Paul Stringfellow
Aug 16, 2022 – Market Radar

GigaOm Radar for Data Loss Prevention v2.0

Table of Contents

1. Summary

Data is at the core of today's enterprise, and ensuring it's protected and secure is at the top of every enterprise's agenda. The cost of data loss is significant and its impact wide ranging. This can be technical (with loss of services impacting operational ability), reputational (damaging relationships and future business success), and/or financial (from loss of business to regulatory fines). Preventing data loss is of paramount importance.

The complexity of the ways data is held today means companies must seek appropriate technology to reduce the risk of loss, and this is true for all businesses regardless of sector, size, or reputation. Finding solutions that address these challenges is essential.

Data loss prevention (DLP) tools operate on several levels. They must be able to determine the risks involved in data usage, whether by identifying sensitive data or by identifying uses of data that present a risk. They must offer mitigation measures when risk is identified to protect the security of the data and the information it contains. And, as enterprise infrastructure evolves, DLP tools must evolve as well, and be able to identify risks to data across many locations—in the data center, enterprise endpoints, and beyond into public cloud and software as a service (SaaS) applications. Increasingly, DLP tools must be risk-

DLP vendors are responding to these needs. Increasingly, solutions are offered as a service from the public cloud, though many vendors still offer onsite solutions for those that need it. They're taking advantage of new ways to integrate with different data repositories to ensure DLP remains effective.

Vendors are also recognizing the growing difficulty of using traditional DLP approaches to solve modern challenges, with many increasingly investing in the use of machine learning (ML) and artificial intelligence (AI) to more effectively and accurately identify risky behavior that poses a threat to data.

The threat of data loss continues to be high, and its potential impact on the enterprise is significant. But leading vendors are responding with levels of innovation that provide more effective protection as enterprises need to act immediately to get a complete picture of their data protection posture and address any shortcomings.

This Radar report reviews the leading DLP vendors, assessing their capabilities against criteria defined in the accompanying "Key Criteria Report for Data Loss Prevention Solutions." This is an update of GigaOm's 2021 report on DLP and it highlights the continued evolution of the market and describes the ways leading vendors have responded to changing data loss challenges and customer demands. Together, our reports give decision-makers an overview of the market, helping them evaluate current platforms and decide where to invest.

HOW TO READ THIS REPORT

This GigaOm report is one of a series of documents that helps IT organizations assess competing solutions in the context of well-defined features and criteria. For a fuller understanding, consider reviewing the following reports:

Key Criteria report: A detailed market sector analysis that assesses the impact that key product features and criteria have on top-line solution characteristics—such as scalability, performance, and TCO—that drive purchase decisions.

GigaOm Radar report: A forward-looking analysis that plots the relative value and progression of vendor solutions along multiple axes based on strategy and execution. The Radar report includes a breakdown of each vendor's offering in the sector.

Solution Profile: An in-depth vendor analysis that builds on the framework developed in the Key Criteria and Radar reports to assess a company's engagement within a technology sector. This analysis includes forward-looking guidance around both strategy and product.

2. Market Categories and Deployment Types

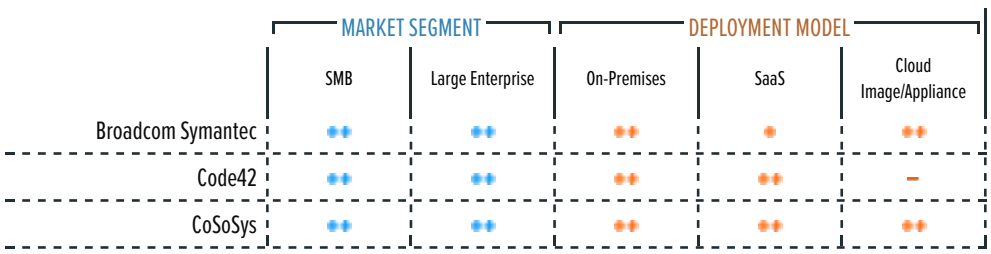
To better understand the market and vendor positioning (**Table 1**), we assess how well solutions for data loss prevention are positioned to serve specific market segments.

- **Small-to-medium business (SMB):** In this category we assess solutions on their ability to meet the needs of organizations ranging from small to medium-sized companies where ease of use and deployment are more important than extensive management functionality, data mobility, and feature set.
- **Large enterprise:** Here offerings are assessed on their ability to support large and business-critical projects. Optimal solutions in this category will have a strong focus on flexibility, performance, data services, and features to improve security and data protection. Scalability is another big differentiator, as is the ability to deploy the same service in different environments.

In addition, we recognize three deployment models: on-premises, software as a service (SaaS), and cloud image/appliance.

- **On-premises:** These solutions are deployed fully on-premises. Though they may have some cloud integration, the entire service can be deployed in a customer data center. These solutions are particularly valuable for those with concerns over cloud security or data locality or those who have a need to support dark-site installations.
- **SaaS:** These solutions are available only in the cloud and delivered as a service that is architected, deployed, delivered, and maintained by a specialist third party. Access to the service is usually via subscription and requires no customer infrastructure beyond potential local plug-ins or agents, usually only from that specific provider. The big advantages of this type of solution are its ease of deployment, ability to quickly scale, and elimination of maintenance costs from the enterprise.
- **Cloud image/appliance**: These deployments are more "bespoke" than typical SaaS solutions, with a cloud-based virtual appliance or installation image deployed inside of an individual enterprise's cloud infrastructure. This infrastructure can either be enterprise-owned or provided via a vendor or vendor partner, but the solution is specific to that enterprise. This approach is useful for those with data sovereignty concerns, with regulatory demands around shared infrastructure, or with specific requirements not met by a SaaS solution, but wanting a cloud-based solution.

Table 1. Vendor Positioning



Forcepoint	++	++	++	–	++
HelpSystems (Digital Guardian)	++	++	++	++	++
Microsoft	++	++	–	++	–
Nightfall.ai	++	++	–	++	–
Proofpoint	++	++	–	++	–

Source: GigaOm 2022

+++ Exceptional: Outstanding focus and execution
++ Capable: Good but with room for improvement
+ Limited: Lacking in execution and use cases
– Not applicable or absent

3. Key Criteria Comparison

Building on the findings from the GigaOm report, "Key Criteria for Evaluating Data Loss Prevention Solutions," **Table 2** summarizes how each vendor included in this research performs in the areas that we consider differentiating and critical in this sector. **Table 3** follows this summary with insight into each product's evaluation metrics—the top-line characteristics that define the impact each will have on the organization.

The objective is to give the reader a snapshot of the technical capabilities of available solutions, define the perimeter of the market landscape, and gauge the potential impact on the business.

