eBook

THALES

CYBERSECURITY

Secure what matters most

See and mitigate risk. Implement proactive visibility, control, protection, and compliance strategies.

cpl.thalesgroup.com

THALES

Contents

An always evolving **risk landscape**

Cyber attackers and malicious actors are becoming increasingly sophisticated. Organizations are responding to the most visible threats but often with limited time, resources, and expertise. At the same time, evolving threats – from bad bots to DDoS attacks and supply chain vulnerabilities – are pushing enterprises into reactive security measures.

These responses often address only the most apparent risks. With rapid changes and a wide range of security needs – internal and external, business and regulatory – it's challenging for organizations to keep up and take coordinated, proactive action.

According to Gartner, Inc.[1], today's cyber attackers move so quickly that organizations are left scrambling to deploy patches and automate controls, and these tactics don't necessarily reduce future risks. There's little time to pause, evaluate, and implement an effective security strategy.

It's not just the changing threat landscape that complicates things; multiple factors make it difficult for enterprises to adopt a more proactive security strategy.

1. Gartner: https://www.gartner.com/en/cybersecurity

THALES

The forces acting against **proactive security**

- Addressing risk across multi-cloud environments
- Taking on the challenge of securing structured and unstructured data (at rest, in motion and in use)
- Managing user identities and permissions on connected devices
- Knowing who is accessing sensitive data or assets, from where and when
- Keeping pace with targeted, autonomous attacks derived from GenAI
- Complying with changing and more stringent regulatory obligations
- Combatting security data silos that arise due to disparate security platforms, products and vendors
- Enabling partners, customers and third parties to be part of a secure ecosystem without increasing the attack surface

Take control of your **security strategy**

With the added strength of Thales, organizations are better equipped than ever before to tackle these challenges and master their security. Our six-step guide provides a blueprint for a proactive security strategy to safeguard your most critical assets, now and in the future.

S **Scope and detect**
to improve visibility of risks

E **Evaluate and prioritize**
the most sensitive apps and data

C **Control access**
to corporate systems and data

U **Unify and protect**
through consolidation and end-to-end security

R **Regulate and comply**
with an expanding raft of legislation

E **Educate and adapt**
based on known and potential future threats

Scope and detect

If you can't identify the risks – or the potential for them to occur – how are you supposed to be proactive?

85% of organizations will embrace a cloud first principle by 2025 [2]

60% of corporate data is in the cloud [3]

≈Half of all internet traffic came from bad bots in 2023 [4]

2. Gartner, Inc.:https://www.gartner.com/en/newsroom/press-releases/2021-11-10-gartner-says-cloud-will-be-the-centerpiece-of-new-digital-experiences
3. Edge Delta: https://edgedelta.com/company/blog/how-many-companies-use-cloud-computing-in-2024#:~:text=94%25%20of%20major%20companies%20worldwide,store%20their%20more%20crucial%20data
4. MSSPAlert: https://www.msspalert.com/news/bots-clutter-and-compromise-the-internet-mssp-imperva-re-

Thales research highlights a disconnect between the C-Suite and IT decision-makers. Security often gains strategic importance only after a breach resulting in reputational damage.

New regulatory rules add to the burden for global enterprises, as they navigate multiple jurisdictions and regimes. These often require regular audits and updates, much of which involves manual patches. This lack of automation drains internal resources, leaving little time to consider security strategically.

What's at stake?

Gaining visibility into these risks demands a coordinated approach. Without it, enterprises will remain on the defensive, with a weakened security posture, exposing operations to increased risks like IP theft, data breaches, and cyberattacks.

How can you be proactive?

Discover the three key steps

1. Define your scope: Establish the boundaries of your enterprise security posture and include all critical assets so you know what you need to protect.

2. Detect all threats: Extend your risk visibility to all apps, data and people then apply real-time monitoring and threat detection capabilities to stay on top of them.

