SOLUTION BRIEF

DB CyberTech Predictive Data Loss Prevention for Structured Data

McAfee® Data Loss Prevention (McAfee® DLP) safeguards intellectual property and ensures compliance by protecting sensitive data wherever it lives—on premises, in the cloud, or at endpoints. Using real-time policy correlated with anomalous structured data in motion, the DB CyberTech Visibility, Privacy and Security solution offers intelligent monitoring, data classification, and end-to-end threat detection. By integrating with McAfee DLP and McAfee® ePolicy Orchestrator® (McAfee® ePO™) software, the combined solution delivers the only complete, end-to-end data protection solution in the market with predictive data protection, including unstructured and structured data. Furthermore, the solution leverages predictive behavioral analysis from DB CyberTech and deep data policy from McAfee DLP to deliver the unprecedented ability to predict threats against structured data before any data is lost.

McAfee Compatible Solution

- DB CyberTech Visibility, Privacy, and Security 6.1
- McAfee DLP 11.2
- McAfee ePolicy Orchestrator 5.10
- Offers intelligent monitoring, data classification, and end-to-end threat detection
- Delivers predictive data protection, including unstructured and structured data

McAfee COMPATIBLE

DB CyberTech

Connect With Us

The Business Problem

Companies today face significant business risk and exposure due to lack of visibility, privacy, and security for structured data in motion. Without visibility into data in motion, undocumented and "Shadow IT" databases remain hidden, and security professionals are blind to the unknown risk of data leakage, such as new access behavior and new databases set up as staging platforms before a breach. Without a strong privacy solution, companies face the daunting challenge of identifying where sensitive data resides and who has access and, as a result, are unable to protect unknown data exfiltration. Cyberattacks targeting high-value structured records continue to increase. These attacks and the resulting data losses have impacted small and large enterprises in the past few years, causing massive financial and reputational damage to businesses. Existing solutions need new capability to counter evolving and increasing volume of attacks.

Historically, companies focus on protecting unstructured data such as email, web traffic, and file shares. Valuable security resources are frequently devoted to keeping sensitive unstructured data from inadvertently leaving an organization. Meanwhile, much larger concentrations of high-value structured data protection rely on data-at-rest scanning of known databases, which leaves undocumented and "Shadow IT" databases exposed, with little or no visibility, classification, or monitoring.

Existing structured data security technology, such as data activity monitors (DAMs), grew out of a need for compliance. As such, they have always been narrowly deployed, offering little or no continuous monitoring and discovery capability—a crucial feature for basic structured data security. Enterprise databases themselves have ceded the role of security to labor-intensive manual processes like role-based access control.

The integration of McAfee DLP and McAfee ePO software with DB CyberTech removes this business risk, jointly protecting high-value structured data by addressing these factors proactively. DB CyberTech's continuous monitoring and intelligent data classification of structured data in motion enable the automatic identification of high-value records. Information is centrally aggregated in McAfee ePO software and DLP modules for immediate visibility to changes across your structured data environment. The synergistic threat detection of the integrated solution complements McAfee data protection solutions and DLP policies for unstructured data and enables predictive visibility into any malicious intent before the high-value structured data is stolen. The very patterns and policy applied to email, web traffic, and file shares can now be used for structured data as well. Relying on predictive behavioral analysis from DB CyberTech, companies can now stop structured data loss before it happens.

Challenges

- No comprehensive solution to address structured data in motion:
  - Scan-based solutions interrogate pre-qualified sets of databases and require heavy instrumentation with high overhead.
  - No easy way to identify undocumented/"Shadow IT" databases.
  - Lack of real-time visibility to understand structured data in motion in real time.
- Lack of the ability to address proactive data privacy and security:
  - Data activity monitors are mainly rear-view-mirror solutions and are compliance and log-oriented.
  - Identity and access control typically stop at the structured data layer at the database.
- Lack of network context or insight to database access, such as SQL queries or schema: Manual policy control such as role-based access control (RBAC) and log analysis don't scale.

