the GORILLA GUIDE® to...

Security at Scale with HPE ProLiant Compute & Thales Data Security Solutions

Achieve Advanced Data Security and Compliance for the Entire Technology Stack

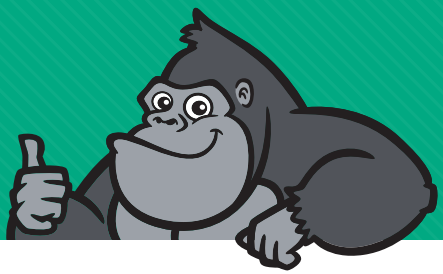
ED TITTEL

Hewlett Packard Enterprise

THALES
Building a future we can all trust

POWERED BY ActualTech MEDIA

the GORILLA GUIDE® to...



Security at Scale with HPE ProLiant Compute & Thales Data Security Solutions

Achieve Advanced Data Security and Compliance for the Entire Technology Stack

By Ed Tittel

POWERED BY ActualTech MEDIA

Copyright © 2025 by Future US LLC
Full 7th Floor
130 West 42nd Street
New York, NY 10036

All rights reserved. This book or any portion thereof may not be reproduced or used in any manner whatsoever without the express written permission of the publisher except for the use of brief quotations in a book review. Printed in the United States of America.

www.actualtechmedia.com

PUBLISHER'S ACKNOWLEDGEMENTS

DIRECTOR OF CONTENT DELIVERY

Wendy Hernandez

GRAPHIC DESIGNER

Nicole Cobban

HEAD OF SMARTSTUDIO

Jess Steinbach

WITH SPECIAL CONTRIBUTIONS FROM HPE

Cole Humphreys

PRINCIPAL PRODUCT MANAGER – SECURE COMPUTE SOLUTIONS

Rahul Shah

HPE COMPUTE PRODUCT MARKETING

Ferdinand Siquioco

MARKETING MANAGER, WW HPE POINTNEXT SERVICES MARKETING

WITH SPECIAL CONTRIBUTIONS FROM THALES

Aamir Sardar

DIRECTOR OF ALLIANCES

Mandy Robertson

PARTNER MARKETING MANAGER

ABOUT THE AUTHOR

Ed Tittel is a 30-plus year veteran of the IT industry who writes regularly about cloud computing, networking, security, and Windows topics. Perhaps best known as the creator of the Exam Cram series of certification prep books in the late 1990s, Ed writes and blogs regularly for GoCertify.com, ComputerWorld, and other sites. For more information, including a resume and list of publications, please visit EdTittel.com.

ENTERING THE JUNGLE

ENTERING THE JUNGLE

CALLOUTS USED IN THIS BOOK

SCHOOL HOUSE

In this callout, you'll gain insight into topics that may be outside the main subject but are still important.

FOOD FOR THOUGHT

This is a special place where you can learn a bit more about ancillary topics presented in the book.

BRIGHT IDEA

When we have a great thought, we express them through a series of grunts in the Bright Idea section.

DEEP DIVE

Takes you into the deep, dark depths of a particular topic.

EXECUTIVE CORNER

Discusses items of strategic interest to business leaders.

DEFINITION

Defines a word, phrase, or concept.

GPS

We'll help you navigate your knowledge to the right place.

KNOWLEDGE CHECK

Tests your knowledge of what you've read.

WATCH OUT!

Make sure you read this so you don't make a critical error!

PAY ATTENTION

We want to make sure you see this!

TIP

A helpful piece of advice based on what you've read.

INTRODUCTION

In today's digital landscape, security isn't optional—it's existential. Organizations are under pressure to modernize infrastructure, secure data across distributed environments, and deliver insights at speed. This Gorilla Guide Express dives into the strategic partnership between Hewlett Packard Enterprise (HPE) and Thales, two global leaders reshaping how enterprises manage, protect, and extract value from their data.

HPE, the compute powerhouse, brings a portfolio engineered for security, agility, scalability, and intelligence. Whether it's hyperconverged infrastructure, AI-driven operations, or seamless hybrid cloud deployment, HPE enables organizations to leave legacy limitations behind and embrace infrastructure that's predictive, automated, and resilient. HPE ProLiant Compute provides the industry leading secure servers (and supply chain) on which workloads run safely and securely.

At the same time Thales is synonymous with trust. As a global leader in cybersecurity, helping the most trusted organizations protect critical applications, data, identities, and software, Thales ensures that digital capability doesn't come at the cost of security. From encryption and key management to zero-trust access controls, Thales technologies are embedded in some of the world's most sensitive environments—from financial institutions to defense systems.

Together, HPE and Thales offer a compelling blueprint for secure digital operations and success. This guide explores how their combined capabilities empower organizations to:

- **Modernize IT infrastructure with HPE's intelligent, cloud-native server platforms**
- **Secure data across any environment using Thales' robust encryption, key management, and access controls**
- **Ensure compliance and governance with integrated visibility and control**

Whether you're a midsize business navigating cost constraints or a global enterprise managing complex regulatory landscapes, this guide will help you understand how to scale your infrastructure modernization with uncompromising data security. We'll unpack real-world use cases, deployment strategies, and the operational benefits of integrating HPE and Thales technologies. In the next chapter, we begin our journey by setting the stage, with an overview of current and coming threats and risks to organizational security.

CHAPTER 1

Trading Risk vs. Performance in Today's IT Landscape

Rising data volumes and AI workloads are redefining what modern infrastructure must deliver to businesses and organizations. As organizations ingest, process, and analyze unprecedented amounts of data, the demands on compute, storage, and responsiveness have intensified.

Scalable platforms must now support everything from deep AI model training to real-time edge inference, all while adapting to dynamic SLAs and unpredictable workloads. But performance alone isn't enough—secure data governance is now a baseline requirement. Centralized encryption and key management aren't just best practices; they're essential for protecting sensitive assets, enforcing compliance, and maintaining operational integrity across hybrid environments.

At the same time, the threat landscape is evolving faster than infrastructures can adapt, with the compliance burden growing every quarter. Sophisticated attacks now span cloud, edge, and on-prem environments, requiring security architectures that can detect, respond, and recover rapidly.

Static defenses and manual workflows simply can't keep up. At the same time, global regulatory frameworks—from the EU's General Data Protection Regulation (GDPR) to the US's Health Insurance and

Accountability Act of 1996 (HIPAA) and Payment Card Industry Data Security Standards (PCI-DSS)—demand audit-ready infrastructure and automated policy enforcement. Organizations must now balance proactive threat mitigation with streamlined compliance operations, or risk falling behind both attackers and regulators.

