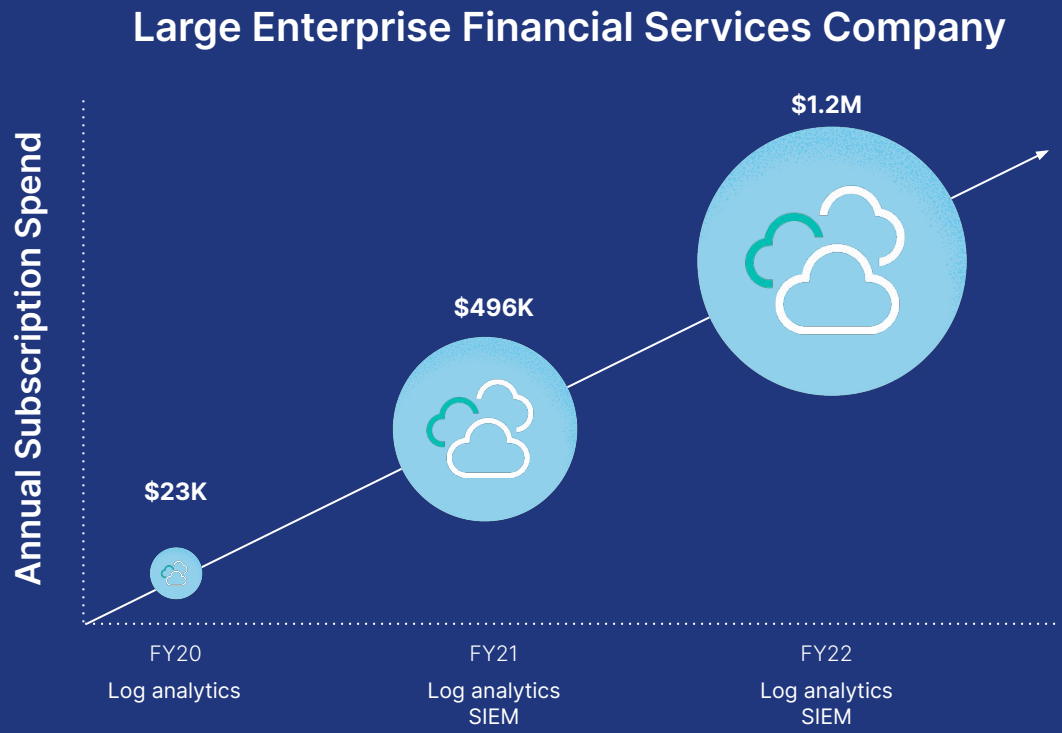


MSP / MSSP / GSI

* $100B AWS (CY22Q2 earnings call), $51B GCP (2021-Q4 Earnings Call), Azure (not published)

elastic

Cloud Acceleration



elastic



Enterprise Focus

Field Focus

- Segmentation / Verticals
- Investment in Enterprise Coverage
- SMB PLG / Automation
- Resource Alignment

elastic



Enterprise Focus

Sales Strategy

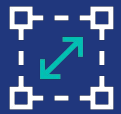
- Field operating system
- Sales methodology
- Talent / development
- Selling motion

elastic



Enterprise Focus

New Customer

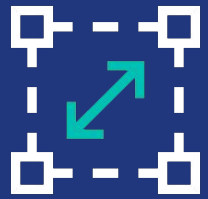


Acquisition / enterprise



Outbound motion (SDR)

elastic

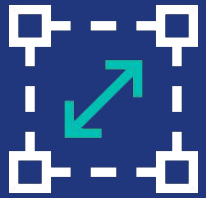


Expansion Across the Platform

Customer Cross-sell

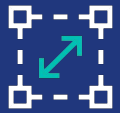
- Net new workloads / solutions
- Outbound takeout / consolidation
- Single pricing model
- Agility via Cloud

elastic



Expansion Across the Platform

Enablement & Instrumentation



Finding whitespace with C360



ID Opportunities for customer value



Upsell with ML/AI



Platinum to Enterprise

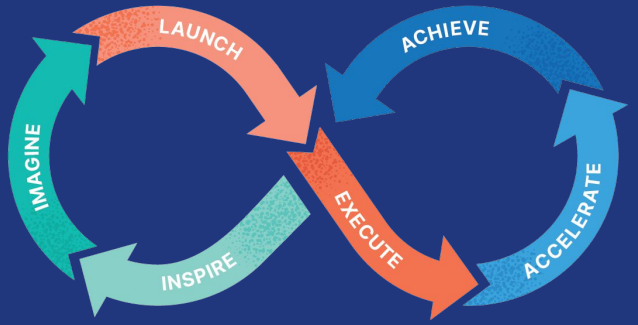
elastic

Expansion Across the Platform

Strategic Selling Methodology

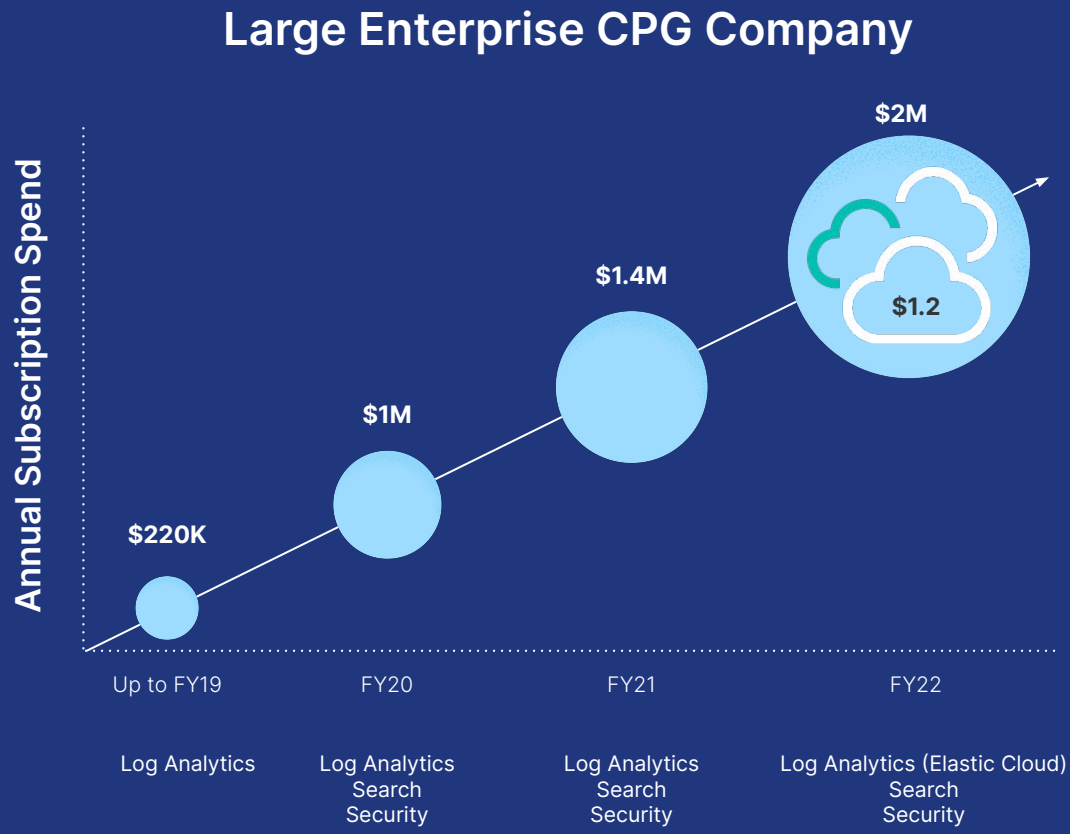
Customer buying journey

Customer lifecycle



elastic

Expansion Across the Platform



elastic

Customer Panel



Rick Laner

Chief Customer Officer

- Consultant to Chief Customer Officer
- International / Local Experience
- 20+ years in Customer Success, Services leadership
- 1 year at Elastic

