IBM Security & Thales

Presents a 4 part series:

ZeroTrust and Your Data

Zero Trust and your Data – Session Schedule

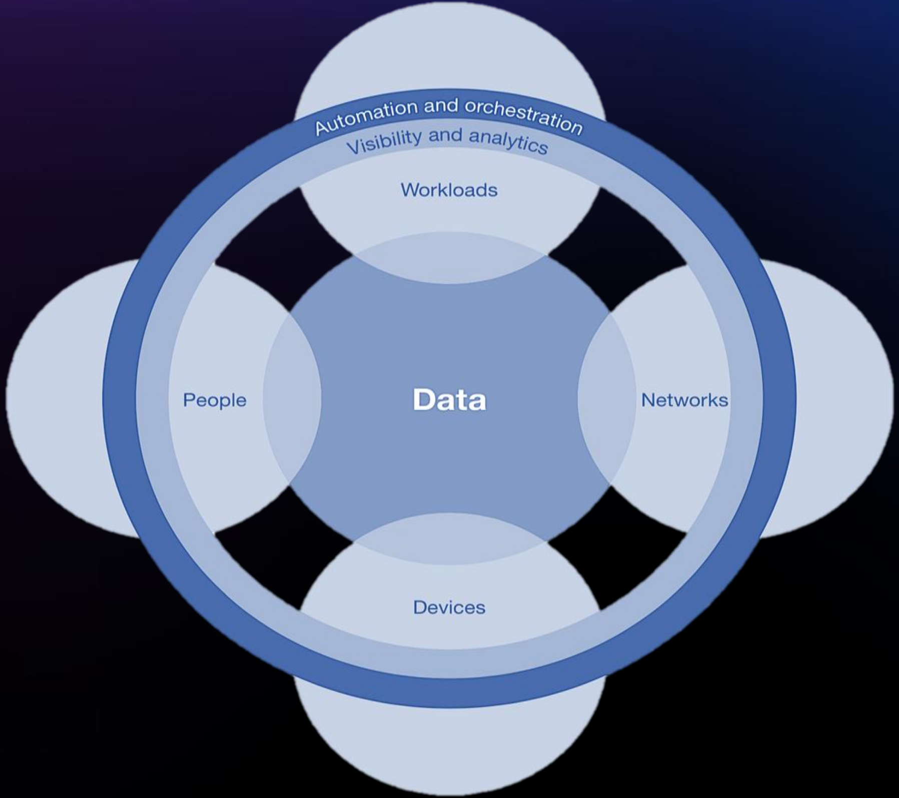
Session 1 : **Zero Trust and your Data: Securing Containers and Managing Access**
June 16th, 2020 2:00 pm

Session 2: **Zero Trust and your Data: Securing Databases and Managing Vulnerabilities**
July 14th, 2020 11:00 am

Session 3: **Zero Trust and your Data: Cloud Data Security and Cloud Keys Management**
Aug 11th, 2020 11:00 am

Session 4: **Zero Trust and your Data: Advanced Threat and Continuous Monitoring**
Sept 8th, 2020 11:00 am

Forrester's Zero Trust Framework



Forrester's Zero Trust Framework

A conceptual and architectural model for how security teams should redesign networks into secure microperimeters, use obfuscation, limit risks associated with excessive user privileges, analytics and automation to improve detection and response.

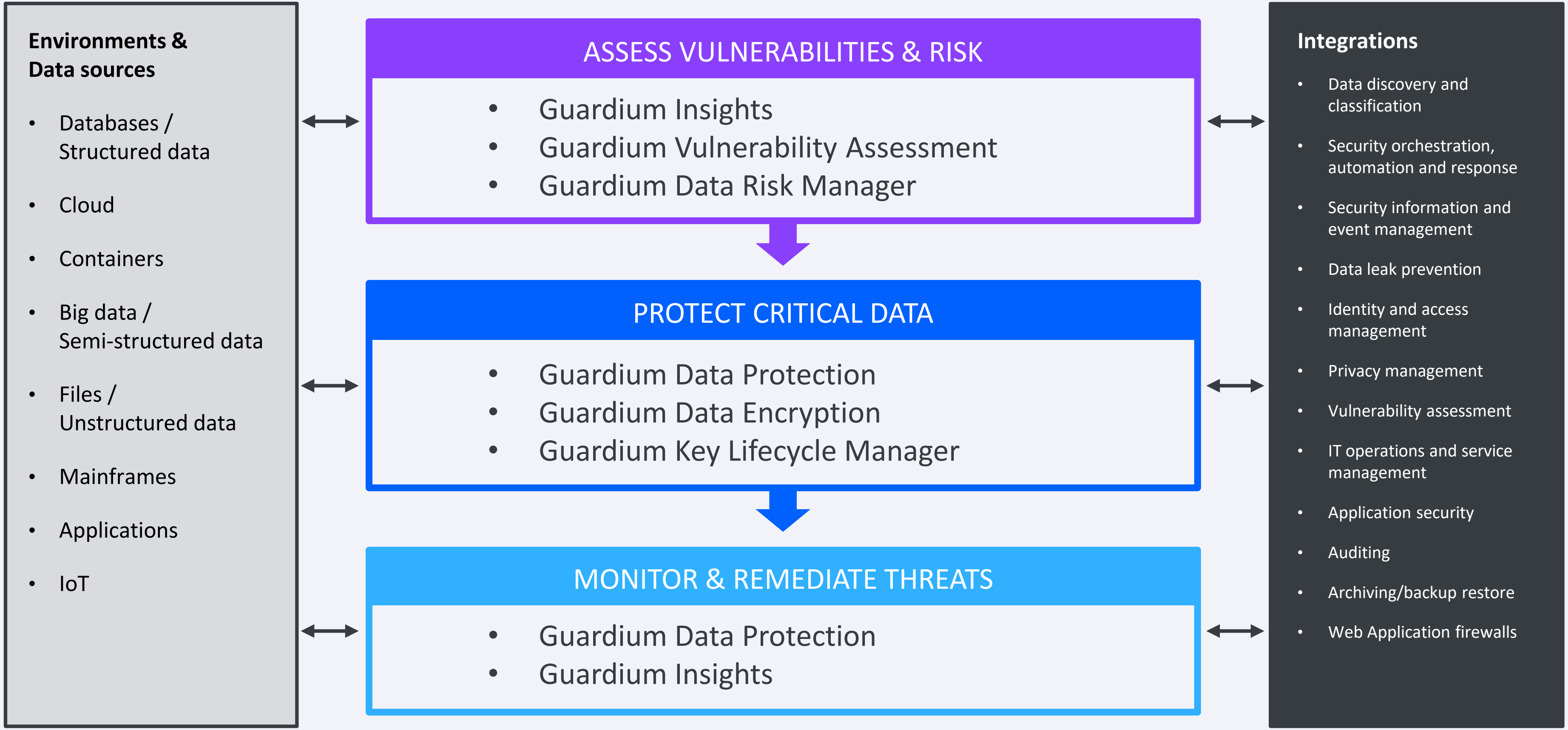
Key Tenants:

- Data-Centric Approach: Security Travels with the Data
- Never Assume Trust: Continuously Use Risk-Based Analysis

A Paradigm Not A Product

- Discover, Classify and Assess Vulnerabilities for all Data
- Darken Multi-Cloud Apps from ALL Networks
- Verify First then Connect
- Least Privileged, App-Session Access based on *Context*
- Encrypt Everything
- Device-App and App-App Micro segments
- Visibility and Control Inside & Outside Perimeter
- Continuous Assessment

Data Security with IBM Security Guardium



Environments & Data sources

- Databases / Structured data
- Cloud
- Containers
- Big data / Semi-structured data
- Files / Unstructured data
- Mainframes
- Applications
- IoT

ASSESS VULNERABILITIES & RISK

- Guardium Insights
- Guardium Vulnerability Assessment
- Guardium Data Risk Manager

PROTECT CRITICAL DATA

- Guardium Data Protection
- Guardium Data Encryption
- Guardium Key Lifecycle Manager

