eBook

THALES
Building a future we can all trust

CYBERSECURITY

The Data Security Playbook for Insurance Leaders

cpl.thalesgroup.com

Contents

Executive Summary: **Protect Trust, Accelerate Transformation**

Insurance is built on trust. Customers hand over their most intimate information (financial records, medical histories, risk profiles), and they expect it to be safe.

Unfortunately, that trust is under pressure. Regulators are raising the bar on compliance, sovereignty, and reporting. Bad actors are striking faster and sharper with AI tools that learn and adapt. **Data security is no longer just IT's problem; it is a top business risk.**

However, there is an opportunity. Modern data security solutions can do more than defend; they can strengthen resilience and accelerate transformation, positioning insurers as true custodians of customer data.

Thales CipherTrust Data Security Platform (CDSP) is one such solution, delivering unified protection, clear compliance, and sovereign control across clouds and on-premises systems. The payoff is real: **fewer breaches, simplified compliance, and confidence that earns loyalty.**

CDSP is much more than just a platform; it is a strategic partner. It guides insurers through shifting regulations, handles the surging tide of data, and secures digital transformation. For the insurance sector, trust is more than policy; it is brand, reputation, and market power. Insurers who invest wisely today will lead tomorrow.

The Insurance Data Security Landscape

Insurers are facing a slew of security challenges. Bad actors are exploiting AI to supercharge their phishing campaigns, generate highly convincing deepfakes, and craft bespoke ransomware attacks.

According to the Verizon 2025 DBIR, system intrusion, social engineering, and web application attacks account for 74% of breaches the insurance sector experienced in the previous year. The most commonly exposed data is personal data (54%), followed by access credentials (22%).

According to the Verizon analysis, third-party involvement doubled year over year (from 15% in 2023 to 30% in 2024), ransomware is present in 44% of breaches (up from 32%), and exploitation of known vulnerabilities is responsible for 20% of initial access cases.

According to the latest IBM Cost of a Data Breach Report, Shadow AI, and AI supply-chain issues are emerging drivers; 20% of organizations reported AI-related incidents and shadow-AI added approximately $670K per breach. On the same topic, the Hiscox Cyber Readiness 2025 Report highlights that over half (57%) of the surveyed organizations said they had experienced a cyber-attack due to AI vulnerabilities.

Finally, Allianz Commercial's 2025 analysis went further, noting that data exfiltration is now a top loss driver, doubling claim severity. At the same time, Hiscox reports that a third (33%) were hit with a substantial fine following an attack.

Data volumes compound the risk. Insurers store sensitive personal and medical records, actuarial models, and historical claims. This trove is a prime target for malefactors who monetize stolen data on underground markets. Add to this the reliance on third-party adjusters, brokers, and cloud vendors, and the attack surface grows further.

Regulatory complexity stretches resources across GDPR, DORA, NAIC, PIPL, NIS2, and NYDFS. The Allianz report noted that privacy litigation has tripled in three years, with class actions and biometric laws raising the stakes. All of this happens against a backdrop of global cyber talent shortages.

For bad actors, insurers remain high-value targets. This means that leaders need to protect their data, simplify compliance, and strengthen resilience. In this environment, adopting a Zero Trust approach to data security, where no user, device, or system is automatically trusted, helps insurers minimize exposure, contain breaches, and maintain full visibility across their data ecosystem.

Although the insurance sector is accustomed to managing risk, it is now time to rethink how it manages sensitive information, modernize controls across its full IT estate, and consider automation to help counter the growing velocity of attacks.

The following sections provide a roadmap for the insurance industry to establish a resilient data security posture.

Regulatory Compliance Made Simple

For insurers, compliance is a constant balancing act. Regulators demand strict controls, yet the frameworks differ by region, and reporting timelines grow tighter every year. The Thales 2025 Data Threat Report showed that almost half (45%) did not pass a recent audit, a sign of difficulties with manual processes and fragmented tooling. However, this statistic goes way beyond mere compliance. 78% of enterprises that failed audits had a breach history, versus just 21% of those that passed compliance. Put simply, the likelihood of experiencing a breach decreased by half among enterprises that passed all their compliance audits.

It is obvious that we need to simplify compliance. The CipherTrust Data Security Platform removes friction from this complexity.

With unified data discovery, monitoring, control, protection, and centralized policy enforcement, CipherTrust Data Security Platform creates a single compliance framework across global operations. Insurers gain consistent visibility into where sensitive data resides, how it is used, and who has access. This visibility makes it possible to demonstrate control to auditors quickly, reducing the burden of preparing for multiple, overlapping audits.

