



# The Data Security Imperative

How AI-powered Data Security From Palo Alto Networks Enables the Modern Workforce

Author: John Grady, Principal Analyst, Cybersecurity  
February 2026



# Contents

Executive Summary.....	3
Most Organizations Still Struggle to Protect Their Sensitive Data.....	3
Reasons Data Security Has Become More Complex.....	5
Key Requirements for a Holistic Approach to Data Security.....	7
AI-supported Classification and Detection .....	8
User Enablement.....	9
A SASE-based, Platform Approach .....	10
Unifying Data Security With Palo Alto Networks' Prisma SASE .....	10
Conclusion.....	13
Appendix.....	14
Methodology .....	14



## Executive Summary

As environments have expanded, data security has simultaneously become more important and more challenging. Organizations relying on traditional enterprise data loss prevention (DLP) approaches continue to struggle with data sprawl, insider risk, balancing user experience, and tool proliferation. This makes it difficult to understand where sensitive data resides, consistently manage and enforce policies, and enable users. Security teams today need a unified solution that delivers accurate classification and detection and comprehensive DLP coverage across all channels while not preventing users from doing their jobs. By offering AI-powered data security within its Prisma SASE solution, Palo Alto Networks helps customers consistently protect their data everywhere in their environment in a unified platform.

**By offering AI-powered data security within its Prisma SASE solution, Palo Alto Networks helps customers consistently protect their data everywhere in their environment in a unified platform.**

## Most Organizations Still Struggle to Protect Their Sensitive Data

Cybersecurity teams have more on their plate than ever. Environments continue to expand due to the use of cloud infrastructure, SaaS applications, and AI, with third-party users and unmanaged devices often requiring access to those resources. At the same time, the threat landscape continues to expand as attackers seek to exploit these changes and leverage AI

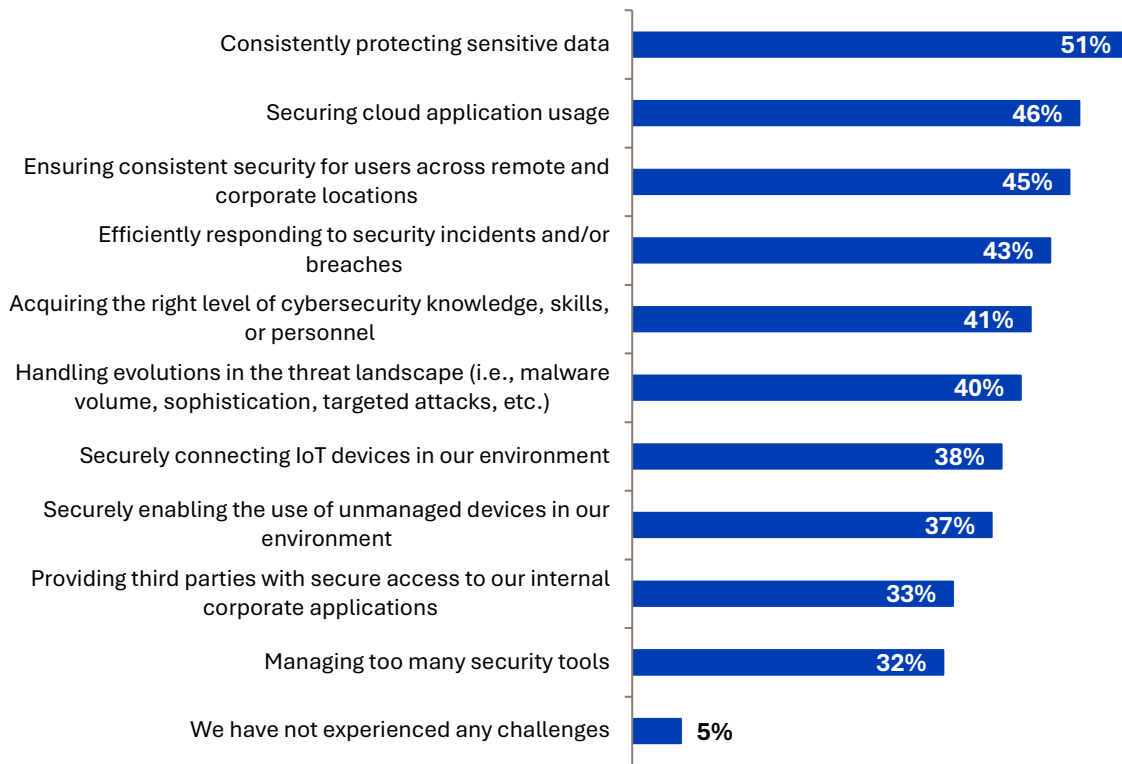
This Omdia White Paper was commissioned by Palo Alto Networks and is distributed under license from TechTarget, Inc.

to optimize their campaigns. Further, security teams themselves are stretched thin and asked to do more with less, often struggling to keep pace.