Table 2. Key Criteria Comparison

	KEY CRITERIA							
	Deployment Location Flexibility	Contextual Awareness	Integration with Collaboration Tools	Integration with Service Desk & SIEM Tools	Breadth of Endpoints	Orchestration & Automation	Reporting & Analytics	Extended User Education
Broadcom Symantec	++	+++	++	+++	+++	+++	+++	++
Code42	+++	+++	++	+++	+++	++	+++	+++
CoSoSys	+++	++	++	++	+++	+++	++	++
DTEX	+++	+++	++	+++	+++	++	+++	++
Forcepoint	++	+++	++	+++	+++	+++	+++	++
HelpSystems (Digital Guardian)	+++	+++	++	+++	+++	+++	+++	+++
Microsoft	++	+++	+++	++	+++	+++	++	+++
Nightfall.ai	++	++	+++	++	+++	+++	+++	++
Proofpoint	++	+++	++	+++	+++	+++	+++	+++

Source: GigaOm 2022

+++ Exceptional: Outstanding focus and execution
++ Capable: Good but with room for improvement
+ Limited: Lacking in execution and use cases
– Not applicable or absent

Table 3. Evaluation Metrics Comparison

	EVALUATION METRICS			
	Ease of Management	Ease of Adoption	Reduced Complexity	Breadth of Business Protection
Broadcom Symantec	+++	++	+++	+++
Code42	+++	+++	++	+++
CoSoSys	+++	+++	+++	++

Forcepoint	+++	+++	+++	+++
HelpSystems (Digital Guardian)	+++	+++	++	+++
Microsoft	++	+++	+++	+++
Nightfall.ai	+++	+++	+++	++
Proofpoint	++	+++	+++	+++

Source: GigaOm 2022

+++ Exceptional: Outstanding focus and execution
++ Capable: Good but with room for improvement
+ Limited: Lacking in execution and use cases
– Not applicable or absent

By combining the information provided in the tables above, the reader can develop a clear understanding of the technical solutions available in the market.

4. GigaOm Radar

This report synthesizes the analysis of key criteria and their impact on evaluation metrics to inform the GigaOm Radar graphic in **Figure 1**. The resulting chart is a forward-looking perspective on all the vendors in this report, based on their products' technical capabilities and feature sets.

The GigaOm Radar plots vendor solutions across a series of concentric rings, with those set closer to the center judged to be of higher overall value. The chart characterizes each vendor on two axes—balancing Maturity versus Innovation, and Feature Play versus Platform Play—while providing an arrow that projects each solution's evolution over the coming 12 to 18 months.

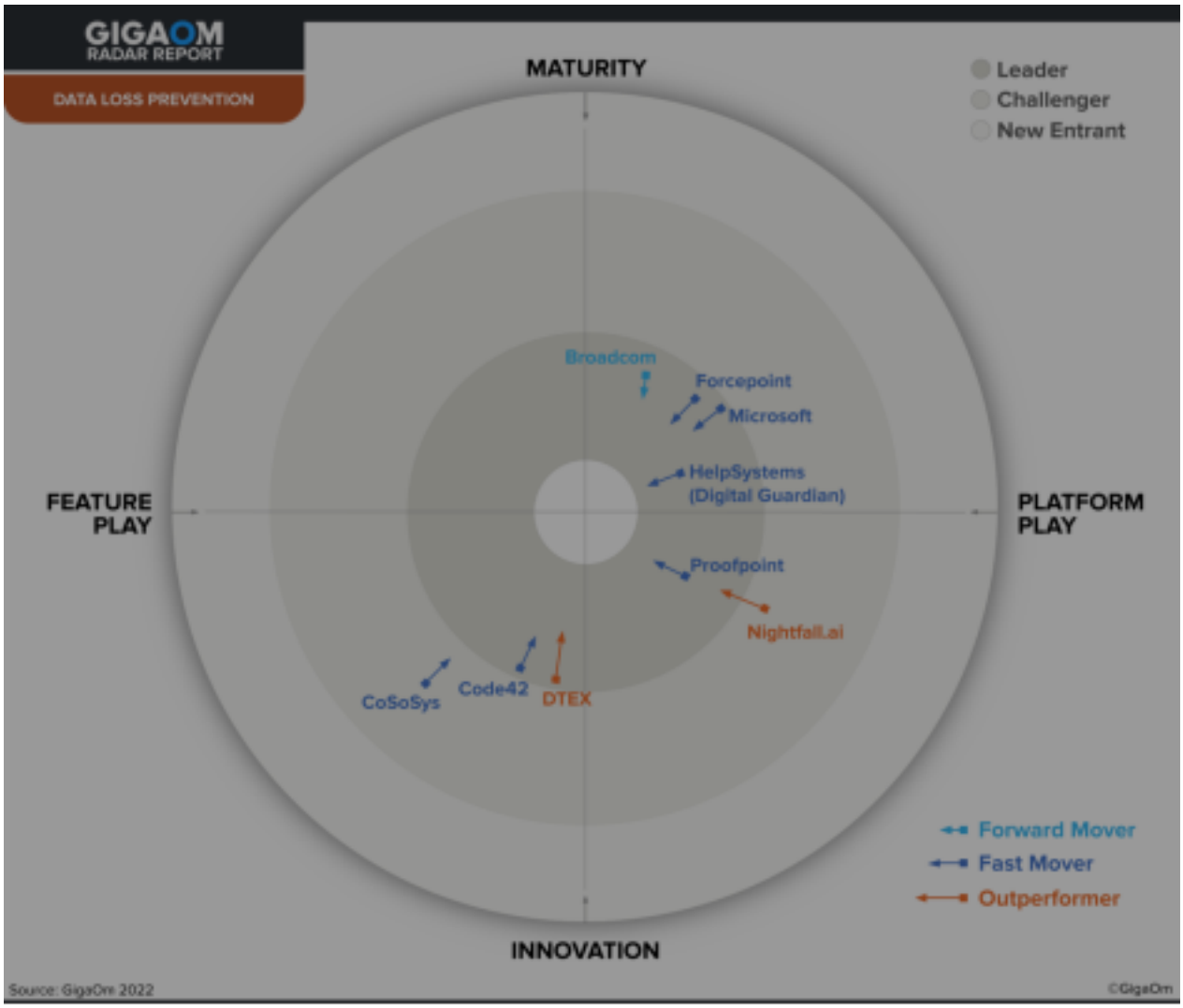


Figure 1. GigaOm Radar for Data Loss Prevention

Most vendors sit in the Innovation half, and many are building risk and threat management into their platforms. DTEX and Code42 are two examples; their insider risk and threat management platforms are now seen as valid DLP approaches. Endpoint specialist CoSoSys is also focused on this strategic direction. Even vendors that offer broader platforms—such as Proofpoint, Microsoft, Forcepoint, and Broadcom—are adopting this approach.

