THE BUNKER

Part of the CYBERFORT group

FACTSHEET

VORMETRIC TRANSPARENT ENCRYPTION FROM THALES-AS-A-SERVICE

Safeguard data everywhere and achieve compliance and access controls

MORE DATA, THREATS AND ENVIRONMENTS

IT security is not static. There are many moving parts and IT security must adapt in-line with the changing environment. As data sets grow and find themselves in the cloud, across virtual systems and within big data platforms, regulatory mandates have to evolve in order to properly safeguard sensitive data.

To help you adapt to these changing demands, we leverage sophisticated Vormetric encryption technology from Thales that offers a strong mix of security, implementation flexibility, and operational efficiency.

INTRODUCING VORMETRIC TRANSPARENT ENCRYPTION-AS-A-SERVICE:

VORMETRIC TRANSPARENT ENCRYPTION FROM THALES IS DESIGNED TO HELP YOUR ORGANISATION ACHIEVE COMPLIANCE WITH DATA PROTECTION MANDATES BY SAFEGUARDING DATA-AT-REST. THIS IS DONE THROUGH ROBUST ENCRYPTION, STRICT ACCESS CONTROLS AND DATA ACCESS AUDIT LOGGING, WHETHER THAT BE ACROSS MULTIPLE CLOUD ENVIRONMENTS, ON-PREMISE OR WITHIN BIG DATA AND CONTAINER ENVIRONMENTS.

ADVANCED HARDWARE-ACCELERATED PROTECTION

With encryption based on the Advanced Encryption Standard (AES) and elliptic curve cryptography (ECC) for key exchange, this solution is FIPS 140-2 Level 1 validated, offering peace of mind that your sensitive data is properly safeguarded to the correct level.

Not only that, but Vormetric Transparent Encryption also leverages the AES hardware encryption capabilities on modern CPUs, delivering encryption with optimal performance even in virtual and cloud environments.

ADVANCED ACCESS CONTROLS FOR BIG DATA (HADOOP)

When implemented in Hadoop environments, access controls are extended to Hadoop users and groups.

FLEXIBLE AND SCALABLE ARCHITECTURE

This solution is available for a broad selection of Windows, Linux, and UNIX platforms, and can be used in physical, virtual, cloud, container and big data environments — regardless of the underlying storage technology. Agents can be located locally on premises as well as across multiple cloud environments, eliminating any bottlenecks and latency.

SAP HANA REVIEWED AND QUALIFIED

SAP has reviewed and qualified Vormetric Transparent Encryption as suitable for use in SAP solution environments.

Telephone: 01304 814800 Email: info@thebunker.net

EMBRACE COST-EFFECTIVE SECURITY WITH ADDED FLEXIBILITY

Our Vormetric Transparent Encryption-as-a-service, is a pay-as-you-go encryption solution that enables you to implement strong data security for users, applications and infrastructure, without having to alter business processes.

OUR VORMETRIC-AS-A-SERVICE OFFERS:

SIMPLE DEPLOYMENT WITH MINIMAL DISRUPTION AND EFFORT

Agents are deployed on servers at the file system or volume level, enabling encryption and access control without requiring changes to applications, infrastructure, systems management tasks or business practices. This service can also alleviate the planned downtime required for initial encryption and scheduled rekeying operations seamlessly by adding the Vormetric Live Data Transformation option to deployments.

STRONG ENCRYPTION

This service only employs strong, standard-based encryption protocols, such as the Advanced Encryption Standard (AES) for data encryption and elliptic curve cryptography (ECC) for key exchange. The agent is FIPS 140-2 Level 1 validated.

CONTINUOUS PROTECTION

Continuous enforcement of policies that protect against unauthorised access by users and processes, as well as creating detailed data access audit logs of all activities.

GRANULAR CONTROLS

Enforcement of granular, least-privileged user access policies that protect data from external attacks and misuse by privileged users. Specific policies can be applied by users – including for administrators with root privileges, other system level users and LDAP/Active Directory users and groups – process, file type, time of day, and other parameters.

SECURITY INTELLIGENCE

Identify and stop threats faster with detailed data access audit logs that not only satisfy compliance and forensic reporting requirements, but also enable data security analytics with popular security information and event management (SIEM) systems.

HARDWARE ACCELERATED ENCRYPTION

Encryption overhead is minimised using the AES hardware encryption capabilities available in modern CPUs (Intel AES-NI, AMD AES-NI, IBM Power8 encryption and Oracle SPARC encryption).

AUTOMATED MAINTENANCE

Vormetric Orchestrator automates deployment, configuration, management and monitoring for Vormetric Transparent Encryption deployments, helping simplify operations, eliminate errors and speed deployments.

COST-EFFECTIVE, FLEXIBLE AND SCALABLE ARCHITECTURE

Deployments consist of Vormetric Transparent Encryption agents and Vormetric Data Security Manager (DSM) appliances. Agents are deployed on servers in environments from data centers to cloud, containers and big data. Policy and key management is centralised at the DSM. The DSM is available as a FIPS 140-2 level, 2 or 3 appliance and features RESTful, SOAP and command line APIs as well as web-based management interfaces.

THE BUNKER PROTOCOL™

The Bunker Protocol™ is an all-encompassing methodology that secures against risk and ensures the most secure IT delivery in the UK.

The Bunker Protocol™ incorporates physical, human and digital security capability and processes and wraps them with a governance and standards layer that ensures that client data and systems are continually secure against threats to confidentiality, integrity and availability.

THIS IS ULTRA SECURE

Physical	Military grade data centres
Human	All employees are fully background checked and our culture starts and ends with security
Digital	We build and integrate systems in-house, ultra secure, from the source code up

Telephone: 01304 814800 Email: info@thebunker.net