Yet even with all these issues at play, the most common challenge security teams said they face is consistently protecting sensitive data, which was cited by 51% of Enterprise Strategy Group (now Omdia) research respondents (see Figure 1).<sup>1</sup> Perhaps more importantly, these issues are not just hypothetical concerns. Over half (52%) of research respondents said their organization has experienced a sensitive data loss event in the last 12 months. Of those, 75% indicated they had experienced at least three such events over that period.<sup>2</sup>

Figure 1: Top Cybersecurity Challenges

**Which of the following cybersecurity challenges have been most impactful to your organization? (Percent of respondents, N=428, multiple responses accepted)**



Source: Omdia

<sup>1</sup> Source: Enterprise Strategy Group (now Omdia) Research Report, [Networking and Security Convergence: Assessing SASE Progress and Best Practices](#), September 2025.

<sup>2</sup> Source: Enterprise Strategy Group (now Omdia) Research Report, [Reinventing Data Loss Prevention: Adapting Data Security to the Generative AI Era](#), May 2025. All Enterprise Strategy Group research references and charts in this White Paper are from this report unless otherwise noted.

This Omdia White Paper was commissioned by Palo Alto Networks and is distributed under license from TechTarget, Inc.

## Reasons Data Security Has Become More Complex

The need to secure corporate data is certainly not a new phenomenon. Successful attacks can result in a variety of negative impacts, including financial loss, reputational damage, operational disruption, customer churn, and more. This makes data security an issue that both technology and business leaders must understand and work to address. Yet there are four key issues that make data security more challenging than ever: data sprawl, overcoming tool proliferation, insider risk, and balancing user experience.

### Data Resides Everywhere and Takes All Forms

The digital enterprise runs on data, and the fact that these environments are now distributed means that corporate data is spread across on-premises data centers, cloud environments, SaaS applications, a variety of devices, and now generative AI apps and large language models (LLMs). In fact, the organizations that have experienced data loss events in the last 12 months noted a myriad of locations from which it was compromised. Cloud storage and file sharing tools were the most common, cited by 46% of organizations, followed closely by generative AI-based applications (43%). But numerous channels of data loss are commonly seen (see Figure 2).

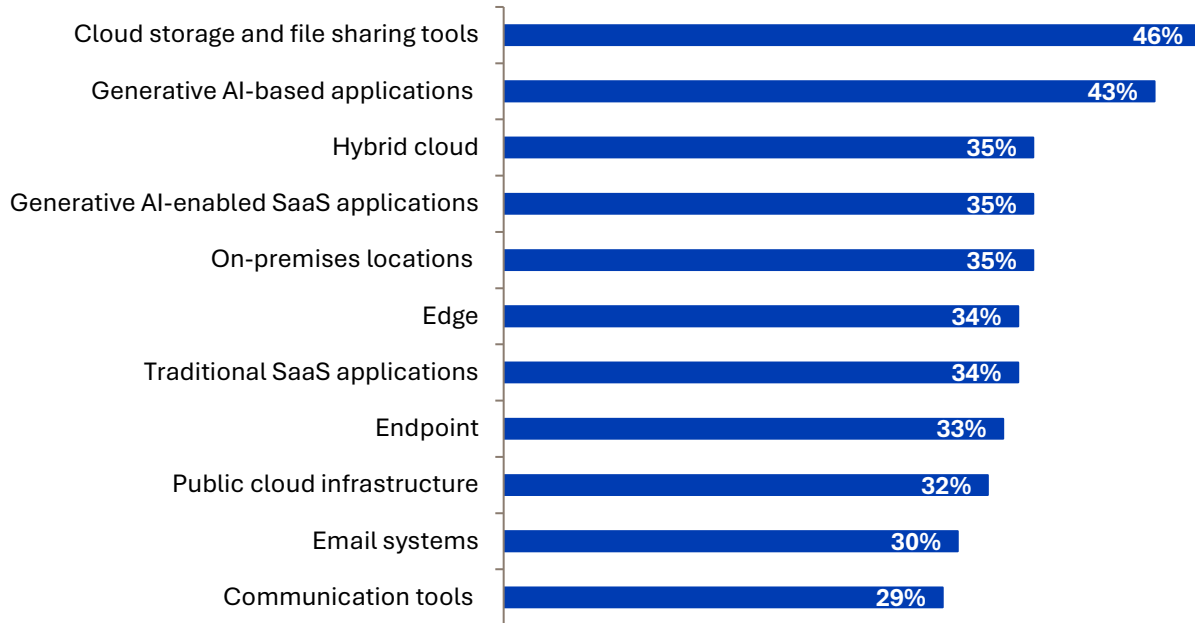
Further, this data can be structured or unstructured and live in a variety of file types, including pictures and audio, which makes securing the data via traditional means more difficult. Identifying a social security number in a spreadsheet full of customer information may be straightforward, but when that same data is unformatted and shared independently via a collaboration tool, visibility can become challenging.

