Hewlett Packard Enterprise

Solution brief

Check if the document is available in the language of your choice.

HPE SECURITY FOR DATA AT REST WITH UTIMACO ESKM

Simple, secure, and compliant encryption with local or cloud key management

Advantages

- Uses native HPE iLO protocol
- VMware® virtual drive coverage
- On-premises or cloud ESKM
- Encrypts data on the cache module of the HPE Smart Array controller
- Interoperable and integrated key manager
- Hardware-based security at highest FIPS levels
- Custom integrations and scaled deployments
- Easy deployment and simple licensing
- Interoperate vESKM with external hardware security module (HSM) to enhance security while managing the keys virtually
- Integrate with the HPE ecosystem and third-party applications using KMIP

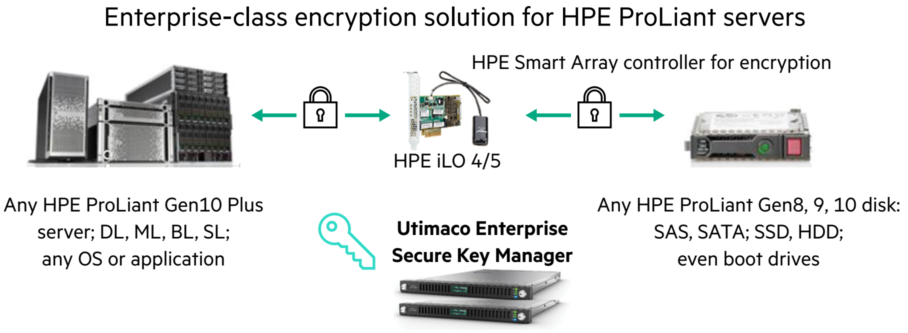
Enterprise-class encryption solution for HPE ProLiant servers
HPE Smart Array controller for encryption
HPE iLO 4/5
Any HPE ProLiant Gen10 Plus server; DL, ML, BL, SL; any OS or application
Utimaco Enterprise Secure Key Manager
Any HPE ProLiant Gen8, 9, 10 disk: SAS, SATA; SSD, HDD; even boot drives

FIGURE 1. HPE's data at-rest security solution component

MAKE YOUR DATA AT REST SECURE AND COMPLIANT

Overview

To minimize the potential impact of a security incident or compromise, you must reduce data access and the ability to access sensitive information on your storage.

Data loss has the potential to not only interrupt your daily business operations but also leaves you vulnerable to legal liability and negative press. What's more, if you're in the financial services, healthcare, government, or other regulated industry, you are also responsible to comply with regulations such as the Payment Card Industry Data Security Standard (PCI-DSS), HIPAA, Sarbanes-Oxley (SOX), and a growing array of other data privacy regulations.

A few types of data that, if lost or compromised, could cause a major business and trust problem for your company include:

- Payment card numbers
- Private customer data including health records
- Financial data about your company or employees
- Trade secrets and intellectual property

This data-at-rest security solution leverages HPE ProLiant DL360/DL380 Gen10 Plus with Utimaco Enterprise Secure Key Manager (ESKM) to deliver outstanding performance, efficient TCO while protecting your sensitive data from intrusion.

KEY FEATURES OF UTIMACO

HPE ProLiant servers with Utimaco ESKM provides a complete solution for unifying and automating an organization's encryption controls by securely creating, protecting, serving, controlling, and auditing access to business- and compliance-critical encryption keys.

HPE ProLiant DL360/DL380 Gen10 Plus is designed as a fully integrated solution and is a Federal Information Processing Standards (FIPS) 140-2 validated secure server appliance. Its standard capabilities include high-availability clustering and failover, secure database, key generation

HPE ProLiant servers

Hewlett Packard Enterprise further extends its security capabilities in a server from distribution and shipping, through its complete lifecycle while it is still active. The new features are built on top of the silicon root of trust technology from HPE. Hardened security features activated during the manufacturing process will offer the following benefits:

- Prevent booting of any compromised operating system (OS) by using new hardening to connect the server firmware security to the operating system by activating the UEFI secure boot
- Reduce attack surface by placing servers in high-security mode to verify user authenticity, which helps ensure that more than four million lines of firmware code is valid and uncompromised
- Avoid tampering of server firmware and hardware using server configuration lock to verify unauthorized addition of options (NICs, drives, and such) or malicious activity by capturing the inventory or a picture of the server, along with its hardware and firmware at the factory to provide protection throughout the supply chain process

and retrieval services, identity and access management for administrators, encryption devices, secure backup and recovery, local certificate authority, and strong audit logging for compliance validation.

HPE ProLiant server with Utimaco ESKM is available as a virtual appliance compliant with FIPS 140-2 Level 1 and as a hardware appliance compliant with FIPS 140-2 Level 2, 3, and 4 providing the right level of security for discrete environments.

MULTI-LEVEL ENCRYPTION COVERAGE AND BENEFITS

You can now encrypt not just for your HDD but for your cache too. Any HDD or SSD in the HPE SmartDrive portfolio for HPE ProLiant servers is supported.

Here are benefits of the data-at-rest security solution from HPE:

- Provides remote key management mode, which allows central key management from just a few servers to more than 25,000 servers and millions of keys with simplified deployment and management.
- Offers HPE Secure Encryption and HPE Data Sanitization that helps you comply with industry regulations and legislation such as PCI-DSS, HIPAA, and SOX.
- Maintains encrypted CPU or I/O performance.
- Removes the disk Defective Media Retention (DMR) cost with instant erase. Delete key(s) and terminate the data at no extra support cost, shredding cost, or environmental waste.
- Decreases complexity by reducing your hassles and expenses. If you use Self-Encrypting Drives (SEDs) instead of this solution, the drives are expensive with limited vendors, mostly not FIPS-validated, and they require local unlock keys.

HPE ProLiant server with Utimaco ESKM supports open standards key management such as Key Management Interoperability Protocol (KMIP). So, you can now maintain your existing third-party servers and add additional HPE ProLiant servers to maintain multiple vendor servers without a need to replace existing servers until the next refresh cycle. There's no dependence on Trusted Platform Module (TPM), OS, or applications.

Its low-touch administration, built-in high availability, FIPS-validated security, and such benefits are fully auditable.

The security solution is fully automated thus leveraging the HPE iLO scripting to align with HPE Smart Storage Array scripting for mass and automated deployment with Utimaco ESKM self-registration support.

It also helps you implement and enforce separation of duties and dual access control by separating the data and keys management.

USE CASES

One of the biggest healthcare and insurance providers uses HPE ProLiant and Utimaco ESKM to protect data across tens of thousands of servers across the globe while implementing separation of duties and access control, and achieving the most stringent HIPAA compliance.

Another leading general aviation company uses HPE ProLiant and HPE storage solutions along with ESKM to protect data-at-rest and third-party database solutions to secure data at the application level implementing one of zero-trust policies.

In conclusion, this HPE data-at-rest solution provides security by encryption technique so that even in the case of a breach, your sensitive data is protected.

LEARN MORE AT

hpe.com/us/en/servers/rack.html

**Make the right purchase decision.
Contact our presales specialists.**

Chat Email Call

Get updates

Hewlett Packard
Enterprise

© Copyright 2021 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

VMware is a registered trademark or trademark of VMware, Inc. and its subsidiaries in the United States and other jurisdictions. All third-party marks are property of their respective owners.