Security Playbook

THALES
CYBERSECURITY

Every Team Needs a Strong Game Plan

cpl.thalesgroup.com

Overview

A strong security game plan needs a winning strategy

To have a successful cybersecurity strategy, much like any sport, it is all about teamwork, coordination, and a solid understanding of roles.

CISOs and other IT leaders, as coaches, have enormous responsibility for a successful strategy. You must be the primary decision-makers, responsible for developing plans, establishing objectives, and adjusting on the fly as the team executes the plan. This role requires a balance of leadership with technical knowledge, providing guidance and motivation, while working with those on the field to improve collective performance.

The players themselves must fully understand both the strategy and objectives, the specific play, and then they get to shine when they showcase their technical expertise that results in a win, create more value from their software and deliver seamless digital experiences for millions of consumers every day.

2026 Threat **Trends**

To create a strategy, CISOs must evaluate the obstacles to overcome and how well the team is set to handle those.

Here are a few items any CISO needs to keep their eyes on for 2026.

- Artificial Intelligence (AI)
- Automated Threats
- Quantum Computing
- Compliance
- Operational Complexity

Artificial Intelligence (AI)

- 2 Million is the daily average of AI-enabled attacks (2025 Bot report)
- 69% cited the fast-changing tech stack ecosystem as the most concerning security risk for GenAI adoption, followed by lack of integrity (64%) (2025 DTR)

Compliance

- 96% of global respondents say their organization's cybersecurity investment has increased due to cybersecurity regulations over the last 12 months (PWC)
- 78% of enterprises that failed compliance audits had a history of prior breaches (2025 DTR) with 45% of respondents cited having failed an audit (2025 DTR)

Quantum Computing

- KPMG surveyed 250 large corporations and found that about 60 percent of organizations in Canada and 78 percent in the US expect quantum computers to become mainstream by 2030.
- 62 percent in Canada and 81 percent in the US admit that they need to do a better job of evaluating their current capabilities to ensure their data remains secure from quantum computing. (KPMG)

Automated Threats

- 55% surge in API data leakage and API violations (2025 Bot Report)
- The United States remains the top targeted country for bot attacks accounting for 53% of all attacks globally (2025 Bot Report) and 76% of all attacks within the Americas
- Over 50% of bot attacks target APIs, the front line of your business (2025 Bot report)

Operational Complexity

- 75% of executives are concerned about cyber and privacy risks resulting from too much complexity in their organizations (PWC)
- 57% of executives citing customer trust and 49% citing brand integrity and loyalty as areas of influence (PWC)
- 61% use five or more tools for data discovery and classification, which can lead to misalignment and conflicting protection policies (2025 DTR)

Offense vs. Defense

Offense

Your Front Line

Offense is about taking the initiative, creating opportunity, and taking control of the game. To do this, you need be proactive, creative, precise, and agile. Mastering coordination will ensure seamless teamwork for collective success.

Defense

Steadfast and Unyielding

Your defensive line aims to counteract or neutralize offensive actions, withstand attacks, and maintain a secure position. To execute properly requires planning, strong stable barriers, resilience, and the ability to anticipate threats and adapt swiftly.

It might seem like in cybersecurity that you only need a good solid defensive line. But like all the best teams, you need the techniques and qualities from both offensive and defensive measures to create a solid strategy.


KNOW
YOUR
PLAYS
Offensive Plays
Your front line is the part of your business that runs into the opponent's zone – your cloud applications and APIs.
Defensive Plays
Your defense will hold the line, ensuring nothing can make its way through. Compliance standards are put in place to be gold standards of defense.

Application Security

Your APIs are taking a hard hit – from bots, AI-enabled attacks, and business logic abuse. What's worse, the rapid rise of API creation means some slip through the cracks unknown, yet still an open vulnerability.

