



Hunting (and stopping!) threats with **Elastic Security**

David Pilato

Developer | Evangelist

@dadoonet



Elastic at a glance

NYSE: ESTC



**Founded
in 2012**



2600+
employees



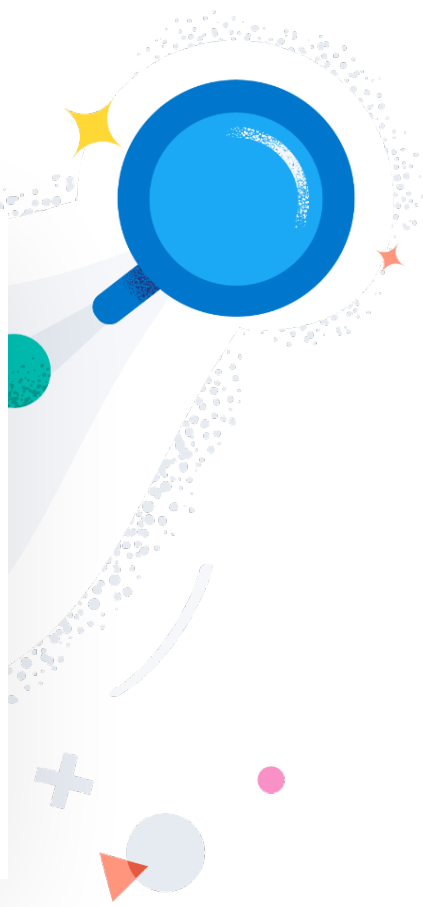
40+
countries with
employees



17,900+
subscriptions



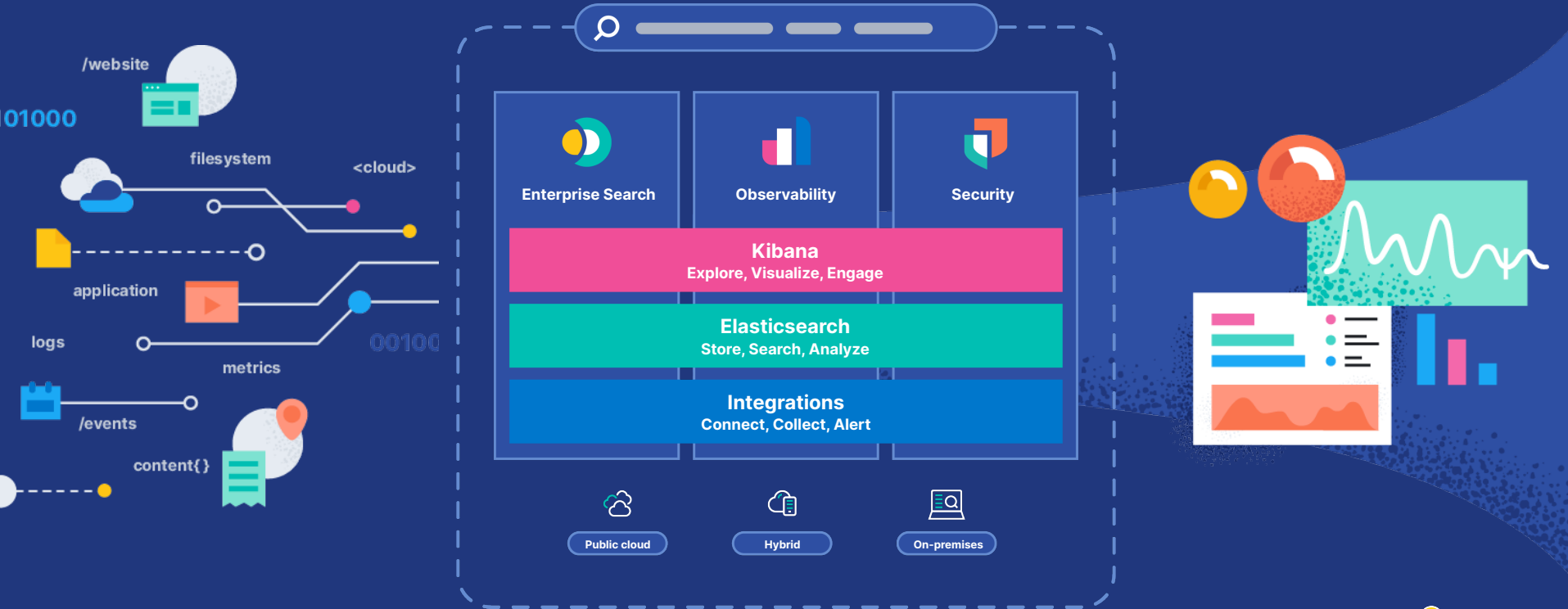
54%
of Fortune 500
companies trust Elastic