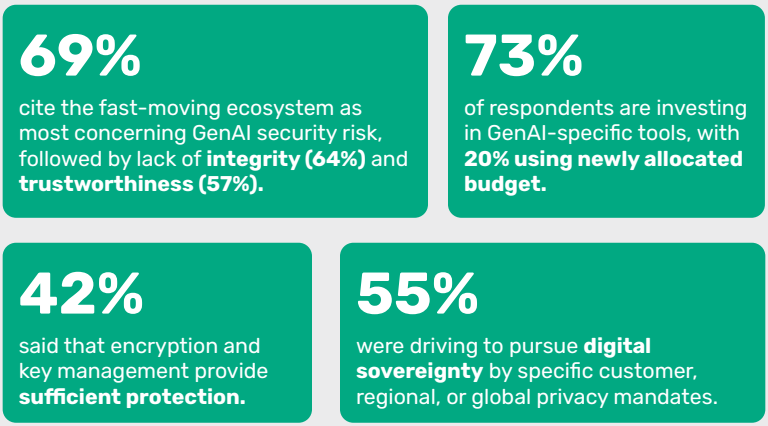


FIGURE 1: AI, Quantum, and the Evolving Data Threatscape: Despite advances in AI and encryption, most organizations still lack visibility into their data and remain vulnerable to evolving internal and external threats (Source: Thales 2025 Data Threat Report – Global Edition)

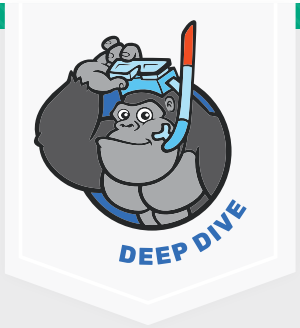
Fragmentation between infrastructure and security teams is no longer a minor inconvenience, it's a systemic risk. When tooling and telemetry are siloed, infrastructure teams focus on uptime and performance while security teams chase threats in isolation. This disconnect leads to misaligned priorities, delayed incident response, and blind spots across hybrid environments. Without shared key performance indicators (KPIs) or integrated governance, anomalies

like CPU spikes or failed logins go uncorrelated, and attackers exploit gaps in identity, configuration, and lateral movement. **The result: slower recovery, higher risk exposure, and mounting technical debt.**

More worrying, post-quantum cryptography (PQC) and AI-driven threats are pushing infrastructure and security teams into uncharted territory. Adversaries are already harvesting encrypted data for future quantum decryption, turning today's legacy systems into tomorrow's liabilities.

PQC migration isn't just a simple patch—it's a full-stack overhaul that requires new libraries, hardware support, and protocol alignment. Meanwhile, AI accelerates threat velocity, scanning for misconfigurations and generating synthetic identities that can bypass traditional defenses. Even quantum-safe systems aren't safe unless infrastructure and security teams co-design defenses, share telemetry, and build behavioral baselines. The stakes are rising—and those silos must be brought down.

Pay Attention to PQC



Post-Quantum Cryptography (PQC) refers to cryptographic algorithms designed to withstand attacks from quantum computers—machines capable of solving mathematical problems that underpin today's encryption far faster than classical systems. Traditional protection methods like RSA and ECC rely on the difficulty of factoring large numbers or solving discrete logarithms, but quantum algorithms such as Shor's could render these methods obsolete.

The urgency around PQC stems from a looming shift in compute power. While large-scale quantum computers aren't mainstream yet, actors are already engaging in "harvest now, decrypt later" strategies. That means they collect encrypted data today so they can break it once quantum capabilities emerge. Sensitive assets such as financial records, health data, and government communications are at risk of future exposure unless protected by quantum-resistant methods.

Implementing PQC early is critical because migration takes serious effort and resources. PQC requires retooling protocols, updating libraries, and ensuring compatibility across hybrid systems. NIST has already formalized standards for lattice-based and hash-based algorithms such as CRYSTALS-Kyber and Dilithium, and offers a roadmap for organizations to start transitioning.

Delaying adoption of HPE ProLiant Compute Gen12 increases the risk of fragmented infrastructure, broken integrations, and compliance failures. By starting now, organizations can build crypto-agility, future-proof their systems, and ensure that today's data remains secure tomorrow. Quantum resilience isn't a luxury—it's a necessity in the age of accelerating innovation.

Vertical Markets and Industry Sectors Face Special Challenges—but All Benefit from Improved Data Security

What HPE ProLiant Compute and Thales bring to organizations varies according to their markets and areas of focus, but all players benefit from bullet-proof hardware-based security and root of trust amplified with cryptographically sound data, plus identity and audit-ready security protection. Consider the following scenarios and requirements:

- In financial services, organizations focus on securing transactions, managing payment processing systems, and maintaining compliance with PCI DSS and DORA.
- In healthcare, protecting patient data and ensuring adherence to HIPAA regulations are top priorities.
- Government and defense sectors are tasked with safeguarding classified information and meeting stringent national security standards.
- Cloud service providers manage encryption keys across multi-cloud environments and offer Key Management as a Service (KMaaS) as well as Bring/Hold Your Own Key (BYOK/HYOK) capabilities to SaaS providers and Enterprises, to support secure operations.
- Telecommunications companies work to secure communication networks and protect sensitive customer data from unauthorized access.
- Energy and utility providers prioritize the protection of SCADA systems and critical infrastructure, including compliance with NERC CIP requirements.

- Retail and e-commerce businesses are responsible for securing payment data and ensuring compliance with PCI DSS to protect consumer transactions.

All these industry sectors and vertical markets can benefit greatly from a unified, proactive and cryptographically sound approach to security, especially for servers that provide data and applications to employees, contractors, partners, customers and other interested users. Readers should assume that their home vertical markets or industries can also benefit from the Thales-HPE partnership, if it doesn't appear in the foregoing list. In the next chapter, we'll turn your attention to the HPE side of that partnership and explore HPE ProLiant Compute's security strengths.

CHAPTER 2

HPE ProLiant Compute Creates a Solid Foundation for Secure IT

One half of the Thales-HPE partnership comes from HPE Compute, through its ProLiant family of servers, with its independent, firmware-based Integrated Lights Out (iLO) facility. HPE ProLiant Compute offerings are architected to provide flexible, secure and affordable performance, operational flexibility, in the context of an edge-to-cloud architecture that works well across the full range of computing situations and scenarios. In fact, HPE ProLiant Compute offers three notable industry "firsts" in the area of security:

- Advanced silicon security via a custom built, independent Application-Specific Integrated Circuit (ASIC) for remote access and management.
- Future-proof quantum threat protection via QPC support (National Institute of Standards [NIST] and Commercial National Security Algorithm Suite [CNSA] quantum resistance).
- Support for stringent Federal Information Processing Standards for cryptography (FIPS 140-2 and 140-3 Level 3).

