

THALES

CYBERSECURITY

How and Why CISOs Drive DSPM Adoption

CISOs have more
responsibility – and more
problems — than ever.

cpl.thalesgroup.com



Table of Contents

The Changing CISO Remit

3

Part 1: The Two Traps of Incomplete DSPM

4

- The Visibility Trap: Discovery Without Risk Reduction
- The False Protection Trap: Security Controls Without Prioritization

4

5

Part 2: What Complete DSPM Looks Like

6

- Complete DSPM Restores Visibility
- Complete DSPM Turns Visibility Into Action
- Complete DSPM Solves the False Protection Trap
- Complete DSPM Provides Tangible Board ROI

6

6

6

6

Part 3: How CISOs Can Drive Complete DSPM Adoption

7

- Governance, Risk, and Compliance Teams
- Breaking Down Organizational Siloes
- Remediation Teams
- The Board
- Start With the Crown Jewels
- Name the Non-Negotiable Constraints
- Resource capacity is the second
- The Model Comes Before the Tool
- Resource capacity is the second

7

7

8

8

9

9

9

9

9

Conclusion

10

The CISO's Strategic Checklist

10

- Crown Jewel Approach
- Managing Down: Team and Operations
- Managing Up: Board and Business Impact
- Constraints and Trade-offs

10

10

10

10

About Thales

11



The Changing CISO Remit

AI adoption and cyber resilience have come to dominate boardroom discussions, which means CISO's remits have expanded beyond traditional cybersecurity responsibilities and into broader data governance and business continuity discussions. Today, CISOs are expected to influence and help govern areas including privacy, operational resilience, and operational technology security.

Boards are also demanding insight into what AI systems access, but CISOs can't always provide accurate answers. The problem is that many legacy solutions provide some coverage, but often lack the visibility, context, and governance needed for AI agents and autonomous systems. That means CISOs are increasingly being held accountable for data-related risks that extend beyond the visibility and control offered by legacy security frameworks.

Regulatory authorities are further complicating matters, with regulations like PCI DSS 4.0, HIPAA, and NIS2 requiring organizations to prove they can implement continuous monitoring, rapid remediation, and demonstrable risk reduction.

These compounding demands mean CISOs have the difficult job of both managing down, making their teams more proactive by improving operational efficiency and resource allocation, and managing up, translating security outcomes into business language.

But not all of this risk is organizational. Some of it lands squarely on the CISO as an individual.

Boards often hold CISOs personally or legally accountable for incidents, and around 77% of security leaders fear losing their jobs after a breach.

In response to these rising stakes, many CISOs are turning to Data Security Posture Management (DSPM). According to Gartner, DSPM adoption is accelerating rapidly and becoming a foundational data security capability, primarily due to AI adoption, cloud migration, and regulatory pressure. Rather than being driven solely by security teams, DSPM adoption is increasingly tied to broader business initiatives around AI governance and data management.

Many CISOs deploy DSPM to solve a visibility problem, but visibility alone is not the value. The real challenge is measurable risk reduction. Customers, regulators, and boards hold CISOs accountable for every material data exposure, regardless of whether it originates from a human user, API, cloud workload, or AI system. If DSPM only identifies risk without reducing it, the organization gains awareness, but not control.

CISOs are not measured on how much risk they can see; they are measured on how much risk they can reduce. The true benefit of DSPM comes from helping security teams identify, prioritize, remediate, and continuously monitor data exposures across the enterprise.

Part 1:

The Two Traps of Incomplete DSPM



The Visibility Trap: Discovery Without Risk Reduction

The first trap is deploying DSPM and expecting discovery to lead to action. Visibility offers the illusion of control, and security teams become very good at measuring exposure. But they don't necessarily shrink exposure windows.

The result? CISOs assume they're protected, and go into board meetings armed with productivity metrics — dashboards showing real-time visibility — but can't show how much they've actually reduced risk.