Making a proactive, precision play requires a unified application security platform that can truly go on the offensive:

- **build** new applications at scale without impacting your business
- **discover**, assess, detect, and mitigate your APIs across all environments with one console eliminating tool sprawl
- **provide** unified layers of WAF, Bot protection, API security, DDoS, and Account Takeover, with a single platform for policy management and comprehensive visibility

Benefits:

Increase revenue – Securely deploy new applications in hours versus weeks while maintaining business continuity
Reduce risk – Shore up blind spots from hidden and insecure APIs, while reducing third party risks
Lower costs – Reduce labor and resource costs with fewer security vendors

Cloud and multi-cloud

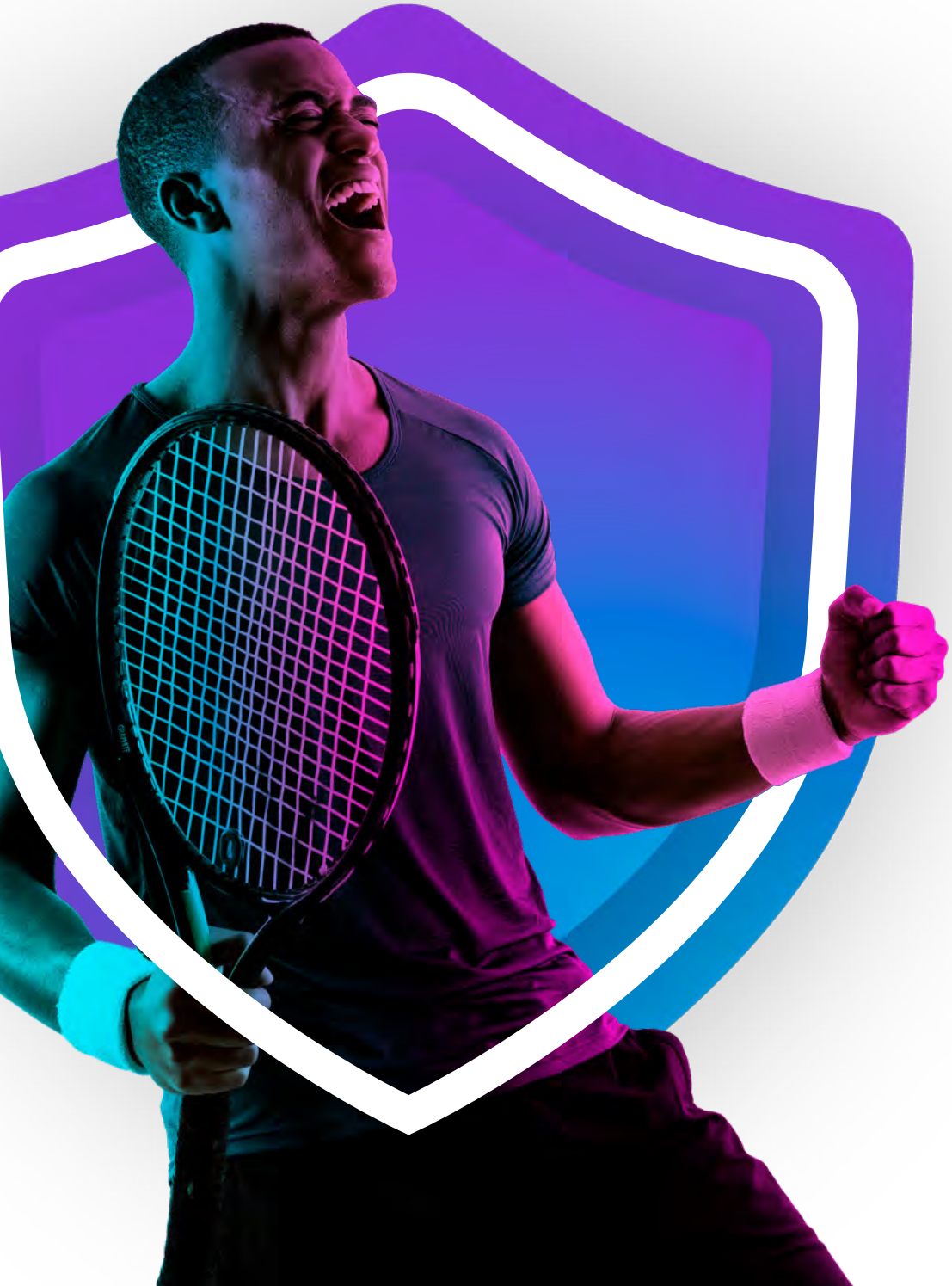
Complexities from a transformation to the cloud often create an infrastructure that has a wide array of security tools. This creates difficulty in migrating data and workloads due to uncertainties such as where the data is and how is it being accessed. The result is slower time to transformation and innovation that can result in revenue loss or worse, a loss in customer trust.