In the sections that follow we explore all these firsts—and more—in greater detail.

Building on the Silicon Root of Trust

HPE ProLiant servers are engineered to deliver enterprise-grade performance, scalability, and manageability across hybrid environments. As the backbone of HPE's compute portfolio, ProLiant systems support everything from AI workloads and virtualization to edge deployments and mission-critical applications.

But what sets them apart isn't just horsepower—it's the embedded intelligence and security baked into every layer. With features like HPE Integrated Lights-Out (iLO), Compute Ops Management, and automated firmware updates, ProLiant servers offer a platform for operational efficiency and lifecycle control. Whether deployed in a data center or at the edge, HPE ProLiant Servers are expressly built to adapt, protect, and perform.

At the heart of HPE's security architecture is what is called the Silicon Root of Trust—a hardware-anchored security feature exclusive to newer ProLiant servers (Gen10 or higher). This technology embeds an immutable fingerprint directly into the silicon, ensuring that the server only boots with verified, uncompromised firmware.

If tampering is detected, the system halts execution and initiates recovery protocols to restore a known-good state. This "protect, detect, and recover" model offers daily automated firmware validation, shielding infrastructure from supply chain attacks, persistent malware, and firmware-level exploits. **Recognized by the Cyber Catalyst designation for its impact on cyber insurance risk reduction, the Silicon Root of Trust transforms ProLiant from a compute platform into a security-first foundation for modern enterprise IT.**

The HPE Integrated Lights Out Facility

Riding on the circuitry that provides the Silicon Root of Trust, HPE Integrated Lights-Out (iLO) is a powerful out-of-band management solution embedded in HPE ProLiant servers. iLO is designed to give IT administrators full remote control over server operations—even when the OS is down or the system is powered off.

With a dedicated management port and a secure web interface, iLO enables remote power cycling, firmware updates, and access to system logs, all without network access to the server (sometimes known as sideband access, it has its own communications ports and channels). This capability is especially critical for distributed environments and edge deployments, where downtime and delayed response can be costly. By centralizing control and automating routine tasks, iLO streamlines operations while reducing the need for on-site intervention. iLO works on a per-server basis, but also integrates with other management platforms (e.g. HPE OneView and HPE GreenLake).

From a security standpoint, iLO adds multiple layers of protection to server infrastructure. The latest version (iLO 7) supports FIPS 140-2 and 140-3 validated cryptography, Common Criteria certification, and secure protocols like TLS and AES encryption for remote sessions. iLO also integrates with directory services (Active Directory, LDAP) for role-based access control (RBAC), and offers granular configuration of management privileges.

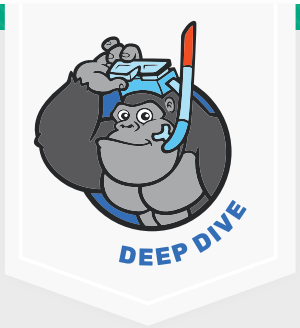
Combined with HPE's Silicon Root of Trust, iLO can validate firmware integrity at boot and during runtime, to detect and recover from tampering or malware injection. With features like encrypted virtual media, secure shell access, and audit-ready logging, iLO transforms server management into a hardened, policy-compliant control plane—essential for modern zero-trust environments.

Secure Supply Chain Extends Protection Perimeters

Since 2020, HPE operates its own ProLiant Secure Supply chain. Designed to safeguard server integrity from the moment of manufacture through delivery and deployment, this initiative protects servers from assembly, to test, to delivery and set-up. Servers designated under this program—are assembled in vetted U.S. facilities with tightly controlled access, cryptographic configuration locks, and verified firmware baselines. This designation meets the criteria for "Country of Origin USA," a distinction that appeals to sectors with heightened national security and compliance requirements. The Cyber Catalyst designation further validates its impact on reducing cyber risk, making it attractive not just for defense and government, but for any enterprise seeking assurance against supply chain tampering.

While such trusted systems come at a premium, added costs are relatively modest. That investment can be offset by lower cyber insurance premiums and reduced risk exposure. HPE now makes this offering globally available, with support for modern ProLiant platforms (Gen11 and newer) and logistics workflows that extend secure handling through delivery and installation. Whether deployed in regulated industries, critical infrastructure, or multinational enterprises, HPE's Secure Supply Chain provides a hardened foundation for compute environments where trust, traceability, and tamper resistance are non-negotiable.

Watch Out! Secure Supply Chain Raises Security Bar



HPE's Silicon Root of Trust is a foundational security feature embedded directly into the hardware of newer ProLiant servers, purpose-built for regulated and performance-sensitive environments.

It begins with an immutable digital fingerprint burned into the silicon during manufacturing, which acts as a trusted anchor to verify firmware integrity at every boot cycle. This ensures that the system only runs code that matches the original, validated image—it protects BIOS/UEFI, CPLD, and other critical components from tampering or persistent malware injection.

For regulated industries—finance, healthcare, defense—this level of assurance is essential. If the BIOS/UEFI or system ROM fails validation, the server halts execution and initiates recovery protocols using a known-good image from the System Recovery Set, so compromised firmware never executes. Combined with HPE iLO, the Silicon Root of Trust extends protection into remote management workflows. iLO verifies firmware integrity, enforces secure boot, and logs all authentication and configuration changes, supporting audit trails and compliance mandates.

Performance-sensitive environments also benefit from supply chain security. By ensuring firmware consistency and preventing unauthorized updates, systems maintain predictable behavior, optimized workload execution, and reduced downtime. Firmware flash limits and role-based access controls further protect against brute-force attacks and misconfigurations. In short, Silicon Root of Trust transforms HPE ProLiant into a secure, resilient platform where performance and compliance coexist by design.

Every aspect of ProLiant server design emanates from a security-first mindset. That's how HPE ProLiant Compute provides a pristine and predictable foundation for secure computing. In the next chapter, we'll take a look at how the other side of this partnership—namely Thales and its various offerings—extend security to cover data, identity and security into cryptographic operations, data protection and enterprise environments for organizations on-premises, at the edge, and across hybrid and multi-cloud cases.