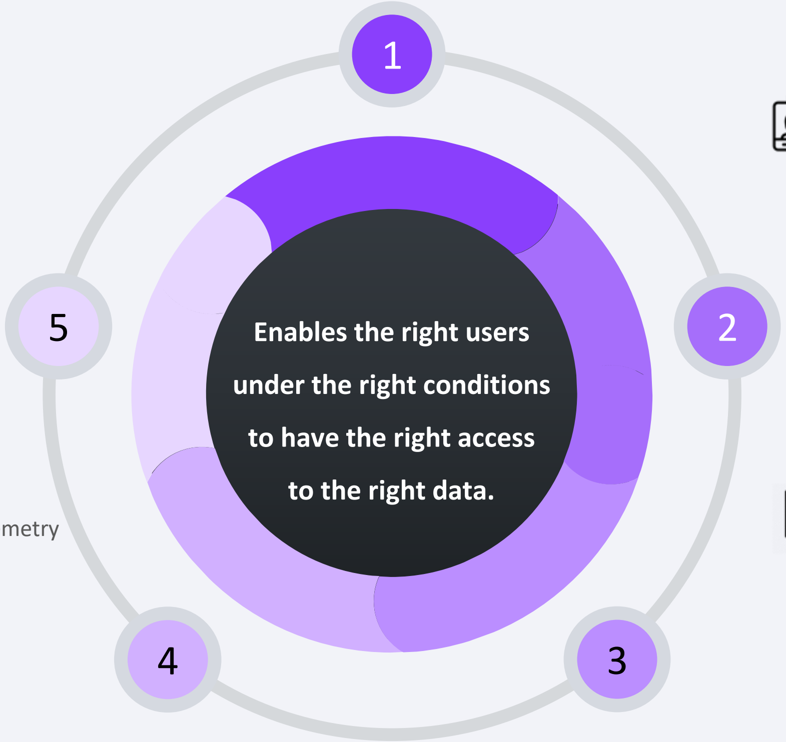
MONITOR & REMEDIATE THREATS

- Guardium Data Protection
- Guardium Insights

Integrations

- Data discovery and classification
- Security orchestration, automation and response
- Security information and event management
- Data leak prevention
- Identity and access management
- Privacy management
- Vulnerability assessment
- IT operations and service management
- Application security
- Auditing
- Archiving/backup restore
- Web Application firewalls

The IBM Security framework for delivering Digital Trust



Enables the right users under the right conditions to have the right access to the right data.

Perform Assessment

- Identify the hybrid multi-cloud IT environment
- Discover & classify data, endpoints, and workloads
- Perform vulnerability assessments

Establish Identity

- Discover, onboard, and classify all users (internal, external, privileged, human, things, apps, devices)
- Support self-service and personalization
- Enable strong multifactor authentication

Define Policy

- Define risk tolerance and access rules aligned to business process
- Establish who should have access to what data and under what conditions
- Always encrypt sensitive data

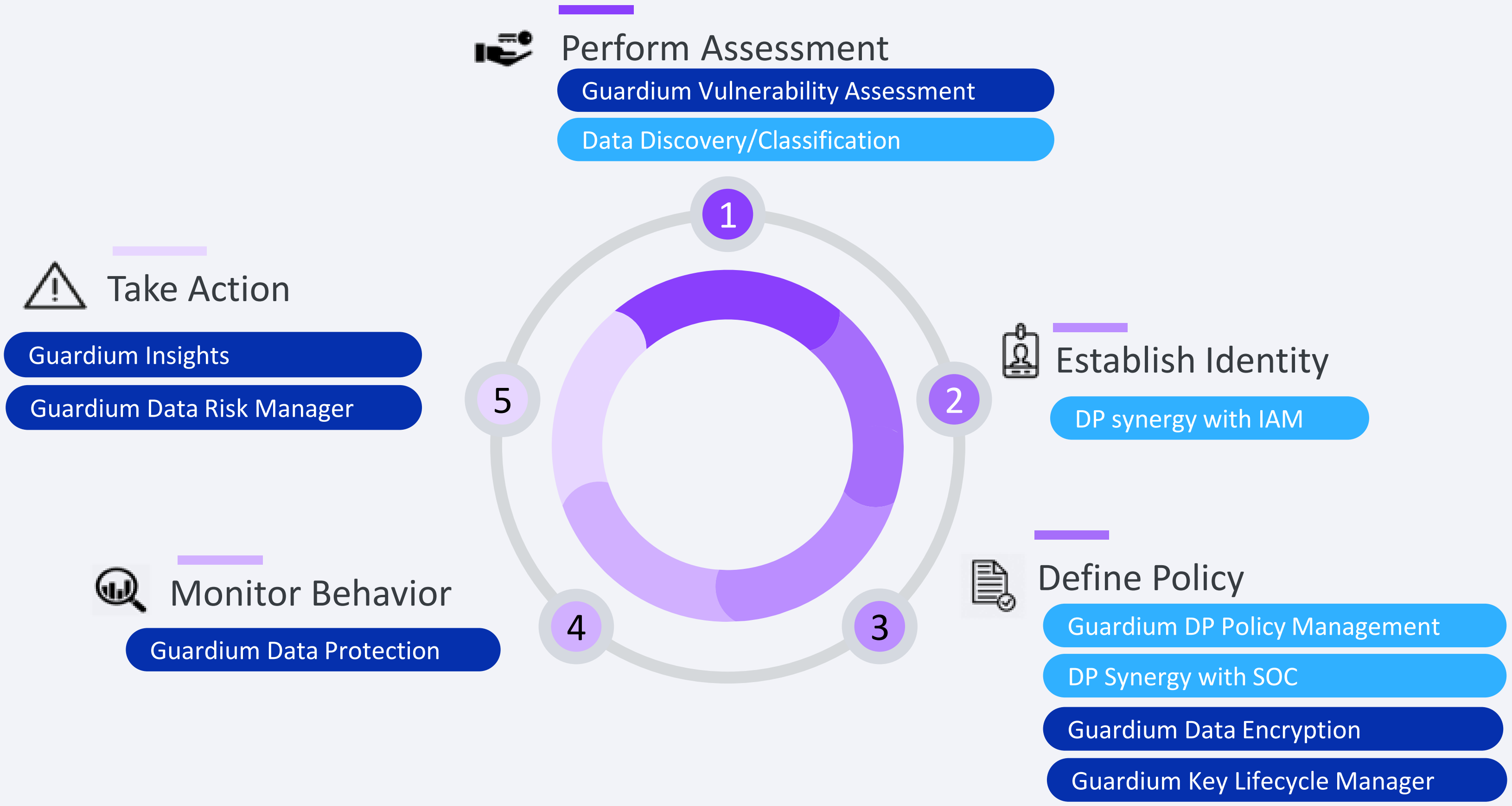
Monitor Behavior

- Deliver data and identity insights and telemetry to the SOC, identifying anomalous user behaviors
- Continuously audit and govern access
- Record sessions for privileged users

Take Action

- Institute proactive reporting and alerts
- Orchestrate responses to remediate potential threats through integration with data and identity systems
- Dynamically adjust actions based on contextual analysis

IBM’s Framework for Delivering Digital Trust



Perform Assessment

- Guardium Vulnerability Assessment
- Data Discovery/Classification

Establish Identity

- DP synergy with IAM

Define Policy

- Guardium DP Policy Management
- DP Synergy with SOC
- Guardium Data Encryption
- Guardium Key Lifecycle Manager

Monitor Behavior

- Guardium Data Protection

Take Action

- Guardium Insights
- Guardium Data Risk Manager

Results from the 2020 Thales Data Threat Report – Federal Edition

101

US federal agency executives

The report concentrates on the results from 101 US federal agency executives with responsibility for, or influence over, IT and data security