salesforce MuleSoft splunk> bmc

elastic

Customer Panel

SAP Concur

USAA®

ECOLAB



Marcel Matus
Development Manager



Biji John
Director, Cloud Security



Kevin Serafin
Director, Incident Response

elastic

Journey to $2B with Profitable Growth

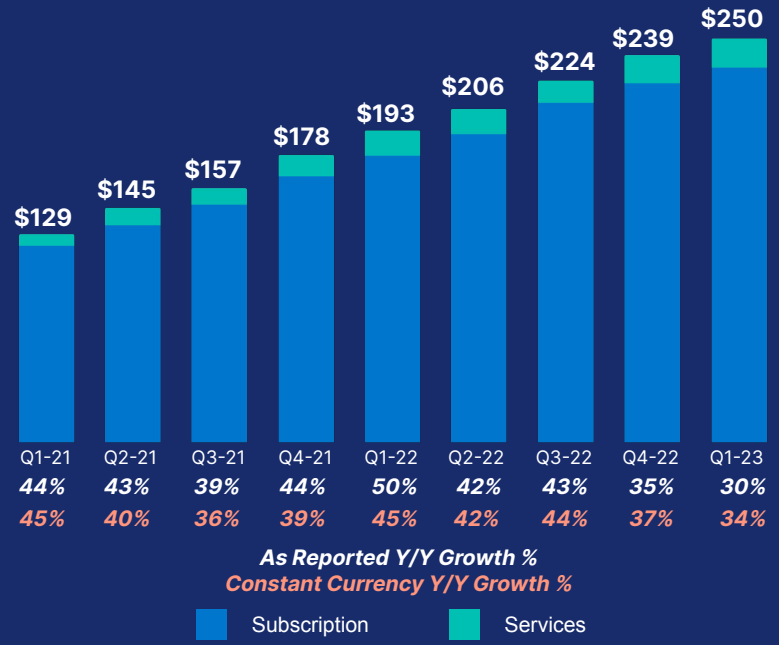


Janesh Moorjani
CFO and COO

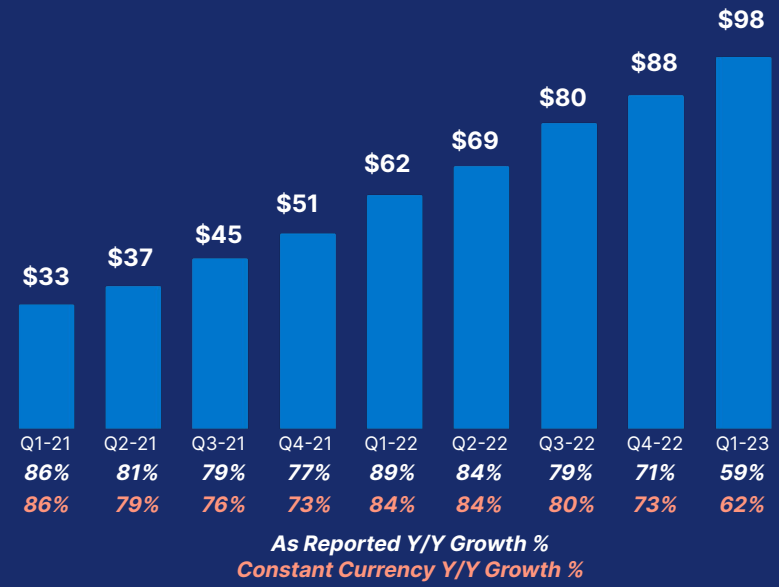
elastic

Strong track record of driving growth

Total Revenue
$ millions



Cloud Revenue
$ millions



elastic

149



Durable Growth – Path to $2B



Driving Profitable Growth

elastic

150



Durable Growth – Path to $2B



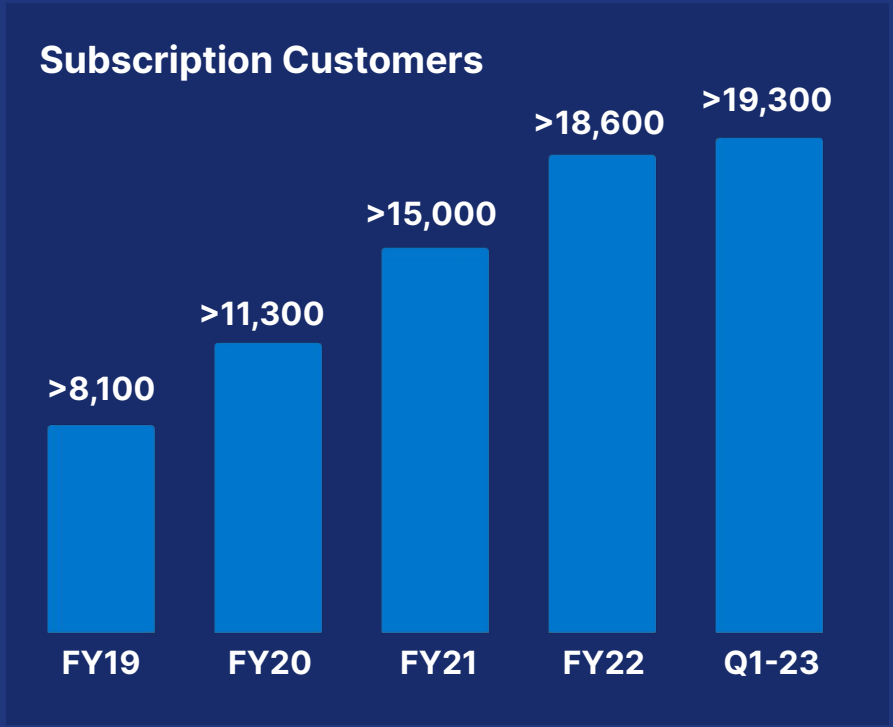
Customer Model
Land & Expand



Deployment Model
Cloud and Self-managed

151

Rapid, Diversified Customer Growth



elastic

152

Customers among the top 10 companies of each industry



10/10

Software Companies



10/10

Media



9/10

Aerospace & Defense



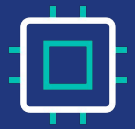
9/10

Telecom Services



9/10

Consumer Durables / Auto



8/10

Technology Hardware & Equipment



7/10

Healthcare Equipment & Services



7/10

Shipping & Transportation



6/10

Utilities

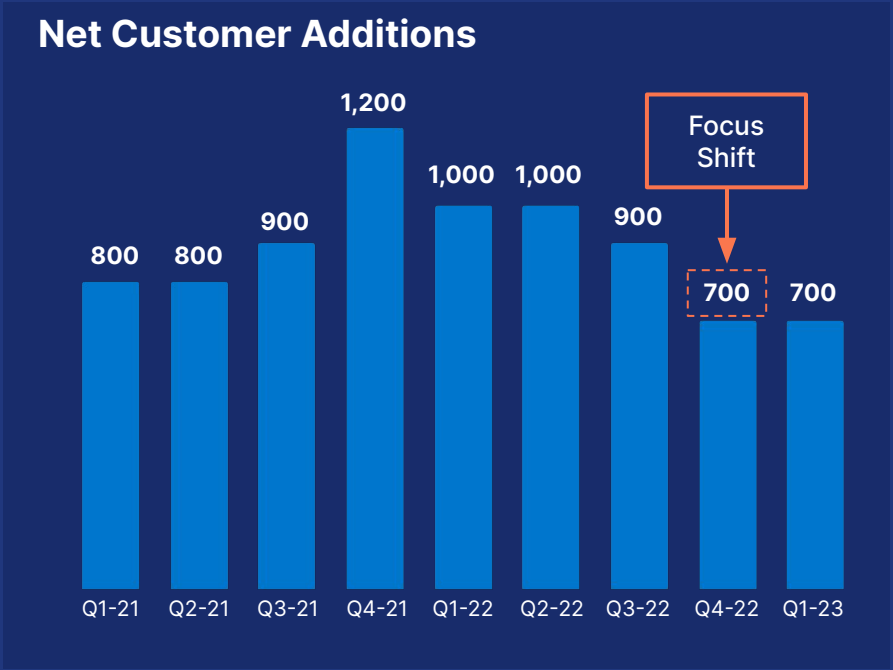


6/10

Diversified Financials

153 As of Q1-23

Strong rate of new customer additions