Take the initiative and create an opportunity to:

- **streamline** your operations
- **consolidate** vendors eliminating redundancies
- **ensuring** workflows can communicate efficiently

Benefits:

Increase revenue – Accelerate innovation with fewer missed deadlines or slow transformations
Reduce risk – Ensure a consistent approach to compliance across cloud and hybrid environments
Lower costs – Reduce operational costs with less tools and resources required



Data Security

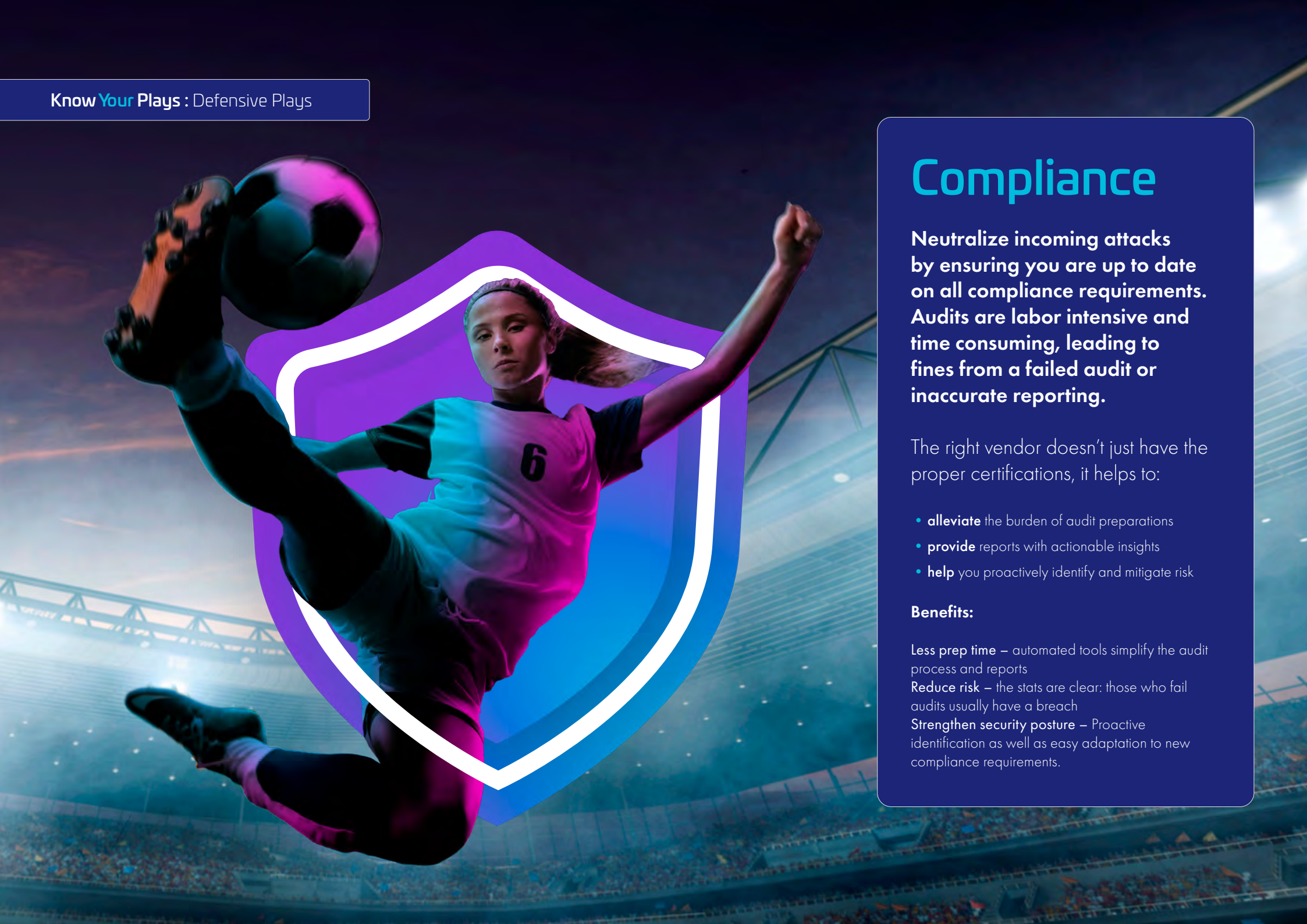
Multiple security processes and tools means there is often unknown and unprotected sensitive data, with no centralized governance. This IT reality combined with an explosion of unstructured data from using AI or collaborative tools means you can quickly get blindsided.