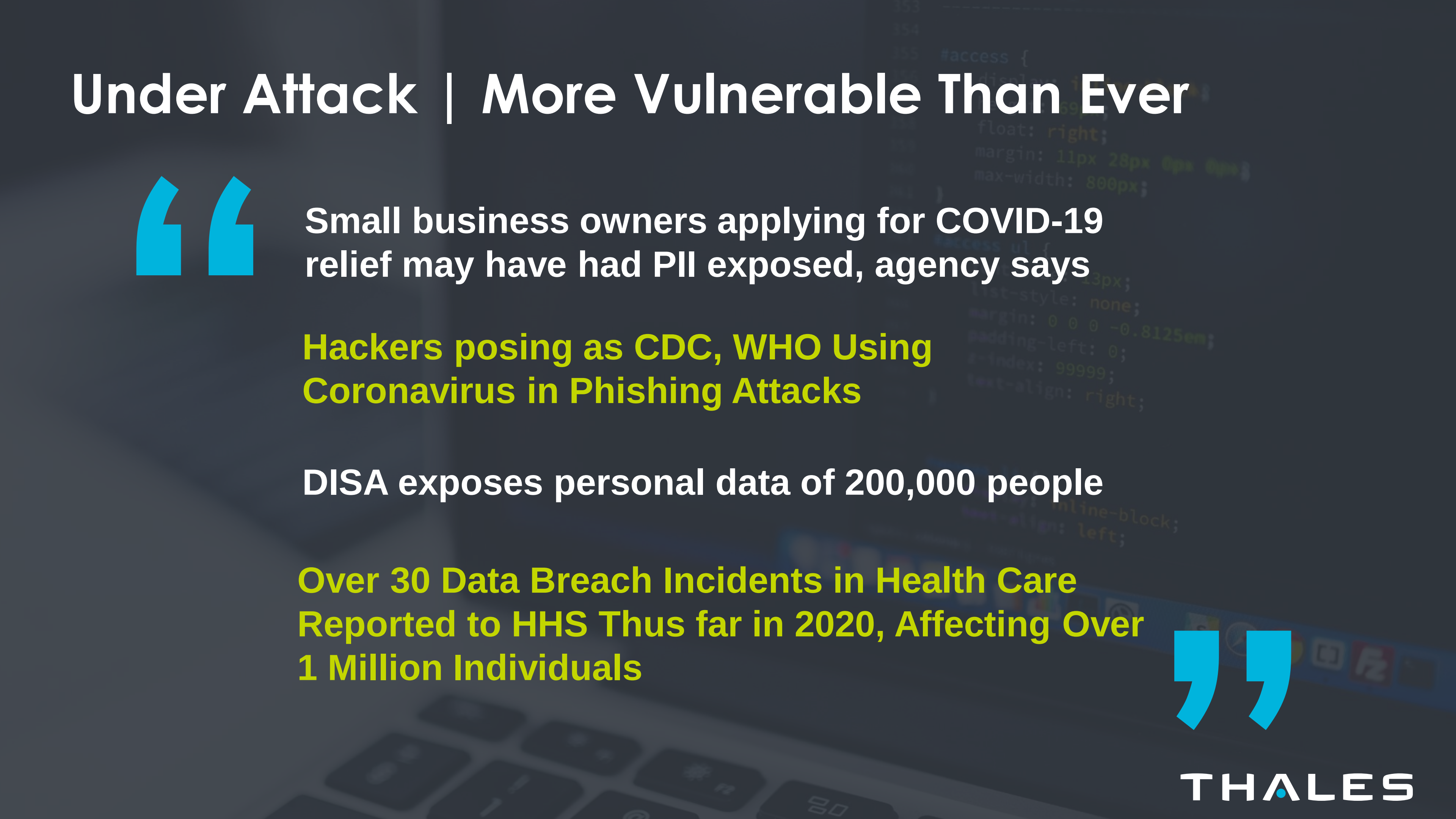
1,723

respondents

from within a total survey set of 1,723 respondents.

Survey, reporting and analysis conducted by IDC, sponsored by Thales.

Under Attack | More Vulnerable Than Ever



“

Small business owners applying for COVID-19 relief may have had PII exposed, agency says

Hackers posing as CDC, WHO Using Coronavirus in Phishing Attacks

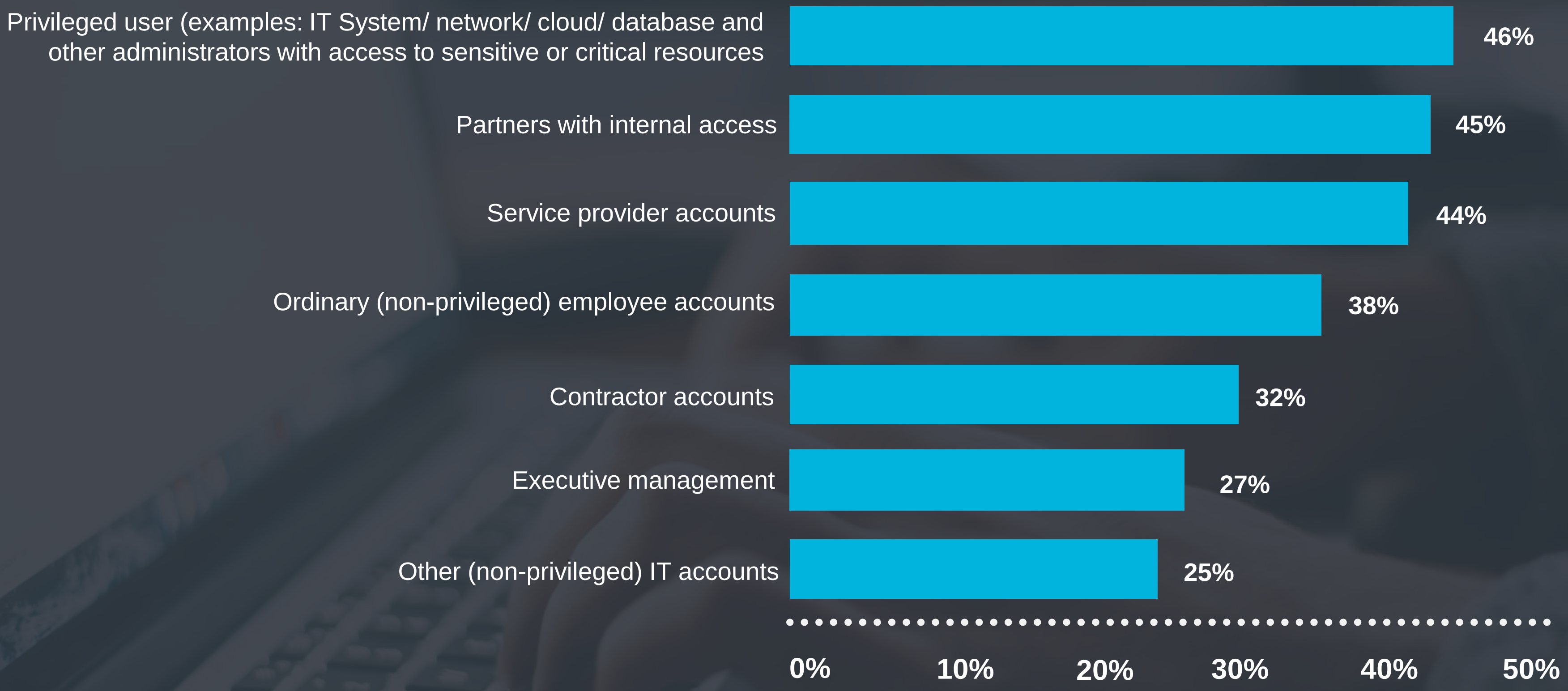
DISA exposes personal data of 200,000 people

Over 30 Data Breach Incidents in Health Care Reported to HHS Thus far in 2020, Affecting Over 1 Million Individuals

”