3. Establish an inventory: Discover, classify and maintain an up-to-date list of all APIs, endpoints, parameters and payloads as time goes on.

Where can Thales help?

Helping you gain full data visibility

Our combined solutions enable you to reduce risks and threats to your data through real-time analytics, monitoring and actionable intelligence. Gain insights into where your data is, who is accessing it and how it's being used with Data Activity Monitoring, Data Risk Analytics and Data Risk Management tools.

Evaluate and prioritize

With sprawling digital ecosystems organizations must continuously assess their environment and develop a methodology to address the most critical security issues.

Prioritizing the security of APIs that handle sensitive data or pose the highest operational risks can help focus efforts.

Part of the evaluation and prioritization process depends on aligning available skills with the need for continuous risk assessments and regular reviews.

What's at stake?

Maintaining a system for ongoing risk evaluation and prioritization may seem like extra effort, but much of it can be automated. The impact on operations could be significant. According to Gartner, Inc., by 2026, organizations emphasizing security investments with a continuous threat exposure management program will reduce security breaches by up to two-thirds.

How can you be proactive?

Discover the three key steps

1. Evaluate what you have/need: Assess your current security measures and their effectiveness and then start to deliver automated, continuous evaluations.

2. Prioritize your risks: Focus on the most critical vulnerabilities first in relation to key business objectives and apply validation tools to reduce priority issues.

3. Engage all departments: Expand your channels of communication to articulate risks in terms other business units understand so they can be proactive too.

Where can Thales help?

Implement a proactive threat centric approach

We encourage enterprises to take a threat-centric approach. The Imperva Data Security Fabric helps you identify potential breaches. For instance, abnormal user behavior that can lead to bad practices, hostile intrusions or data compromises.

Gain full visibility of data across the Enterprise

With the CipherTrust Data Security Platform you get the CipherTrust Data Discovery and Classification tool. This allows you to see all sensitive data held within your enterprise, including across cloud, big data and traditional IT environments.

Creating effective security policies

With support for defining your security policies, locating structured and unstructured data and classifying sensitive information, you can proactively see and then mitigate risks while staying on top of regulatory reporting.

Control access

As digital ecosystems expand, granting data access to people and systems becomes imperative. How can this be achieved without increasing operational risks?

Conducting due diligence on every ecosystem partner's security is complex, costly, and time-consuming, involving more than just the IT Security team and offering no guaranteed protection against future incidents.

What's at stake?

Knowing who is accessing what data from where is a constant challenge for most organizations. A combination of robust access protocols, identity policies, and governance frameworks is essential to protect sensitive information. Zero Trust implementations must provide complete oversight of all threats, while ensuring that people, apps, or APIs requesting access are who they claim to be.

How can you be proactive?

Discover the three key steps

1. **Create robust access policies:** Build coherent and adaptable access policies and governance frameworks to fit your data classifications and business objectives.

2. **Establish access management controls:** Monitor, classify, review, and protect all routes into your data and automate the controls.

3. **Implement Zero Trust properly:** Apply Zero Trust principles to anyone and anything accessing your information to secure your applications at the point of access itself.

Where can Thales help?

End-to-end security across your data, applications and API estate

Our CipherTrust Data Security Platform and Imperva Data Security Fabric give you a comprehensive way to protect your sensitive data – and all paths to it. Layering on the Imperva Application Security Platform allows you to automatically protect your mission-critical applications and APIs. And further tools give you dedicated solutions for CIAM, workforce access and FIDO.