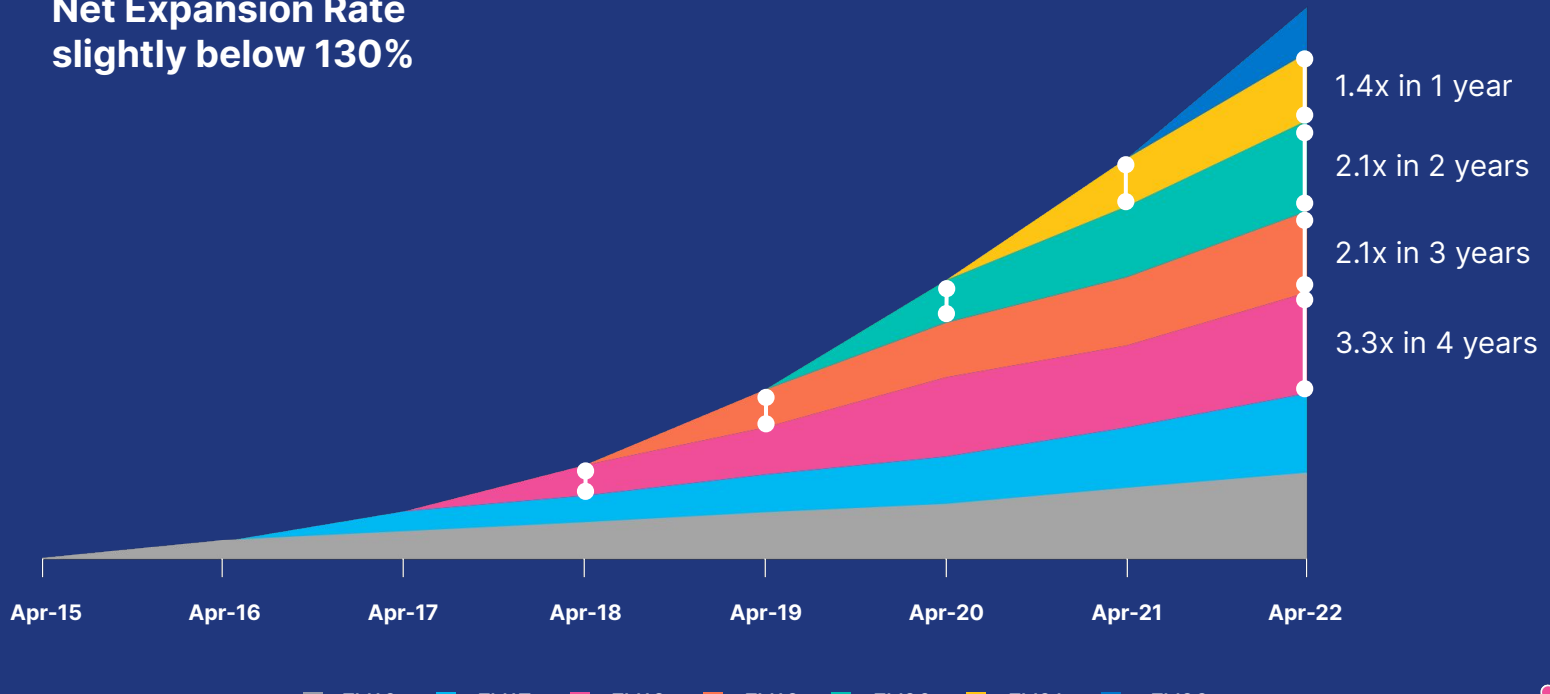


- Over 90% of new customers landed on Cloud
- Monthly Cloud is predominant customer acquisition motion
- Deliberate change in customer acquisition approach starting Q4 22, to focus on customers with greater propensity to buy/expand
  - Leads to higher consumption revenue
  - Leads to better unit economics

154 Net Customer Additions represents quarterly change in reported total subscription customers

Strong expansion across cohorts

Net Expansion Rate slightly below 130%



elastic

155

Elastic's Expansion Vectors



As customer data volume grows



As customers adopt more use cases



As customers adopt more solutions

Almost 400 customers >$100K ACV with 2+ solutions



As customers adopt the cloud

39% of revenue via Cloud, Q1 FY23

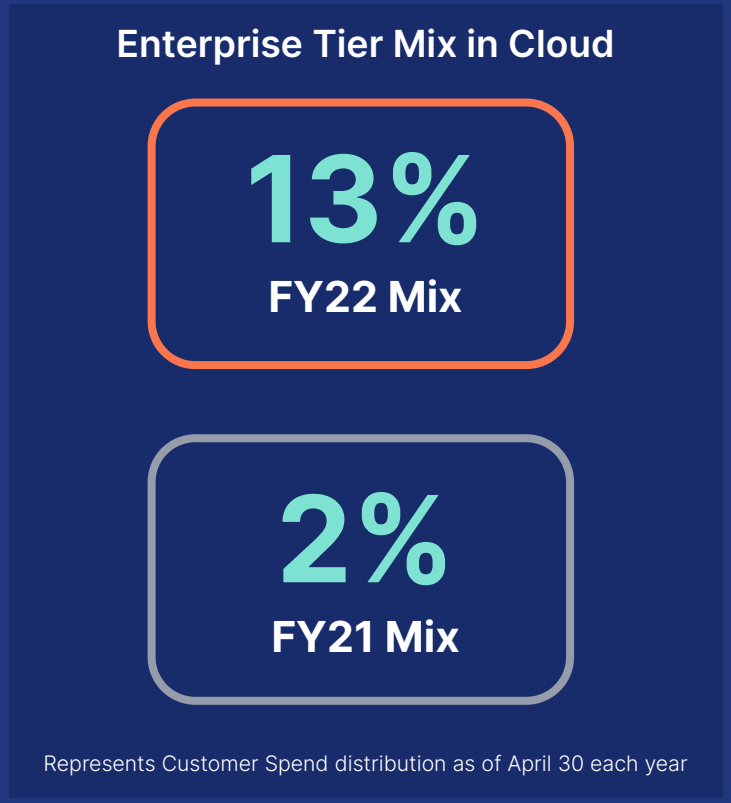


As customers adopt higher subscription tiers

Enterprise tier is the fastest growing tier for Cloud customers

elastic

Cloud Enterprise Subscription tier growing the fastest

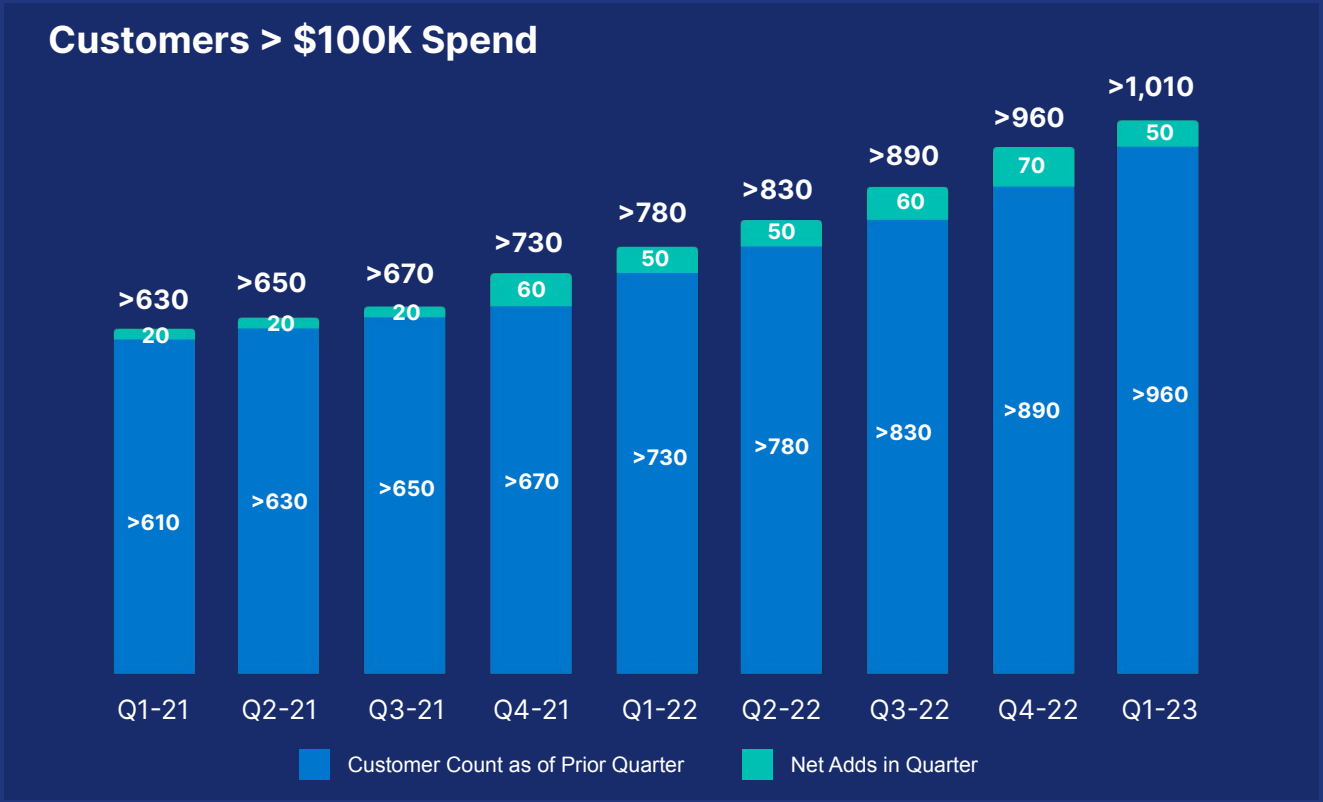


- Enterprise typically 30%-40% list price uplift vs Platinum
- Driven by our innovation engine:
  - Hybrid cross-cluster search & replication
  - Searchable Snapshots
  - Searchable Cold & Frozen storage

