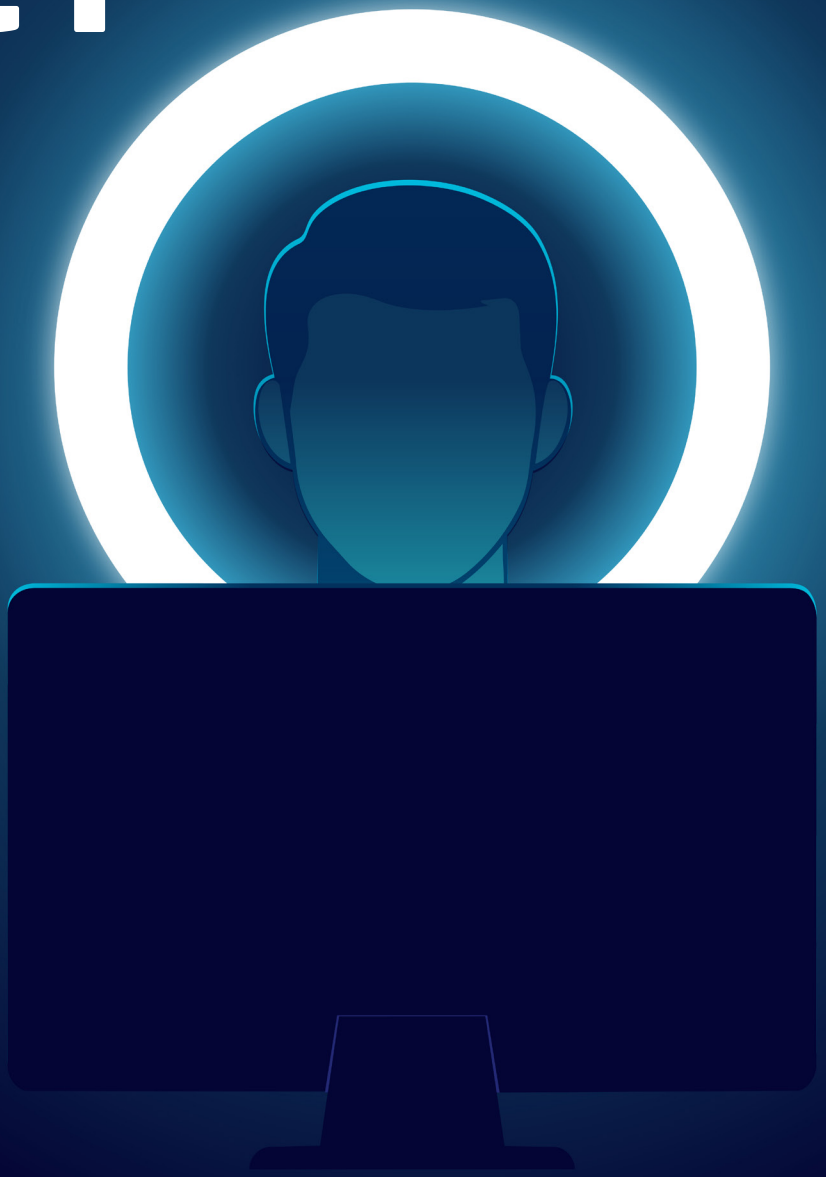
2026

THALES

CYBERSECURITY

THE HALO EFFECT

7 key ways data management can deliver better security outcomes



cpl.thalesgroup.com

#TheHaloEffect

Table of Contents

Introduction

Security-centric data management lies at the heart of the highly secure IT environment that CISOs strive to deliver. But what separates the organizations that truly master it from those that are still catching up?

New research identifies a group of standout performers – **Data Management (DM) Masters** – defined by two core capabilities: they have complete knowledge of where their data is stored across the organization, and they have fully classified that data. When compared against **Data Management (DM) Laggards** – organizations with little confidence in where their data lives and who can classify very little of it – the differences in security outcomes are striking.

The conclusion is clear: good data management underpins great information security. For CISOs, that mastery manifests as DSPM (Data Security Posture Management), moving the organization from reactive firefighting to proactive risk orchestration.

This research was based on a global survey of 3,120 respondents fielded via web survey with targeted populations for each country, aimed at professionals in security and IT management, with annual revenue of less than US$100 million and with US$100 million-$250 million in selected countries. This research was conducted as an observational study and makes no causal claims.

Conducted by

S&P Global
Market Intelligence

Source: 2026 Data Threat Report custom survey from
S&P Global Market Intelligence 451 Research, commissioned by Thales.

The Halo Effect

7 key ways Data Management (DM) Masters pull ahead

A more risk-aware data culture, with less risk of human error

Only 45% **of DM Masters** say human error is the root cause of cloud management infrastructure attacks compared to **57% of DM Laggards**. DM Masters are also less likely to store sensitive data in the cloud.

