The Forrester Wave™: Data Security Portfolio Vendors, Q2 2019

The 13 Providers That Matter Most And How They Stack Up

by Heidi Shey
June 10, 2019

Why Read This Report

In our 25-criterion evaluation of data security portfolio providers, we identified the 13 most significant ones — Dell, Digital Guardian, Forcepoint, Google, GTB Technologies, IBM, Imperva, McAfee, Micro Focus, Microsoft, Oracle, Symantec, and Varonis — and researched, analyzed, and scored them. This report shows how each provider measures up and helps security and risk (S&R) professionals understand the respective strengths of each vendor's portfolio.

Key Takeaways

Google, Symantec, And IBM Lead The Pack

Forrester's research uncovered a market in which Google, Symantec, and IBM are Leaders; Microsoft, Oracle, Varonis, McAfee, Micro Focus, and Forcepoint are Strong Performers; and Digital Guardian, Imperva, GTB Technologies, and Dell are Contenders.

Classification, Deletion, And Obfuscation Are Key Differentiators

As vendors expand their capabilities to approach data security in a holistic way, improved integrations and a range of granular controls that don't impede employee productivity will dictate which providers will lead the pack. Vendors that can provide data controls to support a Zero Trust approach position themselves to successfully deliver integrated data security to their customers.

The Forrester Wave™: Data Security Portfolio Vendors, Q2 2019

The 13 Providers That Matter Most And How They Stack Up

by Heidi Shey
with Stephanie Balaouras, Matthew Flug, and Peggy Dostie

June 10, 2019

Table Of Contents

Related Research Documents

CISOs, Get Ready To Pay More As Tech Titans Enter The Security Market

The Forrester Wave™: Zero Trust eXtended (ZTX) Ecosystem Providers, Q4 2018

The Future Of Data Security And Privacy: Growth And Competitive Differentiation

FORRESTER®

Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA
+1 617-613-6000 | Fax: +1 617-613-5000 | forrester.com

Complete Data Security Vendor Consolidation Is Unrealistic For Most

Major data security vendors and tech titans like Google and Microsoft have expanded their portfolio of capabilities to approach data security in a holistic and integrated fashion. This includes capabilities that align with Forrester's data control framework for: 1) defining the data (discovery and classification); 2) dissecting the data (data intelligence to understand its use and security data analytics to understand threats to the data); and 3) defending the data (measures like access control, inspection of usage patterns, data disposal/deletion, and data obfuscation).[1]

Because this expansion has created overlapping functionality, Forrester clients have asked if it could help them consolidate the number of vendors they use. The short answer: no. Clients also want to know if the native capabilities from a vendor are sufficient for their requirements or if they need a specialized third-party data security vendor. Despite the availability of a comprehensive data security portfolio of capabilities, each vendor has its strengths and specific fit for enterprise requirements. Within this Forrester Wave™, the vendors are not mutually exclusive investments for enterprise data security because:

- **Offerings can focus on structured data, unstructured data, or both.** Even the offerings that focus on both won't satisfy all of your use cases and requirements. For example, your needs for data loss prevention aren't going to overlap with your needs for database monitoring and audit. Your fit for a structured data offering will depend on database types in your environment, while for unstructured data, it can depend on specific controls or coverage for certain file types.
- **A vendor's broader portfolio of capabilities augments its strengths and approach.** This can be building security controls in as native capabilities on top of existing infrastructure — whether it be a database, cloud, or device. It could also be pulling from capabilities of other technologies in the vendor's portfolio, such as risk-based context for controls and decisioning, threat data and telemetry for security analytics, capabilities to support investigations, and more.

Evaluation Summary

The Forrester Wave evaluation highlights Leaders, Strong Performers, Contenders, and Challengers. It's an assessment of the top vendors in the market and does not represent the entire vendor landscape. For example, we don't include major encryption vendors like Gemalto and Thales eSecurity in this Forrester Wave. Despite their having a robust portfolio of encryption-specific offerings for data security, obfuscation (encryption) is one component of the data control framework. An inclusion criteria for this data security portfolio Forrester Wave requires vendors to have at least six out of eight capabilities in the data control framework, of which obfuscation (encryption) is one capability.