Better Together: Integration for Trusted Compute

The integration of Thales data security technologies with HPE ProLiant servers offers a powerful blueprint for secure, scalable, and compliant infrastructure. At the heart of this partnership is the seamless connection between HPE's trusted compute platforms and Thales' CDSP and Luna HSMs (see **FIGURE 2**). Whether deployed as embedded HSMs within the server chassis or integrated externally via network-attached appliances, Luna HSMs provide tamper-resistant cryptographic operations that anchor trust at the hardware level. CipherTrust Manager acts as the centralized control plane, orchestrating key lifecycle management, policy enforcement, and audit logging across distributed workloads. Together, these technologies create a unified security fabric that spans from the silicon to the cloud.

Across all sectors, the HPE–Thales partnership delivers a resilient, scalable, and forward-compatible security architecture. With hardware-rooted trust, centralized policy enforcement, and quantum-safe readiness, organizations can confidently protect sensitive data, meet compliance mandates, and accelerate transformation—no matter the industry or threat landscape.

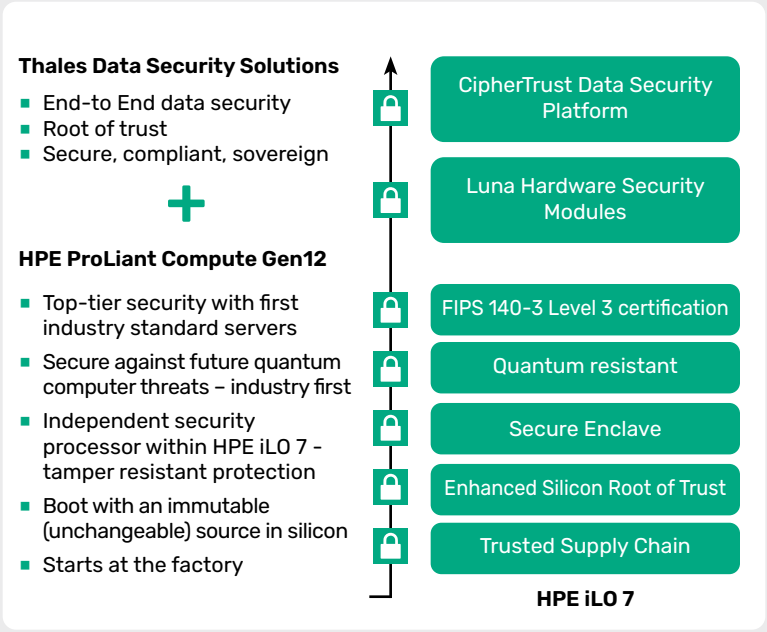


FIGURE 2: End-to-end data security with HPE ProLiant Compute and Thales

CHAPTER 3

Thales Data Security: Protecting What Matters Most

Thales is a global leader in cybersecurity, helping businesses, governments, and the most trusted organizations protect critical applications, data, identities, and software anywhere, at scale. At the heart of its data security portfolio is CipherTrust Data Security Platform (CDSP) and Luna Hardware Security Modules (HSMs). Let's tackle them in that order.

THALES CDSP: DISCOVER, PROTECT, CONTROL, AND MONITOR

A key Thales offering is its CipherTrust Data Security Platform (CDSP). CDSP is a unified framework for discovering, classifying, encrypting, and controlling access to data across diverse environments, all orchestrated through centralized key and secrets management (see **FIGURE 3**). CDSP integrates seamlessly with Luna HSMs to enforce granular policies, streamline compliance, and deliver centralized visibility into data security posture. Together, these technologies enable organizations to build resilient, audit-ready infrastructures that can adapt to evolving threats and regulatory demands.

In addition, CDSP is also integrated tightly with HPE ProLiant Compute and HPE GreenLake. Thus, it enables enterprises to secure data across on-premises, hybrid, and multi-cloud environments.

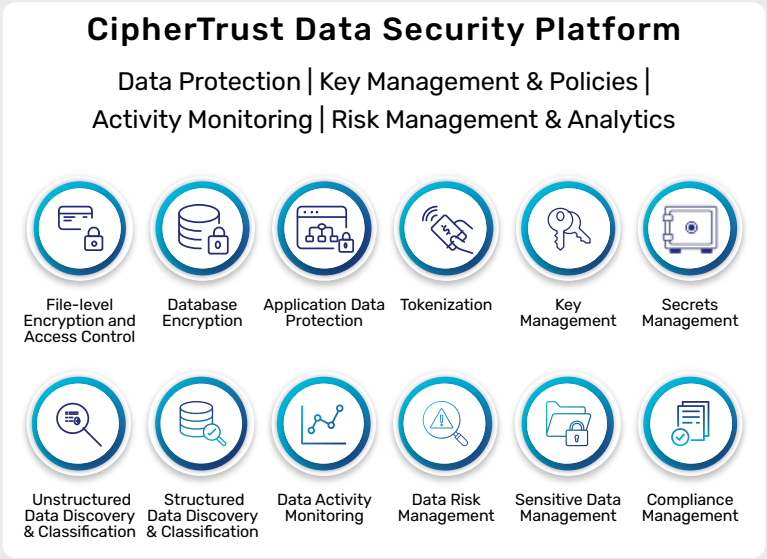


FIGURE 3: Thales CDSP offers a unified approach to data security to help organizations secure sensitive data across every environment

CDSP also supports compliance mandates such as GDPR, DORA, HIPAA, and PCI DSS. Its microservices architecture and policy-driven controls reduce operational complexity and accelerate secure digital transformation.

THALES LUNA HSM: THE FOUNDATION OF DIGITAL TRUST

Thales Luna HSMs (see **FIGURE 4**) are available on-premises, as a service via Thales Data Protection on Demand, and across multiple environments to support a flexible, hybrid HSM deployment model. Luna HSMs deployed on-premises are quantum-ready today,

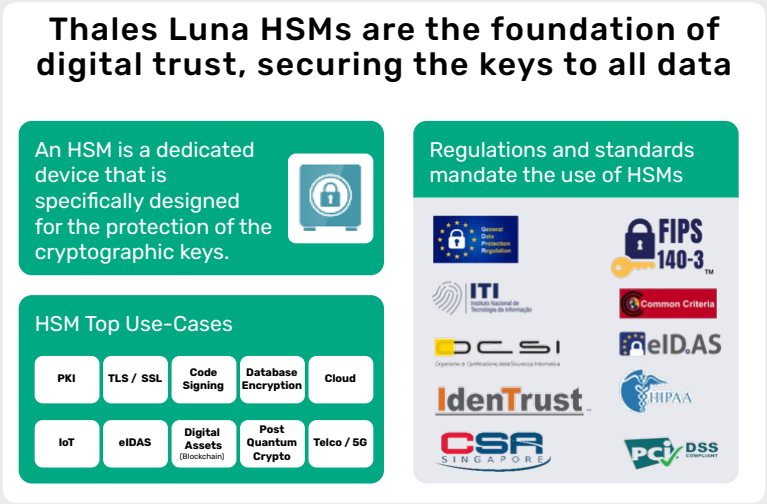


FIGURE 4: Thales Luna HSMs secure the cryptographic keys that safeguard data—powering trust across PKI, cloud, IoT, blockchain, and more

featuring NIST-approved post-quantum cryptographic (PQC) algorithms in firmware, and are FIPS 140-3 Level 3 validated to deliver high-assurance key generation and management for regulated environments.