Several vendors included in our 2021 Radar report appear again in this year's report:

- Digital Guardian—now owned by HelpSystems—maintains a leadership position in the Maturity quadrant; however, it has changed from a Forward Mover to a Fast Mover and evolved from Feature Play to Platform Play. This change was driven by integration with the HelpSystems portfolio, which moved the solution's focus from DLP to a broader range of capabilities.
- Proofpoint maintains its position as a Platform-Play Leader, but has changed from a Forward Mover to a Fast Mover and shifted from the Maturity quadrant to the Innovation quadrant. This is based on its aggressive acquisition strategy that is rapidly driving new innovation into its solution.
- Microsoft moved from Challenger to Leader and Forward Mover to Fast Mover (remaining in the Maturity/Platform quadrant) due to the continual evolution of its solution and improved manageability of its very comprehensive platform.
- Broadcom maintains its position as a Mature Platform-Play Leader and continues to develop its solution. However, its on-premises deployment model remains more traditional, while it invests in cloud-based and SaaS solutions. There are some issues around the perception of product development and focus. But it should be noted that the 15.8 platform is being developed and Broadcom has publicly committed to keeping DLP as a strong part of its cybersecurity business.
- CoSoSys remains a Feature-Play Challenger but has changed from a Forward Mover to Fast Mover and shifted from the Maturity/Feature-Play quadrant to the Innovation/Feature-Play quadrant due to a strong strategic shift in approach and an interesting roadmap.
- DTEX maintains its position as an Innovative Feature-Play Leader, but has changed from a Fast Mover to an Outperformer due to its increasing innovation and willingness to build a better understanding of threats, as demonstrated by its relationship with MITRE.
- Code42 moved from Challenger to Leader in the Innovation/Feature-Play quadrant, and has changed from a Forward Mover to a Fast Mover due to continued rapid evolution of its threat management platform. Threat and risk management is increasingly likely to become the norm for DLP vendors in the future, inspired by the capabilities of vendors such as Code42.

New to this year's Radar report, Forcepoint and Nightfall.ai have different approaches to solving the DLP challenge and both have scored well in this assessment.

- Forcepoint is a Mature Platform-Play Leader in this space, but its continued leadership depends on the success of its risk-adaptive DLP approach. While Forcepoint offers a broad and comprehensive solution, its ability to deliver strong context-driven threat and risk insight will be key to maintaining its position.
- Nightfall.ai was not assessed in our previous report, though we were aware of it, and it has continued to build a strong development platform and customer base in the intervening period and is positioned as an Outperformer. With its API-driven integration capabilities that simplify adoption and a low-code development platform, Nightfall offers a flexible DLP solution.

This market is robust, and each vendor included in this report offers a strong solution to help the enterprise tackle the challenge of preventing data loss. This space is competitive and innovative, which should give confidence to prospective buyers.

INSIDE THE GIGAOM RADAR

The GigaOm Radar weighs each vendor's execution, roadmap, and ability to innovate to plot solutions along two axes, each set as opposing pairs. On the Y axis, **Maturity** recognizes solution stability, strength of ecosystem, and a conservative stance, while **Innovation** highlights technical innovation and a more aggressive approach. On the X axis, **Feature Play** connotes a narrow focus on niche or cutting-edge functionality, while **Platform Play** displays a broader platform focus and commitment to a comprehensive feature set.

The closer to center a solution sits, the better its execution and value, with top performers occupying the inner Leaders circle. The centermost circle is almost always empty, reserved for highly mature and consolidated markets that lack space for further innovation.

The GigaOm Radar offers a forward-looking assessment, plotting the current and projected position of each solution over a 12- to 18-month window. Arrows indicate travel based on strategy and pace of innovation, with vendors designated as Forward Movers, Fast Movers, or Outperformers based on their rate of progression.

Note that the Radar excludes vendor market share as a metric. The focus is on forward-looking analysis that emphasizes the value of innovation and differentiation over incumbent market position.

5. Vendor Insights

Broadcom Symantec DLP

Since its acquisition of Symantec, Broadcom continues to deliver a broad enterprise DLP platform. This is a well-established, mature solution—one that continues to be developed to tackle the challenges of modern data loss prevention.

The DLP offering is part of Broadcom's Symantec Enterprise Cloud platform, which offers a comprehensive base on which to build a robust, data-centric hybrid cloud security strategy.

The information gained this way can help enforce a least privilege model for data use. The platform can deliver insights across a broad range of potential repositories, including cloud, networks, endpoints, and local storage, which allows the solution to build a detailed picture of the data.

Broadcom's solution is deployed using a unified server and single management console alongside endpoint agents, file share, and network scanners as needed. While there's not a full SaaS version of this solution available currently, earlier in 2022 Broadcom added a cloud managed DLP element into its CloudSOC cloud access security broker (CASB) solution, providing a SaaS DLP capability to its customers. The solution can also be deployed onto public cloud infrastructure delivering an option of hybrid deployment for those that need it. The product is licensed and deployed using either the Symantec DLP core solution, which focuses on on-premises requirements, or the Symantec DLP Cloud license, to enable Cloud DLP in its CASB solution.

There's broad coverage of repositories with agents to handle a wide range of platforms, including desktops and servers, databases, and file shares. This coverage is enhanced by the FlexResponse API platform, which allows the solution to present a broad range of API integrations that enable extensive customization, not only of integration with other tools, but also of risk mitigation actions. This approach enhances adoption of the product as well as the breadth of the enterprise that can be covered.

Policy management is good, with a single management console that lets users control and configure all of the core components of the solution. Additions, moves, and changes are then replicated across the broad range of DLP elements including Symantec web gateway, email security, CASB, and endpoint solutions. This kind of single console approach is very attractive to the enterprise, especially those with hybrid infrastructure across multiple locations.

The solution also integrates with Microsoft's Information Protection solution, making it an almost-native part of its own toolset, to deliver additional security to data regardless of whether or not it sits within the enterprise's control. Version 15.8 also introduced integration with ServiceNow, allowing Symantec DLP to be easily absorbed into enterprise service workflows.

Broadcom has an extensive security portfolio and the acquisition of Symantec DLP further enhanced it. The company continues to develop the product, but customers have raised questions about Broadcom's long-term plans for the solution although there have been regular updates to the 15.8 platform. Some customers complain about installation complexity with regard to Broadcom's traditional deployment model and product support. The solution is geared toward the larger enterprise space and that's not expected to change, so it's likely to remain out of reach for smaller businesses.