elastic

157

Strong expansion reflected in customer count >$100K

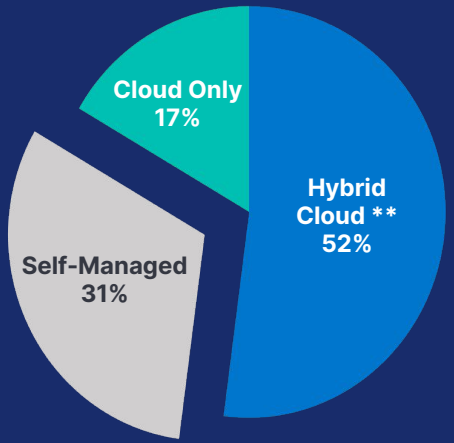


elastic

158

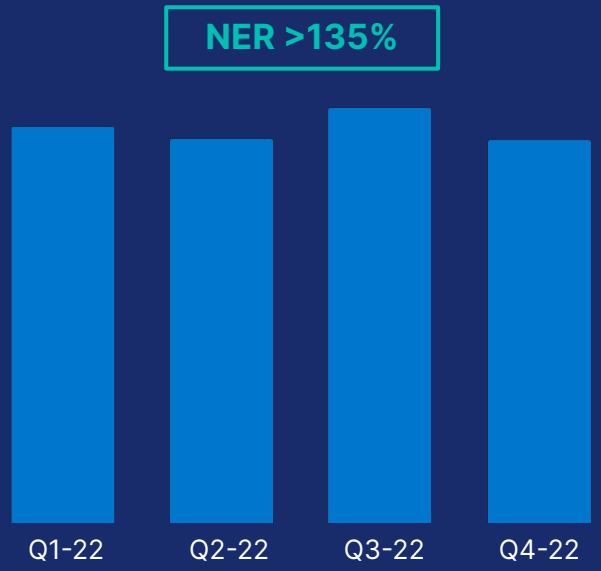
...With significant Cloud opportunity and robust NER

Hybrid Cloud Customers represent significant Cloud expansion opportunity within > $100K Band *



* Based on annual customer spend of > $100K customers at end of FY22
** Hybrid = Customers with both Cloud and Self-Managed contracts

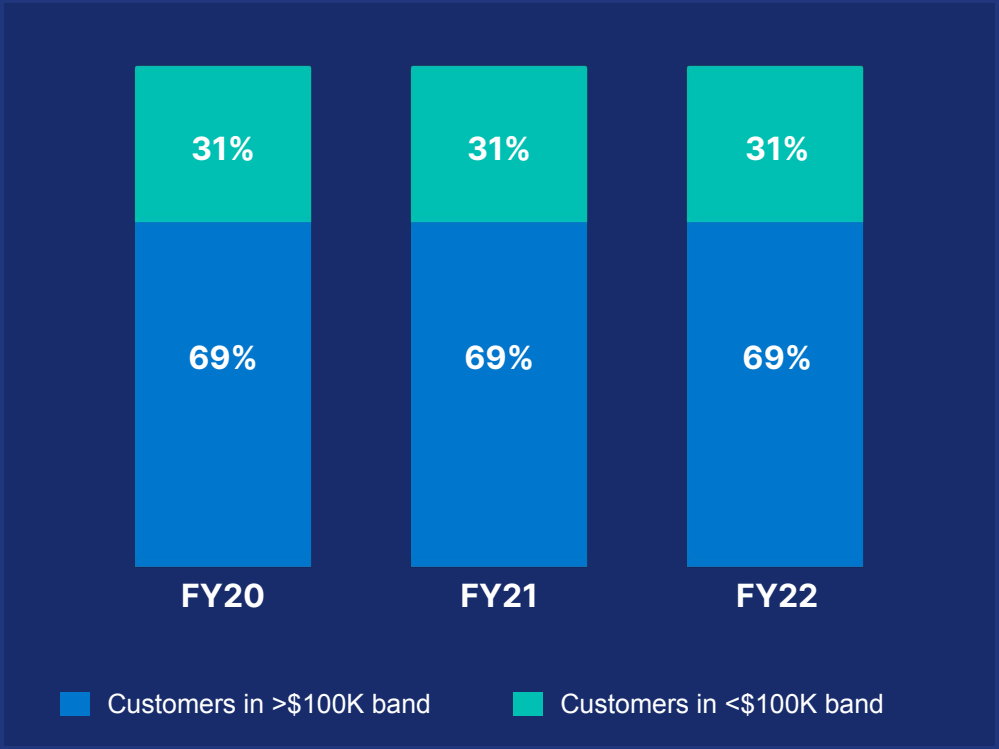
NER For Customers in >$100K Band



elastic

159

Customers >$100K ACV account for 69% of customer spend

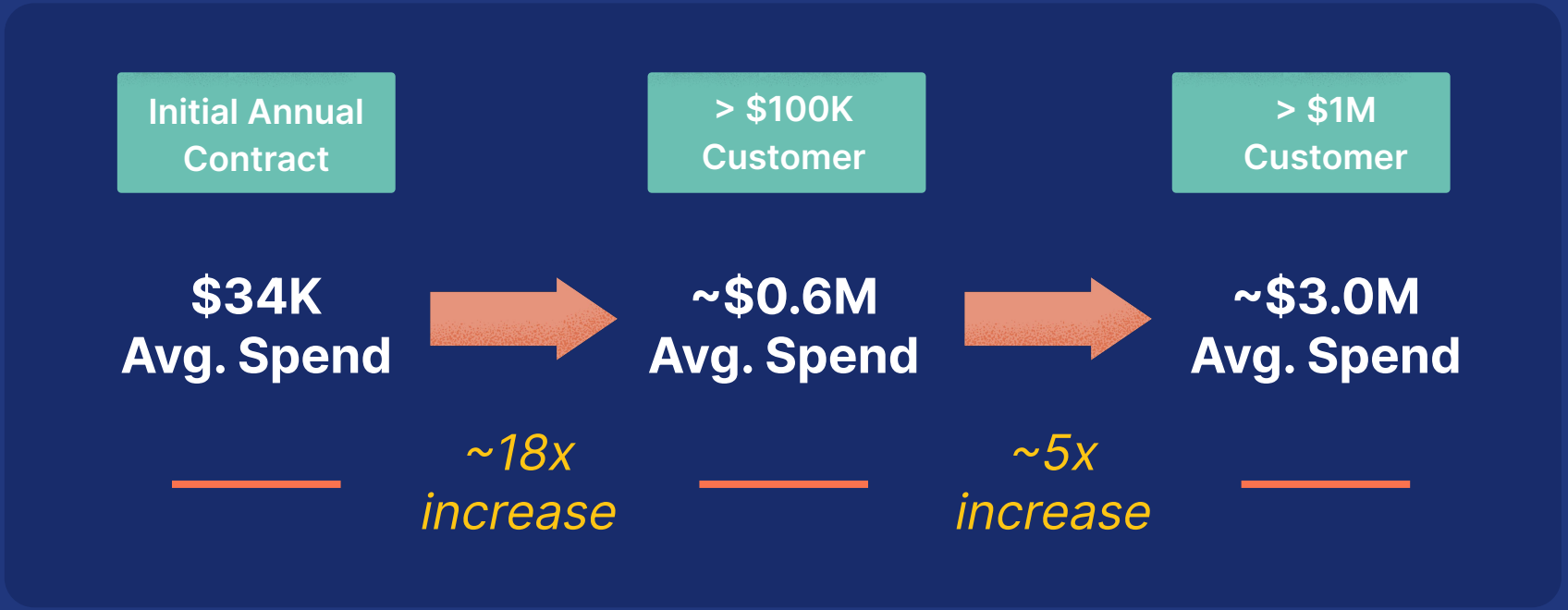


- Customers over $100K ACV have constituted 69% of customer spend on subscriptions in each of FY20, FY21 and FY22
- Consistent mix from:
  - Strong new customer additions and expansion <$100K
  - Expansion >$100K

Customer Spend is the sum of all customers' ACV, or in the case of customers charged on usage-based arrangements, their annualized usage. Excludes Services.

160

Significant opportunity to drive wallet share expansion



161 Excludes Services

Revenue build framework

	FY22
>$100K Customers (end of year)	960+
x Annualized Spend / Customer ($M)	$0.6
÷ Mix	69%
= Total Annual Customer Spend ($B)	**$0.9B**
Subscription Revenue during Year	**$0.8B**
Services Revenue	**$0.1B**
Total Revenue	**$0.9B**

Numbers rounded for presentation purposes. Underlying calculations use more precise measurements.
Annual Customer Spend excludes Services.