We intend this evaluation to be a starting point only and encourage clients to view product evaluations and adapt criteria weightings using the Excel-based vendor comparison tool (see Figure 1 and see Figure 2). Click the link at the beginning of this report on Forrester.com to download the tool.

FIGURE 1 Forrester Wave™: Data Security Portfolio Vendors, Q2 2019

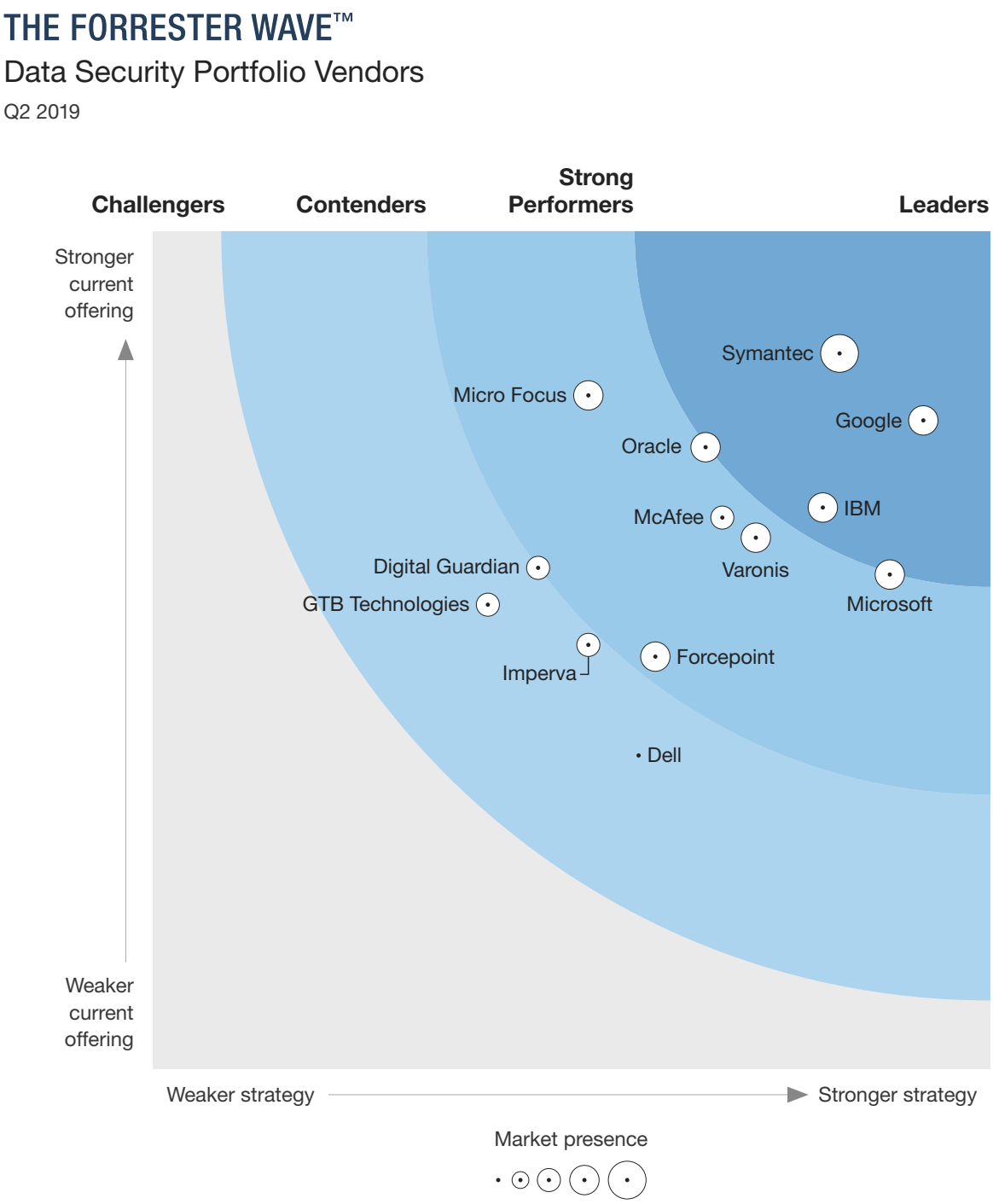

FIGURE 2 Forrester Wave™: Data Security Portfolio Vendors Scorecard, Q2 2019

	Forrester's weighting	Dell	Digital Guardian	Forcepoint	Google	GTB Technologies	IBM	Imperva	McAfee	Micro Focus	Microsoft	Oracle	Symantec	Varonis
Current offering	50%	1.87	2.99	2.46	3.87	2.77	3.35	2.53	3.29	4.02	2.95	3.71	4.27	3.17
Discovery	5%	1.00	3.00	3.00	4.60	3.00	3.00	4.60	3.00	5.00	4.60	4.20	4.60	4.20
Classification	10%	1.40	3.40	3.00	1.40	4.60	1.80	3.00	3.40	4.60	3.00	1.40	5.00	5.00
Data intelligence	15%	1.00	1.00	1.00	5.00	1.00	5.00	3.00	1.00	5.00	3.00	3.00	3.00	3.00
Security data analytics	10%	1.00	5.00	3.60	5.00	1.60	2.20	2.20	5.00	3.60	4.40	3.60	4.40	3.60
Access control	5%	3.00	3.00	3.00	5.00	3.00	3.00	3.00	3.00	5.00	3.00	5.00	5.00	5.00
Inspection	5%	4.00	3.00	3.00	3.00	3.00	3.00	3.00	3.00	3.00	3.00	3.00	3.00	5.00
Deletion	15%	3.00	5.00	0.00	3.00	3.00	1.00	0.00	3.00	1.00	3.00	5.00	5.00	1.00