On top of everything, regulatory pressures continue to mount as organizations must comply with broad federal laws such as the General Data Protection Regulation (GDPR), state mandates such as CCPA, or long-standing industry requirements such as HIPPA, while also navigating new regulations such as the EU's Digital Operational Resilience Act (DORA).

This Omdia White Paper was commissioned by Palo Alto Networks and is distributed under license from TechTarget, Inc.

Figure 2: Locations From Which Data Was Lost

**From which of the following environments did your organization experience a sensitive data loss event in the last 12 months? (Percent of respondents, N=193, multiple responses accepted)**



Source: Omdia

### Disconnected Tools and Policies Lead to Failure

According to the research, enterprises deploy 6 DLP tools, on average, including both discrete DLP tools as well as other tools having DLP functionality. Ensuring consistent policies across these tools for data residing in different locations becomes, at best, an inefficient task and, at worst, an impossible one. In fact, 96% of organizations said the administration and maintenance of their existing DLP technology solutions and policies is at least somewhat challenging.

We've seen security tools in other parts of the stack shift to a platform approach with centralized management and distributed enforcement to provide better security consistency and operational efficiency, with secure access service edge (SASE) being a key example. Data security has reached a tipping point of diminishing returns from siloed point tools. Unfortunately, many organizations continue to follow this approach.

### Users Continue to Be the Weakest Link in the Chain—Even When They Don't Realize It

There are many root causes of data loss incidents; however, many tie back to the users themselves. These incidents can be both intentional and unintentional:

This Omdia White Paper was commissioned by Palo Alto Networks and is distributed under license from TechTarget, Inc.

- 32% cited incidents resulting **from the misuse or sharing of data** with unauthorized users.
- 30% cited incidents from **insiders or authorized users who intentionally or maliciously share** unstructured sensitive data with external parties.
- 28% cited incidents by **insiders or authorized users who unintentionally or negligently share** unstructured sensitive data with external parties.
- 27% cited incidents **due to the misuse of an account via stolen credentials**.

Context matters more than ever to understand not just the user and the data but the intent behind the access.

### Security Teams Can No Longer Simply Say ‘No’

Years ago, security teams had more control, and if they introduced some friction to better ensure protection, that was accepted. Today, businesses cannot afford to work that way. Users need to access and share even sensitive data where appropriate, but with guardrails in place to prevent unintentional exposure. This makes it more difficult for security teams to do their jobs, especially with traditional tools that make binary allow/block decisions. IT and business leaders want the best of both worlds: strong security with a frictionless user experience.

## Key Requirements for a Holistic Approach to Data Security

The concept of unified, multi-channel data security is not new, but, to date, success in this area has been limited. Enterprise DLP tools have been around for years but were historically hard to tune and prone to false positives or false negatives. Dedicated DLP solutions offered custom classifications and stronger detection but were difficult to use. Further, while they may have offered coverage for networks, endpoints, email, and other channels, they often failed to fully unify policy management. Alternatively, DLP capabilities were available in tools for web security, SaaS security, and other solutions but were limited to regular expression and keyword detection rather than supporting custom classification. This limited security effectiveness and, similarly, led to management complexity.

This Omdia White Paper was commissioned by Palo Alto Networks and is distributed under license from TechTarget, Inc.