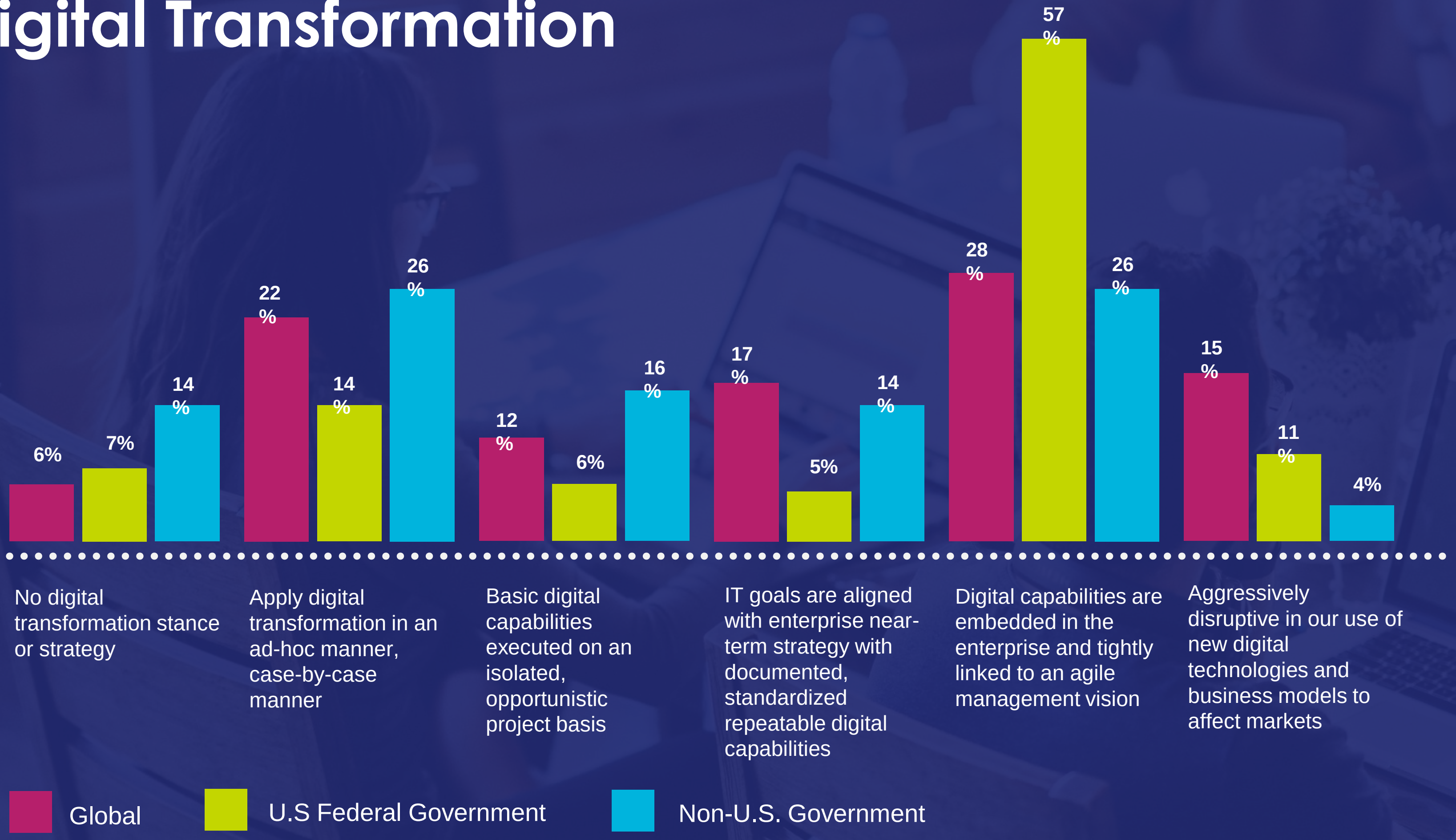
THALES

Internal Data Vectors of Vulnerability



THALES

Digital Transformation



Sensitive Data in the Cloud is Growing

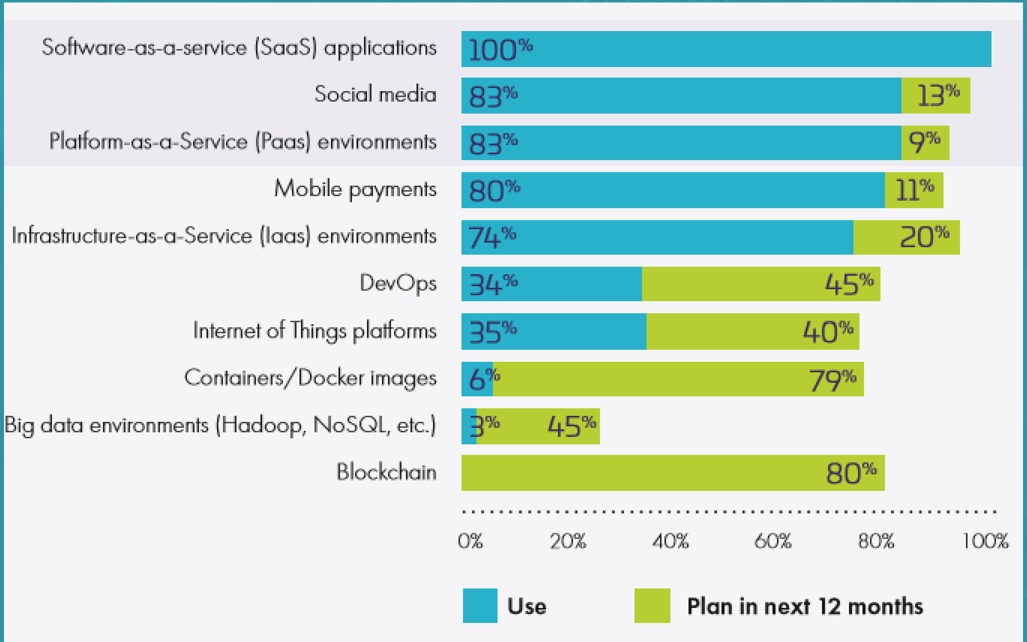
54%

of all U.S Federal government data is stored in the cloud.

51%

of all U.S Federal government data in the cloud is sensitive.

Technology Adoption Levels

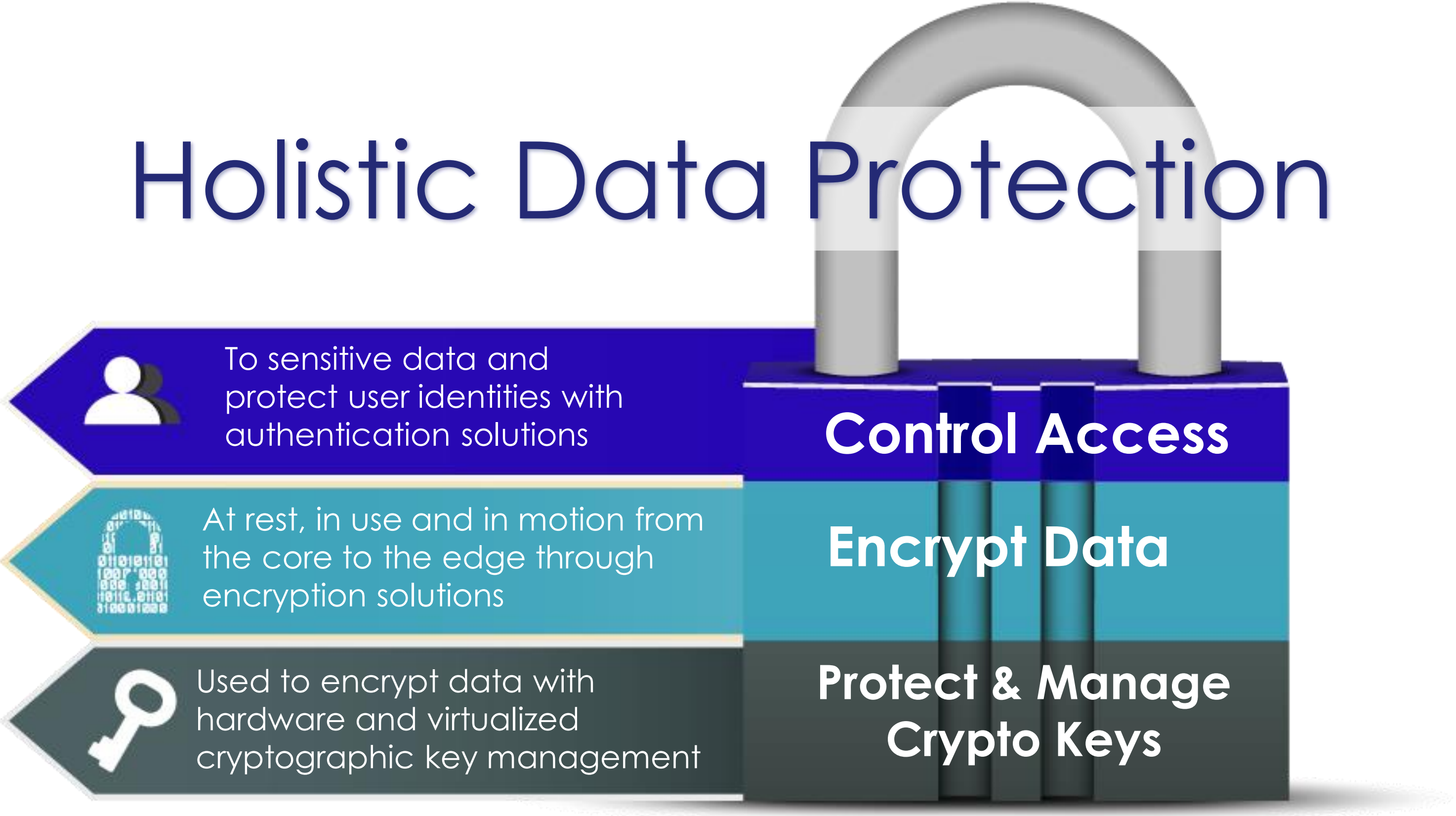


> "Seventy-four percent of U.S. federal government agencies store sensitive data in SaaS applications, 47% store data in IaaS, and 46% store data in PaaS environments."

