Trustwave®

DATA SHEET

# Trustwave DbProtect

## ENTERPRISE DATA SECURITY PLATFORM

- Leverage a highly scalable solution that provides protection for your databases anywhere – on premises or in public, private or hybrid clouds.
- Get a unified view of database assets, vulnerabilities, risk levels, user privileges, anomalies and incidents in real-time with a single dashboard.
- Detect, alert and take corrective action against suspicious activities, intrusions and policy violations in real time.
- Demonstrate compliance with more than one set of business, security, or regulatory policies with powerful, customizable reporting features.

A database is often called the backbone of an organization. Databases contain sensitive and proprietary information - such as employee information, medical records, customer information, financial data and more – making them a prized target for cyber criminals determined to find new ways to access valuable data for large financial payoffs. As databases become more challenging to secure, organizations are also struggling to find and retain resources to implement effective database security controls.

Trustwave DbProtect™ is a highly scalable data security platform that enables organizations to secure their relational databases and big data stores both on premises and in the cloud. Trustwave DBSS automates the security of critical data where it's stored, by uncovering vulnerabilities that would-be attackers could exploit, limiting user access to the most sensitive data and alerting on suspicious activities, intrusions and policy violations. Trustwave DbProtect will also take corrective action, as your team investigates the incident. DbProtect makes it easy to provide business leadership with high-level risk trending, while also providing administrators and analysts the ability drill down into individual or groups of databases to address specific concerns.

DbProtect empowers organizations to uncover database configuration errors, identify access control issues, missing patches, and toxic combination of settings that could lead to privilege escalation attacks, data leakage, denial-of-service (DoS), or unauthorized modification of data held within data stores across their environments.

### Discover and Inventory Database Assets

- Easily identify databases across your entire enterprise along with their respective objects, users and enabled security features within your organization.
- Easily discover and review all the accessible assets, user access levels, and security feature usage throughout your environment.
- Identify and highlight recently added, rogue or missing data store installations and objects.

### Conduct Vulnerability and Configuration Assessments

- Demonstrate effective controls for sensitive data and compliance with more than one set of business, security, or regulatory policies as well as IT audits.
- Examine data stores for vulnerability, configuration, and user rights issues with built-in and customized policies.

### Identify Excessively Privileged User Accounts

- Proactively establish an environment of least privilege by gaining visibility into who has access to your sensitive data by identifying users, roles and privileges.
- Establish meaningful controls that track how users interact with the data and capture an audit trails by identifying who has access to what data and why/how they've been granted that access.

## Implement Risk Mitigation and Compensating Controls

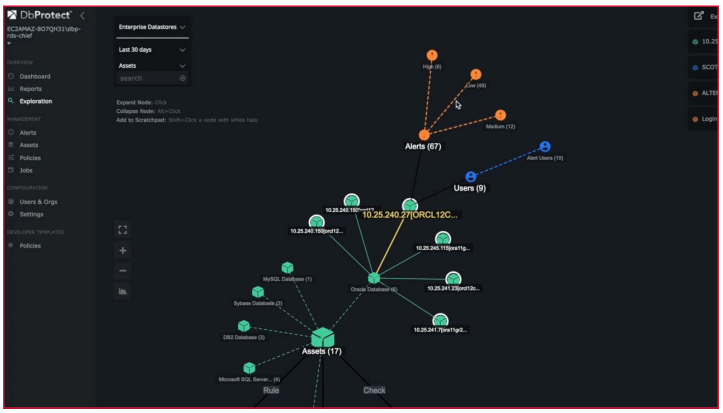
- Reduce your risk of compromise and narrow the scope of required compensating controls by remediating high-risk vulnerabilities and misconfigurations within your database.
- Assign exceptions for vulnerabilities that cannot get remediated or patched in a timely manner
- Using data analytics to associate risk scores with the results/findings of your vulnerability assessment to identify your most exposed systems or groups. You can then focus your efforts where you stand to make the most impact.

## Audit Privileged User Behavior in Real Time

- Collect a forensic audit trail of all privileged activities in a database to meet compliance regulations (including Sarbanes-Oxley) that require tracking of structural changes in your information, which means auditing privileged (administrative) activity, not just the actions of known privileged users.

## Detect, Alert and Respond to Policy Violations in Real Time

- Send alert messages in syslog, snmp, or flat file for operations center personnel to take appropriate action when a security violation is identified.
- Depending on the policy violation and the sensitivity of the affected system or data, automated and scripted responses can contain the threat and give the security team time to investigate and take corrective action.




## Reporting, Integration and Analytics

- The dynamic interface in DbProtect allows you to visualize your threat surface area with consolidated views of vulnerabilities, threats, risks, and compliance efforts across heterogeneous data store environments. Run analytics and report against your current status, demonstrate progress, effectiveness, and operational efficiency
- Evaluate trends and drill down for detailed views of each individual database, group of databases, or databases of specific business units or groups within the enterprise.

Cyber Catalyst

Trustwave DbProtect has received the Cyber Catalyst by Marsh℠ designation. The Cyber Catalyst designation is awarded by participating insurers to products or solutions that the insurers consider effective in reducing cyber risk. Organizations deploying Trustwave DbProtect may qualify for enhanced terms and conditions on cyber insurance policies from a wide variety of participating global insurers.

Trustwave®

For more information: www.trustwave.com



DBP_0919