

IDC MarketScape

IDC MarketScape: Worldwide Digital Forensics in Public Safety 2022 Vendor Assessment

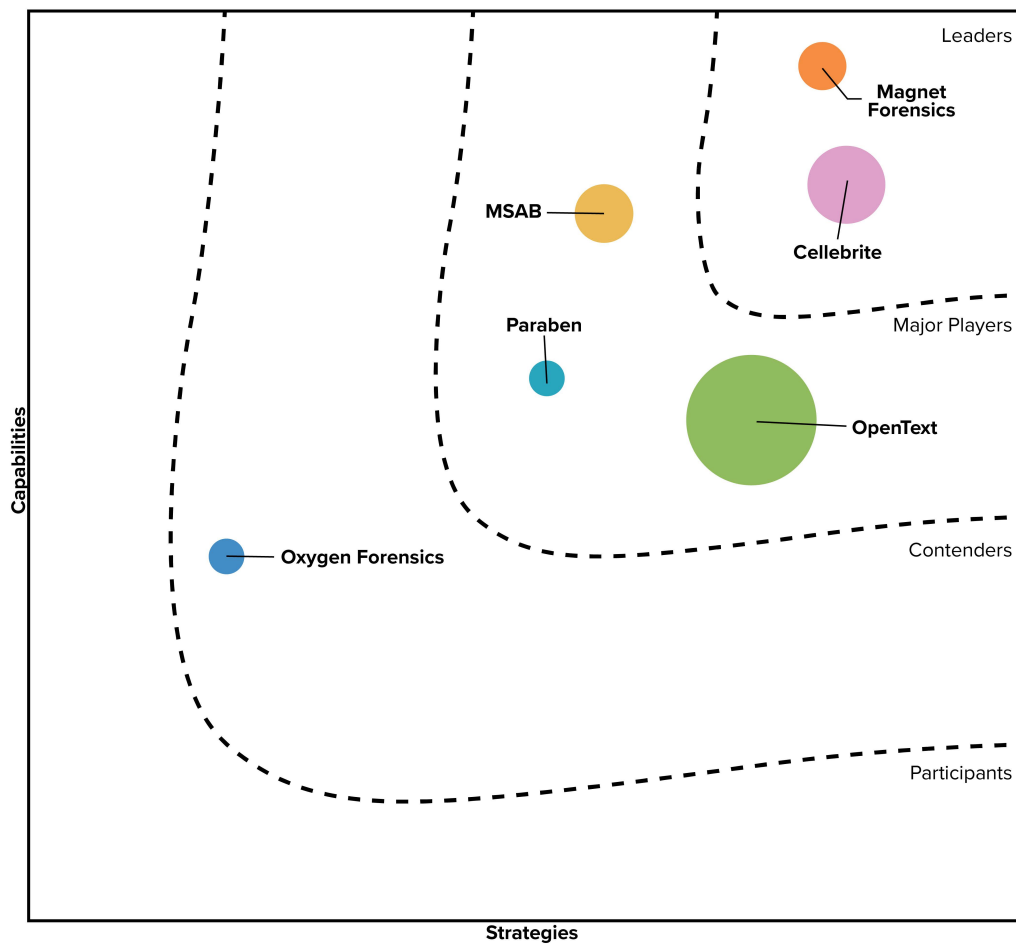
Alison Brooks, Ph.D.

THIS IDC MARKETSCAPE EXCERPT FEATURES OPENTEXT

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape Worldwide Digital Forensics in Public Safety Vendor Assessment
 IDC MarketScape Worldwide Digital Forensics in Public Safety, 2022



Source: IDC, 2022

Please see the Appendix for detailed methodology, market definition, and scoring criteria.

IN THIS EXCERPT

The content for this excerpt was taken directly from IDC MarketScape: Worldwide Digital Forensics in Public Safety 2022 Vendor Assessment by Alison Brooks, Ph.D. (Doc #US48999722). All or parts of the following sections are included in this excerpt: IDC Opinion, IDC MarketScape Vendor Inclusion Criteria, Advice for Technology Buyers, Vendor Summary Profile, Appendix and Learn More. Also included is **Figure 1**.