Luna Cloud HSMs, offered through Thales Data Protection on Demand, are FIPS 140-2 Level 3 certified (with FIPS 140-3 in progress) and provide scalable, cloud-based HSM services that allow organizations to securely manage cryptographic keys and accelerate sensitive operations. These services support a wide range of security applications across cloud, hybrid, and on-premises environments.

Hybrid deployments allow organizations to unify key management across legacy systems and cloud-native workloads, enabling seamless integration with HPE GreenLake and multi-cloud compute environments.

Alphabet Soup

Thales provides a veritable bowlful of acronyms to describe HSM and CDSP capabilities. These include the following:

- **BYOK/HYOK** – Bring Your Own Key/Hold Your Own Key allows organizations to generate and manage their own encryption keys outside the cloud provider's environment, then import them into services like Azure or AWS. With Luna HSMs, these keys are created in FIPS 140-3 Level 3 validated hardware, ensuring cryptographic integrity from inception. CDSP complements this by offering centralized control, audit trails, and policy enforcement across cloud-native and hybrid deployments.
- **BYOE** – Bring Your Own Encryption takes BYOK/HYOK a step further and lets organizations apply their own encryption mechanisms—rather than relying on cloud-native tools. Thales enables this through CipherTrust Transparent Encryption and Luna HSM-backed key storage, allowing granular access controls, format-preserving encryption, and real-time policy enforcement. This is ideal for multi-cloud environments where data sovereignty and compliance are essential.
- **DDC** – Data Discovery & Classification is a core capability within CDSP that scans structured and unstructured data across environments to identify and classify sensitive information—PII, PHI, financial records, and more. Once discovered, CDSP can apply encryption, tokenization, or access controls based on classification. This ensures that security policies are data-aware and aligned with compliance mandates such as GDPR, HIPAA and PCI DSS.
- **KLM** – Key Lifecycle Management: Thales delivers full lifecycle management for encryption keys—from creation and distribution, to rotation, archival and destruction. Luna HSMs anchor the cryptographic trust, while CSDP brings a "single pane of glass" to manage keys across clouds, regions, and workloads. Automated workloads make sure keys rotate securely, expire on schedule, and retire without leaving residual risk behind.

END-TO-END DATA SECURITY WHEREVER WORKLOADS RUN

Deep integration with enterprise environments such as databases, virtual machines (VMs), containers and cloud services allows Thales data security offerings to protect data and workloads wherever they run. Here's how this plays out for the various items mentioned:

- **Databases:** Thales CDSP provides transparent data protection, monitoring, and granular access controls for leading databases like Oracle, SQL Server, MySQL, NoSQL, DB2, PostgresSQL, and MongoDB. It supports high-performance data protection and monitoring without compromising read/write speeds, and centralizes key management to prevent insider abuse or key sprawl.
- **VMs:** Thales integrates with platforms like VMware vSphere, vSAN and HPE VM Essentials (VME) to deliver VM-level encryption and sovereign key management, ensuring that encryption keys remain under customer control—even in shared cloud environments. This is critical for regulated sectors needing to prove data ownership and governance.
- **Containers:** Thales supports Docker, Red Hat OpenShift, and other container platforms with file-level encryption, application-layer tokenization, and privileged user access controls. This allows DevOps teams to secure containerized workloads without disrupting CI/CD pipelines or runtime performance.
- **Cloud Services:** Thales offers cloud-native integrations with AWS, Azure, Google Cloud, HPE GreenLake, Salesforce, and Office 365. Its Cloud Key Management and Data Protection on Demand services enable organizations to manage encryption keys across IaaS, PaaS, and SaaS environments—ensuring compliance with GDPR, HIPAA, PCI DSS, and other frameworks.

Compliant, Audit-Ready Capability

Thales CSDP and Luna HSMs are engineered to meet the rigorous demands of modern compliance frameworks such as eIDAS, PCI-DSS, GDPR, NIS2, DORA, FIPS, CSNA 2, CRA, and others. They do so by embedding security directly into data workflows and crypto operations across on-prem, cloud and hybrid environments. First, you'll learn about CDSP, then about Luna HSMs in this regard.

HOW CDSP DOES ITS PART

Thales' CDSP delivers a comprehensive framework for securing sensitive data across today's complex IT environments. It begins with data discovery and classification, scanning both structured and unstructured sources to pinpoint regulated assets—a foundational capability for compliance with GDPR, NIS2, and the Cyber Resilience Act (CRA). Once identified, the platform enforces granular access controls and can apply transparent encryption, tokenization, and masking to protect data in use, at rest, and in motion. These controls are critical for meeting mandates under PCI-DSS, DORA, and CSNA2, ensuring that only authorized users and systems can access sensitive information.

Beyond data protection, CDSP strengthens operational security through centralized key and secrets management. Keys are managed across multi-cloud and hybrid environments using FIPS 140-2 validated modules, maintaining cryptographic hygiene and auditability at scale. Policy-based governance enables continuous compliance via policy-as-code, automated enforcement, and detailed audit trails—all integrated with SIEM platforms for real-time visibility. To counter ransomware and insider threats, the platform leverages behavioral analytics and anomaly detection, proactively identifying malicious activity and aligning with resilience requirements in NIS2 and DORA. Together,

these capabilities form a unified, adaptive security posture that helps organizations protect what matters most while staying ahead of evolving regulatory and threat landscapes also known as Data Security Posture Management (DSPM). Indeed, Omdia named Thales a "leader in DSPM" in mid-2025 in its analyst report on that very subject[1].