Obfuscation	15%	1.50	1.00	3.00	4.00	2.00	5.00	1.50	3.00	5.00	1.50	5.00	4.00	0.00
Manageability	5%	3.00	4.00	4.00	3.00	5.00	4.00	3.00	4.00	3.00	4.00	4.00	3.00	5.00
Support	5%	3.00	3.00	5.00	3.00	5.00	3.00	3.00	5.00	5.00	1.00	3.00	5.00	5.00
APIs and integrations	10%	1.00	3.00	3.00	5.00	3.00	5.00	5.00	5.00	5.00	3.00	3.00	5.00	5.00
Strategy	50%	2.90	2.30	3.00	4.60	2.00	4.00	2.60	3.40	2.60	4.40	3.30	4.10	3.60
Data security vision and strategy	15%	5.00	3.00	3.00	5.00	1.00	3.00	3.00	3.00	5.00	3.00	3.00	3.00	3.00
Data security execution road map	35%	3.00	1.00	3.00	5.00	3.00	3.00	3.00	3.00	1.00	5.00	3.00	5.00	5.00
Data security market approach	15%	3.00	3.00	3.00	5.00	1.00	5.00	3.00	3.00	3.00	5.00	5.00	3.00	5.00
Data security innovation road map	15%	3.00	3.00	3.00	5.00	3.00	5.00	3.00	3.00	3.00	3.00	3.00	3.00	3.00
Partner ecosystem	20%	1.00	3.00	3.00	3.00	1.00	5.00	1.00	5.00	3.00	5.00	3.00	5.00	1.00
Market presence	0%	1.00	2.80	3.60	3.20	2.30	3.60	2.50	3.00	3.90	3.20	3.70	4.30	3.30
Installed base	40%	1.00	1.00	3.00	5.00	2.00	3.00	1.00	3.00	3.00	5.00	4.00	4.00	3.00
Average deal size	30%	1.00	4.00	3.00	2.00	2.00	4.00	4.00	3.00	5.00	2.00	5.00	4.00	3.00
Mindshare	30%	1.00	4.00	5.00	2.00	3.00	4.00	3.00	3.00	4.00	2.00	2.00	5.00	4.00

All scores are based on a scale of 0 (weak) to 5 (strong).