Ambiguous audit requirements don't help matters. Many auditors see that an organization has deployed DSPM but fail to validate whether risk reduction and remediation processes are in place. The organization passes the audit, so the CISO assumes they're doing everything right.

Organizational silos are the final obstacle to effective risk reduction. Governance and compliance teams often define requirements that lack operational specificity. Security teams deploy tools and generate findings, while data owners and operational teams are responsible for remediation. Without clear accountability across these groups, discovery becomes disconnected from action.

Confidence without action is a liability. Identifying thousands of exposures is only valuable if organizations can prioritize the risks that matter most and resolve them quickly. Otherwise, exposure remains unchanged.



The False Protection Trap: Security Controls Without Prioritization

The other trap is deploying DSPM alongside strong encryption, access controls, and DLP, but failing to prioritize which data those controls protect.

The result is a dangerous illusion of security: organizations assume their most critical data is protected, but without a process to continuously discover and re-evaluate what falls outside that protected scope, significant exposures stay invisible by default. They often only surface during an audit, regulatory investigation, or breach.

The reason is structural. Machine identities, APIs, third-party integrations, and automated

workflows create data access paths that fall outside traditional security tools and the organization's protection model.

This typically happens for one of two reasons: organizations layer new tools onto existing environments without modernizing how they discover data, or cultural inertia stalls the adoption of modern security frameworks, trapping teams in a cycle of reactive patching.

Either way, security teams end up with no visibility into machine identities and their behavior, leaving CISOs accountable for data access they can neither track nor verify.

Non-human access compounds this risk. In the [2026 Thales Data Threat Report](#), **70%** of organizations rank AI as top data security risk, and the [IBM 2026 Cost of a Data Breach Report](#) found that there has been a **56% increase** in AI-driven attacks.



Part 2:

What Complete DSPM Looks Like

A complete DSPM deployment delivers a continuous cycle of knowing, deciding, protecting, and proving. It answers five core organizational questions:

Where does sensitive data reside?

What exactly is it?

How is the organization using it?

Who has access to it?

What concrete steps is the organization taking to secure it?

Complete DSPM Restores Visibility

A complete DSPM deployment closes the visibility trap at its source: continuous, automated discovery across the full data estate. Not a point-in-time scan, but a live picture of where sensitive data lives, what it is, and who and what can access it, updated as the environment changes.

Complete DSPM Turns Visibility Into Action

Rather than simply alerting teams to exposures, complete DSPM identifies the data at risk, assesses the potential impact, assigns ownership, and drives remediation to reduce risk. This is how you manage down effectively: your team gets faster triage, clearer ownership, and automated routine.

Mature organizations see remediation collapse from months to days, and audit preparation gets measurably lighter.

Complete DSPM Solves the False Protection Trap

Complete DSPM prevents the false sense of security outlined above by continuously and automatically discovering all data assets across the entire infrastructure and prioritizing protection based on risk and criticality.

Complete DSPM Provides Tangible Board ROI

Instead of presenting the board with productivity metrics and a picture of risk, CISOs show reduced exposure windows, risk, and regulatory fine exposure - crucially measured over time. You're no longer reporting what you found, but what you fixed and what that fix means to the business.

Complete DSPM answers five questions consistently, anytime:

Where is sensitive data?

What is it?

Who has access to it?

How is it being used?

What are we doing about it?

Incomplete DSPM answers only some of these. The CISO's accountability is for all five, operationalized continuously across all data types, access patterns, and verticals.

Part 3:

How CISOs Can Drive Complete DSPM Adoption



Breaking Down Organizational Siloes

When different departments fail to communicate and understand each other's roles, each one ends up owning a piece of the problem with no one owning the whole. GRC sets policies, security deploys tools, and operations runs infrastructure. As a result, no single team is accountable for reducing the organization's overall data exposure window.

In its [Buyer's Guide for DSPM](#), Gartner recommends a structured requirements-gathering process involving all relevant stakeholders: security, risk management, IT operations, and data governance.