Securing Containers and Managing Access

Protecting Data From the Core to the Cloud to the Field

Holistic Data Protection



Control Access

To sensitive data and protect user identities with authentication solutions

Encrypt Data

At rest, in use and in motion from the core to the edge through encryption solutions

Protect & Manage Crypto Keys

Used to encrypt data with hardware and virtualized cryptographic key management

Vormetric Data Security Platform

Enabling compliance, breach protection and secure digital transformation

A single scalable platform for data-at-rest security

Centralized policy and key management and easily expanded to new use cases for low TCO

Digital transformation security for data migrating to cloud, big data, and container environments

Transparent encryption

For file systems, volumes, big data and containers across clouds and data centers

Application encryption

Easily incorporate encryption into applications with standards-based APIs and interfaces.

Key management

For database TDE key management and KMIP devices

Tokenization and data masking

Format-preserving tokenization and policy-based dynamic data masking for display security.

Cloud key management

Easily manage encryption keys and policies across cloud environments

Vormetric Data Security Manager

Centralized management and policy for all Vormetric Platform products

- FIPS 140-2 Level 1 virtual appliance
  - available in Azure, AWS, VMware, HyperV, and KVM compatible formats
- FIPS 140-2 Level 2 hardware appliance
- FIPS 140-2 Level 3 hardware appliance, including internal HSM

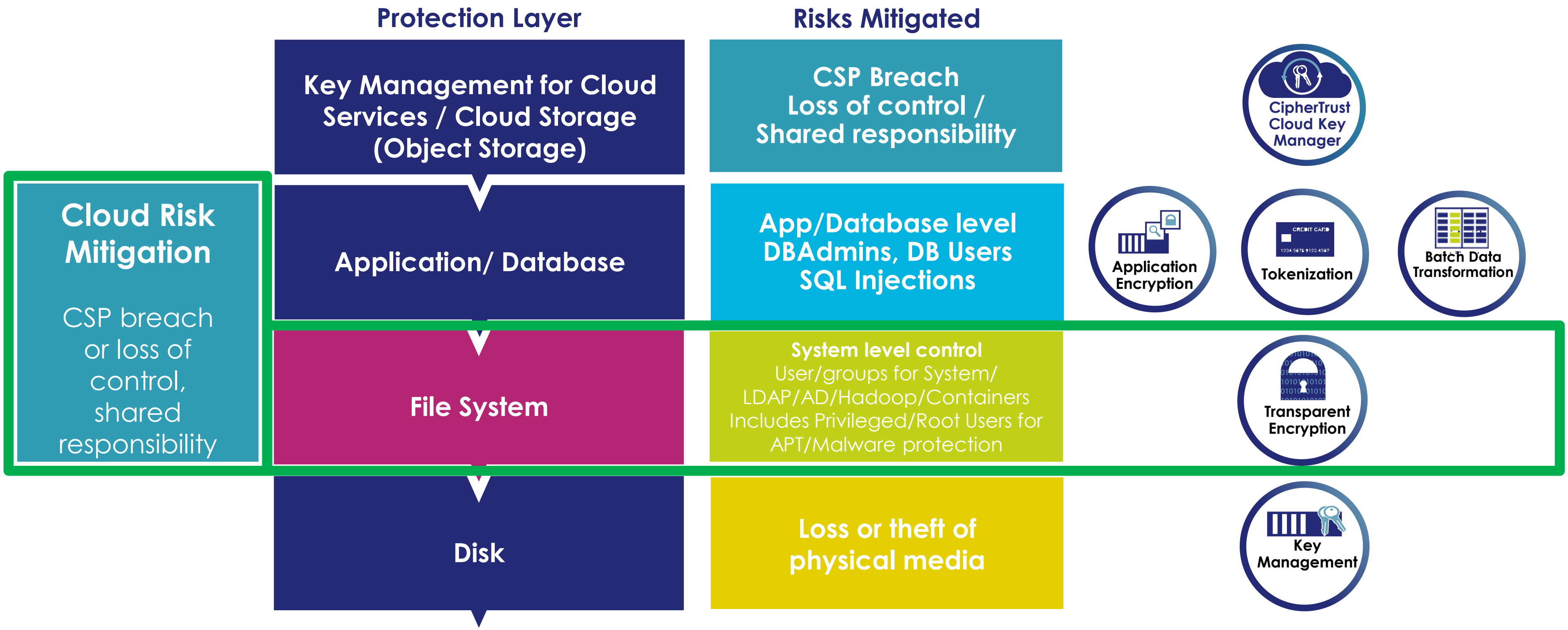
Common Criteria

FIPS VALIDATED 140-2 TM

THALES

Thales Transparent Encryption

Vormetric Transparent Encryption: Protection Layers



Protection Layer	Risks Mitigated
Key Management for Cloud Services / Cloud Storage (Object Storage)	CSP Breach Loss of control / Shared responsibility
Application/ Database	App/Database level DBAdmins, DB Users SQL Injections
File System	**System level control** User/groups for System/ LDAP/AD/Hadoop/Containers Includes Privileged/Root Users for APT/Malware protection
Disk	Loss or theft of physical media

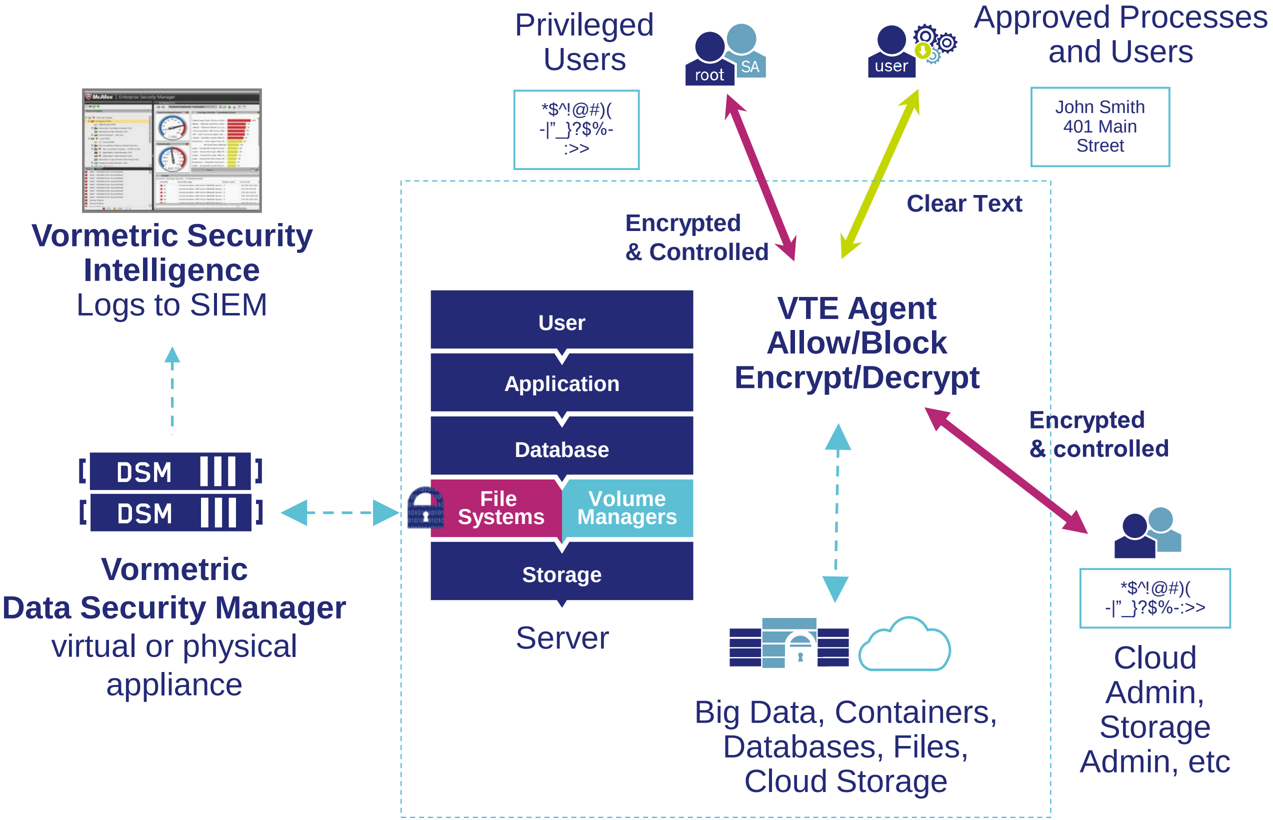
Cloud Risk Mitigation

CSP breach or loss of control, shared responsibility

Vormetric Transparent Encryption

Transparently protects file system, volume data-at-rest

- No changes to applications or workflows required
- Encryption and Key Management – lock down data
- Fine-grained access controls – Only decrypt data for authorized users and processes including system, Active Directory/LDAP, container (OpenShift and Docker) and Hadoop users
- Detailed data access audit logs integrate easily with SIEM systems to detect attacks in process



