



powerbroker[®] desktops

DLP Edition

PowerBroker[®] Desktops DLP

PowerBroker Desktops DLP Edition is a powerful data control and monitoring solution to the problem of data privacy and confidentiality in IT infrastructure.

PowerBroker Desktops DLP Edition effectively replaces individual security tools, such as content-aware DLP, device control, e-mail control, web control, access control to files and more, combining them into unified data control policy, delivered through Microsoft's Group Policy infrastructure.

Regulatory Compliance

PowerBroker[®] Desktops DLP helps organizations protect confidential data and control data flow to comply with PCI, Sarbanes-Oxley, GLB, HIPAA and personal information encryption policies.

About BeyondTrust

BeyondTrust is a proven leader with more than 25 years of experience. More than half of the companies listed on the Dow Jones, eight of the 10 largest banks, seven of the 10 largest aerospace and defense firms, and six of the 10 largest U.S. pharmaceutical companies rely on BeyondTrust to secure their enterprise.

PowerBroker[®] Desktops DLP

BeyondTrust is the global leader in privilege authorization management, access control and security solutions for virtualization and cloud computing environments.

BeyondTrust empowers IT governance to strengthen security, improve productivity, drive compliance and reduce expense. The company's products eliminate the risk of intentional, accidental and indirect misuse of privileges on desktops and servers in heterogeneous IT systems.

Data Loss Prevention with PowerBroker[®] Desktops DLP

PowerBroker[®] Desktops DLP Edition is a powerful data control and monitoring solution to the problem of data privacy and confidentiality in IT infrastructure. PowerBroker Desktops DLP Edition replaces individual security tools, such as content-aware DLP, device control, e-mail control, web control, access control to files and more, combining them into unified data control policy, delivered through Microsoft's Group Policy infrastructure.

Loss of customer account details, exposure of confidential information and theft of sensitive data cost companies up to 5% of revenue every year. Additionally, insiders, employees and contractors who have authorized access to confidential data, are responsible for 70% of total data leaks.

PowerBroker Desktops DLP bridges strong security with user-friendly, simple operations, with enhanced "Active Profiler" technology that marries "set and forget" principles with effective data loss prevention. PowerBroker DLP provides comprehensive coverage of various data leak channels, including covert channels associated with data-in-processing.

Key Benefits

- Immediate mitigation of major data leak threats (insiders, hackers, malware, device loss)
- 100% coverage of data loss channels and data types
- Audit and Monitor data with metrics to assess data leak risks and the effectiveness of security policy
- Active Profiler automatically detects suspicious activity leading to sensitive data leaks
- Encryption of sensitive data on desktops and laptops
- Recognition of sensitive content in over 500 file formats
- Low resources requirements for implementation
- Leverages existing investment in Active Directory and Group Policy

Active Profiler

In comparison with other DLP solutions, PowerBroker Desktops DLP bridges strong security and simplicity of operations enhanced by unique “Active Profiler” technology that marries “set and forget” principle with effective data leak prevention.

“Active Profiler” is a unique innovative technology that routinely creates user’s behavior profiles relating to sensitive content operations. PBDLP automatically detects potential data leaks and sends warnings to a system administrator. The Profiler is fully transparent control that prevents data leaks and does not require change of user behavior. This innovative approach turns DLP into a new commodity class, such as anti-virus solutions, breaking application barriers for many organizations. PBDLP provides provides strong security via comprehensive coverage of various data leak channels, which include covert channels associated with various applications (e.g., data-in-processing). Addressing covert channels allows companies to effectively defeat malicious data leaks by insiders as well as by malware and intruders.



PowerBroker Desktops DLP Reporting Dashboard

Implementation at Your Pace

PowerBroker Desktops DLP revolutionizes the DLP implementation by setting new implementation stages that allow you to effectively protect data at any level of complexity and available resources depending on the objectives. The implementation starts from automatic threat detection and then gradually moves to sensitive data classification, encryption, isolation and data access control. The initial step requires no additional resources and each subsequent step increases security/compliance level. With sensitive file encryption, device and web access control with PowerBroker Desktops DLP, organizations receive added value beyond a conventional DLP solution.

PowerBroker[®] Desktops DLP Allows Organizations to Regain Control Over Data

Security

- Comprehensive control of various data leak channels
- Addressing all data leak threats including insiders external intruders and device loss
- Automatic alarms upon detection of threatening activity
- Dramatically lower exposure to operational, financial and confidentiality risks

Compliance

- Meet compliance with regulations, such as PCI DSS, HIPAA, SOX, GLBA
- Advanced reporting and auditing
- Identify most dangerous corporate data movements
- Identify faulty business processes
- Forensic analysis for root cause determination
- Access individual audit records for in-depth analysis

Productivity

- Set of fully transparent controls that do not require change of user behavior
- Low TCO due to minimal IT and distributed resource requirements
- Virtually no limitation on number of users, due to de-centralized endpoint solution
- No impacts on user endpoints

System Requirements

PowerBroker Desktops DLP Client

- Windows XP, Windows Vista, Windows 7 or Windows Server 2003/2008
- Disk Space: 100 MB
- RAM: 256 MB Minimum

Reporting Server

- CPU: 1GHz or better
- RAM: 1 GB
- Disk Space: 4 GB