The CISO can turn that recommendation into practice by making accountability explicit across three relationships: GRC, remediation, and the board. Two sit within the organization; one sits above it.

- GRC and remediation are where the CISO manages down: turning vague mandates into owned, measurable work.
- The board is where the CISO manages up: translating that work into financial and liability terms the board is accountable for.

Governance, Risk, and Compliance Teams

GRC teams are the logical starting point. They need to move from vague compliance checkboxes to specific, operationally testable requirements. Instead of «implement continuous monitoring,» the requirement becomes:

- Discover all sensitive data in databases, SaaS applications, and backups within 30 days
- Triage exposures within 5 business days and assign severity
- Remediate critical exposures within 7 days, non-critical within 30 days
- Define critical data: customer PII, payment data, trade secrets

These specifics force GRC to understand technical realities. They learn, for example, that databases need time to patch safely, and that SaaS applications have different remediation timelines than on-premises systems. Specific requirements force alignment between what GRC mandates and what security and operations can execute.

Remediation Teams

As we've said, visibility alone does not reduce risk.

Every exposure identified by DSPM must be assigned to a team with both the authority and expertise to resolve it. Effective remediation teams combine technical ownership with business context, ensuring that risks are prioritized, addressed, and closed within agreed timeframes.

Each specific remediation team must own its specific domain:

- DBA owns database exposures
- AppSec owns application exposures
- Infrastructure owns system and cloud exposures

The Board

Boards don't need a walkthrough of the risk register. They need a number: what's exposed, what it would cost, and what's being done about it.

That number has gotten more expensive to ignore. The [2026 IBM Cost of a Data Breach Report](#) puts the global average cost of a breach at \$4.99M, a 12% year-over-year increase and a record high. And boards are asking sharper questions than they used to, particularly about AI: in the 2026 Thales Data Threat Report, 70% of organizations now rank AI as their top data security risk.

Under Article 20 of NIS2, board members can be held personally liable for cybersecurity failures, not just the organization. In the most serious cases, regulators can seek to bar an executive from managerial roles entirely. That combination — financial exposure quantified in dollars and liability exposure quantified in regulation — means the CISO who can answer the board's question in board terms isn't just informing the board. They're protecting it.

Each team must own its SLAs and commit to closure rates. In exchange for that ownership, security teams provide a prioritized triage list, and automation to handle routine remediations such as encryption or access revocation.

This matters more than it used to. The [2026 Verizon Data Breach Investigations Report](#) found the median time to patch a known vulnerability has grown from 32 to 43 days industry-wide, a 34% increase. Attackers are moving faster; most organizations' remediation is moving slower. A CISO who can point to closure rates measured in days, not weeks, isn't just running a tighter team. They're winning the race, which is exactly the story that builds credibility with the board.

Organization-specific metrics CISOs can use to make this case include:

- Number and severity of data breach incidents
- Mean time to detect (MTTD)
- Number of high-risk vulnerabilities identified
- Percentage of compliance with security regulations and policies
- Exposure windows
- Risk reduction trends

A common mistake is treating DSPM as a technology project. Successful CISOs treat DSPM as an operational transformation. First define how the organization will discover, prioritize, remediate, and prove reductions in data risk. Then select a DSPM solution that supports that model.



The Model Comes Before the Tool

CISOs need to define how the organization will operationalize the DSPM cycle before entering into any vendor conversations. The idea isn't to design perfect processes, but to design realistic processes the organization can execute. Only after defining this model can the CISO move on to evaluating tools.

Start With the Crown Jewels

Boiling the ocean by attempting a sitewide DSPM rollout is a recipe for strategic failure. A blanket implementation creates immediate budget friction with the CFO, obscures measurable ROI for the board, and paralyzes engineering teams under an avalanche of unprioritized alerts.

It's far more practical to start with the crown jewels: the 2-5% of data that matters most to the business. Triage becomes manageable because there are fewer alerts to sift through, and remediation happens fast enough to matter.