162

Bridge to $2B

	FY22	Illustrative Scenario →	FY25
>$100K Customers	960+	45 new customers / qtr	1,500+
x Annualized Spend / Customer ($M)	$0.6	18% annual growth (NER is significantly higher)	$1.0
÷ Mix	69%	Maintain mix	69%
= Total Annual Customer Spend ($B)	**$0.9B**		**$2.2B**
Subscription Revenue	**$0.8B**	No changes in rev rec	**$1.9B**
Services Revenue	**$0.1B**	No change in % of total revenue	**$0.1B**
Total Revenue	**$0.9B**		**$2.0B**

** Numbers rounded for presentation purposes. Underlying calculations use more precise measurements. Annual Customer Spend excludes Services.

elastic

163

Bridge to $2bn: Core assumptions

Assumption	Observations
45 quarterly net adds >$100K	• Significantly stronger historical track record • Not dependent on new logos – Projected 1,500+ customers (compared to existing base of 3,000+ enterprise & public sector accounts)
18% spend growth per customer	• Net Expansion Rate is already over 135%, representing significant upside potential • New customers expand rapidly
69% mix from >$100K customers	• Same mix as FY20-FY22

164

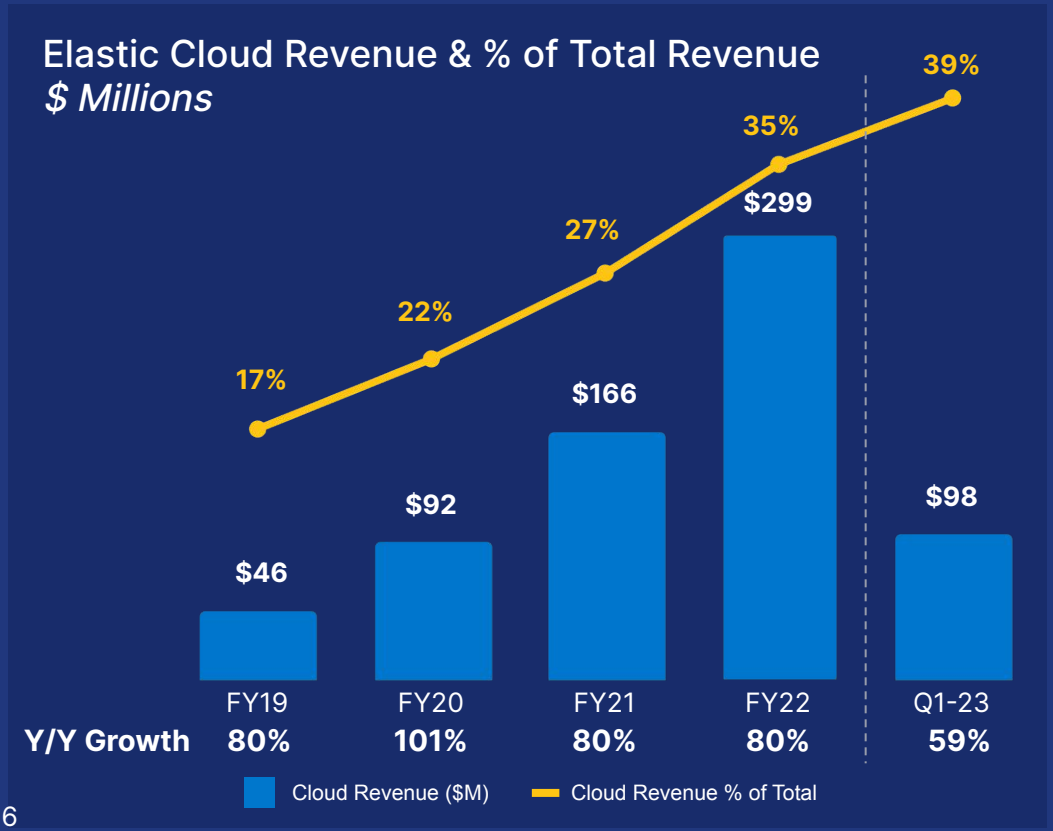


Deployment Model

Cloud and Self-managed

165

Robust Elastic Cloud growth



elastic

Sustaining the Cloud Momentum



Track record of growth at scale

~$400M run-rate with 62% Y/Y CC growth



Organic Growth

Expansion from workload growth, not driving forced migrations from self-managed



Strong customer acquisition

>90% of customers land on Cloud



Robust expansion

>140% NER for several quarters: expand within and across solutions; upsell to Enterprise tier