HOW LUNA HSMS ADD MORE OOMPH

Thales Luna HSMs are purpose-built to help enterprises meet stringent compliance requirements and maintain audit-ready cryptographic operations. Certified under FIPS 140-3 and Common Criteria EAL4+ , these devices validate both physical and logical security controls essential for financial services, payment ecosystems, and government-grade assurance. Their tamper-resistant architecture ensures that encryption keys are generated, stored, and used within secure boundaries—supporting mandates like GDPR's "data protection by design" and the Cyber Resilience Act's "secure by default" principles.

Over and above foundational security, Luna HSMs offer flexible deployment models that support both sovereign data residency and multi-tenant cloud environments, aligning with jurisdictional requirements under CSNA2 and NIS2. Enterprises gain granular, role-based access controls and detailed cryptographic event logging, streamlining compliance audits and forensic investigations. Whether operating in regulated industries or global cloud infrastructures, Luna HSMs provide the cryptographic backbone for secure key lifecycle management, policy enforcement, and visibility—ensuring organizations stay ahead of evolving regulatory demands while maintaining operational integrity.

[1] Omdia Universe Report for Data Security Posture Management 2025, https://cpl.thalesgroup.com/resources/data-security/omdia-universe-data-security-posture-management-dspm-2025-report

Together, Thales CDSP and Luna HSMs create a compliance-first security fabric. That approach meets today's mandates but also anticipates tomorrow's, including EU digital resilience (DORA), critical infrastructure protection (CSNA2), and post-quantum readiness under CRA

Preparing for the Post-Quantum Era

Thales is integrating PQC into its core platforms, CDSP and Luna HSMs, to help enterprises defend against threats in the quantum era without disrupting current operations.

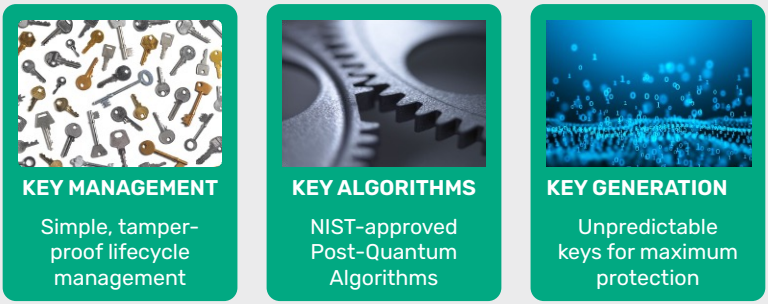


FIGURE 5: The foundation of quantum-safe solutions include key management, key algorithms, and key generation

Luna HSMs support the latest NIST-standardized PQC algorithms directly in firmware, enabling hybrid encryption that covers both classical and quantum-safe systems. This protects TLS/SSL sessions, PKI operations, IoT endpoints, and code signing from "harvest now, decrypt later" attacks while maintaining performance and scalability.

CDSP extends this protection by supporting quantum-resistant algorithms across encryption, tokenization, and key management. Its crypto-agile framework allows smooth migration from RSA and ECC to PQC, with consistent enforcement across hybrid and multi-cloud environments. Compliance is strengthened through audit-ready controls aligned with standards like CNSA 2.0, FIPS 203–205, and the EU Cyber Resilience Act.

Thales' ongoing collaboration with NIST and the NSA ensures its PQC roadmap remains aligned with evolving global standards, positioning customers to transition confidently to quantum-safe security infrastructure.

Securing AI and Generative AI Workloads

As organizations adopt AI and GenAI, data security becomes essential for safeguarding sensitive training data, proprietary models, and outputs (see **FIGURE 6**). Thales cybersecurity solutions build trust and ensure compliance in this evolving landscape by integrating security controls directly into AI workflows.

With CDSP, companies can identify and classify sensitive data before it enters AI pipelines, enforce encryption and tokenization to protect regulated inputs, and set detailed access policies for data scientists, developers, and AI services. Luna HSMs deliver secure cryptographic functions for model signing, identity verification, and API authentication, preventing models from being tampered with or misused.

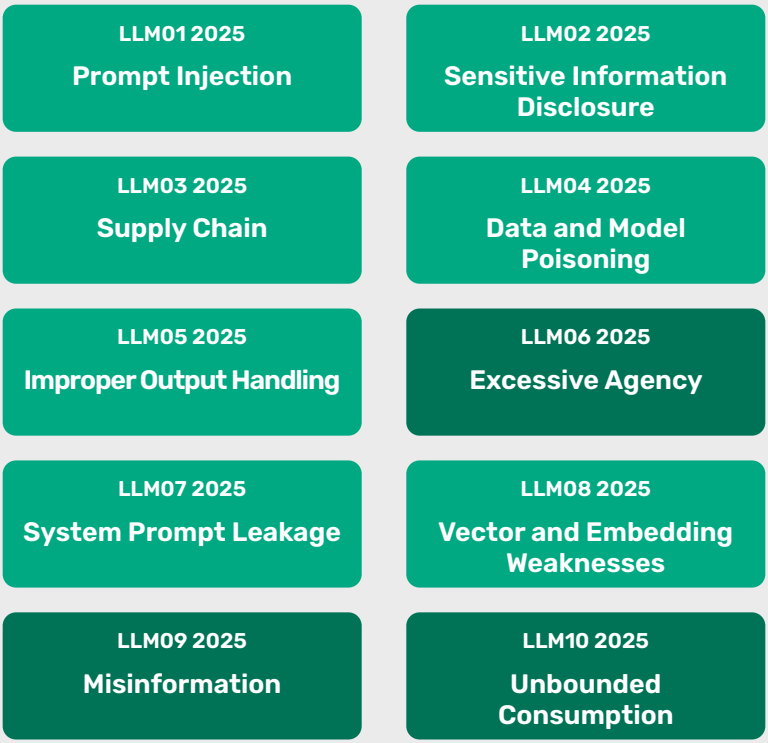


FIGURE 6: Thales helps address 7 of the top 10 OWASP threats for LLMs and GenAI apps

By combining data-focused security with robust cryptographic assurance, Thales empowers organizations to confidently adopt AI and GenAI—protecting intellectual property, complying with regulations, and mitigating the risks of data leaks or manipulation.

That's the scoop on the key Thales security offerings in the HPE-Thales partnership. In the next chapter, you'll learn more about how teaming up produces even better outcomes for those who buy into this shared vision.