It should be noted that since our previous report, the vendor's rate of innovation for this solution does not match that of some of its competitors. However, as is the case with mature and comprehensive solutions, innovation is a far more complex and difficult undertaking, so it can take longer to see results.

Strengths: This is a very comprehensive platform, driven by good strategic planning and an understanding of the current challenges posed by DLP in the enterprise. The least-privilege data model is a smart one and will appeal to many enterprises.

Challenges: Multiple solution components lead to some complexity. Broadcom's solution is still very much a product for large enterprises, and out of reach for smaller businesses because of cost and complexity. Customers have raised concerns over support standards and around the long-term development and innovation of the solution. However, continuing regular updates to the 15.8 platform may quell concerns.

Code42 Incydr

Code42 is focused on threat and risk analysis rather than traditional DLP. While some may view this as an incomplete approach to DLP, many see the shift of focus to threat management as essential to the way that data is protected. This is the area where Code42 is strong, and it's highlighted in the way its customers advocate its approach.

Code42 sees the focus on threat management as a response to the failings of DLP centered on sensitive information and the blocking of data. It suggests that, as the amount of data grows and the workforce requires more flexibility, traditional methods are no longer workable and increasingly inaccurate. Instead, its focus is on understanding the context and user intent as they access data. It accomplishes this by gathering detailed information via its lightweight endpoint agent and using its powerful analytics engine to assess risk.

The advantage of this non-intrusive risk assessment is that it allows an enterprise to modernize its approach to DLP. Instead of starting from a position of block and restrict, it can begin from an assumption that users have positive intent. This allows the enterprise to analyze data usage and risk without hindering workflow or productivity, but it can also, when needed, identify risks quickly. Moreover, this approach can help ease adoption by reducing potential impact on both user and operational experience.

Incydr builds its contextual view of data usage via wide-ranging integrations with multiple data repositories, including SaaS services such as OneDrive, Box, Google Drive, and, more broadly, Microsoft 365 and Google Workspace. Code42 supplements this list with good integrations into enterprise case management and legal systems, which helps further its understanding of users. All features are presented via an intuitive dashboard.

Code42 also provides a good native education platform via Incydr Instructor, which enables security teams to identify training opportunities and service them with both proactive and situational training as appropriate.

In our 2021 Radar report, we highlighted two areas of potential weakness. First was the platform's lack of built-in mitigation capabilities. However, this has been addressed to some degree via custom integrations with third-party access management and user identity tools (achieving this through integration is the usual approach for vendors). It's now possible through the management console to select appropriate immediate mitigation actions when risk is detected. For potentially malicious actions, this may include removing escalated privileges or reducing user access permissions. For actions that may be seen as accidental, it's possible to use the same approach to immediately point the user at the training modules of its Instructor platform. Currently, the range of actions within the platform are limited to manual mitigations, but this is not at the expense of its ability to send rich risk data to connected security orchestration, automation, and response (SOAR) tools that carry out more complex automated orchestrations to mitigate risk.

Secondly, we observed that the inability to automatically interrogate file contents for sensitive information may also be a concern. However, in the intervening period, it's clear that this is becoming less of an issue as enterprises focus more on threat management. This shift in focus means that the content of the data is less of a concern than the behavior of those who access it.

Code42 Incydr is a powerful threat detection platform, and as the market moves increasingly to a threat and risk management approach for DLP, this kind of

Strengths: Code42 claims its lack of reliance on data classifications allows Incydr to rapidly provide detailed insider risk analysis, which benefits return on investment (ROI). Access to this analysis is aided by an intuitive management dashboard allowing users to quickly identify issues. The solution also includes a broad range of integrations and has a good ability to track data movement across multiple platforms. The Instructor platform brings additional value and will help build user education and understanding.

Challenges: The threat and risk approach to DLP is increasingly the trend, but for enterprises whose approach is based around more traditional DLP blocking and classification, this may not be the right product. The introduction of mitigation actions is welcome, although they may still be a little limited for those looking at complex orchestrations that still rely on external integration.

CoSoSys, Endpoint Protector

CoSoSys Endpoint Protector is a well-established cross-platform endpoint DLP tool; the latest from a vendor that shipped its first DLP product in 2008.

The solution comprises four products that can be individually licensed: Device Control, Enforced Encryption, Content Aware Protection, and eDiscovery. Implementation offerings are flexible, with customers able to either take the product as a fully managed SaaS platform or deploy their own solution directly to a public cloud infrastructure as a service (IaaS) platform or on-premises as a virtual appliance (with support for multiple virtualization platforms).

CoSoSys has developed its solution impressively since our 2021 Radar report and addressed a number of identified weaknesses. This helped the company reach a broader range of customers, with success in larger enterprises as well as extending its presence in North America.

The technical model remains focused on endpoints and requires deployment of a lightweight agent across its supported operating systems (Windows, Linux, and macOS). As with all solutions that require an agent, this step may add installation complexity. However, the agent offers functional equivalence across all platforms, ensuring consistency of experience—an important part of easing adoption and simplifying management. It's also worth noting that as an endpoint-based solution, the agent can still enforce its DLP controls, even when users are disconnected from the network.

Since our 2021 Radar report, the solution's identity provider integration has been extended in the admin console to better support a greater number of identity management platforms and control access. Integration with security information and event management (SIEM) solutions has also been improved, now providing more detailed information to them to enable better reporting on endpoint behavior. Both of these improvements are essential for enabling a business to leverage existing investments.

Also notable is the addition of self-remediation for end users, which, with appropriate justification, allows users to share information that would otherwise be blocked. This feature helps improve efficiency and reduce management overhead.

These changes improved an already good platform; however, it's some of the vendor's longer-term aims that will be most appealing to enterprises. As anyone dealing with enterprise data security will appreciate, solutions introduced into a security stack should not only integrate with existing tools, but together they should all add value to each other by enriching information and enabling the orchestration of actions across the stack to more effectively secure data.

This is exactly how CoSoSys has planned to develop Endpoint Protector. It understands that its agent-based solution has information unique to the endpoint that can help the enterprise make more informed decisions around potential threats and mitigation steps. To achieve this goal, it's making significant investment in the solution's API capabilities, including enabling its server product to provide enhanced information to SIEM and SOAR platforms. It will also make the server tools fully manageable via API.

There are also plans to change the behavior of the endpoint agent by opening up its API capabilities. This will allow it to act not only as an agent, but also as a sensor, so it can feed rich information back to the broader enterprise security stack.