Vormetric Security Intelligence
Logs to SIEM

Vormetric
Data Security Manager
virtual or physical
appliance

Privileged Users

*$^!@#)(
-|"_}?$%-
:>>

Approved Processes and Users

John Smith
401 Main
Street

Encrypted
& Controlled

Clear Text

VTE Agent
Allow/Block
Encrypt/Decrypt

Encrypted
& controlled

*$^!@#)(
-|"_}?$%-:>>

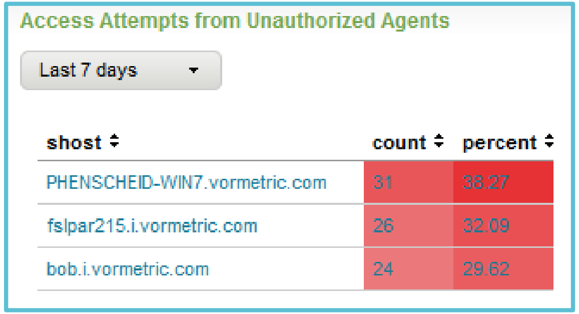
Server

Big Data, Containers, Databases, Files, Cloud Storage

Cloud Admin, Storage Admin, etc

Compliance Reporting and Insider Abuse / APT Detection

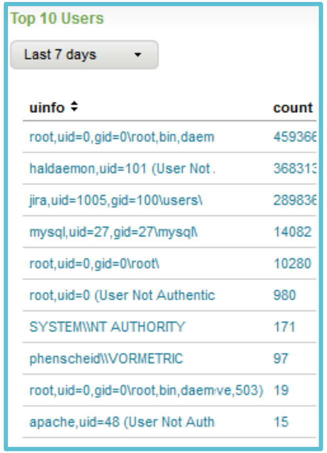
- Supports compliance reporting and audits
- Reveals unauthorized access attempts to protected data
- Identify compromised users, administrators and applications
- Identify attacks on data such as APTs or malicious insiders
- Invaluable for post-breach forensics



Access Attempts from Unauthorized Agents

Last 7 days ▾

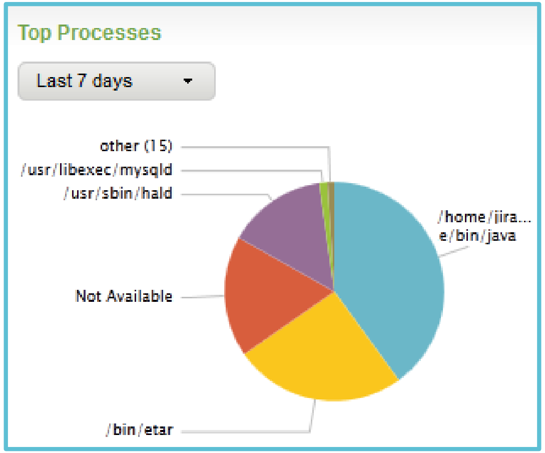
shost ↕	count ↕	percent ↕
PHENSCHEID-WIN7.vormetric.com	31	38.27
fslpar215.i.vormetric.com	26	32.09
bob.i.vormetric.com	24	29.62



Top 10 Users

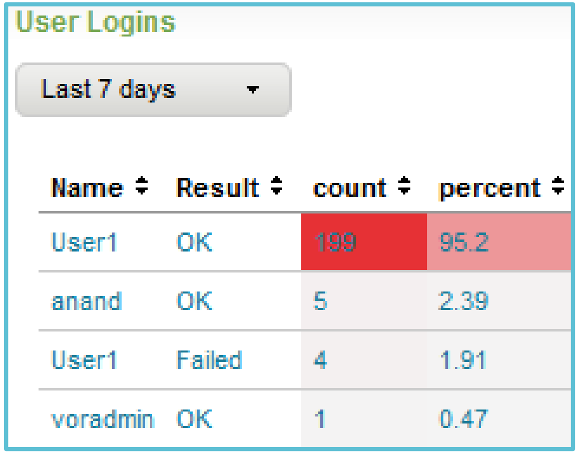
Last 7 days ▾

uinfo ↕	count
root,uid=0,gid=0\root,bin,daem	459366
haldaemon,uid=101 (User Not .	368313
jira,uid=1005,gid=100\users\	289836
mysql,uid=27,gid=27\mysql\	14082
root,uid=0,gid=0\root\	10280
root,uid=0 (User Not Authentic	980
SYSTEM\\NT AUTHORITY	171
phenscheid\\VORMETRIC	97
root,uid=0,gid=0\root,bin,daem-ve,503)	19
apache,uid=48 (User Not Auth	15



Top Processes

Last 7 days ▾



User Logins

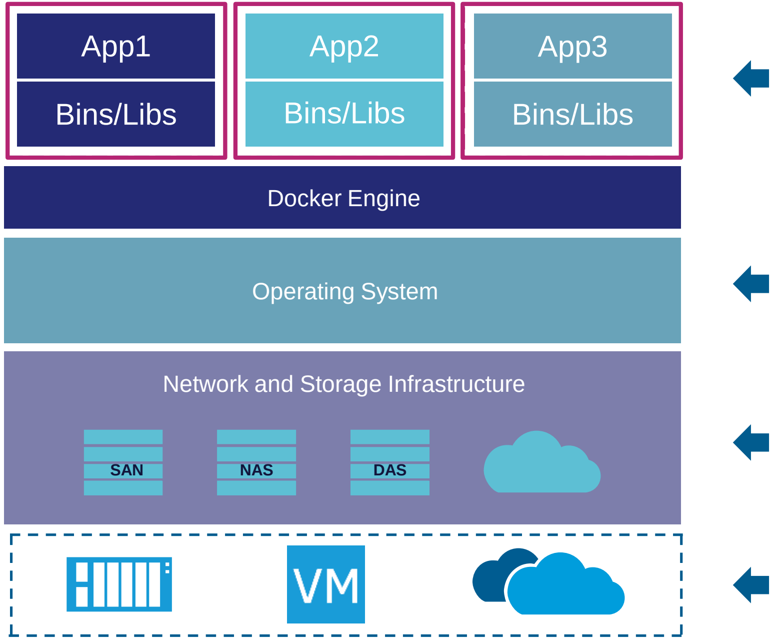
Last 7 days ▾

Name ↕	Result ↕	count ↕	percent ↕
User1	OK	199	95.2
anand	OK	5	2.39
User1	Failed	4	1.91
voradmin	OK	1	0.47

THALES

Container Security

Container Security Challenges



Meeting Compliance and Regulatory Requirements

- Many privacy regulations and compliance regimes require encryption and/or access controls to sensitive data

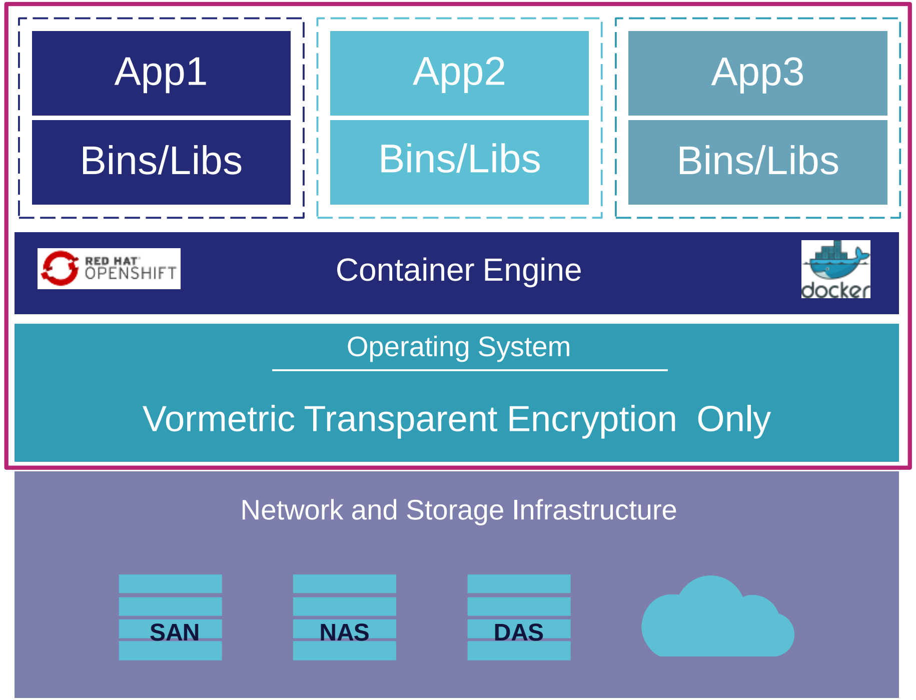
Containers can be run as root

- Root privilege escalation attacks can expose container data
- **Docker** – runs as root by default
- **OpenShift** - If root is enabled (required for many imported Docker images) OpenShift administrators have access to all container images and data