Vendor Offerings

Forrester included 13 vendors in this assessment: Dell, Digital Guardian, Forcepoint, Google, GTB Technologies, IBM, Imperva, McAfee, Micro Focus, Microsoft, Oracle, Symantec, and Varonis (see Figure 3).

FIGURE 3 Evaluated Vendors And Product Information

Vendor	Product evaluated
Dell	Dell Data Guardian v2.4
Digital Guardian	Digital Guardian Data Protection Platform v7.5
Forcepoint	Forcepoint Dynamic Data Protection Suite
Google	Google Cloud Data Loss Prevention Cloud Security Command Center G Suite Security Center G Suite Security Investigation Tool Cloud Audit Logging Cloud IAM VPC Service Controls GCP Firewalls Organization Policy Identity-Aware Proxy Cloud Identity Cloud Key Management Service Cloud-Hosted Hardware Security Module Asylo BeyondCorp
GTB Technologies	Data Security that Works Portfolio v15.6
IBM	Guardium Data Protection v10.6 Guardium Data Encryption v3.0 Multi-Cloud Data Encryption v2.3 Data Risk Manager v2.0 Guardium Analyzer v1.0 Security Key Lifecycle Manager v4.0
Imperva	Imperva Data Security, including: Data Protection v13.4 Data Risk Analytics v2.4 Data Masking v13.2

FIGURE 3 Evaluated Vendors And Product Information (Cont.)

Vendor	Product evaluated
McAfee	McAfee DLP v11.2 McAfee Database Security v4.6.6 McAfee MVISION Cloud McAfee ESM (SIEM) v11.1 McAfee Active Response/EDR v4.6 McAfee Complete Data Protection suite (Endpoint Encryption) v5.0 McAfee ePO v5.10
Micro Focus	Structured Data Manager v7.6.1 ControlPoint v5.6.1 Voltage SecureData v6.6 ArcSight (ESM v7.0. ADP v2.31, Investigate v2.3 and UBA v6.1) NetIQ Access Manager v4.4
Microsoft	Microsoft 365, including: Azure Information Protection Microsoft Cloud App Security Data Loss Prevention Windows Information Protection Intune
Oracle	Oracle Security Portfolio, including: Database v19 Audit Vault and Database Firewall v12.2 Key Vault v12.2 Data Masking and Subsetting v13.3 Database Security Assessment Tool v2.1
Symantec	Symantec Information Protection
Varonis	Data Security Platform v7.2

Vendor Profiles

Our analysis uncovered the following strengths and weaknesses of individual vendors.

Leaders

› **Google puts cloud and cloud security at the center of its strategy.** Capabilities from Google Cloud Platform, G Suite, Cloud Security Command Center, G Suite Security Center, BeyondCorp, and more are a part of Google's overall portfolio. There is support for hybrid environments (multi-cloud and on-premises) and use of open source models where it's possible to enable integration and portability. Its tools are software-based, available in management console or via APIs, and enable organizations to ease into automation to scale data security efforts.

Google supports a Zero Trust approach with its capabilities to identify data, map flows, encrypt, control access, and automate. Strengths include depth and granularity in access control and security data analytics. Weaknesses include user-driven data classification and file encryption. Customers appreciate Google's ease of deployment and scalability of its capabilities. Google is a good fit for buyers whose infrastructure runs on Google Cloud and G Suite.