Specifically, CipherTrust Data Security Platform and Imperva Data Security Fabric enables business to:

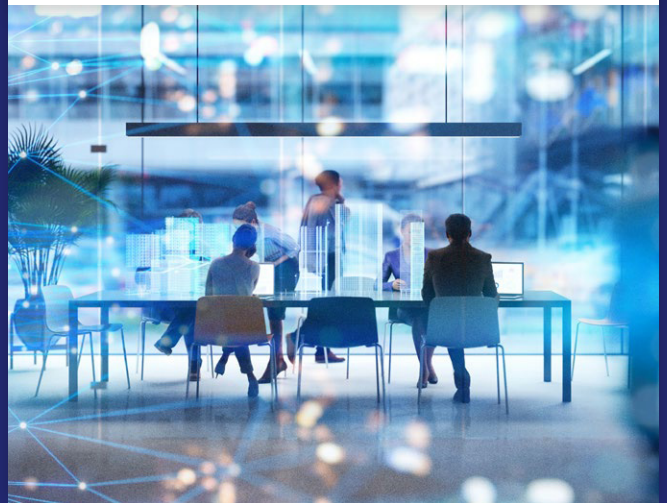
- Discover and classify data anywhere.
- Get real-time observability of threats to data.
- Protect sensitive data at rest, in motion, and in use.
- Control and protect keys and secrets anywhere.

Creating a secure digital environment for external users

Our OneWelcome Identity Platform orchestrates frictionless yet secure and trusted digital journeys for your external users like consumers, partners and suppliers. It provides secure access to apps for anyone at scale. It also addresses critical areas like data privacy, delegation and consent management.

Unify and protect

Management of a diverse IT estate and siloed systems from multiple suppliers can lead to poor visibility of an overall security posture, making it challenging to monitor, detect, and respond swiftly to incidents.



Whether it's bad bots, phishing attacks, or supply chain vulnerabilities, known blind spots in security can be filled. Yet, as cyber-attacks grow more sophisticated, there's a temptation to buy solutions that promise quick fixes without considering how they integrate with existing systems.

What's at stake?

Vendor consolidation is widely recognized as the solution, but it's easier said than done. A recent Informatica study found that 55% of respondents have over 1,000 active data sources in their enterprise, with 50% using five or more management tools in 2023[5]. CIO.com asked its audience if they plan to consolidate vendors in the next 12 months – 95% confirmed they do[6].

Establishing a unified platform or single vendor for security tools requires confidence that it can handle everything needed, from cloud software to access keys and hardware to virtual appliances. The goal isn't just to reduce costs through consolidation but to do so while improving your security posture.

5. Informatica research:https://accelerationeconomy.com/data/informatica-research-highlights-data-sprawl-why-management-needs-to-be-unified/

6. CIO: https://www.cio.com/article/657327/what-it-executives-are-saying-about-vendor-consolida-

Unify and protect

How can you be proactive?

Discover the three key steps

1. Assess vendor capabilities: Evaluate the platform and tools to ensure you will be able to consolidate security solutions effectively and cost-efficiently.

2. Focus on end-to-end protection: Check that platforms cover your needs from start-to-finish – including data at rest, in motion and in use.

3. Think of the future: Get clarity on the vendor's roadmap for future security requirements – from coverage of GenAI to forthcoming regulatory rules.

Where can Thales help?

With the most comprehensive portfolio of products and services from a single supplier, we help you protect your data, apps and APIs and secure access to your systems.

Protect data sophisticated encryption and access controls

CipherTrust Data Discovery and Classification can be used to proactively protect at-risk data by remediating at risk data stores via encryption and access controls. It's findings can be coupled with CipherTrust Transparent Encryption tools to close security gaps and improve compliance.

While our CipherTrust Manager acts as the central hub for key lifecycle management – available in physical and virtual form factors or as a Service. With our combined investment in R&D, you'll also have access to future innovations that respond to emerging security needs.

Protecting mission critical apps and APIs from external threats

Our Application Security Patform automatically protects your mission critical apps and APIs from DDoS, bad bot and supply chain attacks.

While our CipherTrust Data Security Platform and Imperva Data Security Fabric secure sensitive data whether it's at rest, in motion or in use and provide insights into data access and quantify risk.

Regulate and comply

DORA, CPRA, GDPR, NIS2, LGPD, PCI DSS 4.0—the list of legislation affecting enterprises keeps growing. Each regulation demands specific compliance, with its own penalties.