Strong Consumption Patterns

Resilient use cases;
Customer success investments



Sustained, Organic Mix Shift to Cloud

39% of **Total Revenue**
32% in **Q1 22**
25% in **Q1 21**



GTM Momentum

Marketing motions, Field performance, Compensation, Customer 360

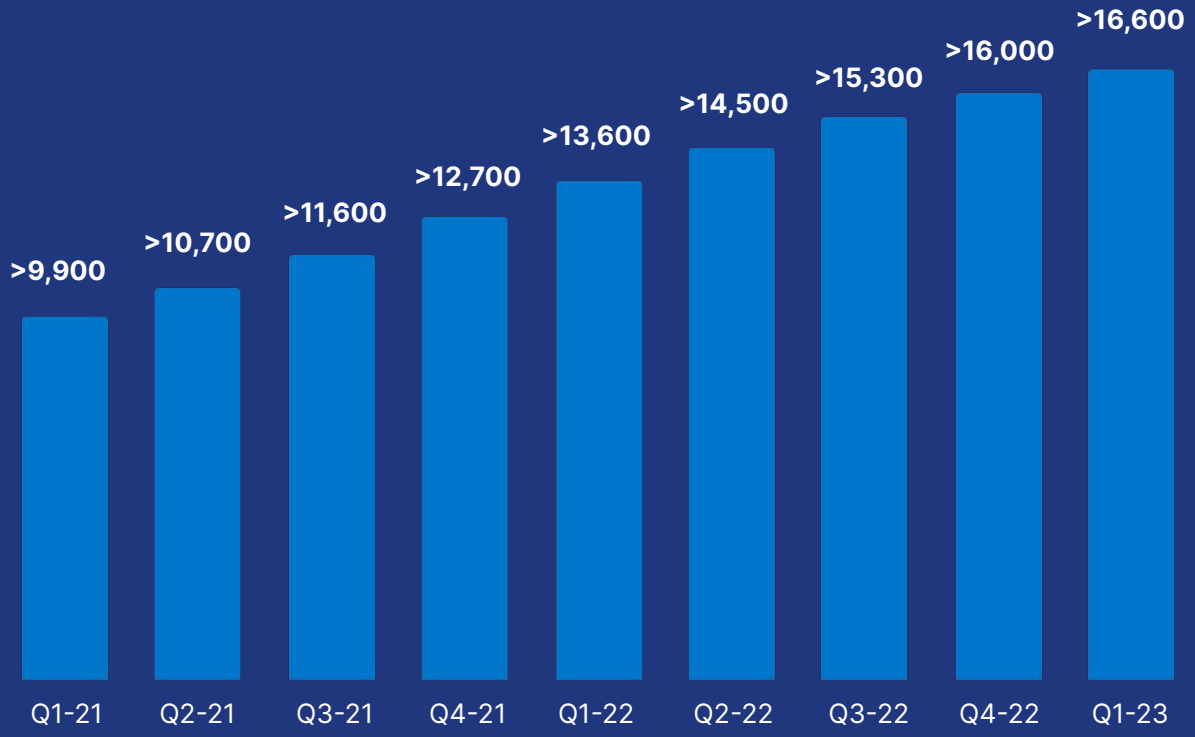


Thriving Hyperscaler Partnerships

>100% revenue growth

Data as of Q1 FY23, unless stated otherwise; CC = Constant Currency

Elastic Cloud customer growth



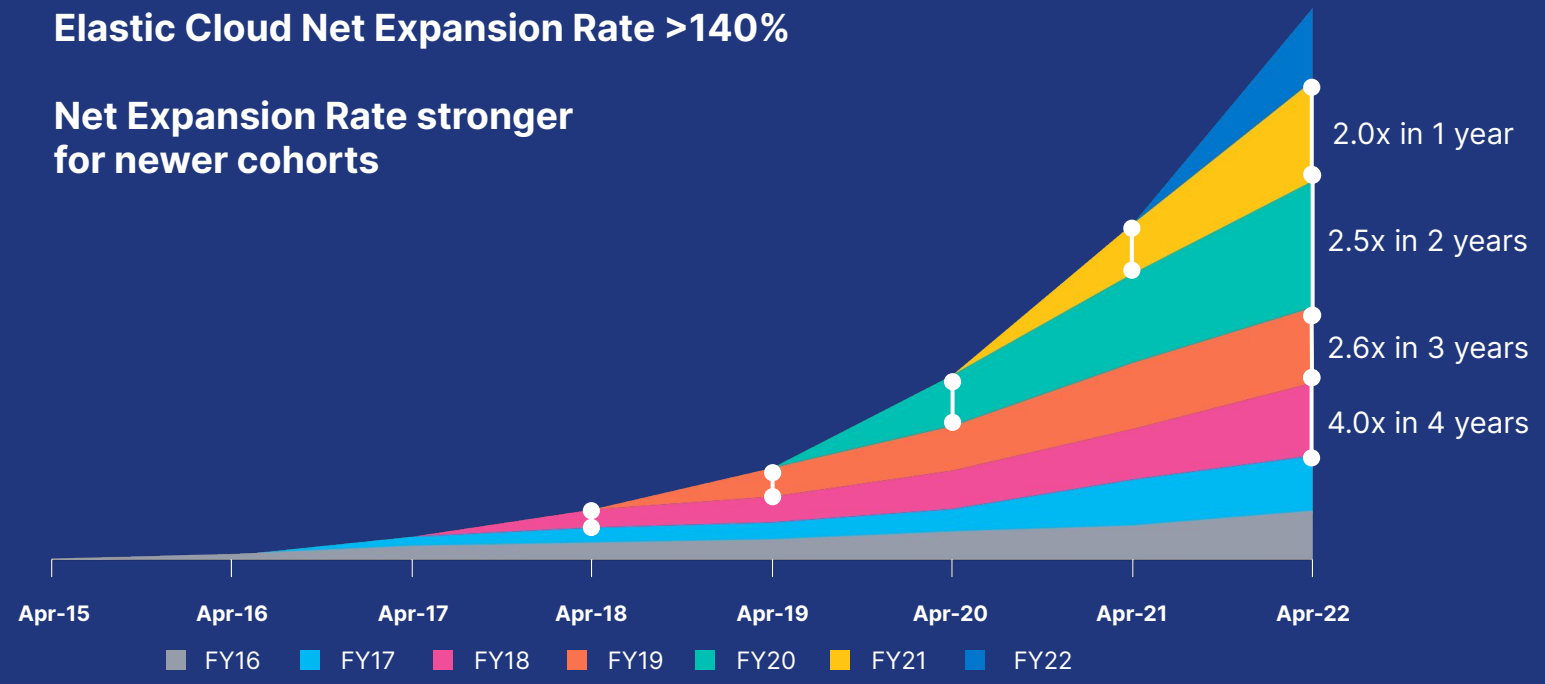
Includes customers with Hybrid Cloud deployments

elastic

Strong expansion across cohorts in Cloud

Elastic Cloud Net Expansion Rate >140%

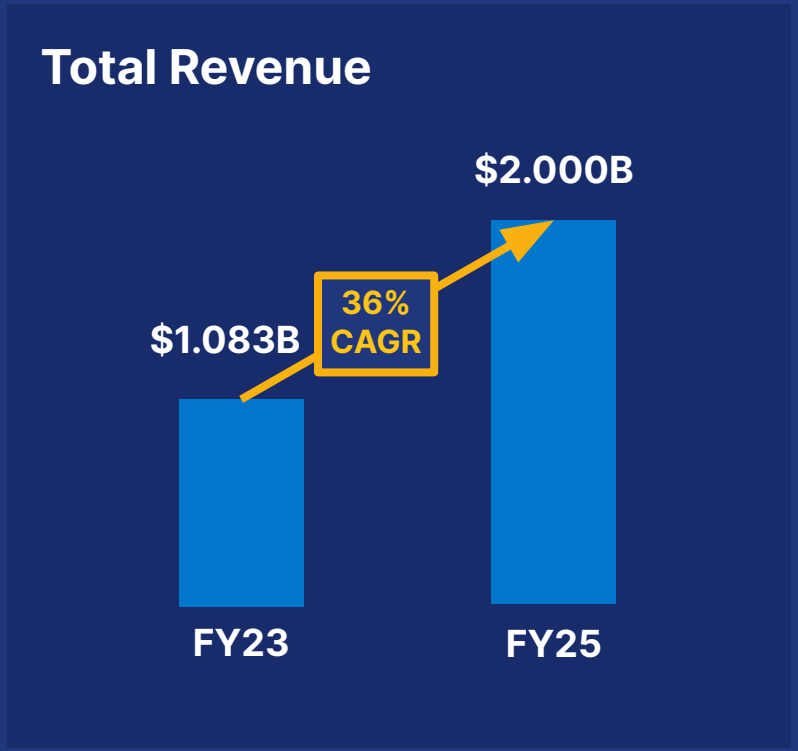
Net Expansion Rate stronger for newer cohorts



elastic

169

FY24 and FY25 Growth Model



- Strong start to FY23 revenue growth
  - Q1 23: 34% Y/Y CC
  - Q2 23: 32% Y/Y CC guidance
- Increased cloud mix of ~6%-7% per year provides natural Y/Y growth acceleration of ~3% in FY24 and additional ~3% in FY25
- Self-managed grows at natural rate (no forced installed base migration)

FY23 revenue and growth rate represent mid-point of guidance issued on August 25, 2022.

CC= Constant Currency

elastic

170



Driving Profitable Growth

171

Operating leverage inherent in the model

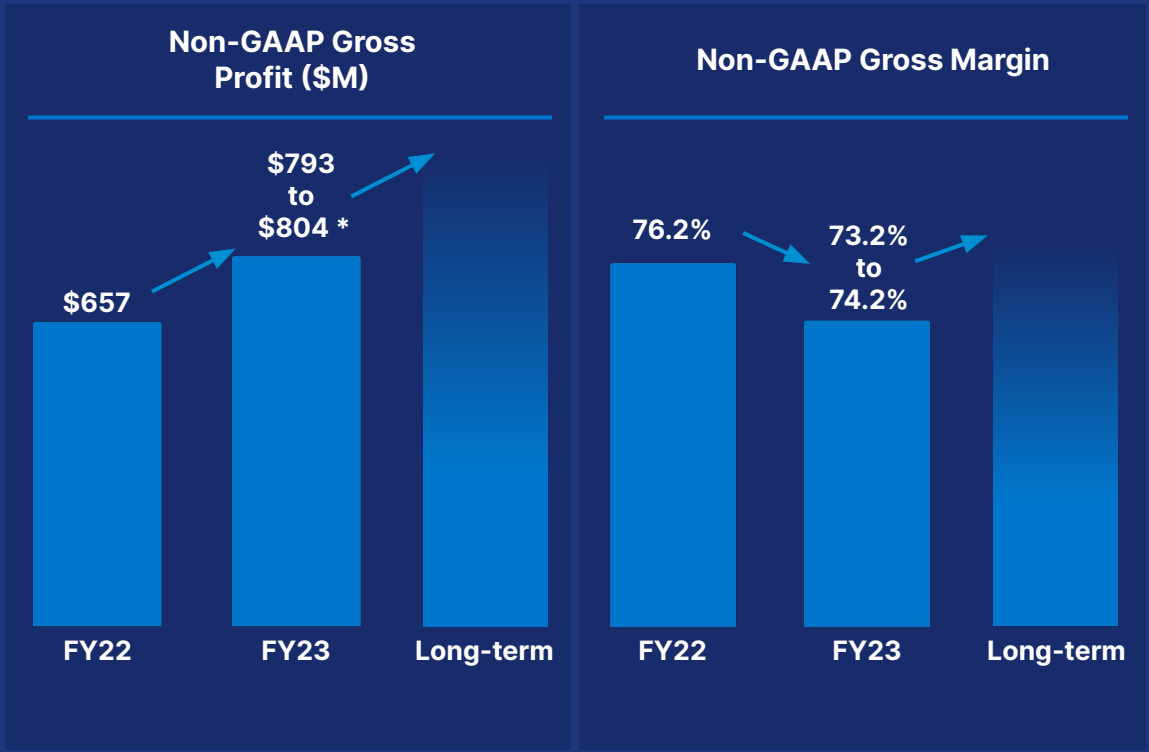
	FY18	FY22	FY23*
Non-GAAP Operating Margin %	-20.0%	0.1%	0.5%
Adjusted Free Cash Flow Margin %	-14.9%	1.2%	Slightly positive

FY23: Absorbing ~200-300 bps gross margin impact from Cloud mix shift plus return of travel (~$8M-$12M)

** Guidance midpoint/outlook as previously provided on August 25, 2022*

172

Non-GAAP gross margin leverage



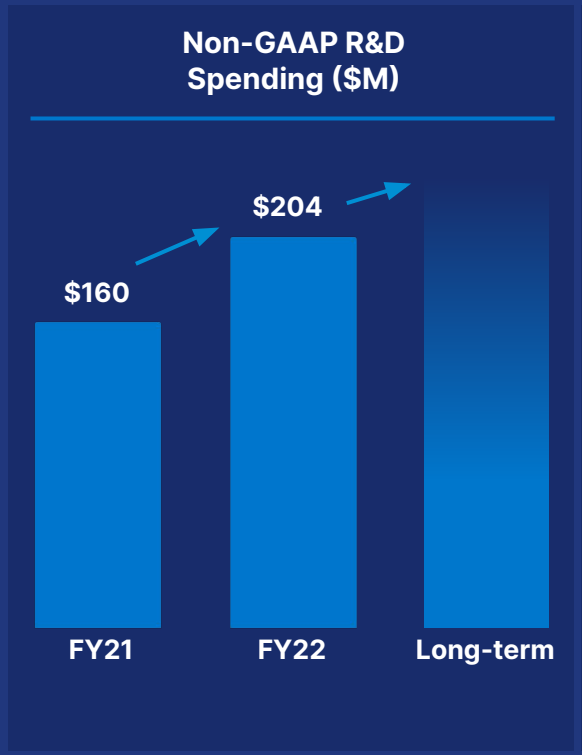
- Elastic Cloud to remain a modest headwind to FY23 non-GAAP gross margin (~200-300 bps)
- Non-GAAP gross margin leverage through:
  - Higher Enterprise tier mix
  - Investments in product architecture
  - Infra cost efficiencies
  - Operational efficiencies