› **Symantec blends information protection and advanced threat protection.** These core services support what Symantec calls its Integrated Cyber Defense platform, covering endpoint, email, network, and cloud via a unified platform architecture. Its data security capabilities span across data loss prevention, data classification, encryption, rights management, authentication, and more. It's committed to an open platform that fuels integration with third-party technology vendors to ensure interoperability and supportability.

Symantec supports a Zero Trust approach across a broad array of capabilities spanning data, endpoint, and network security.[2] In data security, strengths include robust visibility and control via data loss prevention, access control, and encryption. Weaknesses include manageability and methods of data obfuscation beyond encryption. Customers appreciate Symantec's premium level of support. Symantec is a good fit for buyers seeking integrated data-centric controls.

› **IBM focuses on a data risk management approach for compliance and data security.** IBM Security Guardium is a family of products that includes Guardium Data Protection, Guardium Data Encryption, Multi-Cloud Data Encryption, Data Risk Manager, Guardium Analyzer, and Security Key Lifecycle Manager. It addresses data risks across on-premises, hybrid, and multi-cloud. Capabilities primarily support structured data, with some support for unstructured data.

IBM supports a Zero Trust approach with capabilities that span data security, security automation and orchestration, and security analytics. In data security, strengths include data intelligence that brings together data risk and business context, in addition to obfuscation capabilities such as encryption and dynamic data masking. Weaknesses include native Guardium security data analytics, access control, and data deletion capabilities. Customers are generally satisfied with IBM's support and willingness to help, although its documentation could use improvement. IBM is a good fit for buyers seeking to centrally reduce and manage data risks across disparate database environments.

Strong Performers

› **Microsoft covers a wide set of capabilities for data security and compliance.** Capabilities within Microsoft 365 to support data security are under the Microsoft Information Protection umbrella and include Azure Information Protection, Microsoft Cloud App Security, Data Loss Prevention, Windows Information Protection, and Intune. This native, embedded approach protects data across devices, applications, cloud services, and on-premises in Microsoft environments. Microsoft Cloud App Security can extend coverage to non-Microsoft environments.

Microsoft supports a Zero Trust approach with its capabilities to identify data, control access, and analyze security data for anomalies.[3] Strengths include ease of deployment and manageability. Weaknesses include support and obfuscation capabilities beyond encryption. Customers appreciated the ease of deployment and configuration of data security capabilities, although the consistency of support quality could use improvement. Microsoft is a good fit for buyers whose infrastructure primarily runs on Microsoft and are looking for an integrated approach to compliance in their Microsoft environment.

› **Oracle offers a holistic and well-defined approach for database security.** Capabilities for data security extend from the network edge down to the underlying storage, from Oracle Audit Vault and Database Firewall, Key Vault, Data Masking and Subsetting, and Database Security Assessment Tool. Oracle aims to allow for customers to meet any database-related security control objective within their portfolio.

Oracle supports a Zero Trust approach with its capabilities to identify data, enable least privilege, obfuscate data, and provide visibility and security analytics. Strengths include effectiveness of identifying data, access control (particularly strong separation of duties), and data obfuscation (including support for full transparent data encryption). Weaknesses include ability to extend capabilities beyond Oracle databases. Customers see clear benefits for database security, with strong quality assurance from Oracle, and would like to see even greater focus on QA since it's a critical capability. Oracle is a good fit for buyers whose organizations' database environment is primarily Oracle or are looking to embed controls closer to their Oracle databases in an environment with a mix of Oracle and other database types.[4]

› **Varonis bridges the gap between identity and data for visibility and control.** Its unified data security platform analyzes data, account activity, and user behavior to determine an appropriate course of action that can include automation. A notable component of the platform is its data access governance capabilities that audit and map who can access data as well as what they do with it across file and email systems, on-premises, and in the cloud. Varonis primarily focuses on unstructured and semi-structured data.

Varonis supports a Zero Trust approach with its capabilities to identify data, provide visibility and audit for data access and use, enable least privilege, and support automation. Strengths include access control, manageability, support, and integrations. Weaknesses include native obfuscation capabilities such as encryption and data masking. Customers have positive feedback regarding ease of deployment and the quality of support. Varonis is a good fit for buyers looking to systematically reduce risk and sustain least privilege as their foundation for data protection and compliance.