Here you need to really hold the line, yet be anticipatory and agile with:

- **Secure** data both on-premises and in the cloud including centralized, flexible key management
- **Insight** into who, what, where and how critical assets are accessed
- **Future-proof** protection that doesn't slow down revenue engines

Benefits:

Increase revenue – Accelerate innovation and AI adoption with confidence
Reduce risk – Focus on the risks that have the biggest impact on your organization
Lower costs – Reduce both operational and capital expenses with a centralized platform



Compliance

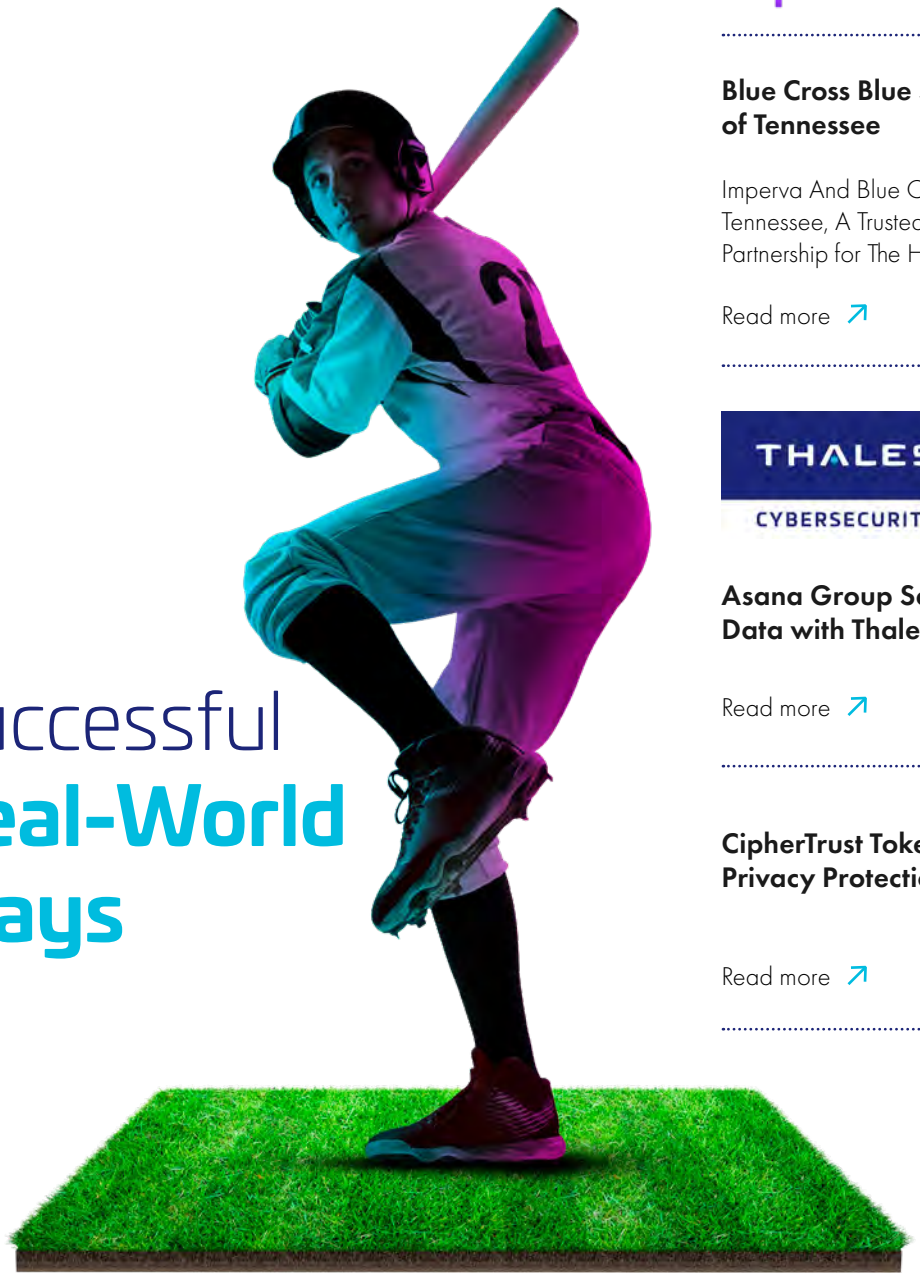
Neutralize incoming attacks by ensuring you are up to date on all compliance requirements. Audits are labor intensive and time consuming, leading to fines from a failed audit or inaccurate reporting.