To properly protect data in today's complex environments, security teams need a new approach that improves visibility, reduces complexity, and, ultimately, enables users to do their jobs without putting sensitive data at risk. This requires advanced, enterprise-grade DLP supported by AI, natively integrated as part of a multi-channel platform to unify protection and management. This approach should help reduce deployment and management complexity, promote consistency, and, ultimately, improve data security efficacy.

**To properly protect data in today's complex environments, security teams need a new approach that improves visibility, reduces complexity, and, ultimately, enables users to do their jobs without putting sensitive data at risk.**

## AI-supported Classification and Detection

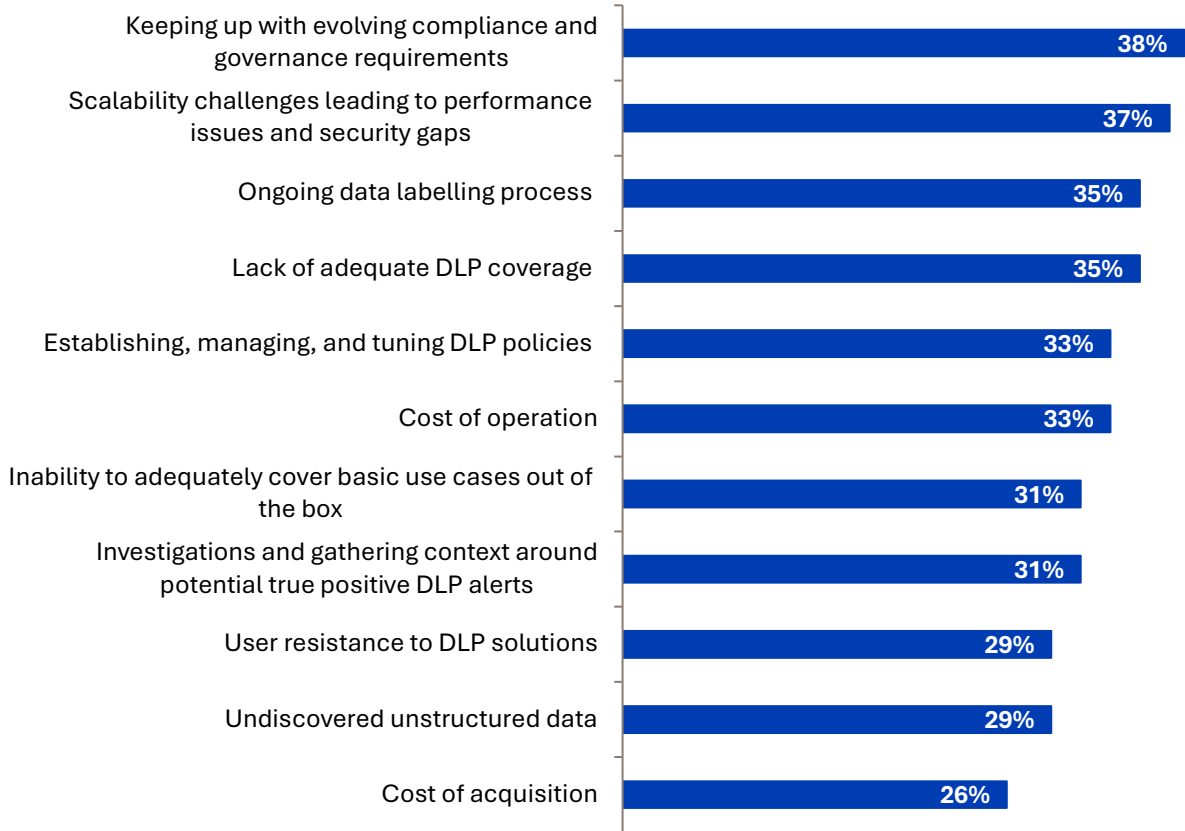
Security starts with visibility, and with regard to data security, organizations are struggling with this fundamental step. Specifically, 35% cited frustration with ongoing data labeling processes; 33% with establishing, managing, and tuning DLP policies; 31% with out-of-the-box coverage; and 29% with undiscovered unstructured data (see Figure 3).

There are countless examples of how AI can help security teams, but data security is one of the most promising. Rather than relying on either fully predefined patterns that leave gaps or fully custom data classification that doesn't scale, AI-powered classification not only greatly expands out-of-the-box classifications but also continuously learns to increase accuracy. AI-powered analytics also help to classify and detect unstructured data that traditional solutions miss. From a detection perspective, improved accuracy via AI-enabled detections can help improve operational efficiency. Organizations report that, on average, 38% of DLP alerts turn out to be false positives. This results in untold time being wasted chasing alerts that are not actually incidents.