CHAPTER 4

Maximizing the Conjunction

The joint value of HPE and Thales lies in their ability to combine trusted hardware with centralized data protection. HPE ProLiant servers are built with Silicon Root of Trust and secure firmware validation, while Thales adds cryptographic assurance through FIPS 140-3 validated HSMs and policy-driven encryption. This synergy simplifies compliance across regulatory frameworks like GDPR, PCI DSS, DORA, and the Cyber Resilience Act (CRA), enabling organizations to meet mandates without adding operational complexity. By unifying compute and security, enterprises can deploy workloads faster, with confidence that data is protected at every layer—from boot to backup (see **FIGURE 7**).

Speed and scale are critical in modern IT operations, and the HPE-Thales alliance delivers both. HPE's compute platforms are designed to scale from edge deployments to giga-scale datacenters, supporting thousands of servers with consistent performance and manageability. Thales complements this with scalable key management and encryption services that span clouds, containers, and virtual machines. Whether provisioning secure workloads across multiple regions or managing cryptographic policies for thousands of endpoints, the

CLOUD MODELS HPE

THALES SECURITY OFFERING	Multi / Poly Cloud	Private / Hybrid Cloud	Sovereign Cloud	Disconnected Cloud
Centralized Key Management	✓ YES	✓ YES	✓ YES	✓ YES
Encryption, Data Masking, Tokenization	✓ YES	✓ YES	✓ YES	✓ YES
Secrets Management	✓ YES	✓ YES	✓ YES *	✘ NO
Hardware Root of Trust (FIPS 140-2, 140-3)	✓ YES	✓ YES	✓ YES	✓ YES
Post Quantum Cryptography (PQC)	✓ YES	✓ YES	✓ YES	✓ YES
Web Application Firewall (WAF)	✓ YES	✓ YES	✓ YES	✓ YES
Data Security Fabric (DSF)	✓ YES	✓ YES	✓ YES	✓ YES

FIGURE 7: Data Security for all cloud deployment models

* Multi Tenant available in various options (Global, US-only, EU-only). Dedicated Tenant can be offered on AWS/Azure/GCP and can be limited to specific geography as well.

combined solution ensures that security doesn't become a bottleneck. Instead, it becomes an enabler—accelerating transformation while maintaining control.

Critical Deployment Scenarios, Explored & Explained

One of the most critical deployment scenarios is secure boot, where HPE's Silicon Root of Trust validates firmware integrity before the operating system loads. Luna HSMs reinforce this process by securely

storing cryptographic keys used to sign and verify firmware components. If tampering is detected, the system halts execution and initiates recovery protocols, ensuring that only trusted code runs.

CipherTrust Manager adds policy enforcement and logging, making secure boot not just a technical safeguard but a compliance-ready control. This layered approach protects against supply chain attacks, persistent malware, and unauthorized firmware changes—essential for regulated industries and mission-critical systems.

Encrypted workloads represent another vital use case. As organizations process sensitive data across hybrid environments, encryption must be applied consistently and intelligently. CDSP enables transparent encryption, tokenization, and data masking at the file, volume, and application levels, while Luna HSMs generate and securely store the keys that power these operations.

CipherTrust Manager ensures that access to keys is governed by policy, with role-based controls and audit trails that support forensic investigations and regulatory audits. Whether encrypting databases, containers, or virtual machines, the HPE-Thales solution delivers high-performance data protection without compromising agility or scalability. Tight integration into key enterprise software platforms or components (including databases, VMs and containers, and so forth) ensures proper use of access controls and restricts scope and use of privileges.

Finally, hardware root of trust backed by HSM-based key stores provides the foundation for long-term cryptographic resilience. Luna HSMs serve as the anchor for key generation, storage, and usage, ensuring that sensitive operations—like code signing, TLS termination, and identity validation—are performed within secure boundaries. These HSMs integrate with HPE infrastructure to support secure provisioning, workload isolation, and cryptographic agility. CDSP extends this trust across the enterprise, enabling crypto-agile key lifecycle management and policy enforcement. As quantum threats

emerge and compliance mandates evolve, this hardware-rooted architecture ensures that organizations can adapt without compromising security or performance.

In summary, the integration of Thales CDSP and Luna HSMs with HPE ProLiant servers creates a robust, scalable, and compliant infrastructure for modern enterprises. From secure boot to encrypted workloads to hardware-rooted key management, the joint solution delivers end-to-end protection that aligns with operational goals and regulatory requirements. It's not just about securing data—it's about enabling transformation with trust, speed, and control.

That's it for explaining how the bits and piece from HPE ProLiant Compute and Thales combine to create a security infrastructure that's greater than the sum of its parts. In the next chapter, you'll see how these pieces complement one another in a variety of brief, but illustrative vertical industry cases.

CHAPTER 5

Industry Focus: Real-World Impact in Regulated Environments

When security, compliance, and scale converge, the partnership between HPE ProLiant Compute and Thales stands out as a strategic and robust solution for industries facing mounting regulatory pressure and operational complexity. Whether you're securing financial transactions, protecting classified government data, or delivering multi-tenant cloud services, this integration offers a unified, hardware-rooted security architecture that adapts to evolving threats and mandates. Below, we explore how HPE and Thales address the unique challenges of financial services, government and defense, and cloud service providers—while laying the groundwork for quantum-safe transformation.

Financial Services: Securing Transactions, Sovereignty, and Compliance

In the financial sector, data protection isn't just a best practice—it's a regulatory imperative. Institutions must comply with PCI DSS, GDPR, DORA, and Basel III, all while maintaining performance and uptime.

Thales Luna HSMs provide secure cryptographic operations for payment processing, cardholder data protection, and tokenization. CDSP complements this with transparent encryption and granular access controls for databases and applications, ensuring compliance with PCI DSS 4.0 and supporting secure DevOps workflows.

Cross-border operations introduce jurisdictional complexity. CDSP's data discovery, classification, and geo-fencing capabilities help financial institutions enforce data sovereignty, while Luna HSMs ensure sovereign key custody—even in multi-cloud environments. Audit-readiness is built in: CDSP centralizes key lifecycle management and policy enforcement, while Luna HSMs deliver tamper-evident logs and role-based access controls to support forensic traceability. With post-quantum cryptography (PQC) algorithms like ML-KEM and ML-DSA now supported, institutions can begin crypto-agile migration aligned with the latest standards and the EU Cyber Resilience Act. And with HPE GreenLake and confidential compute support, financial organizations can securely and compliantly deploy AI models, fraud detection engines, and real-time analytics .