Infrastructure Control

- Often cloud hosted or shared internal Virtual environment
- Multiple possible container sources
- Who owns the infrastructure it runs on?
- What level of trust?

Vormetric Container Security



Protect and control access to container images and instances

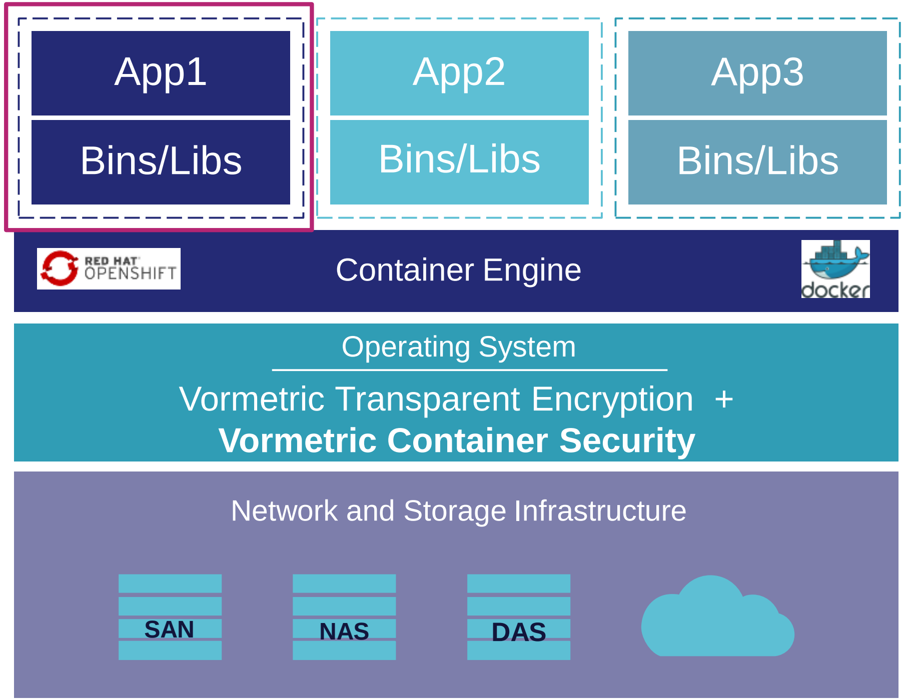
Encryption, Access Controls and Security Intelligence

- Encrypt containers
- Limit container access and use by policy to Docker or OpenShift environment
- Limit use of containers to only authorized (signed) environment instances
- Limit access to data resources used by containers to the container environment

Benefits

- No impact on operation of the Docker or OpenShift environment
- No changes to container images
- Report unauthorized access attempts

Vormetric Container Security



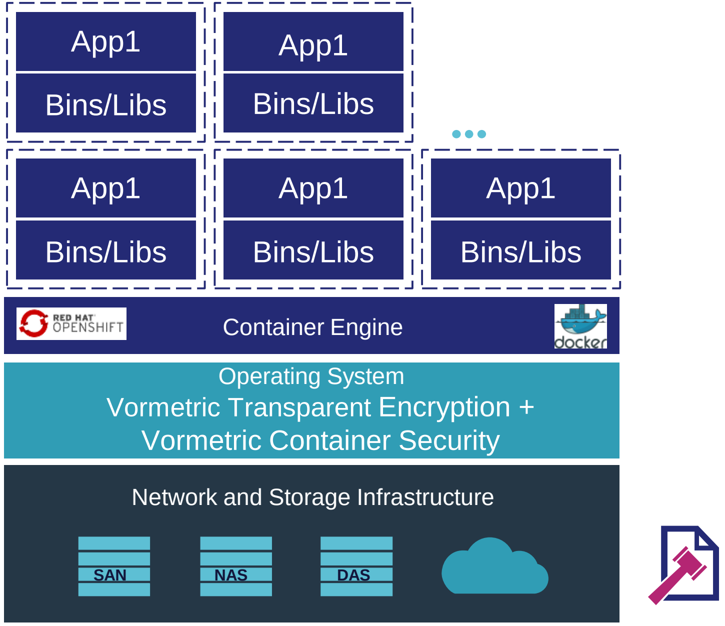
Extends Vormetric Transparent Encryption data-at-rest security controls

- Encrypt data generated and stored locally within a container by an application, or within linked external storage
- Data access controls work with both container and system level users
- Security intelligence with detailed data access audit logs now available for containers and linked data stores

Additional Benefits

- Protect against root/privileged/unauthorized user access within containers
- Protect data against privilege escalation attacks from other containers
- Easily isolate data access between containers

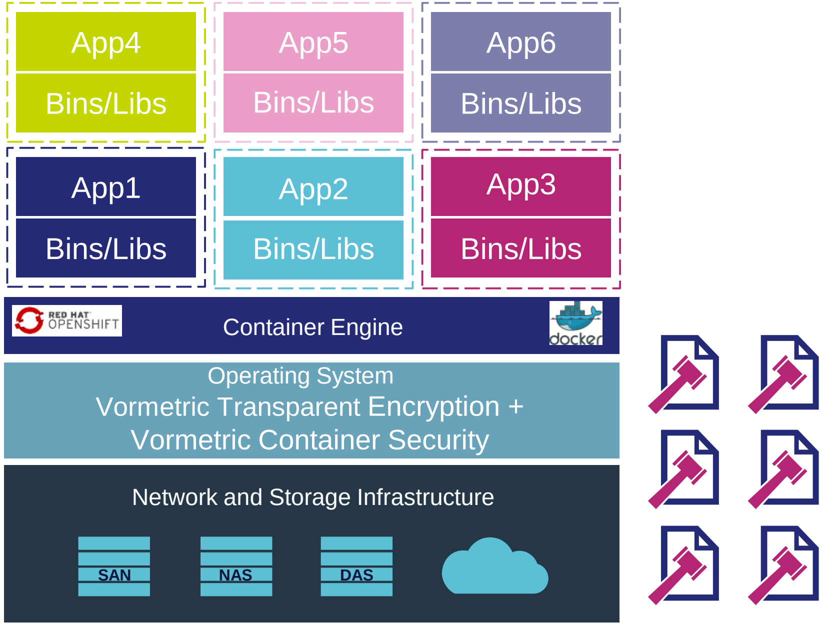
Container Security Supports Data Security



Microservices Scaling

Single Policy

Add more App instances to scale service capacity
Every new container instance has the same policy