Compliance is often viewed as an essential outcome due to the significant risks of noncompliance, such fines, but the reputational damage can be even more costly. Trust, though intangible, is crucial for maintaining confidence in operations, CSR commitments, and ESG credentials.

Many organizations assume their partners, like cloud providers, will handle compliance for them – however, the responsibility ultimately rests with the organization itself.

They need a strategic partner to help assess existing technology, evaluate internal skills, and develop a compliance approach tailored to their needs.

What's at stake?

Compliance demands strict processes and procedures, but they don't need to be separate from the broader goal of enterprise security. In fact, integrating compliance as a key component of security can save costs, reduce complexity, and boost confidence in business operations.

How can you be proactive?

Discover the three key steps

1. Challenge the status quo: Focus attention on the added value of compliance tools, such as fraud detection data that provides customer insights that lead to innovations.

2. Automate compliance
Improve the accuracy of compliance and security reporting across borders while reducing manual effort to save costs.

3.Make it a foundation: Build compliance into all security platforms so there is no duplication of data or effort.

Where can Thales help?

Compliance is a primary driver for the tools we design. Whether looking at it from a regulatory, data sovereignty or efficiency perspective, we aim to serve the twin objectives of compliance and security in all our tools.

Accelerating compliance with trust and agility

Through encryption and tokenization, masking or secrets management, we secure sensitive data wherever it is while reducing the risks of data breaches and non-compliance.

Thales is a trusted, know partner who, through extensive knowledge of the industry and the threat landscape, are able to 'see around corners' and develop technology that will prevent certain types of attacks, even before government organizations build compliance / regulation around them.

Educate and adapt

The biggest challenge to implementing a proactive security strategy is standing still.

Enterprises must adopt an adaptive and proactive security posture. This goes beyond technical and operational needs.

Security must be a business priority for everyone, the C-Suite, in particular, need to view security differently. Instead of reacting only after a breach, executives need compelling reasons to give security the strategic importance it deserves.

What's at stake?

Gaining buy-in from senior stakeholders will accelerate efforts to maintain a proactive security strategy. The result? A comprehensive, cost-effective, and compliant security posture that adapts to future demands and ultimately protects what matters most.

How can you be proactive?

Discover the three key steps

1. **Offer continuous training:** Keep your team and the wider business up to date on the latest security threats and best practices.

2. **Change the language:** Simplify the way security is talked about in the organization by focusing on the impact of decisions (taken or untaken) on business operations.

3. **Flex as you go:** Review and adapt your security strategy to maintain a robust security posture in the face of evolving threats and vulnerabilities.

Where can Thales help?

Instilling security behaviors through the enterprise

Our Consulting Services will guide and enable your teams through the security maturity steps of gaining visibility, governance, actionable insights, and automated actions.

Our Professional Services can help you align your people, process and technology to improve your security posture throughout.

Elevate your proficiency in harnessing these cuttingedge solutions with the Thales Technical Training and Certification program.

Secure what matters most: **Take control of your security strategy**

Data security may not be considered a strategic business initiative in every organization. But when you consider the cost of a data breach in terms of lost IP or regulatory fines, the potential competitive advantages of being a trusted partner and the significant savings from vendor consolidation then there is much to gain from a holistic approach.

At the heart of these business outcomes is a proactive security posture built on the framework outlined in this guide. Recognizing the importance of these foundations and addressing them will enable you to increase:

- Visibility into risks and threats
- Control over access to sensitive assets
- Protection for critical data and applications
- Compliance with stringent regulations

Thales solutions enable you to achieve this faster by integrating your security tools and reducing your risk exposure. Our solutions safeguard your applications, data and identities from end-to-end in any location and at any scale. So you can secure what matters most to your organization.

THALES

THALES

CYBERSECURITY

Contact us

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

cpl.thalesgroup.com

Thales - May 2026 • GHv2