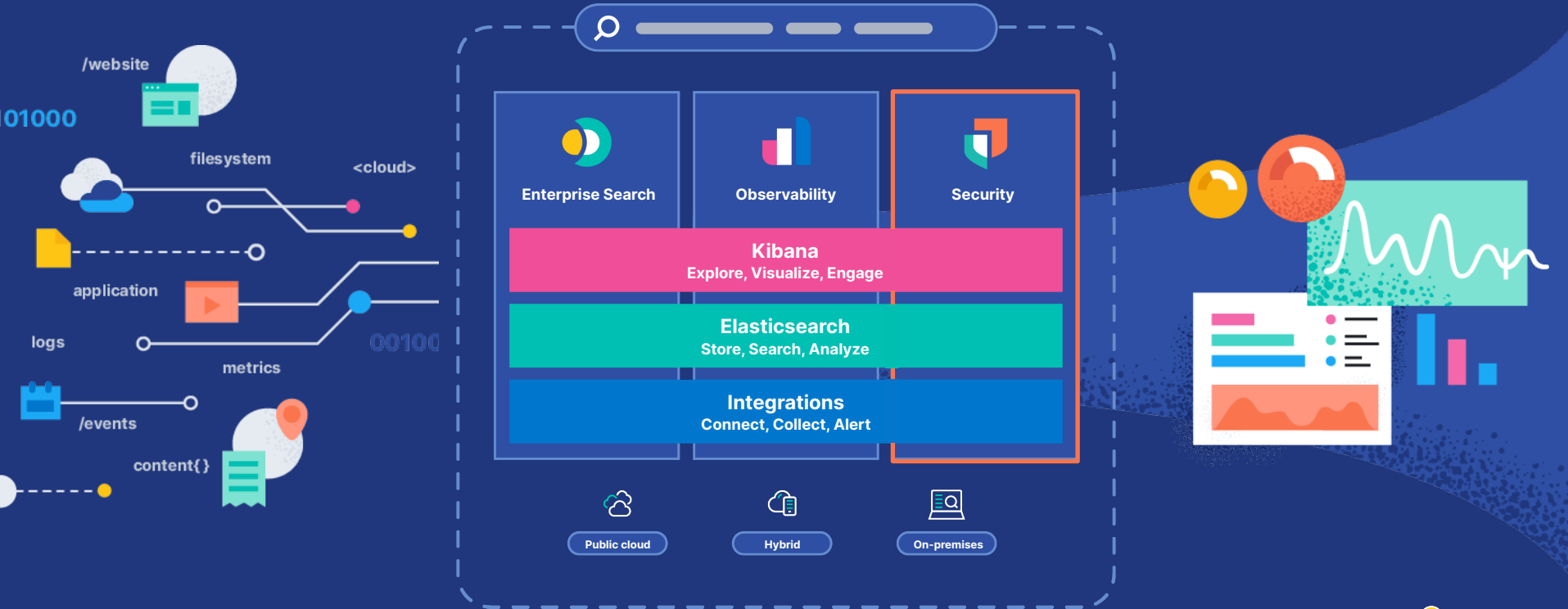
The Elastic Search Platform



The Elastic Search Platform



The Elastic Search Platform



The background is a solid dark blue. It features several decorative elements: a large circle in the top-left corner, split vertically with an orange left half and a pink right half, both containing a fine dot pattern; a smaller solid blue circle in the top-center; a large cyan circle in the bottom-right corner, also with a dot pattern; and several horizontal bars of varying lengths and colors (dark blue, light blue, and pink) scattered across the top and bottom edges.

Demo

BEST PLATFORM FOR Security



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



Search enables real-time, holistic visibility for all SecOps



Search reduces dwell times to minimize or avoid damage

Elastic named a Niche Player in the 2021 Gartner Magic Quadrant for SIEM

Magic Quadrant for Security Information and Event Management, Kelly Kavanagh, Toby Bussa, John Collins, May 2021

This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from [insert client name or reprint URL].

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

Figure 1: Magic Quadrant for Security Information and Event Management



Source: Gartner (June 2021)

The best way to consume Elastic



Amazon Web Services



Google Cloud



Microsoft Azure

Relationships with all
the **technology partners**
you work with and trust





SEARCH. SOLVE. SUCCEED.

Emirates NBD banks on Elastic to secure billions in assets and increase customer satisfaction and trust

























967

Bank branches with data points of customer transactions inside and outside, logging multiple terabytes of data/day

“We used to take days to find out where a problem was. Now we're doing it in a matter of minutes with Elastic, and our customers are the benefactors. This reduction in mean time to resolution was something we couldn't do with our legacy solutions.”

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

The Elastic Search Platform *is for everyone*

TECHNOLOGY	FINANCE	TELCO	CONSUMER	HEALTHCARE	PUBLIC SECTOR	AUTOMOTIVE / TRANSPORTATION	RETAIL
 Adobe	 BARCLAYS	 orange™	Uber	VITAS® Healthcare		 Volvo Group	
 CISCO	 ZURICH	 Bell	 Grab	 UCLA Health	 OAK RIDGE National Laboratory	Airbus	
 workday.	 USAA®	 SoftBank	 tinder.	Yale NewHaven Health	 United States™ Census Bureau	 Travelport	 ebay™
 Microsoft	collector bank	verizon✓	ACTIVISION BLIZZARD	MAYO CLINIC 	 JPL Jet Propulsion Laboratory	 CSX TRANSPORTATION	
 INGRAM MICRO	 Postbank	T Mobile	lyft	 Pfizer	 WILSON NORTH CAROLINA		 Walgreens
							



Hunting (and stopping!) threats with **Elastic Security**

David Pilato

Developer | Evangelist

@dadoonet