Isolate for Multitenancy and Compliance

Separate Policies for Each Container

No container sees another container's data

RedHat + Vormetric Transparent Encryption

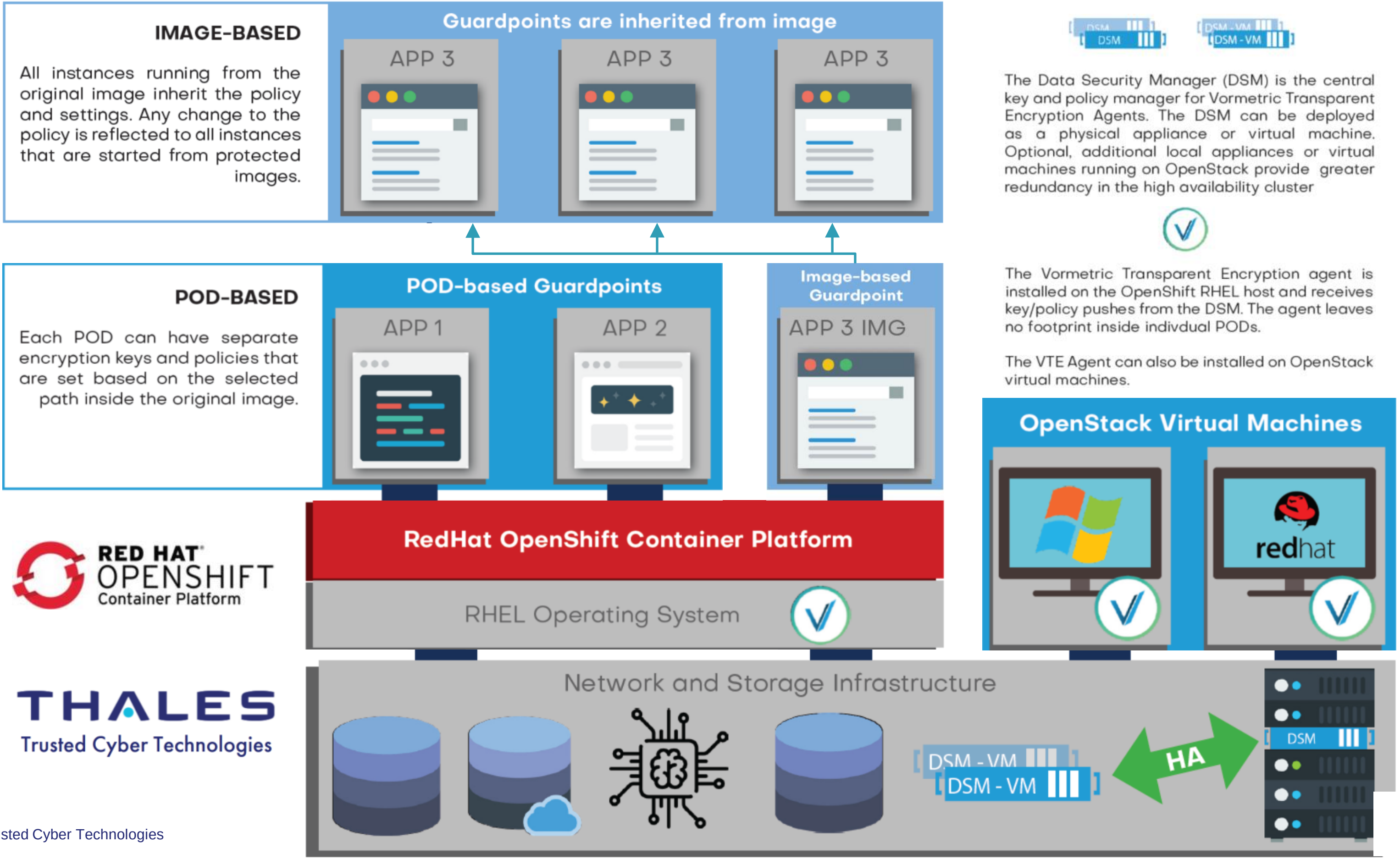


IMAGE-BASED

All instances running from the original image inherit the policy and settings. Any change to the policy is reflected to all instances that are started from protected images.

POD-BASED

Each POD can have separate encryption keys and policies that are set based on the selected path inside the original image.

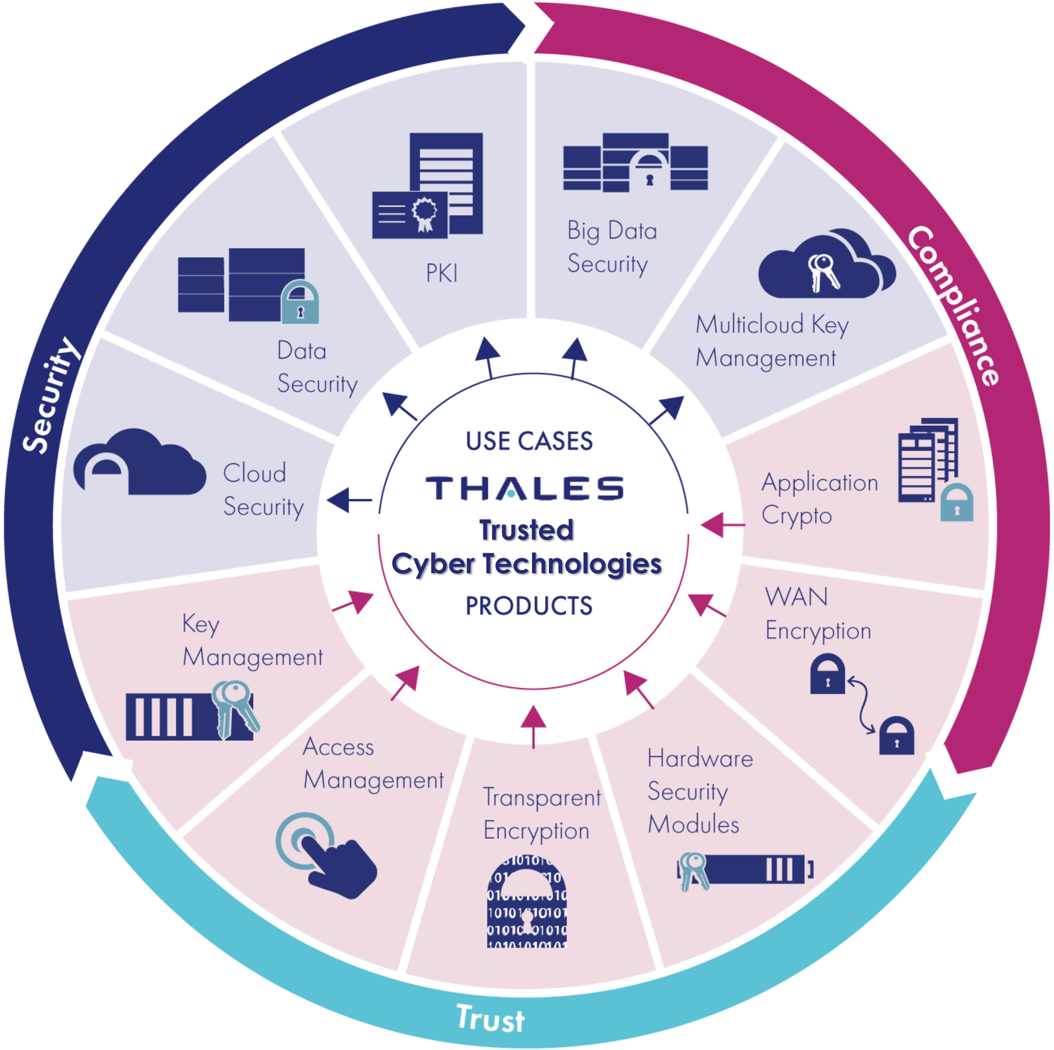
The Data Security Manager (DSM) is the central key and policy manager for Vormetric Transparent Encryption Agents. The DSM can be deployed as a physical appliance or virtual machine. Optional, additional local appliances or virtual machines running on OpenStack provide greater redundancy in the high availability cluster

The Vormetric Transparent Encryption agent is installed on the OpenShift RHEL host and receives key/policy pushes from the DSM. The agent leaves no footprint inside indivdual PODs.

The VTE Agent can also be installed on OpenStack virtual machines.

RED HAT OPENSHIFT Container Platform

THALES
Trusted Cyber Technologies



Thales TCT Data Security Portfolio Solutions

- **Enterprise Key Management** centrally manages policies and encryption keys for all Thales data security products
- **Data-at-Rest Encryption with Access Control** secures any database, container, file or volume across large agencies and implementations
- **Application Encryption** provides a simple framework to deliver field level encryption
- **Cloud Key Management** establishes strong controls over encryption keys and policies for data encryption by cloud services.
- **Security Intelligence** accelerates the detection of APTs, Insider Threats and compliance report generation.
- **Network Encryption** provides end-to-end, authenticated encryption for data in transit using standards-based algorithms.
- **Hardware Security Modules** serve as “trust anchors” that protect an organization’s cryptographic infrastructure.
- **Certificate-based, multi-factor authentication** controls access sensitive data and protect user identities.

Thank you

Follow us on:

ibm.com/security

securityintelligence.com

ibm.com/security/community

xforce.ibmcloud.com

@ibmsecurity

youtube.com/ibmsecurity

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.

IBM