McAfee and DB CyberTech Integrated Solution

DB CyberTech's continuous monitoring of network traffic automatically identifies all structured data assets, including documented and undocumented databases. This information is now available in the single-pane-of-glass management platform, McAfee ePO software. This capability enables customers to view new structured data assets as they come online and differs from scanning-based solutions, which are limited to the documented target and frequency of each scan.

DB CyberTech uses intelligent data classification to automatically identify high-value data within the structured data conversation. This information is now also available in McAfee ePO software. This capability enables the user to efficiently find their database assets and take the necessary action to protect, report on, and monitor them, eliminating the need to look through millions of statements manually. The integrated capability enables users to correlate the location of their most sensitive structured data with other threats visible in McAfee ePO software.

Finally, DB CyberTech uses real-time predictive behavioral modeling combined with data classification results to detect suspicious database activity indicative of future sensitive data loss. The integrated solution cross-correlates this activity with McAfee DLP policy applied to the data involved to generate extremely high-quality incidents in McAfee ePO software.

The combined solution has all the bases covered. Companies are now able to proactively detect malicious intent of data loss before the data is stolen or staged from their highest concentration of sensitive structured data—the database. This complete, next-generation privacy and security solution can easily be deployed as an extension to existing solutions.

Innovative and Powerful

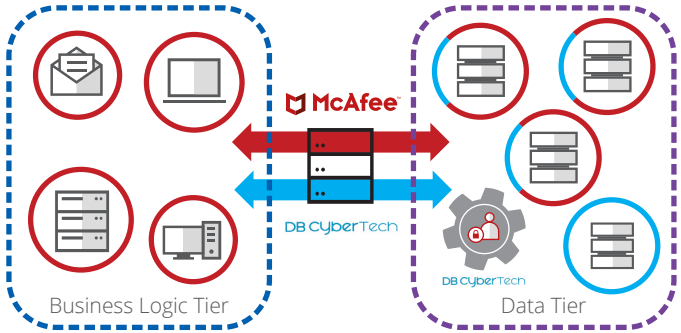
The integration of DB CyberTech visibility and privacy with McAfee DLP and McAfee ePO software is the only complete solution in the market covering both structured data and unstructured data. It goes beyond database activity monitoring, which is inherently limited to where database activity monitoring agents are installed and fills the gaps left by backward-looking scanning approaches with continuous monitoring of structured data access.

This innovative and differentiated solution enables users to track threats from deep in the database to the endpoint. By combining the independent behavioral analysis of conversations between the client and the database from DB CyberTech and the data policy from McAfee DLP, users receive high-quality, integrated threat detection that can truly address advanced persistent threats throughout the organization and over time.