Getting these elements right is key to CoSoSys's ability to develop its customer base, especially in the larger enterprise.

There is potential risk here. While strategically its approach is in line with the industry, delivering this solution in a timely manner will be essential to achieving success. Many of these capabilities will be found in future releases. For now, the solution is still device-centric rather than user-centric, and still lacks some of the capabilities of its broader platform competitors.

Endpoint Protector is a good endpoint solution and CoSoSys is a company with big ambitions in this space, and one to consider as part of your DLP and data security strategy.

Strengths: Endpoint Protector continues to deliver a broad range of endpoint controls that are cross-platform and consistent on Windows, Linux, and Mac, which is a great help to those looking to drive adoption across mixed operating system estates. Improvements in how the management console operates and its ability to provide richer data to SIEM tools will make it more attractive to larger enterprises. With a good roadmap that shows the business developing quickly, this will be a platform of interest for those looking at intelligent endpoint DLP.

Challenges: Many of the key changes that will make this product interesting to a wider audience are planned for future releases. While the roadmap is in line with enterprise demand, its lack of in-deployment validation will be of concern to some. Those wishing for a single platform that covers more than just endpoints will also find it limiting.

DTEX InTERCEPT

DTEX Systems is one of a number of vendors that recognizes the importance of threat analytics as part of effective DLP. To assess threats, it looks broadly at a number of vectors to determine how any piece of information is being used. DTEX does not rely solely on data classification (although that still plays a role). Instead, it uses a data lineage approach, not looking at individual data actions in isolation but rather at the who, what, where, when, and why of usage to build a more detailed and accurate picture of user intent. The risk is then assessed, scored, and presented via an impressive dashboard that gives security teams the relevant threat information to make quick decisions on any specific risk, as well as the ability to anonymize information before sharing it so as to remove the risk of inherent bias.

A major concern had been its limited mitigation capabilities. Though it provided detailed threat indications, security analysts were not able to act upon them from within its system. Now, however, users can be disrupted and high-risk user activities can be shut off directly from the solution, either manually or automatically.

There's also been increased integration with endpoint protection platforms, such as Windows Defender, as well as platforms like Crowdstrike that deliver endpoint protection but do not offer DLP—an increasing trend among modern endpoint detection and response and extended detection and response (EDR/XDR) solutions. By integrating with these platforms, InTERCEPT can take rich data that better informs its platform and adds value to an enterprise's endpoint protection investment. The importance of finding security tools that integrate and add value to existing investments should not be underestimated.

InTERCEPT has also been improved in the way it interacts with users to both notify and educate them when their activities present potential risk. Rather than relying on pop-ups as it previously did, the solution now sends informative emails, using these as a way to deliver "teachable moments" to users to enhance their understanding of risk.

A significant value of DTEX's approach is in the way it allows a customer to adopt its technology. The enterprise is able to build a detailed picture of user threat and risk, allowing it to gain confidence in the efficacy of DTEX's solution before taking advantage of its enforcement and mitigation automation. By doing this, it reduces the problems posed by false positives and subsequently helps to improve adoption as well as ease the management and administration burden.

Interestingly, while DTEX's strategy has focused on user intent rather than more traditional data classification approaches to identify threats to data, it has recognized that classification does have a place. It has therefore developed integration with Microsoft's cloud-based data classification engine (and is doing so for Google DLP) to provide data classification capabilities to enhance its customers' data security approach where needed.

While the platform already supports good integration and management capabilities, InTERCEPT's ability to integrate more broadly via its extensive API access is excellent, allowing customers to build custom integrations and make InTERCEPT a core part of its enterprise security orchestration and automation toolset.

Since our last report, DTEX has worked very closely with MITRE to research how best to deal with data security threats as they evolve and how threats have changed in response to evolving enterprise operational environments, especially the growth of remote working. DTEX hopes this has helped it to become more accurate and effective in its approach. It's proud to be the first vendor to work with MITRE in this way.

With its focus on risk and threat management, DTEX InTERCEPT continues to offer a good solution for dealing with the evolving DLP threat landscape. However, while it's becoming clear that a threat-based approach is likely to become the norm for DLP, offering better context and fewer false positives for some, it may require more effort than those users are ready for, and so a more traditional DLP tool may be more appropriate. It should also be noted the solution is designed for larger and more complex enterprises.

Strengths: The holistic approach and wide-ranging integrations enable customers to build a very accurate model around risk and threat. Support for a broad range of endpoint devices helps to ensure robust coverage across the enterprise. The developments in mitigation automation in the solution since our previous report will increase its attractiveness.

Challenges: The product targets larger enterprises, potentially taking it out of the reach of some. Its approach based around understanding insider threats does need some investment, which may be off-putting for those looking for an "easier" path, even if the outcome of that work is a more context-rich and accurate solution.

Forcepoint

Forcepoint is an established and respected vendor in the security market, offering solutions with various capabilities since the mid 1990s. We didn't cover its DLP solution in our previous report, but Forcepoint is a strong vendor for consideration. The vendor, because of its maturity, has taken a more traditional approach; however, it's starting to develop a risk-adaptive DLP solution. This brings increased focus on insider risk and it uses this information to enhance the capabilities of its traditional rules-based DLP mitigation approach.

The solution is flexible, can be deployed on-premises and in the cloud, and it supports a hybrid approach as well for those that need it. It also includes a large number of out-of-the-box DLP policies that speed up initial adoption. A broad array of solution components supports cloud integration with major SaaS platforms, networks, servers, and a CASB solution to scan for potential risk across cloud applications. Forcepoint can use all of these infrastructure points to feed both its traditional and risk-adaptive DLP capabilities.

There's a good level of integration with other enterprise tools via APIs and REST APIs to support automation and orchestration of mitigation actions. This includes recently released REST APIs for policy management to enhance integration with SIEM and SOAR solutions. The endpoint client has support for Windows and macOS and provides good insight into end-user activity. It also includes an enforcement mechanism to capture and stop potential risky activity. Users are educated about the possible risk via popups to coach them and improve awareness.

Management and operations are streamlined, and a single management console delivers consistent management across the broad platform. The console looks a little dated compared to some competitors, though this should improve as the risk-adaptive DLP management elements are delivered via a fresher, cleaner interface. Data is presented more clearly, which allows admins and operations staff to quickly see changes in user risk scoring and investigate what's going on.

Forcepoint also integrates with both Microsoft Information Protection and Boldon James to provide classification and labeling capabilities for organizations that need more than just DLP, including an increased focus on governance and compliance.