Less susceptible to AI/LLM attacks

Only 18% **of DM Masters** experience unbounded consumption attacks compared to **63% of DM Laggards**.

Much less likely to fail a compliance audit

81% **of DM Masters** passed their most recent audit vs **14% of DM Laggards**

Ready to respond to new data sovereignty challenges

31% **of DM Masters** treat physical cloud location as critical for all workloads compared to **20% of DM Laggards**. DM Masters rely on data discovery and classification as the essential first step to navigating any jurisdiction shift.

Much less likely to be breached in the cloud

67% **of DM Masters** are unbreached in cloud vs **35% for Laggards**. DM Masters reduce their attack surface through good data practices and controls.

A simpler, more coherent toolset

44%

of DM Masters are likely to use 4 or fewer data management tools and are more likely to avoid tool sprawl compared to Laggards.

Better prepared for a quantum future

46%

of DM Masters are actively exploring quantum computing vs **42% of Laggards**.

1. Much less likely to fail a compliance audit

Compliance isn't just a checkbox; it's a byproduct of high-quality data governance. For organizations in regulated sectors such as finance, healthcare, defense, and energy, a compliance audit is a high-stakes investigation. Whether navigating SOC 2, ISO, GDPR, CCPA, PHI, or SOX, the regulatory burden is heavy and growing.

Data Management Masters are nearly 6x less likely to have failed a compliance audit in the past 12 months compared to Laggards. Overall, just 14% of DM Laggards say they did not fail a compliance audit, which is a striking contrast to the 81% of DM Masters who have not failed such an audit. This is in part due to a greater emphasis on DSPM, which provides automated, continuous visibility into where sensitive data is stored, making good compliance an ongoing state of being rather than an unexpected fire drill. Good compliance also reduces breach risk, avoids fines, and cuts the overall cost of keeping pace with regulation.

NEARLY 6X LESS LIKELY TO FAIL COMPLIANCE AUDIT IN THE PAST YEAR

Question: Has your organization failed a compliance audit in the past 12 months? Answer: No

2. Less susceptible to AI/LLM attacks

The explosion of AI and agentic tools is transforming the data security landscape. LLM integration introduces new attack vectors that firewalls and traditional defences aren't designed to catch – from deep fakes used to capture sensitive information, to unbounded consumption attacks that overwhelm a company's AI infrastructure with a flood of complex requests, spiking costs and potentially crashing servers.

DM Masters experience fewer AI/LLM attacks across the board. Their progress on data management and classification puts them in a stronger defensive position. The contrast with Data Management Laggards is sharp: **DM Laggards are more than 3x more likely to see increases in unbounded consumption attacks**. DM Masters are also less likely to be experiencing the single fastest-growing threat – deep fake-related misinformation. Better data management delivers greater risk visibility and control.

3X LESS LIKELY TO SEE AN INCREASE IN UNBOUNDED CONSUMPTION AI/LLM ATTACKS

Question: Which type of AI/LLM attacks are you seeing increase? Answer: Unbounded Consumption

3. A more risk-aware data culture, with less risk of human error

Cloud storage offers infinite scalability, but it also creates a vast perimeter that is difficult to police. Sensitive data finds its way into the cloud through shadow IT, developer testing, automated backups, and countless other routes that are hard to monitor without the right practices in place.

When Data Management Masters do experience cloud infrastructure attacks, human error or misconfiguration is a root cause in 45% of cases, compared to 57% among DM Laggards. This reflects a more risk-aware data culture built through strong data management practices. DM Masters are also less likely to store sensitive data in the cloud in the first place: an average of 50% of their cloud-stored data is sensitive, versus 54% for DM Laggards. The difference may seem small, but at enterprise scale this can represent petabytes of exposure.

4. Ready to respond to new data sovereignty challenges

Against a backdrop of significant geopolitical volatility, organizations are facing real uncertainty about where to store their data. Some that previously insisted on in-country data centers are moving to offshore clouds due to heightened risks of attack; others are doing the reverse. Other options are also gaining traction, such as disconnected cloud. Along with these shifts, CISOs are exploring new key management options, including BYOK (bring your own key) and HYOK (hold your own key), which in turn enable a "cloud your way" approach that provides maximum flexibility.