This Omdia White Paper was commissioned by Palo Alto Networks and is distributed under license from TechTarget, Inc.

Figure 3: Frustrations With DLP Technology

**What are your organization’s biggest frustrations with DLP technology? (Percent of respondents, N=370, multiple responses accepted)**



Source: Omdia

## User Enablement

Historically, data security has been a binary motion: Determine who the user is and what data they are accessing and issue an allow or block decision. Today, there are more inputs than ever to assess. The user and the data remain the baseline, but the application, device, and context of the user’s activity is critical information that must be considered:

- From an application perspective, uploading certain types of data to a corporate ChatGPT instance may be permissible, while the same upload to the public version may be deemed a risk. This makes understanding the difference between the instances and enforcing different policies critical.
- Similarly, security teams may want to consider different policies when users access data from a corporate-issued managed device versus an unmanaged device.

This Omdia White Paper was commissioned by Palo Alto Networks and is distributed under license from TechTarget, Inc.

- Even when all the right boxes are checked, taking the user’s activity and the resulting risk level into account is important. Attackers using stolen credentials, as well as malicious or negligent insiders, can appear benign on the surface even when they are not.

Flexibility in dealing with the various permutations of these scenarios is critical. Rather than simply blocking a user trying to share data with a public generative AI application instance, a better alternative may be a policy to coach and direct them to the corporate instance. Instead of blocking access from an unmanaged personal device, a policy granting restricted read-only access may be enough in some instances, which allows the user to remain productive.

## A SASE-based, Platform Approach

SASE architectures have become the default standard for securing user access to public applications (including generative AI), private applications, and the internet. This access ultimately results in users interacting with data, which makes it a logical place for modern DLP to live. While not always thought of as a core SASE capability, nearly half of organizations said DLP will be a starting point (25%) or secondary consideration (24%) in their SASE adoption,<sup>3</sup> showing the growing connection between the two.

A SASE-based platform approach to DLP converges both the management and enforcement of policies across all channels, including the network perimeter, the cloud, the endpoint, and the browser, which is most often used to access corporate data. Further, specific coverage for generative AI applications has become particularly important as usage has grown and the risk of sensitive data being uploaded to these applications has risen. Because SASE often connects users to all these resources and locations, it only makes sense that data security should be a key component of the architecture.

# Unifying Data Security With Palo Alto Networks’ Prisma SASE

Palo Alto Networks Enterprise DLP, as part of its Prisma SASE platform, helps customers consistently protect sensitive data across their entire environment and over all channels. Because Prisma SASE helps secure access for internal and external users, accessing cloud, on-premises, SaaS, and generative AI applications from managed and unmanaged

---

<sup>3</sup> Source: Enterprise Strategy Group (now Omdia) Research Report, [Networking and Security Convergence: Assessing SASE Progress and Best Practices](#), September 2025.

This Omdia White Paper was commissioned by Palo Alto Networks and is distributed under license from TechTarget, Inc.

devices across corporate and remote locations, DLP coverage is provided across on-premises networks, cloud, hybrid users, email, endpoints, and more. This architecture enables customers to uniformly consume the same Enterprise DLP capabilities and functionality across multiple pillars of its SASE estate. Three of the most important areas include:

- **SaaS security.** SaaS security starts with discovering and classifying the SaaS applications in use across the organization, including shadow usage. Only then can protection be put in place. As part of this process, Enterprise DLP helps security teams understand the sensitive data (both data-at-rest and data-in-motion) within these applications and then apply policies to prevent leakage. This includes minimizing inadvertent exposure and reducing malicious insider risk. This not only helps improve security but supports and simplifies compliance efforts as well.
- **AI access security.** While, in many ways, public generative AI applications are an extension of the SaaS ecosystem, the way these applications consume and disseminate data creates the need for a dedicated set of controls. This includes real-time visibility of not only access but also usage relative to the prompts being entered. At this point, access control policies can be created based on risks such as whether the application trains on data. From an Enterprise DLP perspective, the data being uploaded to these applications can be controlled on an instance-by-instance basis.
- **Prisma Browser.** Last mile Enterprise DLP controls can also be implemented in the browser via Prisma Browser. Because activity-level controls are visible in the browser, actions such as copy/paste, upload/download, share, print, screenshot, and more can all be controlled. This differs from traditional DLP policy models that primarily had allow or block capabilities, enabling adaptive, context-based responses and minimizing business friction. This architecture supports consistent data security across the environment, from discovery to enforcement.