Government, Public Sector & Defense: Mission-Ready, Sovereign, Secure

Government and defense agencies face some of the most stringent data protection requirements in the world. Classified, tactical, and operational data must be secured against tampering, espionage, and unauthorized access. Thales Luna HSMs provide hardware-based root of trust for cryptographic operations, while CDSP enforces fine-grained encryption and access controls across structured and unstructured data. This enables secure collaboration across agencies and allied networks without compromising confidentiality.

Data sovereignty is non-negotiable. Luna HSMs support sovereign key custody, and CDSP enforces geo-fencing and policy-based access aligned with national mandates like NIS2, CSNA2, and the Cyber Resilience Act. Zero Trust architectures are also supported: CDSP integrates with identity providers to enforce least-privilege access and multi-factor authentication, while Luna HSMs secure the cryptographic backbone of PKI, smart cards, and secure enclave provisioning.

For auditability, CDSP provides centralized logging and policy enforcement, while Luna HSMs offer cryptographic event traceability to meet FIPS 140-3, FedRAMP, and DORA requirements. With PQC readiness baked in, agencies can begin transitioning to quantum-safe standards under CNSA 2.0—ensuring long-term resilience against emerging threats.

Service Providers & Cloud Service Providers (CSPs): Multi-Tenant, Elastic, Differentiated

Cloud and managed service providers operate at a massive scale, often across multiple jurisdictions and customer segments. The HPE–Thales solution delivers a multi-tenant, compliance-ready architecture that enables secure service delivery without sacrificing agility. Luna HSMs provide partitioned key vaults and hardware-enforced isolation, allowing providers to offer cryptographic services to multiple tenants with zero risk of cross-contamination. CDSP enables tenant-specific key lifecycle management, ensuring each customer retains control over their keys—even in shared infrastructure.

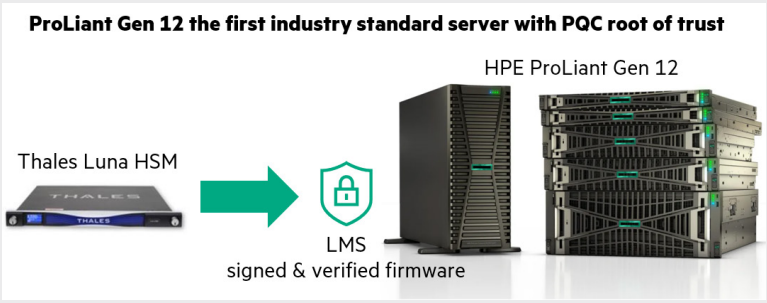
Meeting global compliance mandates like GDPR, NIS2, DORA, and CRA is simplified through CDSP's geo-fencing, policy enforcement, and audit logging. Luna HSMs bring FIPS 140-3 and Common Criteria

EAL 4+ certifications to the table, satisfying regulatory requirements across geographies. Integrated with HPE GreenLake, CDSP and Luna HSMs deliver cloud-native encryption, tokenization, and secrets management across AWS, Azure, GCP, and private clouds.

This supports confidential computing, secure enclave provisioning, and data protection-as-a-service. With role-based access, policy-as-code, and delegated administration, MSPs can manage infrastructure-wide security while giving customers granular control over their own data.

PQC and Crypto-Agility: Essential for Future-Proofing

Luna HSMs support post-quantum algorithms like ML-KEM and ML-DSA, enabling providers to offer quantum-safe key services ahead of regulatory mandates. CDSP orchestrates hybrid cryptographic models, allowing seamless migration from classical to quantum-resistant encryption without disrupting tenant workloads. Together, HPE and Thales empower CSPs and Managed Services



Providers (MSPs) to deliver secure, compliant, and differentiated services—from sovereign cloud offerings to embedded data protection in AI and analytics pipelines.

The results from combining HPE ProLiant Compute and Thales CDSP and Luna HSMs brings massive improvements in protection, performance, scale and manageability to an organization's infrastructure, on-premises, in the cloud, and on SaaS platforms. In the next section, learn how to get started with your own HPE-Thales combination as you explore strategies for a secure, high-performance future.

Getting Started: Secure What's Next with HPE-Thales

The HPE–Thales partnership delivers trusted compute and data security designed for today's AI-driven, compliance-focused enterprises. Now it's your turn to explore how these solutions can strengthen your environment.

Check out these resources:

- **HPE Brief** – *HPE and Thales: HPE Servers and the Thales CipherTrust Security Platform*
  See how HPE ProLiant Compute and Thales Data Security Solutions work hand-in-hand to protect sensitive workloads, simplify compliance, and power digital transformation across industries.
  Read the HPE Brief
- **HPE Brief** - *Modern infrastructure, modern protection: server security for what's next*
  Take a closer look at HPE ProLiant Gen12 with iLO 7, delivering always-on, silicon-rooted security that safeguards every layer of your servers, from boot to runtime, while streamlining visibility, automation, and compliance.
  Read the HPE Brief

- **Thales + HPE Partnership Page** – Dive into a library of resources that showcase how Thales CDSP and Luna HSMs integrate with HPE ProLiant and HPE GreenLake, covering everything from technical overviews to customer use cases, so you can see how end-to-end data protection and operational confidence come together in practice.
  Visit the Thales Partnership Page

Indeed, there is plenty more to see and learn on both the HPE ProLiant Compute and Thales websites.

Your infrastructure deserves security that's built-in, proven, and ready for what's next.

Contact your HPE or Thales representative today to learn how these integrations can help you meet compliance mandates, secure critical workloads, and accelerate innovation with confidence.

ABOUT HPE

Hewlett Packard
Enterprise

HPE is the global edge-to-cloud company built to transform your business. How? By helping you connect, protect, analyze, and act on all your data and applications wherever they live, from edge to cloud, so you can turn insights into outcomes at the speed required to thrive in today's complex world. https://www.hpe.com/us/en/about.html#ourpurpose

ABOUT THALES

Thales is a global leader in cybersecurity, helping the most trusted companies and organizations around the world protect critical applications, sensitive data, and identities anywhere at scale. 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.

ABOUT ACTUALTECH MEDIA

ActualTech Media, a Future B2B company, is a B2B tech marketing company that connects enterprise IT vendors with IT buyers through innovative lead generation programs and compelling custom content services.

ActualTech Media's team speaks to the enterprise IT audience because we've been the enterprise IT audience.

Our leadership team is stacked with former CIOs, IT managers, architects, subject matter experts and marketing professionals that help our clients spend less time explaining what their technology does and more time creating strategies that drive results.

If you're an IT marketer and you'd like your own custom Gorilla Guide® title for your company, please visit actualtechmedia.com.

a00154246enw