The result isn't just faster remediation. It's a defensible story: a small, bounded scope where the CISO can demonstrate exactly what changed and why, before scaling the same operating model to larger datasets.

Name the Non-Negotiable Constraints

An operating model has to fit the organization's real constraints, which means naming them before anyone starts designing processes.

Budget is the first constraint. A limited budget narrows the scope to the crown jewels; a larger one buys broader coverage. Either way, the CISO who names this constraint upfront is negotiating from a position of control, not asking for forgiveness later for a scope they never chose.

Resource capacity is the second

A DSPM program that assumes time security and engineering teams don't have will fail regardless of how well it's designed. Where teams are understaffed, automation and triage efficiency have to be the priority, and baselining current team capacity before the program starts is what lets a CISO later show the board how much throughput improved per person, not just how much the team is doing.

Risk tolerance is the third: the false-positive rate, automation boundary, or remediation latency the organization can actually live with. Naming this early gives the team clear guardrails to optimize against, and gives the CISO a specific, defensible answer when the board asks how DSPM's risk appetite aligns with the organization's.

Regulatory and contractual obligations are the fourth, and often the most useful. What mandates certain visibility, automation, or reporting effectively defines the non-negotiable scope, the crown jewels that were never optional. Framed this way, DSPM becomes compliance insurance in front of the board, which strengthens the investment case rather than just justifying it.

Resource capacity is the second

Comprehensive visibility, instant remediation, zero false positives, and zero operational cost is not a realistic combination. Trade-offs are a necessary part of any operating model, and naming them early, rather than discovering them under pressure, is what keeps them intentional.

Some examples include:

- Trading accuracy for speed by prioritizing metadata scanning over full scanning
- Trading breadth for depth by monitoring crown jewels intensively rather than everything shallowly
- Trading automation for control by introducing manual gates on remediation rather than automating everything
- Trading responsiveness for cost by choosing between quarterly reviews and real-time decisioning

Once those trade-offs are decided, the team can design an operating model that actually satisfies them, rather than one that quietly breaks the first time it's tested.

Conclusion

DSPM adoption isn't a project with an end date. It's an operating model that has to keep working as the data, the regulations, and the board's questions change.

What doesn't change is the CISO's dual accountability: to run a tighter operation

than the year before, and to prove it in terms the board can act on. The CISOs who treat those as one job, not two, are the ones whose DSPM investment survives the next budget cycle, and whose tenure survives the next audit.

The CISO's Strategic Checklist

Use this checklist to clarify your strategic position and manage both up and down effectively.

Crown Jewel Approach

- Define the crown jewels: the 2-5% of data that matters most to the business
- Confirm the team can execute this scope within 6-12 months before expanding it

Managing Up: Board and Business Impact

- Pick the one metric that proves DSPM's value to the board, and report it consistently
- Set a baseline for crown jewel exposure today, and a target for the next review
- Translate every risk reduction into a business or liability term before it reaches the board

Managing Down: Team and Operations

- Baseline current team capacity before DSPM, so the throughput gain is provable afterward
- Automate the remediations that don't need a human judgment call, and free the team for the ones that do
- Target one visible win in the first 90 days to build credibility with engineering

Constraints and Trade-offs

- Name the budget ceiling before scope is designed, not after
- Decide what's non-negotiable: regulatory, contractual, or board-mandated
- Choose the trade-off consciously: speed, depth, control, or cost. Don't let the tool choose it later



About Thales

Thales is a global leader in cybersecurity, helping businesses, governments, and the most trusted organizations in the world protect critical applications, sensitive data, identities, and software anywhere, at scale — with the highest ROI. With more than **30,000 customers**, including 58% of the Fortune Global 500, our solutions are deployed in 148 countries around the world. Through our innovative services and integrated platforms, Thales helps customers achieve better visibility of risks, defend against cyber threats, close compliance gaps, and deliver trusted digital experiences for billions of consumers every day.

Contact Us:

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

THALES

CYBERSECURITY

[Contact us](#)

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

cpl.thalesgroup.com