The big development for Forcepoint DLP is the shift to the risk adaptive model. This is a strategic play meant to ensure that the company continues to advance in line with the evolution of the DLP market, which is becoming more risk- and threat-oriented, trying to mitigate risk while also allowing customers to be proactive in reducing threats.

The platform is well-liked by customers, although there are some complaints about the cumbersome nature of reporting and the legacy feel of its

some of these issues.

Forcepoint delivers an effective platform with a wide range of capabilities to not only identify risk but also enforce strong controls across the entire enterprise.

Strengths: The solution offers broad coverage across the enterprise from endpoint to network and cloud. Its traditional DLP functions are powerful, allowing for the deployment of granular and flexible controls. Customers like its ease of adoption with a broad range of out-of-the-box DLP policies. The shift to risk-adaptive DLP is important and ensures the company strategy will follow that of the industry in general.

Challenges: The move to risk-adaptive DLP is important for Forcepoint to keep it relevant in an adapting market. However, it's still early, and its solution may not have the maturity or capability of those that have been developing threat and risk management longer. The management consoles look a little dated (though this may be addressed in its new software release), and some customers report issues with the performance of the reporting tools.

HelpSystems (Digital Guardian)

Digital Guardian (DG) is well-established and well-regarded within the data security space, with a broad and robust platform that provides visibility and contextual awareness of data use, enabling a more accurate assessment of data risk.

The platform is described as cloud-native, with a SaaS-based main engine. However, some on-premises components are still needed to provide deeper insight and deal with more traditional areas, such as discovery and network DLP.

DG scored well in our previous report, and it remains strong in capabilities such as being able to warn of potential risks to data without predefined rules, good user notifications, clear dashboards, and broad platform coverage, which eases adoption and management for users and operations teams alike, and provides an enterprise with extensive protection across multiple repositories.

In October 2021, DG was acquired by HelpSystems, a software company with a focus on automation and security that has been moving along an aggressive acquisition trail, building a broad portfolio of solutions. The acquisition is already paying dividends; DG now integrates with some of HelpSystems' other acquired solutions, extending DG's already industry-leading capabilities and filling some gaps.

Three of HelpSystems' acquisitions in particular will be of interest to enterprises, especially those looking to consolidate their security stack and reduce the number of vendors they rely on.

The acquisition of Boldon James and Titus, a data governance and classification vendor, in June 2020, was the first step in enhancing DG's capabilities, particularly the ability to investigate data and build classification rules. While data classification may not be strictly necessary for DLP, for many enterprises it's a foundational element of their data security strategy and can help to define more robust data security rules.

DG's integration with HelpSystems' Vera (acquired December 2020) is also intriguing. An important evolution for DLP is the ability to protect data outside of the direct control of an organization. For many, this is achieved by integrating with Microsoft Information Protection (MIP), though few have native capabilities to do so. This is what Vera brings to DG as a self-contained information protection solution that allows DG to deliver robust controls to documents as they move outside of an enterprise. For those using MIP, this integration remains and can still be used. While Vera has some functionality gaps at present, it's a valid option for those who do not wish to invest in MIP.

One other significant technical move is DG's development of API integrations with SaaS platforms. Already developed for MS Teams, with others to follow, this native app platform integration begins a move away from reliance on endpoint agents. This will help DG to remain competitive against innovative vendors who have built their platforms in this way, reducing installation time, complexity, and risk.

An area of concern for some is pricing, though the HelpSystems acquisition resulted in some more aggressively priced license bundles targeting midsized businesses. Additionally, with DG now one of many products within a larger company's portfolio, there are questions as to whether its development focus will remain. However, initial signs are good, with portfolio integration already paying dividends. Where these integrations have occurred, there's also consolidated support with a single call to protect all elements of the DG platform. In fact, a single consolidated administration interface that covers the entire HelpSystems range is being developed.

DG remains a very strong offering for DLP, and while it retains its traditional capabilities, there is also a strong commitment to innovation. With access to the broader HelpSystems portfolio, it continues to develop capabilities and coverage that will certainly appeal to large and mid-sized enterprises.

Strengths: Already a strong solution, DG was made even stronger with capabilities from the HelpSystems portfolio, which have filled previous gaps. Clear dashboards and breadth of coverage will be valuable to those with complex estates and data in multiple repositories. HelpSystems' overall strategy will be attractive to enterprises that are keen to consolidate security vendors and want to focus on those with a broad portfolio of solutions.

Challenges: Cost will remain a challenge for some, especially at the smaller end, as will the need to deploy agents to fully exploit DG's capability, which adds complexity to the rollout for those with large and complex endpoint estates. The acquisition by HelpSystems will concern some, especially around continued development focus as well as uncertainty about whether the portfolio can be successfully integrated, although early signs are promising.

Microsoft DLP

In our previous report, Microsoft was positioned in the Challengers circle. Though its approach was comprehensive, it was limited in some areas, such as being very much focused on the Microsoft customer. To fully benefit from its impressive capabilities, customers had to be invested in the Microsoft cloud, specifically in Microsoft 365.

Though much of that remains true, it would be wrong to say Microsoft's DLP offerings have not improved. The company continues to invest in improving how its customers can build effective protection for their data using the powerful capabilities of its platform.

This ongoing investment in its security solutions gives customers a wide range of options for information security, from basic blocking of data to much more nuanced risk and threat management capabilities. Its DLP offering now sits within the Microsoft Purview brand, which brings its compliance portfolio and

securely use and share data as needed.

Microsoft's DLP is driven primarily via the former compliance console (now Microsoft Purview), which provides multiple elements to help deliver a DLP policy, including new services such as Priva to identify personal data and provide risk and threat analysis. Priva is a good example of Microsoft's development of its risk management approach (privacy risk in this instance), which helps an enterprise to identify risky behavior, regardless of the data being accessed, and act accordingly. As the threat of data loss becomes ever more complex, this risk- and threat-based approach is likely to become the standard for DLP.

Microsoft, as you'd expect, builds DLP into much of what it does across its cloud portfolio as well as third-party clouds via Microsoft Defender for Cloud Apps. It also extends to onboarded Windows 10 and 11 devices (with appropriate user licenses). These devices easily integrate with Microsoft's core DLP engine, allowing enterprises to build detailed insight into the use of data across a Windows estate. This integration has also been extended to macOS, with devices running Catalina 10.15 and higher also able to be enrolled into Microsoft's DLP offering.

DLP capabilities are extensive and easy to apply broadly across the infrastructure, with many of these capabilities seamlessly integrated into the Microsoft stack. DLP rules (and broader information protection rules) are also easily enforced on mobile devices via the Office suite and Microsoft mobile apps.