EMEA

GDPR and DORA mandate strict controls, with sovereignty rules requiring data to remain in-country.

AMER

Federal regulations such as NAIC and state laws like NYDFS add a patchwork of compliance obligations, from cybersecurity requirements to privacy rights.

APJ

China's PIPL and India's localisation mandates place sovereignty front and center.

Many insurers are aligning their compliance programs with Zero Trust principles, ensuring that access to sensitive data is continuously verified and governed under least-privilege models. Thales solutions help enforce these principles seamlessly across hybrid and multi-cloud environments.

CipherTrust Data Security Platform helps meet all of these requirements with consistent encryption, external key management, and automated reporting. This reduces audit fatigue, accelerates compliance tasks, and lowers the risk of fines. For insurers facing rising litigation and regulatory scrutiny, compliance made simple is a strategic advantage. In practice, insurers can cut compliance reporting timelines from weeks to days, free scarce talent from manual tasks, and focus resources on innovation.

Sovereign Data Control Across Cloud and Legacy Environments

For insurers, sovereignty is no longer an option. Regulators need assurance that all sensitive customer data is under the insurer's control, not the cloud providers. Customers need peace of mind that their data cannot fall into the hands of any foreign entities.

CipherTrust Data Security Platform delivers the tools to meet both expectations.

Using external key management, hardware security modules, and advanced encryption, insurers can enforce who controls access to sensitive data. Sovereignty becomes tangible instead of aspirational. Even when workloads are migrated to the cloud, insurers keep full and exclusive control over the keys, making sure that neither cloud providers nor unauthorized parties can access regulated data.

This control extends across all environments. Hybrid and multi-cloud strategies can be pursued with confidence. Use cases become immediate and clear: underwriting teams can analyze sensitive profiles without fear of exposure, claims adjusters can access data safely, and large reinsurance operations can share the information they need across borders without fear of violating local sovereignty laws.

With CDSP, sovereignty is not a barrier to transformation; it becomes an enabler. It helps insurers bring their operations into the modern age without sacrificing compliance. It also allows them to scale services without eroding trust and innovate while staying well within the boundaries laid out by global regulations. True sovereignty is about keeping control while gaining agility.

Mitigating Third-Party and Cloud Risks

Insurers cannot operate without a complex ecosystem of partners, including brokers, reinsurers, adjusters, and cloud vendors. Each relationship widens the attack surface; in fact, Verizon's DBIR noted that third-party involvement in breaches has doubled to 30%.

This matters to insurers. The Allianz report found that contingent business interruption from supply chain failures now accounts for 15% of large claim value.

For most insurance organizations, third-party and cloud risk are Achilles' heels. Managing them needs a careful strategy:

Continuous monitoring

Maintain clear, real-time visibility into vendor compliance, risk scores, and any past incident history. Knowing where potential weak points exist allows insurers to act before a minor issue becomes a major breach.

Strong encryption and access controls

Enforce robust encryption and granular access policies whenever third parties connect to your systems. Limiting exposure at every entry point ensures sensitive data remains secure, even when external partners touch it.

Incident readiness

Always be prepared for security events. Have enforceable notification clauses and well-rehearsed response plans in place. A rapid, coordinated response plan mitigates damage, protects clients, and demonstrates operational resilience to watchdogs.

Cloud-specific safeguards

Insist on audit rights, exit strategies, and clear shared responsibility agreements with all cloud providers. These measures make sure that insurers stay in control of their data, maintain compliance, and can respond decisively when needed.

CipherTrust Data Security Platform strengthens this posture. By extending encryption and key management policies to third parties, insurers can enforce consistent protection across their ecosystem. Data is secured at rest, in motion, and in use; irrespective of who handles it. The result is not blind trust, but verified resilience.

The reality is simple: insurers cannot avoid third-party dependence, but they can choose to manage it with discipline. CDSP arms insurers with the visibility they need to identify weak points and the tools to enforce security standards consistently. In an ecosystem where a single vendor's lapse can cascade into large-scale disruption, this capability is key.

Insurance-Focused Use Cases and Success Scenarios

A recent statement from the UK's ICO underlines what's at stake: it is the insurers' "duty to protect the data entrusted ... by millions of people." The Information Commissioner goes one step further:

Maintaining good cybersecurity is fundamental to economic growth and security. With so many cyber attacks in the headlines, our message is clear: every organization, no matter how large, must take proactive steps to keep people's data secure. Cyber criminals don't wait, so businesses can't afford to wait either - taking action today could prevent the worst from happening tomorrow.