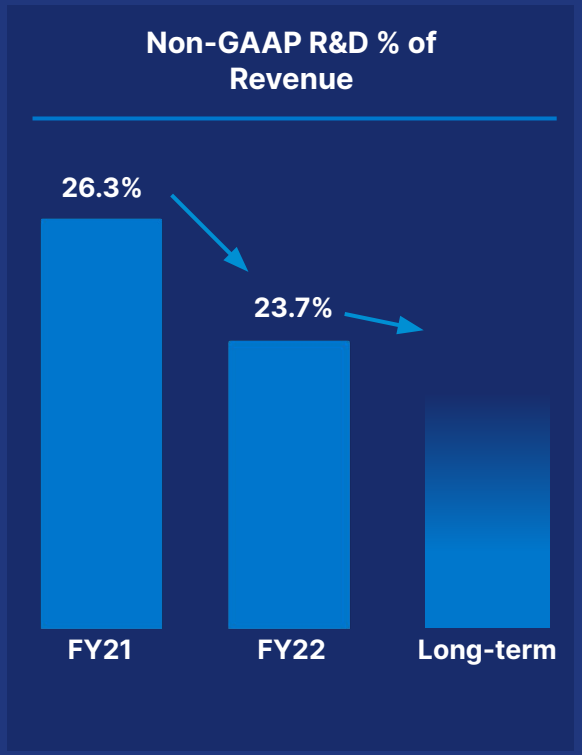
* Based on mid-point of revenue guidance provided on August 25, 2022 and 200-300 bps reduction compared to FY22
See appendix for GAAP to non-GAAP reconciliations.

elastic

173

Increasing R&D investment and innovation while driving leverage



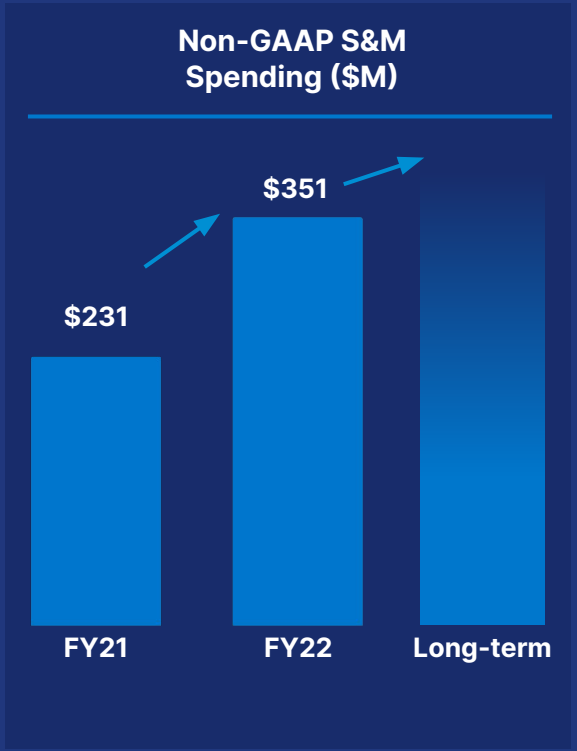


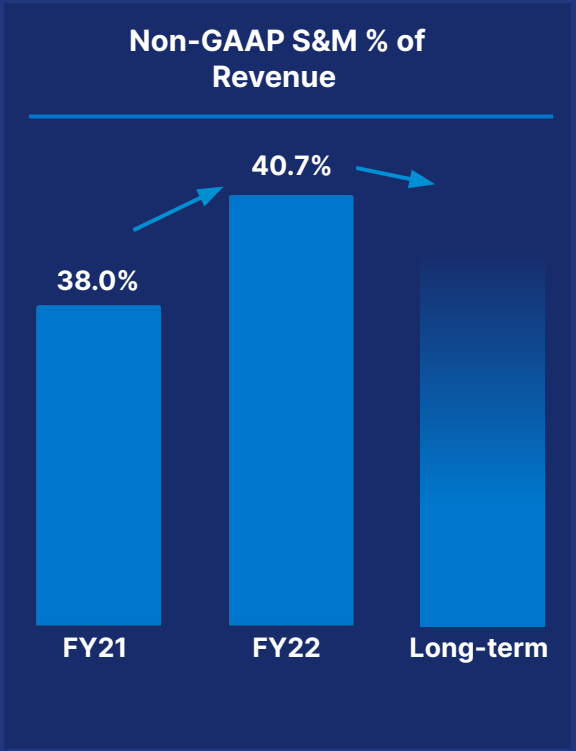
- High velocity of innovation with proprietary features drives competitive advantage and rapid monetization
- Operating leverage through:
  - Single code base across Stack and Solutions
  - Features in Stack leveraged across Solutions
  - Distributed engineering team
  - Top line growth > investment growth

elastic

174

Scaling Go-to-Market efficiently to drive growth



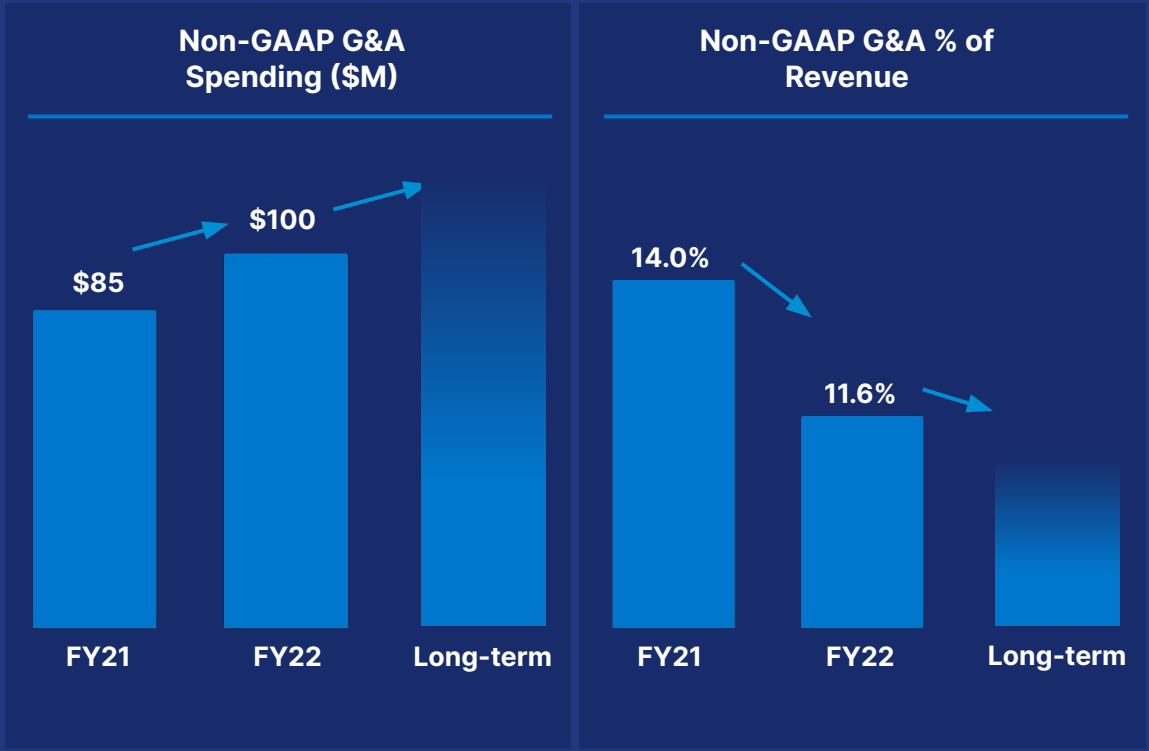


- Cloud focus + Enterprise focus
- 1Q-3Q FY22 accelerated build of sales capacity; continued but disciplined investment since
- Focus on customers with higher propensity to spend
- Operating leverage through:
  - Sales productivity
  - Cloud more efficient
  - Hyperscalers: efficient growth engine
  - Product investments make adoption and scaling easier → less sales effort
  - Top line growth > investment growth

elastic

175

G&A leverage natural with scale



- Top line growth > investment growth
- Continued efficiencies with scale

elastic

176

Long-term Financial Framework

Re-accelerating top line while delivering non-GAAP operating margin expansion

- $2B in total revenue by FY25; Recurring revenue > 90% of total revenue
- Cloud 50% of total revenue in Q4 24
- Non-GAAP Operating Margin expansion by several percentage points in FY24 and FY25
  - Trajectory of ~20 percentage points improvement from FY18 to FY23*
- Adjusted Free Cash Flow margin trend similar to non-GAAP operating margin trend in FY24 and FY25
- Maintain conservative balance sheet
- Pursue tuck-in acquisitions opportunistically
- Target ~5% annual share dilution (excluding acquisitions)

177 * Based on FY23 guidance issued on August 25, 2022.