Microsoft has also put a lot of work into simplifying management and reporting, and bringing much of this together under Microsoft Purview is a good start. The administration console is improved and informative, but still falls a bit short in clarity and intuitiveness in comparison with other vendors. However, Microsoft's main data security and compliance controls, including risk and threat analytics, can all be found in the console, providing a more centralized management approach than it did previously.

However, some concerns still remain. For those not using the Microsoft cloud platforms, this solution is unlikely to be a contender. Licensing can still be complex and E5-level licenses are required to fully enable access to all capabilities. Some of the DLP rules are also difficult to get right, especially when working with the customization of sensitivity types, and troubleshooting rules can also be difficult.

That said, it's clear Microsoft takes its security stack seriously and continues to improve its capabilities and effectiveness. For those using Microsoft's cloud, this is a very effective and powerful approach that will meet the needs of most enterprises.

Strengths: The range of capabilities and seamless integration with Microsoft's broader 365 stack is impressive. Native support for Windows and its productivity applications means there's little end device configuration required, allowing for a quick and frictionless rollout. The capabilities of Purview are extensive, which allows an enterprise to build much further than more traditional DLP with investments in risk and threat management, which means enterprise investment here will not be wasted as more move to these approaches for DLP.

Challenges: Microsoft's management consoles are not as impressive as some of its key competitors, and not all features are as intelligent or easy to deploy as would be desired. Access to the full capabilities of these powerful tools is available only on the more advanced SKUs, which adds significant cost for those not already invested and will be off-putting to some.

Nightfall.ai

While Nightfall.ai was not included in our last report, we did have the opportunity to look at its approach and development plans, so it's good to see this intriguing approach to DLP is having success.

Formed in 2018, Nightfall.ai is designed as a platform on which its customers can rapidly develop their own bespoke solution. This isn't to say that Nightfall.ai has not already helped its customers by developing its own solutions and integrations with leading SaaS platforms, but the real power of the solution is its DLP engine.

The solution employs no endpoint agents or collectors to gather information about data usage, instead using an approach that is strictly API-driven. This allows it to deliver an almost native DLP capability to any application that can supply the necessary APIs to a developer armed with the Nightfall development platform and the requisite knowledge.

This is a particularly slick approach to the DLP challenge, with no need to place anything inline or to make any changes to workflow or user interaction. This in turn improves adoption and ease of implementation and reduces deployment risk. The solution exploits the platform's own capabilities to extract information that can then be pushed into the detection engine to build a picture of the risks posed to an enterprise's data assets. This native integration also helps to hide complexity from users, who don't see any changes to their application experience.

The solution also provides an attractive dashboard to "front end" its data usage intelligence engine, which is deployed as a SaaS offering (although it's also available as a custom on-premises build). The focus on accuracy will be appreciated by an enterprise considering this solution; the investment made in its ML capabilities is designed to help reduce false positives, which in turn reduces alert fatigue, simplifies management for ops teams, and reduces user adoption pushback.

Nightfall.ai has continued to invest in its developer platform, which will be key to its ongoing success. The developer platform provides a low-code solution to help developers quickly integrate its engine into enterprise applications, whether this is done with off-the-shelf apps (a number of which, such as Google Workspace, already have prebuilt integrations) or with custom apps, including those in the cloud as well as in the data center. These capabilities have led to the solution being used for new use cases by customers who have worked with the product's existing integrations and, with Nightfall's intuitive development platform, have quickly built their own and extended the application's use. The development platform provides customers with almost limitless potential to build integrations into any enterprise data repository.

The approach to remediation is also helpful, allowing much of it to be done within the enterprise application itself, rather than externally or within the Nightfall solution. This will also ease adoption and reduce challenges by allowing operations staff and users to handle DLP within familiar interfaces.

Nightfall's open API-driven approach to DLP will be increasingly adopted, especially with the ever-growing range of cloud apps in use by enterprises. Integrating directly with those cloud apps, rather than relying on DLP at the endpoint or network layer to address the risks of data leakage, is much more in

However, Nightfall.ai will not be suitable for all. The real power of the solution lies within the DLP engine and the accompanying developer platform. And while some prebuilt integrations exist for those who prefer an out-of-the-box solution covering a broad range of repositories to developing custom ones, some buyers may be put off.

That said, Nightfall.ai is a very attractive proposition for those who wish to develop a more bespoke DLP approach for their business and have the time and skills internally to take advantage of its developer platform. For those organizations, its rapid deployment, high accuracy, and developer-centric approach will be very attractive.

Strengths: The native API integration is slick and easy, and no infrastructure or agents need to be deployed for the detection engine to gather platform data to make judgments on risk. This enables rapid, low-cost deployment. A focus on accuracy is also welcome, as nothing derails the use of DLP more than low accuracy. The development platform provides the enterprise with an ability to create almost limitless integrations to protect its data in a vast range of repositories.

Challenges: The limited number of prebuilt platform integrations will be off-putting to those who do not wish to develop custom ones. The lack of end-to-end monitoring of endpoints and traditional infrastructure may also be a negative for some, as will the absence of user behavior analytics for those who wish to apply more context to their decision-making processes.

Proofpoint

Proofpoint is long-established in the security field. It scored well in our 2021 Radar report, was positioned in the Leaders circle, and has continued to develop its DLP solution. The solution scored well previously because of its people-centric focus, which ensured a more contextual approach was applied to risk, which then offered insight into the types of data being accessed as well as an understanding of by whom, why, and how the data is being used, leveraging the information to create a risk profile.

This people-centric approach is what has driven Proofpoint's continued improvement and has greatly strengthened its offerings. In recent years, Proofpoint has developed its platform via a number of smart acquisitions, building on its traditional email-based solutions. Since 2019, acquisition of ObserveIT, InteliSecure, and recently Dathena, has allowed it to reposition its solution from traditional DLP to a more modern threat management approach.

The solution's architecture comprises several major components: cross-channel DLP, endpoint, CASB, insider threat management, email DLP, and web security. All major components are cloud-based and feed the SaaS-delivered unified alert and remediation dashboard.

The solution also integrates well with third-party systems such as SOAR and SIEM solutions, as well as threat and identity platforms such as Palo Alto, Zscaler, and Okta. It also integrates well with third-party telemetry data, which brings additional richness to users accessing corporate data and helps reveal potential threats.

This breadth of infrastructure information gathering puts Proofpoint in a strong position to deliver detailed and accurate threat information, which can then be used to mitigate risk automatically, or to effectively plan a threat protection strategy.