› **McAfee builds on a device to cloud data security approach, with an open architecture.** McAfee's core product family supporting its data security portfolio includes Data Loss Prevention, Database Security, MVISION Cloud (SaaS), Enterprise Security Manager, Active Response/EDR, Complete Data Protection suite (Endpoint Encryption), Web Protection, and ePolicy Orchestrator

(ePO). It provides an integrated approach to unify endpoint, network, and cloud data security across on-premises and cloud environments. McAfee OpenDXL enables information sharing between security products to support automated remediation.

McAfee supports a Zero Trust approach with a range of capabilities across data, endpoint, and cloud security, in addition to security analytics. In data security, strengths include security data analytics, encryption, manageability of operations, and integrations. Weaknesses include data intelligence such as data risk insights and business context of data. Customers have positive feedback regarding ePO for management and improvements with support. McAfee is a good fit for buyers seeking to centralize management of data protection policies and incident management from devices to cloud.

- **Micro Focus offers security capability breadth across a family of products.** Capabilities to support data security are available in Structured Data Manager, ControlPoint, Voltage SecureData, ArcSight, and NetIQ. Each can function independently, with added value via integration across a broader portfolio that continues to expand via acquisitions. Micro Focus provides coverage for structured and unstructured data, with control options for data elements, file shares, data stores, and applications where the data resides.

  Micro Focus supports a Zero Trust approach with its capabilities to identify data, control access, obfuscate data, and analyze security data for anomalies. Strengths include encryption, access control, integrations, and support. Weaknesses include data deletion and manageability. Customers appreciate the quality and proactiveness of support, although they are left wanting more when it comes to innovation and road map commitments. Micro Focus is a good fit for buyers looking for big data security and capabilities for data encryption, pseudonymization, tokenization, and data masking to secure data at rest, in use, and in motion.

- **Forcepoint takes a risk-adaptive approach for data security and compliance.** Forcepoint's Dynamic Data Protection Suite covers endpoint, email, network, and cloud, and is also available as standalone components: DLP, behavior analytics, and CASB. Its open Converged Security Platform delivers its capabilities through a cloud architecture.

  Forcepoint supports a Zero Trust approach with its capabilities across data security and user behavior analytics.[5] Strengths include security data analytics, encryption, and manageability. Weaknesses include data deletion and broader business data risk intelligence. Customers appreciate its ease of deployment and are generally satisfied with quality of support. Forcepoint is a good fit for buyers looking to dynamically enable appropriate actions and controls to support compliance and protect intellectual property based on user interactions with data and reduce investigation time across platforms.

Contenders

› **Digital Guardian builds on a foundation of DLP, EDR, and security analytics.** The cloud-based Digital Guardian Data Protection Platform covers endpoint, data repositories, cloud, and network. Digital Guardian offers data protection independent of threat actor, data type, system, application, device, or point of access. It accomplishes this via a kernel-level agent that provides rich insight into the users, application, system, and data events on endpoints to enable data security controls. Digital Guardian also provides its capabilities as a managed service.

Digital Guardian supports a Zero Trust approach with its capabilities across data and endpoint security. Strengths include data deletion in addition to visibility and security data analytics derived from insights via its combined DLP, UBA, and EDR capabilities. Weaknesses include data obfuscation and broader business data risk intelligence. Customers speak highly of Digital Guardian's depth of visibility on the endpoint and of how support capabilities are improving, though they acknowledge that the agent can cause challenges and incompatibilities. Digital Guardian is a good fit for buyers challenged with unstructured data, requiring intellectual property protection, and looking for an offering capable of providing EDR and DLP functionality on a single agent. It's also a good fit for those who want these offerings as a managed service.