CipherTrust Data Security Platform equips insurers with the capabilities they need to stay ahead of evolving data risks:

- Protection: Encrypt, tokenize, and mask sensitive information at every stage, wherever it resides, ensuring that critical data remains secure across all environments.
- Key & Secrets: Offers centralized, external control over encryption keys across both cloud and legacy systems, giving insurers consistent oversight and reducing the risk of unauthorized access.
- Classification and Discovery: Provides full visibility into where sensitive data lives, helping insurers understand exposure, prioritize protection, and simplify compliance with data privacy regulations.
- Behavior Analytics: Monitors user and system activity to detect anomalies early, enabling proactive intervention before potential breaches or misuse can escalate.

CDSP helps insurers "maintain good cybersecurity" and is already delivering value across insurance processes:

- Claims processing: Third-party adjusters need access to personal and medical data. CipherTrust Data Security Platform enables encrypted, auditable access, ensuring compliance with privacy rules while accelerating claims handling.
- Underwriting: Sensitive risk and medical data must be analyzed without compromising privacy. CDSP secures the data while allowing analytics to run at scale, supporting faster, data-driven decisions.
- Digital transformation: Many legacy applications and data are being migrated to the cloud. CipherTrust Data Security Platform enforces encryption and key control during the transition, so that data sovereignty is maintained, and migration risk is limited.
- Cyber insurance readiness: Carriers and brokers increasingly demand proof of resilience. CDSP equips insurers to demonstrate strong controls, lowering premiums and improving insurability.

Recommended Metrics and Next Steps

Insurance leaders need to focus on the metrics that matter when it comes to managing data risk and regulatory compliance. Key indicators include:

- **What percentage of sensitive data is encrypted:** Ensuring that critical information (PII and PHI) is protected across all environments.
- **Vendor compliance scores:** Measuring how well third parties adhere to contractual and regulatory obligations, reducing exposure to downstream risks.
- **Time to detect and report incidents:** Speed is critical; faster detection and reporting can prevent minor issues from becoming major breaches.
- **Audit-readiness scores:** Demonstrating preparedness for regulatory reviews and internal audits builds confidence with stakeholders.
- **Reduction in regulatory fines and penalties:** Tracking this metric shows the tangible impact of proactive data governance and risk management.

To turn these insights into action, insurers can take practical steps to strengthen their data security posture:

- **Conduct a data compliance readiness check:** Benchmark your current position against industry standards and identify gaps.
- **Prioritize high-value use cases:** Focus on areas where you see the greatest operational and regulatory impact, such as claims, underwriting, and reinsurance.
- **Partner with Thales:** Leverage workshops and tailored security roadmaps to align strategy, tools, and processes with evolving compliance demands.

By tracking the right metrics, insurers gain insight. By following a formal data security roadmap, they gain control. Compliance stops being a reaction. It becomes a strategy.

The tools exist. The metrics are clear, as is the path forward. It is tangible, actionable, and immediate.

Insurers who embrace these practices do more than comply. They reduce risk, move faster, and signal trust to the market. Their reputation grows while confidence rises.

Over time, something greater emerges.
A foundation, solid and reliable.

Building a Resilient, Compliant, and Trusted Insurance Business

Insurance cannot exist without trust. Every policy, every claim, and every interaction depend on it. Unfortunately, this trust is fragile. The world grows more complex every day as cyber threats evolve, regulations multiply, and supply chains stretch across continents.

In this environment, resilience is not optional, compliance is not a box to check, and sovereignty over data is no longer a technical detail.

CipherTrust Data Security Platform delivers all three: **unmatched control, simplified compliance, and end-to-end data protection across cloud, hybrid, and on-premises environments.** The CDSP platform gives insurers the power to **embed Zero Trust principles**, reduce risk, accelerate transformation, and demonstrate accountability at every touchpoint.

The outcome is more than security. It is confidence that regulators will see adherence, partners will see reliability, and customers will see a steward they can trust.

Trust can be the edge that sets insurers apart. With CipherTrust Data Security Platform, that edge is real, visible, measurable, and enduring. Protect it, strengthen it, and lead with it.

Change is the only constant. In a market where transformation never slows, insurers who lead with trust, resilience, and compliance set new benchmarks, shape the future of the insurance industry, and earn lasting confidence.

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.

THALES

Building a future we can all trust

Contact us

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

cpl.thalesgroup.com