The right vendor doesn't just have the proper certifications, it helps to:

- **alleviate** the burden of audit preparations
- **provide** reports with actionable insights
- **help** you proactively identify and mitigate risk

Benefits:

Less prep time – automated tools simplify the audit process and reports
Reduce risk – the stats are clear: those who fail audits usually have a breach
Strengthen security posture – Proactive identification as well as easy adaptation to new compliance requirements.



Successful **Real-World Plays**

imperva

Blue Cross Blue Shield of Tennessee

Imperva And Blue Cross Shield of Tennessee, A Trusted Cybersecurity Partnership for The Healthcare Industry.

Read more ↗

Keystone RV

Keystone RV Stops a Large-Scale DDoS Attack with Imperva DDoS Protection.

Read more ↗

DigiCert

DigiCert Automates Protection of Their AWS Environment with Imperva

Read more ↗

THALES
CYBERSECURITY

Asana Group Secures Healthcare Data with Thales

Read more ↗

Luna HSM Encryption for Mitsubishi Electric Sanda Works

Read more ↗

CipherTrust Tokenization for Customer Privacy Protection

Read more ↗

Global Mobile Network Operator Deploys Portfolio of Thales Solutions as Centralized Data Security Solution for Entire Enterprise

Read more ↗

About Thales

Thales is a global leader in cybersecurity, helping the most trusted organizations protect critical applications, data, identities, and software anywhere, at scale. Through Thales' integrated platforms, customers achieve better visibility of risks, defend against cyber threats, close compliance gaps, and deliver trusted digital experiences for billions of consumers every day.

Your Strategy Scoreboard

In the world of cyber resiliency, just like in professional sports, preparation and consistency are paramount.

Thinking of the 2026 trends and risks, some questions to ask yourself to ensure readiness include:

Looked at the AI tools your organization is using now, and planning to implement? Have you determined the specific risks they pose, and how well prepared your team is to handle any incidents?

Have you begun your post-quantum cryptography transformation plan? Outlining which items are top priority for protection? Have you already secured any long-life data subject to Harvest Now, Decrypt Later risks?

Looked at the AI tools your organization is using now, and planning to implement? Have you determined the specific risks they pose, and how well prepared your team is to handle any incidents?

If your organization has failed an audit, knowing that almost 80% of those who fail audits experience a breach, do you have your incident plan ready? Or have you outlined the key areas where you need to send in your hardest hitters?

Have you integrated API and automated threat risks into your organizational risk framework? Do you have an assigned ownership for API and related risks such as bot attacks? Have you determined a budget specific for application security tools?

What is your plan to have the right level of security spending given your organization's risk tolerance? Have you determined the trade-offs you face between cost efficiency and comprehensive security coverage? Have you looked at conducting a tool redundancy exercise?

Every good coach knows that they are not alone when it comes to building a solid strategy.
Relying on the experts will help you achieve your goals.

Reach out to Thales today.

THALES

CYBERSECURITY

Contact us

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

cpl.thalesgroup.com