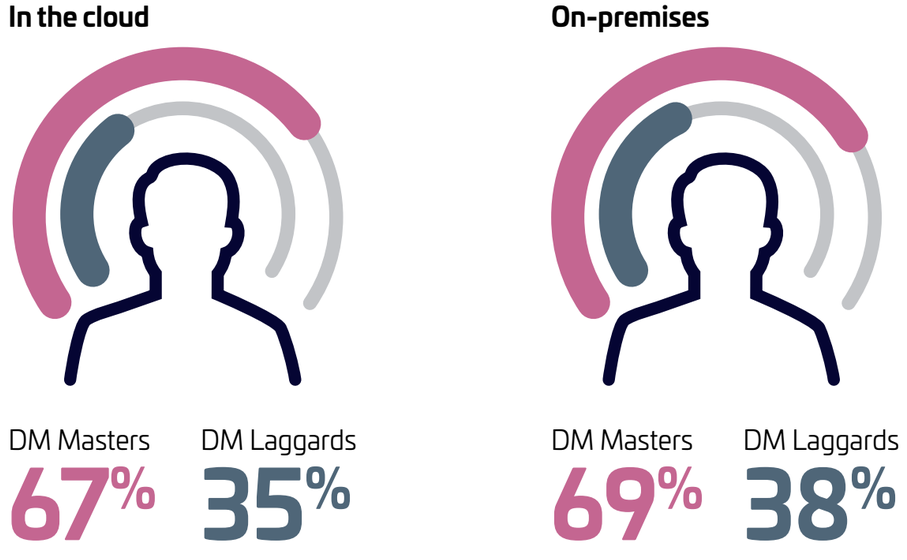
For any organization navigating a shift in jurisdiction, and thus a revised approach to data sovereignty, the fundamental first step is data discovery and classification (DDC). This is precisely where Data Management Masters shine; they are significantly more likely to say that the physical location of cloud infrastructure is important for all workloads (31% vs 20%), reflecting a more disciplined, sovereignty-aware approach to data placement.

5. Much less likely to be breached in the cloud

Data Management Masters are nearly half as likely to report having been breached — whether on-premises or in the cloud. In the cloud, 67% of DM Masters reported no breach, versus just 35% of DM Laggards. On-premises, the gap is similarly stark: 69% versus 38%.

This isn't luck. It's the product of good data practices and controls that reduce the attack surface. In a breach landscape that increasingly relies on "logging in" rather than "breaking in" – exploiting legitimate but compromised credentials – organizations that know their data and govern access to it are simply harder to compromise. DM Masters are more likely to have tools that automatically flag or block configurations that don't meet security policies, preventing the kind of simple misconfigurations, such as a database set to "public" instead of "private", that leaves the door open to attackers. Among DM Masters who have experienced a breach, human error is less likely to be the root cause as a result: this is the case for 27% of cases, compared to 34% for DM Laggards. In turn, this reduces the potential size and costs of breaches and also supports improved regulatory adherence.

NEARLY 2X LESS LIKELY TO BE BREACHED IN THE CLOUD



Question: Has your organization ever been breached? Answer: No

6. A simpler, more coherent toolset

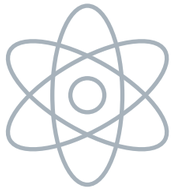
Tool sprawl is a hidden security risk. When organizations rely on dozens of disconnected tools, each one creates a new data silo. If the cloud security tool doesn't communicate with the identity management tool, attackers can move between them undetected.

Data Management Masters recognize this. They are more likely to use four tools or fewer across all data management areas, giving them greater coherence and fewer gaps. DM Laggards, by contrast, are more likely to struggle with compatibility issues when trying to consolidate their security tooling. Many DM Masters are moving toward unified DSPM platforms — integrating data discovery and risk assessment into a single tool. This cuts complexity while increasing effectiveness, particularly when it comes to identifying, assessing, and remediating risks.

7. Better prepared for a quantum future

Quantum computing presents enormous promise — and significant new security risks. The so-called quantum apocalypse is a definite threat; many governments and banks are already developing strategies to mitigate it. DM Masters are more likely to be actively experimenting with quantum computing or exploring options for it (46% vs 42% for DM Laggards).

The three core steps in quantum preparedness — discovery (providing an inventory of vulnerable assets), risk analysis, and remediation — map directly onto the strengths of DM Masters. Those who are better at data management and classification have a head start on the quantum journey, with the inventories, classification frameworks, and risk protocols already in place.



What separates the best from the rest

The research paints a consistent picture: **those organizations that invest in knowing where their data lives and what it is – and that build the tools, processes, and culture to manage it properly – realize compounding security benefits across every threat vector**.

In turn, many are pushing to reduce complexity and anticipate new risks. As part of this, **many are making use of DSPM as a strategic capability**: providing automated discovery, classification, and remediation, and maintaining a virtuous circle of increased security without added tool proliferation. If DSPM provides the radar, data protection is the shield. Good data management is the foundation that supports great information security.

The DSPM difference

What connects the DM Masters is Data Security Posture Management (DSPM), which provides the conditions that make data mastery possible. Organizations that understand their data – where it is, what it is, who can reach it – are the ones that outperform.

Request a demo →

THALES

CYBERSECURITY

cpl.thalesgroup.com/data-threat-report

For contact information, please visit
cpl.thalesgroup.com/contact-us