› **Imperva provides database and risk visibility to support remediation and compliance.** Imperva Data Security includes its data protection, data risk analytics, and data masking capabilities. The broader portfolio covers application security to support its goal of unifying application, user, and data security on-premises and in the cloud. Capabilities primarily support structured and semi-structured data.

Imperva supports a Zero Trust approach with capabilities to identify data, enable least privilege, and provide visibility. Strengths include security data analytics outcomes, access control, and API integrations. Weaknesses include unstructured data, encryption, and partner network. Customers generally found the solutions reasonable to manage, although some had challenges with false positives in data classification. Imperva is a good fit for buyers seeking greater database visibility, as well as intelligence about data risks and user behaviors, across multiple database environments.

› **GTB Technologies offers breadth via DLP, content-aware IRM, and application control.** Its Data Security that Works Platform covers endpoint, email, network, and cloud. Deployment can be on-premises, hybrid, or cloud-based. Innovation is mainly fueled by customer requests, and GTB's growth as a DLP provider over the past decade has primarily been via word of mouth from happy customers. Technologies capabilities are also available as a managed service.

GTB Technologies supports a Zero Trust approach with its capabilities to identify data, classify data, control access, encrypt, and provide visibility. Strengths include manageability (notable in both ease of deployment and ongoing operations) and data classification. Weaknesses include security data analytics and broader business data risk intelligence. Customers speak highly of GTB

Technologies' ease of use, breadth of functionality, and quality of support. GTB Technologies is a good fit for buyers looking for an easy-to-manage, feature-rich DLP offering with OCR and rights management capabilities.

› **Dell enables seamless control with a focus on usability and efficient collaboration.** Dell Data Guardian is a relative newcomer for data security offerings, having been on the market for about two years. It's a cloud-based offering that covers unstructured data at rest and in motion. Primarily endpoint-focused today, there are information protection capabilities for cloud-native applications and repositories on the road map. Dell Data Guardian is a part of Dell's Unified Workspace, a vision for the modern workplace that also incorporates capabilities from VMware Workspace ONE.

Dell supports a Zero Trust approach with its capabilities across data security and trusted devices. In data security, strengths include access control to enable least privilege, encryption, and manageability. Weaknesses include identifying data, broader business data risk intelligence, and integrations. Customers appreciate the responsiveness of support. Dell is a good fit for buyers looking to protect data wherever it is and seeking an integrated offering to deploy, secure, manage, and support endpoints (including BYOD).

Evaluation Overview

We evaluated vendors against 25 criteria, which we grouped into three high-level categories:

› **Current offering.** Each vendor's position on the vertical axis of the Forrester Wave graphic indicates the strength of its current offering. Key criteria for these solutions include capabilities for data discovery and classification, data intelligence, security data analytics, access control, data inspection, data deletion, data obfuscation, solution manageability, vendor support, APIs and integrations.

› **Strategy.** Placement on the horizontal axis indicates the strength of the vendors' strategies. We evaluated vision and strategy, strategy execution road map, market approach, innovation road map, and partner ecosystem.

› **Market presence.** Represented by the size of the markers on the graphic, our market presence scores reflect each vendor's current installed base, average deal size, and mindshare as a strategic data security vendor for enterprises.

Vendor Inclusion Criteria

Forrester included 13 vendors in the assessment: Dell, Digital Guardian, Forcepoint, Google, GTB Technologies, IBM, Imperva, McAfee, Micro Focus, Microsoft, Oracle, Symantec, and Varonis. Each of these vendors has:

› **A sizable customer base.** Vendors have more than 1,000 enterprise customers.

› **Notable revenues.** Vendors have at least $80 million in annual revenue.

› **A broad range of capabilities for data security.** Vendors have native capabilities in at least six out of eight components of Forrester's data control framework: 1) data discovery; 2) data classification; 3) data intelligence; 4) security data analytics; 5) access control; 6) data inspection; 7) data deletion; and 8) data obfuscation.