IDC OPINION

Reining in the digital deluge is a sizable challenge for every organization in 2022, but it is particularly challenging for law enforcement, wrestling with exponential growth in the volume, variety, and velocity of data coming into the investigative organization.

Exponential Growth in the Volume of Data

According to IDC's Global DataSphere 2021-2025 Forecast, the amount of digital data created over the next five years will be:

- At least 2.5x the amount of data created over the past 10 years
- Over 2x the amount of data created since the advent of digital storage

As part of this evaluation, IDC spoke with dozens of organizations using digital forensics solutions in criminal investigations. Among the technology buyers IDC spoke with, we noted a commonality in the challenges they face and a wide range of agency approaches to managing digital forensics solutions. Historically, digital forensics was focused on a singular device (a laptop) or a small number of smartphones. Today, the challenge is managing the information from a large number of devices and an almost limitless number of heterogeneous data sources. Each of the vendors in this study was able to conduct forensic analyses of upward of 30,000 different smartphone profiles. Very large data sets coming from call detail records, mobile phones, and laptops, as well as telecom, cloud, and internet service providers, complicate this further. Outpacing traditional resources, workflow, and processes, agencies are looking for efficient solutions that transform time-intensive workflows.

Exponential Growth in the Variety of Data Being Analyzed

The digital universe is rapidly expanding, spurred on by the adoption of a dizzying array of digital assets, smartphones, IoT devices, and large cloud-generated data sets. Net-new data sources are being woven into the investigative process continuously; drone video footage was a rarity five years ago, for example, and algorithmic DNA databases are now regularly searched to generate leads in homicide cases. More recently, agencies are having to incorporate open source intelligence (OSINT), wearables, in-car diagnostics, gaming consoles, routers, Bluetooth data, and a host of geotagged data that needs to be mined from the cloud.

The pressure to quickly extract, process, manage, and analyze these mounting data sources is challenging. Delays in processing evidence lengthen the time to trial, and this in turn is leading to cases being stayed because delays breach a citizen's rights to a timely trial. At the same time, digital evidence is increasingly relevant to a wider range of investigations; better analytic tools and collaborative capabilities are needed to enable agencies to leverage evidence much faster in many more cases.

IDC MARKETSCOPE VENDOR INCLUSION CRITERIA

This IDC study provides an assessment of vendors offering global, end-to-end digital forensics capabilities in government and public safety. Typically, IDC MarketScape documents analyze popular vendors in a given market; the smaller subset of six vendors in this analysis is attributable to this being a niche area within public safety.

Specifically, vendors were included in this IDC MarketScape if they were an end-to-end solution provider (in contrast with the specialty forensics tool providers) and if they operated in at least three of the following geographies:

- North America
- South America
- Western Europe
- Central and Eastern Europe
- The Middle East and Africa
- Asia/Pacific (including Japan)

ADVICE FOR TECHNOLOGY BUYERS

Given our expectations that the volume, variety, and velocity of data coming into police agencies are likely to continue to increase, technology buyers should be purchasing solutions from vendors focused on the following:

- **Automation.** The automation of workflow and processing capabilities will be pivotal to agencies coping with this fast-paced environment.
- **Cloud compute platform power.** Cloud compute platforms will grow in importance as a means to enhance processing power and to provide agencies with the ability to scale for volume.
- **Ethics, privacy, and transparency.** Solutions that are able to manage technological overreach are growing in importance. Focusing on overreach is important as it addresses privacy and surveillance concerns, but it also indirectly lessens the volume issues associated with forensic extraction.
- **Innovation.** Research and development (R&D) expenditures are critical to staying ahead of emerging technological challenges in this space.
- **Value partnerships.** There is a renewed focus on trusted value partners as agencies are looking to work with vendors that truly understand the complexities of criminal investigations today.

