Trustwave®

DATA SHEET

Trustwave Data Protection Practice

PROTECT YOUR DATA, WHEREVER IT IS CREATED, STORED OR PROCESSED

Benefits

- Make the best use of limited resources while securing high value assets
- Effectively balance innovation and risk with a data centric approach
- Gain access to specialized data security skills as needed
- Ensure data protection, regardless of where it is created, stored or processed
- Leverage the benefits of the Cloud within tolerable risk levels.

As the value of data rises there has also been a corresponding increase in the sophistication of cyber threats targeting organizations. Data is no longer created, stored and processed exclusively within the traditional network perimeter. As more organizations move to the cloud, they must manage increasing levels of complexity and data dispersion. Combined with large data breaches and increased scrutiny from regulators, organizations must balance innovation with better data protection. And do it all with limited resources.

Trustwave Data Protection Practice Overview

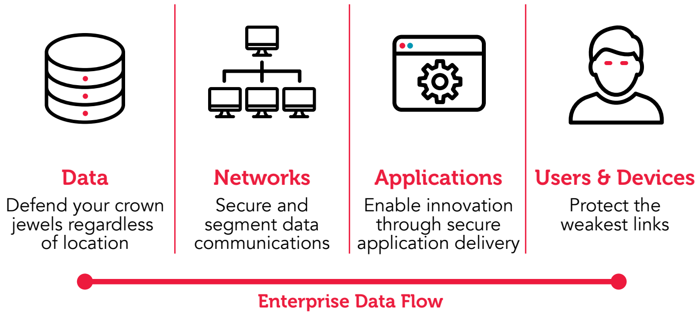
The Trustwave Data Protection Practice combines consulting, systems integration and managed security services to deliver data-driven risk management programs that optimize resources to protect data. Our Data Protection Practice helps clients better defend their operations against threats, such as insider threats, data exfiltration, and ransomware, to meet compliance mandates, mitigate risk and safely rollout innovative cloud initiatives.

We accomplish this by combining basic security principles, such as assigning access rights based on least privilege and accounting for adequate separation of duties, with advanced defense in depth techniques that cover technical, operational and administrative controls, along with appropriate technical architectures that can enforce data protection measures regardless of where the data is stored, used or processed.

Data-Centric Architecture

Trustwave's data-centric architecture helps reduce risk by integrating people, process and technology across Trustwave technologies and third-party security solutions. Our architecture starts with defining and applying appropriate data controls, such as discovering and classifying data, deploying data loss prevention (DLP) tools on the network and endpoints, in email and the cloud, or monitoring and preventing malicious database activity.

In addition to the processes and tools that directly protect data, such as applying rights on a least privilege basis, database activity monitoring (DAM) and encryption solutions, our architecture also includes secondary data controls, such as managing access control across networks, applications and users and the devices they use to interact with and process data.



Data
Defend your crown jewels regardless of location

Networks
Secure and segment data communications

Applications
Enable innovation through secure application delivery

Users & Devices
Protect the weakest links

Enterprise Data Flow

Essential Components of a Data-Centric Architecture

Elements within each security component may include:

Data

- Data protection program transformation and build-out
- Data protection strategy and planning
- Data discovery and classification
- Data flow mapping
- Data loss prevention (DLP)
- Database activity monitoring (DAM)
- Encryption/Enterprise Rights Management (ERM)

Networks

- Network segmentation
- Network security scanning and penetration testing
- Managed Secure Web Gateway (SWG)
- Managed Cloud Access Security Broker (CASB)
- Managed Firewall/Unified Threat Management (UTM)/Intrusion Detection and Prevention System (IDPS)

Applications

- Secure Development Training (SDT)
- Application Security Scanning and Penetration Testing
- Managed Web Application Firewall (WAF)

Users & Devices

- User Awareness and Education/Security Awareness Education (SAE)
- Managed Detection and Response for Endpoints (MDRe)
- Endpoint Protection such as Antivirus (AV) and Host Intrusion Prevention System (HIPS)

A Transformation Methodology for Success

We collaborate with our clients to provide security expertise from experts in our data protection practice using the Plan, Build Run transformation model. Each project may incorporate one or more elements of the methodology listed below.

Plan

Our Planning services help clients transform their data protection program into a sustainable operating model that delivers repeatable results and facilitates continuous improvement and program maturation.

- Define what is critical data and why is it important to your organization
- Identify process and data dependencies and understand the data flows
- Discover and classify where sensitive data is located
- Identify program gaps and prioritize the remediation options

Build

The Build phase helps clients improve and develop their programs over time. In addition to operational process optimization, our Build services design, implement and transition new data-centric technical solutions.

- Implement and baseline data protection controls
- Build out and help mature the data protection program
- Normalize tools and operational procedures

Run

Our Run services fully operationalize the data protection program improvements defined and implemented during the Plan and Build phases. All services are supported by Trustwave's global footprint and extensive experience delivering high value managed security services.

- Data policy and threat alert monitoring
- Threat, policy and change management
- Tools and device management
- Incident response

Trustwave Data Risk Strategy & Planning

The Trustwave Data Risk Strategy & Planning engagement operationalizes the risk assessment process for data regardless of where is it created, stored, or processed. This modular consulting engagement leverages standard tools and procedures to:

1. Facilitate data-centric security maturity workshop(s) and targeted interviews
2. Analyze data protection program documentation
3. Analyze data-flow mapping documentation (optional)
4. Define a data-centric security program target state (optional)
5. Execute automated and manual security scans (optional)
6. Identify gaps, design strategy & render a prioritized 2-year roadmap
7. Deliver executive level presentation

For more information: www.trustwave.com