Re-accelerating top line while delivering non-GAAP operating margin expansion

- Strong product-market fit with differentiated value proposition across solutions
- Track record of strong, consistent GTM execution
- On track to achieve goal of Cloud at 50% of revenue in Q4 FY24
- Confident path to $2B in revenue in FY25 with sustainable customer land-and-expand motion, strong new customer additions and robust net expansion rates
- Committed to non-GAAP operating margin expansion and conservative balance sheet management

elastic

178

Q&A

elastic

Appendix

elastic

Demonstrated success in growing solutions rapidly

	FY22 Mix	FY22 Growth Rate	Path to $2B (FY25)
Security	~ 25%	Fastest	• Land: SIEM • Expand: endpoint + cloud security
Observability	40%+	In-line with overall	• Land: log analytics • Expand: APM + Infr. monitoring
Enterprise Search + Stack	~ 35%	Slower than overall	• Land: App Search • Expand: Other use cases • “Stack” includes long-tail of use cases

Mix based on ACV bookings from CRM system. Does not include monthly cloud.

elastic

181

Elastic Cloud contracting models

Annual Model

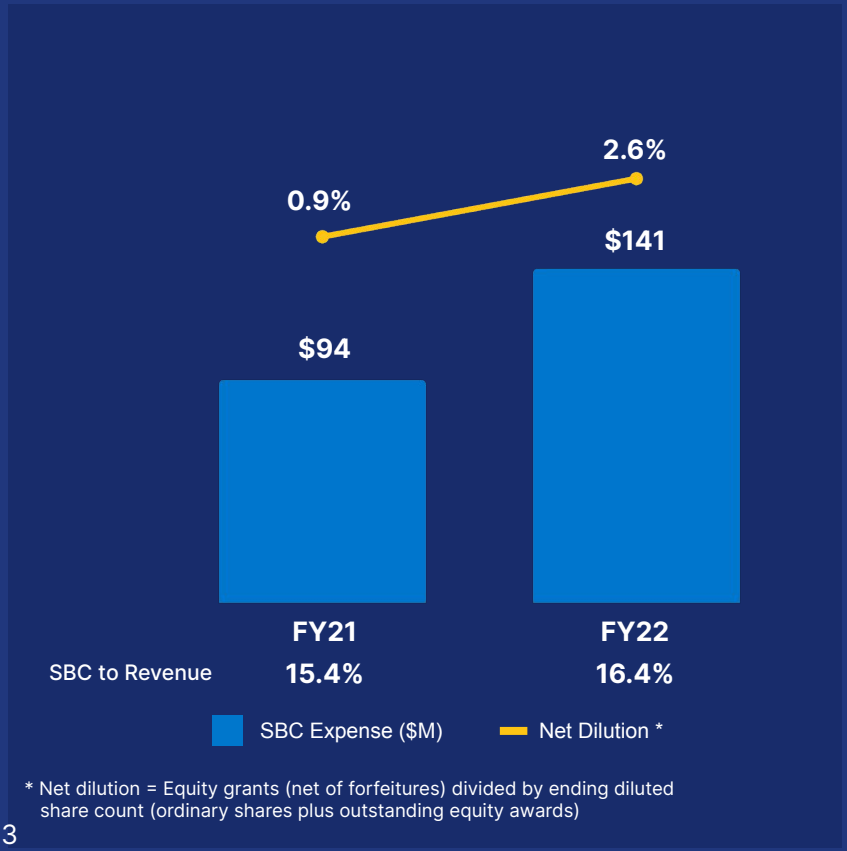
- Committed capacity contracts, mainly consumption-based
- Typically one year or longer
- Generally billed annually in advance, but faster consumption burns down deferred revenue and RPO faster than in a ratable model

Monthly Model

- Month-to-month self-service option - efficient customer acquisition engine
- Includes on-demand usage above contracted levels for annual customers
- May fluctuate in mix as customers sign more annual contracts and based on variability of usage
- Includes monthly royalties from cloud OEM partners
- Invoiced in arrears; no deferred revenue or RPO

elastic

SBC Expense and Net Dilution



- Focused on managing economic impact of stock grants, i.e. dilution
- Managed FY22 dilution (2.6%) comfortably below target (5%) despite market volatility
- Targeting ~5% annual share count dilution (excluding acquisitions)

elastic

SBC Exp

GAAP to Non-GAAP Reconciliations

Gross Profit and Gross Margin

$ in millions, except percentages	**FY22**
GAAP gross profit	**$630.2**
(+) Stock based compensation	14.8
(+) Amortization of acquired intangibles	10.5
(+) Employer payroll taxes on employee stock transactions	1.4
Non-GAAP gross profit	**$656.9**
GAAP subscription gross margin %	**73.1%**
(+) Stock based compensation	1.7%
(+) Amortization of acquired intangibles	1.2%
(+) Employer payroll taxes on employee stock transactions	0.2%
Non-GAAP subscription gross margin %	**76.2%**

A reconciliation of non-GAAP measures for gross profit and gross margin to corresponding GAAP measures for gross profit and gross margin for FY23 is not available without unreasonable effort due to the uncertainty regarding, and the potential variability of, many of the costs and expenses that may be incurred in the future.

Sums may not add to totals due to rounding

GAAP to Non-GAAP Reconciliations

Operating Margin

	FY18	FY22
GAAP operating margin %	**(30.0%)**	**(20.1%)**
(+) Stock based compensation	8.0%	16.4%
(+) Amortization of acquired intangibles	1.3%	1.8%
(+) Acquisition-related expenses	0.8%	0.9%
(+) Employer payroll taxes on employee stock transactions	0.0%	1.2%
Non-GAAP operating margin %	**(20.0%)**	**0.1%**

A reconciliation of non-GAAP operating margin guidance to GAAP operating margin guidance for FY23 is not available without unreasonable effort due to the uncertainty regarding, and the potential variability of, many of the costs and expenses that may be incurred in the future.

Sums may not add to totals due to rounding

GAAP to Non-GAAP Reconciliations

Operating Expenses

$ in millions, except percentages	FY21	FY22	FY21 % of Revenue	FY22 % of Revenue
GAAP sales & marketing expenses	**$273.9**	**$406.7**	**45.0%**	**47.2%**
(-) Stock based compensation	(31.6)	(45.8)	(5.2%)	(5.3%)
(-) Amortization of acquired intangibles	(5.7)	(5.3)	(0.9%)	(0.6%)
(-) Employer payroll taxes on employee stock transactions	(5.4)	(4.3)	(0.9%)	(0.5%)
Non-GAAP sales & marketing expenses	**$231.2**	**$351.3**	**38.0%**	**40.7%**
GAAP research & development expenses	**$199.2**	**$273.8**	**32.7%**	**31.7%**
(-) Stock based compensation	(35.3)	(59.9)	(5.8%)	(6.9%)
(-) Acquisition-related expenses	0.0	(6.1)	0.0%	(0.7%)
(-) Employer payroll taxes on employee stock transactions	(3.7)	(3.3)	(0.6%)	(0.4%)
Non-GAAP research & development expenses	**$160.3**	**$204.4**	**26.3%**	**23.7%**
GAAP general & administrative expenses	**$103.8**	**$123.4**	**17.1%**	**14.3%**
(-) Stock based compensation	(14.9)	(20.7)	(2.4%)	(2.4%)
(-) Acquisition-related expenses	0.0	(1.5)	0.0%	(0.2%)
(-) Employer payroll taxes on employee stock transactions	(4.0)	(1.0)	(0.7%)	(0.1%)
Non-GAAP general & administrative expenses	**$85.0**	**$100.3**	**14.0%**	**11.6%**

Sums may not add to totals due to rounding

GAAP to Non-GAAP Reconciliations

Adjusted Free Cash Flow Margin

	FY18	FY22
Net cash provided by (used in) operating activities (as a percentage of total revenue)	**(13.0%)**	**0.7%**
(-) Purchase of property and equipment (as a percentage of total revenue)	(1.9%)	(0.3%)
(-) Capitalization of internal-use software (as a percentage of total revenue)	-	(0.6%)
(+) Interest paid on long-term debt (as a percentage of total revenue)	-	1.4%
Adjusted free cash flow margin	**(14.9%)**	**1.2%**

Sums may not add to totals due to rounding

187