VENDOR SUMMARY PROFILE

This section briefly explains IDC's key observations resulting in a vendor's position in the IDC MarketScape. While every vendor is evaluated against each of the criteria outlined in the Appendix, the description here provides a summary of strengths and challenges.

OpenText

OpenText is positioned in the Major Players category in this 2022 IDC MarketScape for worldwide digital forensics in public safety.

OpenText's EnCase solution suite is considered the original pioneer of digital forensics. Launched in 1997 by Guidance Software, Guidance was acquired by Canadian enterprise information management software company, OpenText, in 2017. In addition to digital forensics, EnCase provides solutions in the cybersecurity and ediscovery markets.

Quick facts about OpenText are as follows:

- **Globalization:** Headquartered in Waterloo, Ontario; has regional headquarters in California (United States), Sydney (Asia/Pacific and Japan), and Munich (Europe, the Middle East, and Africa)
- **Employees:** OpenText – 14,000 people worldwide in 60 different countries, with the proportion of employees working specifically with EnCase being substantially smaller, approximately 500 in total
- **Deployments:** Digital forensics solutions used by over 150,000 customers
- **Industries:** Digital forensics business derived from both public safety agencies and corporate enterprises
- **Delivery models supported:** On premises and single-tenant private cloud
- **Software:**
 - EnCase Forensic
 - EnCase Mobile Investigator
 - EnCase Endpoint Investigator (for network investigations)
- **Hardware:**
 - Tableau Forensic duplicators, imagers, and write blockers

Strengths

OpenText's EnCase software forged the digital forensics market starting in the late 1990s. It has been historically perceived as the gold standard for forensic extraction and analysis as it is forensically tested, repeatable, and defensible in court. EnCase is well established in the law enforcement community. Customer interviews conducted for this study stressed the solution's reliability, one of EnCase's key differentiators: *"The product has a long use history; it is tested and understood by the courts."* For many agencies, defensibility in the courtroom is the most important element of digital forensics, and for this reason, it is broadly deployed and trusted by police and the courts.

EnCase is a foundational tool for most large agencies, which tend to be multitool environments by default. Because EnCase was the first tool in market, investigators are very familiar with how to use it successfully; for many agencies, EnCase is their default tool. The depth of analysis – thoroughness – conducted by EnCase is excellent. The solution's advanced search capabilities are very well regarded.

EnCase has a broad, engaged community of tools and specialized scripts, known as EnScripts, on its AppCentral platform. Ten years ago, the solution provider realized that it needed to broaden its script/development capabilities to the community to address niche agency needs quickly. Today, this tool base has grown to over 200 scripts that allow users to conduct specialized operations.

Agencies consider the EnCase solution to be good value. While it is neither the most nor the least expensive solution in the forensics environment, agencies believe it fulfills their needs at a reasonable price point. EnCase's prices are not increasing dramatically like some of the other providers analyzed in this study.

Last, EnCase's certification process is very comprehensive and highly coveted and thus valued in the investigative community.

Challenges

While OpenText is working on a road map to further modernize its digital forensics platform and extend its capabilities in cloud and social media forensics, the company needs to speed up its pace of innovation. The company's solutions feel somewhat dated in terms of its architecture and intuitive user interface; this is typical of offerings that have been successful in an earlier technology generation. Lack of solution automation is also a challenge for EnCase. This is increasingly unacceptable for agencies in this space as it furthers agency bottleneck issues. Version consistency was also a noted challenge; customers felt that there were abrupt changes from one version to the next. Last, EnCase would benefit from refocusing customer service efforts on the public safety space, as the company feels swallowed up in the larger organization since the 2017 acquisition.

Consider OpenText When

Public safety agencies should consider the EnCase solution when thoroughness, speed, triage, and courtroom validation are their top priorities. Agencies should consider EnCase when they value a solution's historical track record.

APPENDIX

Reading an IDC MarketScape Graph

For the purposes of this analysis, IDC divided potential key measures for success into two primary categories: capabilities and strategies.