## Enterprise DLP

Palo Alto Networks' Enterprise DLP is driven by Precision AI® data classification. This provides more than 140 AI-based classifiers out of the box to automate data discovery and classification. Pattern matching with regex and keywords is augmented with ML models, which are trained on diverse datasets, leveraging LLMs. This improves accuracy and reduces false positives. Hundreds of out-of-the-box data patterns augmented with ML and LLMs are available across categories such as personally identifiable information, GDPR requirements, financial, and more.

Palo Alto Networks also leverages a customer-driven feedback loop where users can report false positives for specific detections, along with the reasoning for context. Additionally, for customers that need more specificity, Enterprise DLP allows for models to be trained with

This Omdia White Paper was commissioned by Palo Alto Networks and is distributed under license from TechTarget, Inc.

sample intellectual property (IP) to find exact matches or similar datasets based on custom thresholds. These models can be tuned and retrained to ensure high accuracy and expanded over time to cover new types of IP.

Enterprise DLP also supports security and IT teams with unified intelligent and proactive operations. Consistent security is ensured with a single set of policies and unified management across all enforcement channels. Rules can be easily adjusted across all channels to ensure compliance. This simplifies workflows for improved operational efficiency and reduces the chance of manual errors from replicating policies.



## Conclusion

For too long data, security and DLP, in particular, have been relegated to a check box item to meet compliance mandates—not because protecting sensitive data is unimportant but because the tools available failed to meet the needs of the modern, distributed enterprise. However, the criticality of protecting sensitive data to maintain business operations, ensure customer trust, and prevent financial repercussions has never been clearer.

Security teams need a new approach that not only improves classification and detection accuracy but is also usable, promotes management efficiency, and acts as an enabler, rather than a blocker, to user productivity. Palo Alto Networks' AI-powered Enterprise DLP coupled with Prisma SASE helps customers unify data security and consistently protect data everywhere in their environment across all channels.

# Appendix

## Methodology

The conclusions in this white paper are the opinion of the analyst, supported by multiple surveys of North American IT decision-makers responsible for data security and secure access service edge.

**John Grady, Principal Analyst, Cybersecurity**  
[askananalyst@omdia.com](mailto:askananalyst@omdia.com)



### Omdia consulting

Omdia is a market-leading data, research, and consulting business focused on helping digital service providers, technology companies, and enterprise decision makers thrive in the connected digital economy. Through our global base of analysts, we offer expert analysis and strategic insight across the IT, telecoms, and media industries.

We create business advantage for our customers by providing actionable insight to support business planning, product development, and go-to-market initiatives.

Our unique combination of authoritative data, market analysis, and vertical industry expertise is designed to empower decision-making, helping our clients profit from new technologies and capitalize on evolving business models.

Omdia is part of Informa TechTarget, a B2B information services business serving the technology, media, and telecoms sector. The Informa group is listed on the London Stock Exchange.

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help your company identify future trends and opportunities.

### Get in touch

[www.omdia.com](http://www.omdia.com)  
[askananalyst@omdia.com](mailto:askananalyst@omdia.com)



### Copyright notice and disclaimer

The Omdia research, data, and information referenced herein (the "Omdia Materials") are the copyrighted property of TechTarget, Inc. and its subsidiaries or affiliates (together "Informa TechTarget") or its third-party data providers and represent data, research, opinions, or viewpoints published by Informa TechTarget and are not representations of fact.

The Omdia Materials reflect information and opinions from the original publication date and not from the date of this document. The information and opinions expressed in the Omdia Materials are subject to change without notice, and Informa TechTarget does not have any duty or responsibility to update the Omdia Materials or this publication as a result.

Omdia Materials are delivered on an "as-is" and "as-available" basis. No representation or warranty, express or implied, is made as to the fairness, accuracy, completeness, or correctness of the information, opinions, and conclusions contained in Omdia Materials.

To the maximum extent permitted by law, Informa TechTarget and its affiliates, officers, directors, employees, agents, and third-party data providers disclaim any liability (including, without limitation, any liability arising from fault or negligence) as to the accuracy or completeness or use of the Omdia Materials. Informa TechTarget will not, under any circumstance whatsoever, be liable for any trading, investment, commercial, or other decisions based on or made in reliance of the Omdia Materials.