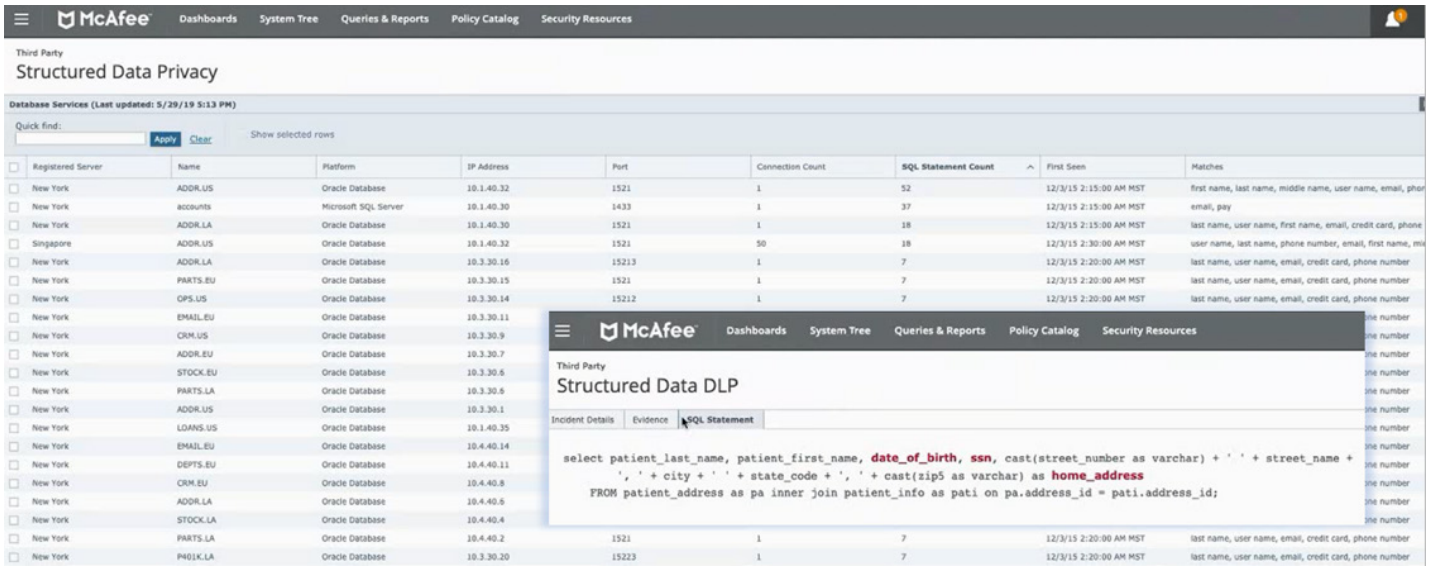
Our Integration

- Working in concert with McAfee Data Loss Prevention, the DB CyberTech solution automatically discovers all documented and undocumented databases, including "Shadow IT" with high-value elements. It performs deep Layer 7 database protocol decoding and then applies a structured data classifier to classify high-value elements and enable monitoring of sensitive structured data in real time.
- High-quality detection enables McAfee DLP to apply uniform policy to structured data protection.
- The DB CyberTech solution is complementary to new and existing McAfee DLP solutions as an add-on to enable predictive data loss prevention. The McAfee ePO software extension can be added as a third-party module, which enables a single pane of glass for managing the entire integrated solution.

The DB CyberTech deployment is nonintrusive, with no instrumentation, agents, or preselected list of assets required. Its continuous monitoring and intelligent structured data classification automatically identify documented and undocumented databases, and high-value records not visible to solutions that are targeted at data at rest. Moreover, DB CyberTech's built-in machine learning technology detects malicious access to high-value data without rules or any explicit knowledge of the underlying database infrastructure.



- DB CyberTech:
  - Insights into sensitive data access and undocumented databases
  - Threat detection for structured data with predictive behavioral analysis
- McAfee DLP:
  - Protection of data at rest
  - Incorporate threat info from DB CyberTech and apply uniform DLP policies



Results

- The comprehensive visibility into documented and undocumented databases, including "Shadow IT" structured data, enables strong security, privacy, and compliance for high-value database assets.
- Easy deployment without agents and processing is done out of band, with no impact to network performance.
- Automatic and real-time visibility and detection of likely data leakages enable proactive security protection while allowing limited security teams to do more.
- Behavior-focused machine learning combined with classified context provides predictive analysis and high level of threat detection to help companies to stay ahead of malicious activities and initiate proactive actions.

About McAfee Data Loss Prevention

McAfee Data Loss Prevention software delivers the highest levels of protection for sensitive data, while greatly reducing the cost and complexity of safeguarding business-critical information. McAfee data protection is delivered through the McAfee ePO platform for streamlined deployment, management, updates, and reports.

About DB CyberTech

DB CyberTech pioneered predictive data loss prevention for databases. Our patented technologies are based on deep protocol extraction, machine learning, and behavioral analysis. We provide real-time visibility and continuous situational awareness of all conversations between databases and their connected clients because you can't protect what you can't see. Through non-intrusive analysis of data in motion, we discover database assets, classify high-value structured data, and identify imminent threats of data loss during the earliest phases of an attack—before any data loss has occurred.

www.dbcybertech.com

Learn More

For more information, visit **www.mcafee.com**.

2821 Mission College Blvd.
Santa Clara, CA 95054
888.847.8766
www.mcafee.com