Positioning on the y-axis reflects the vendor's current capabilities and menu of services and how well aligned the vendor is to customer needs. The capabilities category focuses on the capabilities of the company and product today, here and now. Under this category, IDC analysts will look at how well a vendor is building/delivering capabilities that enable it to execute its chosen strategy in the market.

Positioning on the x-axis, or strategies axis, indicates how well the vendor's future strategy aligns with what customers will require in three to five years. The strategies category focuses on high-level decisions and underlying assumptions about offerings, customer segments, and business and go-to-market plans for the next three to five years.

The size of the individual vendor markers in the IDC MarketScape represents the market share of each individual vendor within the specific market segment being assessed.

IDC MarketScape Methodology

IDC MarketScape criteria selection, weightings, and vendor scores represent well-researched IDC judgment about the market and specific vendors. IDC analysts tailor the range of standard characteristics by which vendors are measured through structured discussions, surveys, and

interviews with market leaders, participants, and end users. Market weightings are based on user interviews, buyer surveys, and the input of IDC experts in each market. IDC analysts base individual vendor scores, and ultimately vendor positions on the IDC MarketScape, on detailed surveys and interviews with the vendors, publicly available information, and end-user experiences in an effort to provide an accurate and consistent assessment of each vendor's characteristics, behavior, and capability.

Market Definition

Digital forensics is a division of forensic science encompassing the recovery, investigation, validation, and analysis of evidence found in digital devices such as laptops or smartphones and on digital databases, networks, and platforms including social media platforms and cloud-hosted data repositories. Digital forensics can occur in multiple locations (on scene, in the field, at a special-purpose location, and in the lab). Digital evidence can be forensically triaged, with some analysis occurring on scene, with a more comprehensive analysis following in the lab. Digital forensics solutions help investigators collect, analyze, and preserve digital evidence.

LEARN MORE

Related Research

- *The Biggest Investigation in U.S. History: The January 6, 2021, Capitol Riot* (IDC #US47903421, June 2021)
- *Increasing Interest in Surveillance Regulation Requires Vendor Involvement* (IDC #cUS47701621, May 2021)
- *How Can Data-Driven Policing Transform Operations?* (IDC #US47583421, April 2021)
- *IDC Market Glance: Data-Driven Policing, 1Q21* (IDC #US45994621, February 2021)
- *IDC MarketScape: Worldwide Digital Evidence Management Solutions for Law Enforcement 2020 Vendor Assessment* (IDC #US44848219, November 2020)

Synopsis

This IDC study provides an assessment of vendors offering global, end-to-end digital forensics capabilities in government and public safety. Law enforcement agencies today struggle with managing data and information coming from a large number of devices and an almost limitless number of heterogeneous data sources. Very large data sets coming from call detail records, mobile phones, and laptops, as well as telecom, cloud, and internet service providers, complicate this further. Outpacing traditional resources, workflow, and processes, agencies are looking for efficient solutions that transform time-intensive workflows.

“Digital forensics solution providers are pivotal to the modernization of criminal investigations. They provide federal, state, and local law enforcement agencies with the tools and processes to meet their mission, an increasing challenge given the data deluge agencies are currently addressing,” said Alison Brooks, research vice president, Worldwide Public Safety, IDC.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

140 Kendrick Street
Building B
Needham, MA 02494
USA
508.872.8200
Twitter: @IDC
blogs.idc.com
www.idc.com

Copyright and Trademark Notice

This IDC research document was published as part of an IDC continuous intelligence service, providing written research, analyst interactions, telebriefings, and conferences. Visit www.idc.com to learn more about IDC subscription and consulting services. To view a list of IDC offices worldwide, visit www.idc.com/offices. Please contact the IDC Hotline at 800.343.4952, ext. 7988 (or +1.508.988.7988) or sales@idc.com for information on applying the price of this document toward the purchase of an IDC service or for information on additional copies or web rights. IDC and IDC MarketScape are trademarks of International Data Group, Inc.

Copyright 2022 IDC. Reproduction is forbidden unless authorized. All rights reserved.