One of its main developments since our last report was the shift from traditional DLP to a more insider threat management approach, in line with a number of key vendors in this space. While infrastructure integration plays a key part in this advance, it's significantly enhanced by the use of its dual-purpose endpoint agent. This agent can be used simply for DLP or, via a license activation, can also be used for insider threat management, collecting deep insight into all endpoint activity when a piece of data is accessed.

This detailed insight can be used to further fine-tune DLP rules to help reduce false positives. It can also be used to improve the identification of risky actions, so as to better understand user intent when accessing data.

Another major advance has been the integration of the Dathena solution, whose ML intelligence engine allowed Proofpoint to greatly enhance its data classification capabilities to help customers classify data at scale more effectively. This engine has huge value in easing an enterprise's adoption and management of the solution and helping to drive ROI more quickly. Using it in conjunction with insider threat analysis ensures that information at risk can be identified and protected more quickly.

The breadth of the platform also means it provides capabilities that are unique to Proofpoint's approach. For example, via its email protection platform, the solution can determine whether a user has recently been the target of a phishing attack, and this information can then be used across the broader solution to identify that user as potentially a higher risk.

The solution provides a number of powerful dashboards and reports to help executives and security professionals better understand the threat landscape in the organization. It also includes a supplier risk explorer module that allows an enterprise to gain insight into the security of its supply chain. This information is crucial in assisting relevant groups to ensure their enterprise data is protected across the entire supply chain.

The company has also invested in its own managed services (alongside a growing number of managed services from specialized partners), which allows an enterprise to use this powerful DLP and threat management platform as a service, an increasingly attractive option for many.

As with all vendors growing via acquisition, the main concern will be the ability to effectively integrate solutions together commercially and operationally.

Strengths: This is a solution that continues to develop, and the shift from traditional DLP to both DLP and threat management provides an impressively broad and effective solution. Its people-centric view of understanding intent rather than blocking based on content will help enterprises to be more effective in adoption and reduce user impact. The development of ML-based classification will also help customers more broadly understand their data and how it should be protected.

Challenges: Ensuring successful integration of an ever-expanding portfolio will remain a challenge that can impact manageability. However, the vendor is aware of this drawback, as some users report sluggish performance from the consoles and a disjointed administration experience.

6. Analyst's Take

innovative ways to try to steal valuable data assets.

Our research shows that the increased threat landscape is not only understood by malicious actors, but also by leading vendors that are actively working to find ways of staying ahead of the bad actors. This is evident in the number of vendors that appear in the Innovation half of our radar.

A key innovation is the shift away from traditional DLP, built around sensitive information and blocking, to a more comprehensive approach built around risk and threat management. This difference is important because understanding user intent will become increasingly valuable to enterprises as they seek to manage data security risks in the most effective way.

Noteworthy as well are changes in the way solutions are deployed, with increasing numbers of vendors turning to API-driven approaches to manage and orchestrate, as well as to integrate with platforms they aim to protect. SaaS-based solutions are increasingly dominant, although a number of solutions retain the option of on-premises deployment.

Vendors are also reacting to the need to ensure integration among all elements of the security stack, not only to ease management but also to ensure that they maximize the value of new and existing investments.

For those looking for new solutions in this space, the quality of the available options is excellent, as indicated by the number of vendors in our Leaders circle and the number of rapidly innovating Challengers who may offer a more specific solution or platform upon which an enterprise can build.

If you are looking to adopt a DLP solution or review and enhance an existing approach, our research raised a number of areas for consideration.

- First, consider whether your organization would be better served by a more traditional DLP approach or one based on advanced risk and threat management. A risk-based approach may take more time to adopt and implement but it may be more effective in the long term.
- It's also important to understand the types of platforms that need protecting, as this will help you understand the level of coverage needed. Does the solution require integration with SaaS platforms only? Or is more comprehensive network and endpoint coverage required?
- Consider as well the type of data security your environment needs. Are you interested in just stopping the misuse of data, or do you need to apply stricter governance and compliance controls? If so, solutions that offer data classification may be more appropriate.

This research offers insight into DLP, providing clarity about the challenges involved and the range of solutions available to meet the multiple demands of today's businesses.

7. About Paul Stringfellow

Paul Stringfellow
Paul Stringfellow has more than 25 years of experience in the IT industry helping organizations of all kinds and sizes to use technology to deliver strong business outcomes. Today that work focuses mainly on helping enterprises understand how to manage their data to ensure it is protected, secure, compliant, and available. He is still very much a "hands-on" practitioner and continues to be involved in a diverse range of data projects. Paul has been recognized across the industry and has spoken at many industry, vendor, and community events. He writes for a number of industry publications to share his enthusiasm for technology and to help others to realize its value.

Paul hosts his own enterprise technology webcast and writes regularly on his blog.

8. About GigaOm

GigaOm provides technical, operational, and business advice for IT's strategic digital enterprise and business initiatives. Enterprise business leaders, CIOs, and technology organizations partner with GigaOm for practical, actionable, strategic, and visionary advice for modernizing and transforming their business. GigaOm's advice empowers enterprises to successfully compete in an increasingly complicated business atmosphere that requires a solid understanding of constantly changing customer demands.

GigaOm works directly with enterprises both inside and outside of the IT organization to apply proven research and methodologies designed to avoid pitfalls and roadblocks while balancing risk and innovation. Research methodologies include but are not limited to adoption and benchmarking surveys, use cases, interviews, ROI/TCO, market landscapes, strategic trends, and technical benchmarks. Our analysts possess 20+ years of experience advising a spectrum of clients from early adopters to mainstream enterprises.

GigaOm's perspective is that of the unbiased enterprise practitioner. Through this perspective, GigaOm connects with engaged and loyal subscribers on a deep and meaningful level.

9. Copyright

Security & Risk

Knowingly Corporation
3905 State Street #7-448
Santa Barbara, CA 93105-5107

Subscribe to our monthly analyst insights

Stay on top of emerging trends by joining our newsletter, a monthly publication from our leading network of analysts.

Our Research

- Cloud, Infrastructure, & Management
- DevOps
- Data, Analytics, & AI
- Security & Risk
- Network and Edge
- People, Processes, & Applications

For Practitioners

- Research Subscription
- Analyst Videos
- TCO & Benchmark
- Radars
- Advisory Services
- Key Criteria
- Business & Technology Impact
- Sonars
- GigaBrief

For Vendors

- TCO & Benchmark
- Radars
- Key Criteria
- Business & Technology Impact
- Advisory Services
- Sonars
- Analyst Videos

- GigaBrief
- Value Engineering

Resources

- Blog
- Case Studies
- On-Demand Webinars
- GigaOm Research FAQs
- Guides

Company

- Why GigaOm
- Our Team
- Analysts
- Partners
- Press Room
- Careers
- Contact Us