› **An established partnership ecosystem.** Vendors have a strong partner ecosystem consisting of distributors, channel partners, system integrators, and technology partners, in addition to key security technology vendors for integration to help support a Zero Trust approach to security.

Supplemental Material

Online Resource

We publish all our Forrester Wave scores and weightings in an Excel file that provides detailed product evaluations and customizable rankings; download this tool by clicking the link at the beginning of this report on Forrester.com. We intend these scores and default weightings to serve only as a starting point and encourage readers to adapt the weightings to fit their individual needs.

The Forrester Wave Methodology

A Forrester Wave is a guide for buyers considering their purchasing options in a technology marketplace. To offer an equitable process for all participants, Forrester follows The Forrester Wave™ Methodology Guide to evaluate participating vendors.

In our review, we conduct primary research to develop a list of vendors to consider for the evaluation. From that initial pool of vendors, we narrow our final list based on the inclusion criteria. We then gather details of product and strategy through a detailed questionnaire, demos/briefings, and customer reference surveys/interviews. We use those inputs, along with the analyst's experience and expertise in the marketplace, to score vendors, using a relative rating system that compares each vendor against the others in the evaluation.

We include the Forrester Wave publishing date (quarter and year) clearly in the title of each Forrester Wave report. We evaluated the vendors participating in this Forrester Wave using materials they provided to us by March 27, 2019 and did not allow additional information after that point. We encourage readers to evaluate how the market and vendor offerings change over time.

In accordance with The Forrester Wave™ Vendor Review Policy, Forrester asks vendors to review our findings prior to publishing to check for accuracy. Vendors marked as nonparticipating vendors in the Forrester Wave graphic met our defined inclusion criteria but declined to participate in or contributed only partially to the evaluation. We score these vendors in accordance with The Forrester Wave™ And The Forrester New Wave™ Nonparticipating And Incomplete Participation Vendor Policy and publish their positioning along with those of the vendors.

Integrity Policy

We conduct all our research, including Forrester Wave evaluations, in accordance with the Integrity Policy posted on our website.

Endnotes

[1] For more detail on this framework, see the Forrester report "The Future Of Data Security And Privacy: Growth And Competitive Differentiation."

[2] Zero Trust is somewhat new to Symantec, and the company is quickly ramping up its strategic alignment to the broader ZTX framework. See the Forrester report "The Forrester Wave™: Zero Trust eXtended (ZTX) Ecosystem Providers, Q4 2018."

[3] Microsoft has been noted as understanding the needs of Zero Trust enterprises and use cases, but the users we interviewed often referred to the vendor solution set as slow to roll out. See the Forrester report "The Forrester Wave™: Zero Trust eXtended (ZTX) Ecosystem Providers, Q4 2018."

[4] See the Forrester report "The Forrester Wave™: Database-As-A-Service, Q2 2019."

[5] Forcepoint sets a strong standard in analytics and data control when compared with the ZTX framework requirements. See the Forrester report "The Forrester Wave™: Zero Trust eXtended (ZTX) Ecosystem Providers, Q4 2018."

FORRESTER®
CHALLENGE THINKING. LEAD CHANGE.

We work with business and technology leaders to develop customer-obsessed strategies that drive growth.

PRODUCTS AND SERVICES

- Core research and tools
- Data and analytics
- Peer collaboration
- Analyst engagement
- Consulting
- Events

Forrester's research and insights are tailored to your role and critical business initiatives.

ROLES WE SERVE

Marketing & Strategy Professionals

CMO
B2B Marketing
B2C Marketing
Customer Experience
Customer Insights
eBusiness & Channel Strategy

Technology Management Professionals

CIO
Application Development & Delivery
Enterprise Architecture
Infrastructure & Operations
- Security & Risk

Sourcing & Vendor Management

Technology Industry Professionals

Analyst Relations

CLIENT SUPPORT

For information on hard-copy or electronic reprints, please contact Client Support at +1 866-367-7378, +1 617-613-5730, or clientsupport@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.