

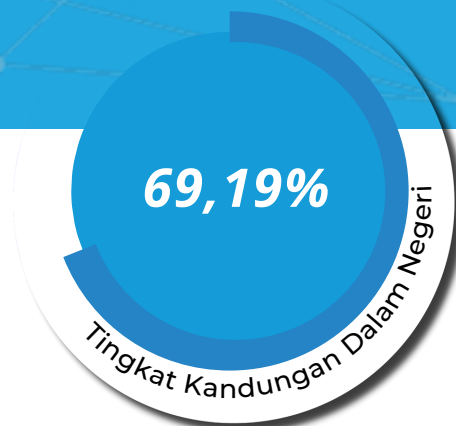
Data Sheet TKMT Risk Management DLP

www.tkm-teknologi.id



Melindungi perusahaan dari kebocoran informasi rahasia, mengontrol data saat istirahat dan data dalam perjalanan.

Memantau semua saluran transfer data populer, menganalisis informasi, mendeteksi dan mencegah pelanggaran, memberikan laporan kepada penanggung jawab.



TKMT RISK MANAGEMENT MEMBANTU BISNIS DALAM BANYAK CARA

- Melindungi informasi rahasia dari kebocoran selama penyimpanan, penggunaan, dan transfer
- Memfasilitasi inventarisasi perangkat lunak dan perangkat keras
- Mengenkripsi data untuk mencegahnya digunakan di luar perusahaan
- Melaporkan peristiwa tidak teratur dalam jaringan, seperti menyalin data ke perangkat penyimpanan yang dapat dilepas atau menghapus sejumlah besar file

DATA PENTING SELALU TERLIHAT

TKMT Risk Management DLP solusi DCAP (audit dan perlindungan data-sentris) untuk audit otomatis penyimpanan informasi, mencari pelanggaran akses dan melacak perubahan yang dilakukan pada data penting.

TKMT Risk Management DLP menyelesaikan tugas-tugas berikut:

Klasifikasi data rentan

Menemukan file dalam aliran dokumen yang berisi informasi penting, dan menetapkan tipe tertentu untuk setiap file: data pribadi, rahasia dagang, nomor kartu kredit, dll.

Pengarsipan dokumen penting

Membuat salinan bayangan dari file penting yang ditemukan di PC, server atau folder jaringan, menyimpan riwayat revisi mereka. Arsip data rahasia membantu dalam penyelidikan insiden dan memastikan pemulihan informasi yang hilang.

Audit hak akses

Memfasilitasi kontrol akses informasi rahasia – secara otomatis memantau sumber daya terbuka, file yang tersedia untuk pengguna atau grup tertentu, akun istimewa.

Pemantauan aktivitas pengguna

Mengaudit operasi pengguna dalam sistem file. Spesialis yang bertanggung jawab untuk mitigasi risiko selalu memiliki informasi tentang perubahan yang dibuat pada file yang diperbarui (membuat, mengedit, memindahkan, menghapus, dll.).

Contacts:

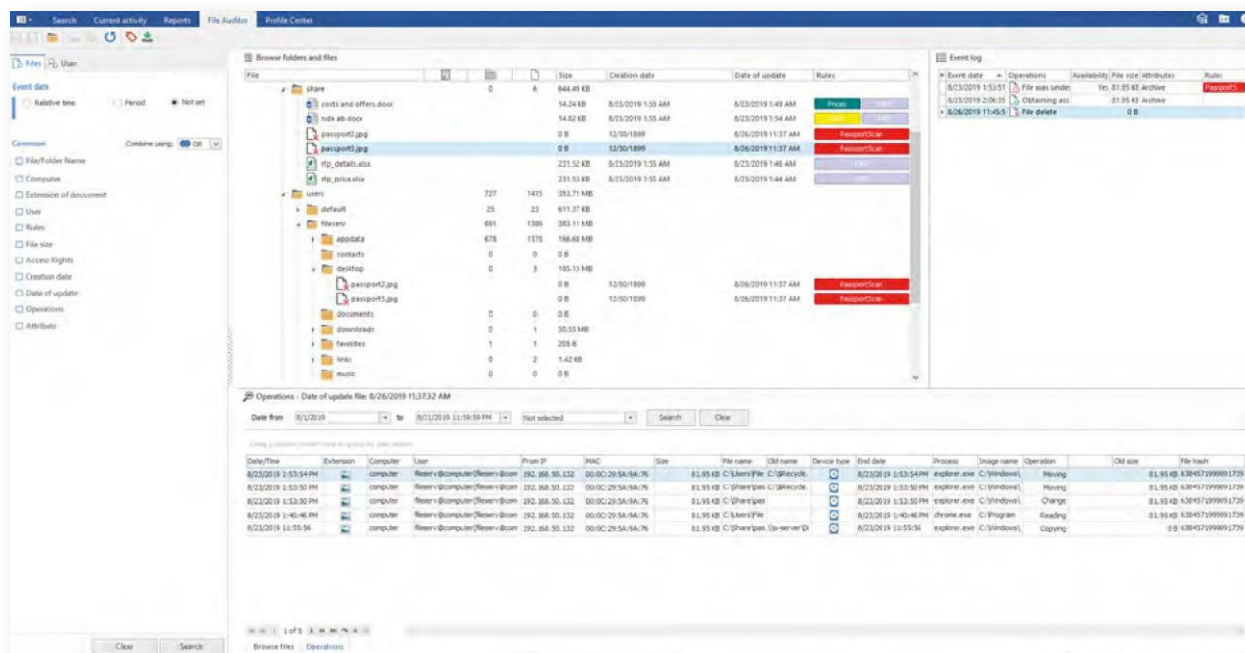
www.tkm-teknologi.id

Email : support@tkm-teknologi.com

+62 811-1552-270

TKMT Risk Management DLP

Jumlah data yang disimpan perusahaan rata-rata sangat besar. Dan beberapa data ini berisi informasi rahasia: data pribadi dan keuangan, spesifikasi, gambar, dll. Setiap kelompok data sensitif harus disimpan, diproses, dan didistribusikan sesuai dengan aturan yang sesuai.



Audit dari berkas yang berisi informasi rahasia.

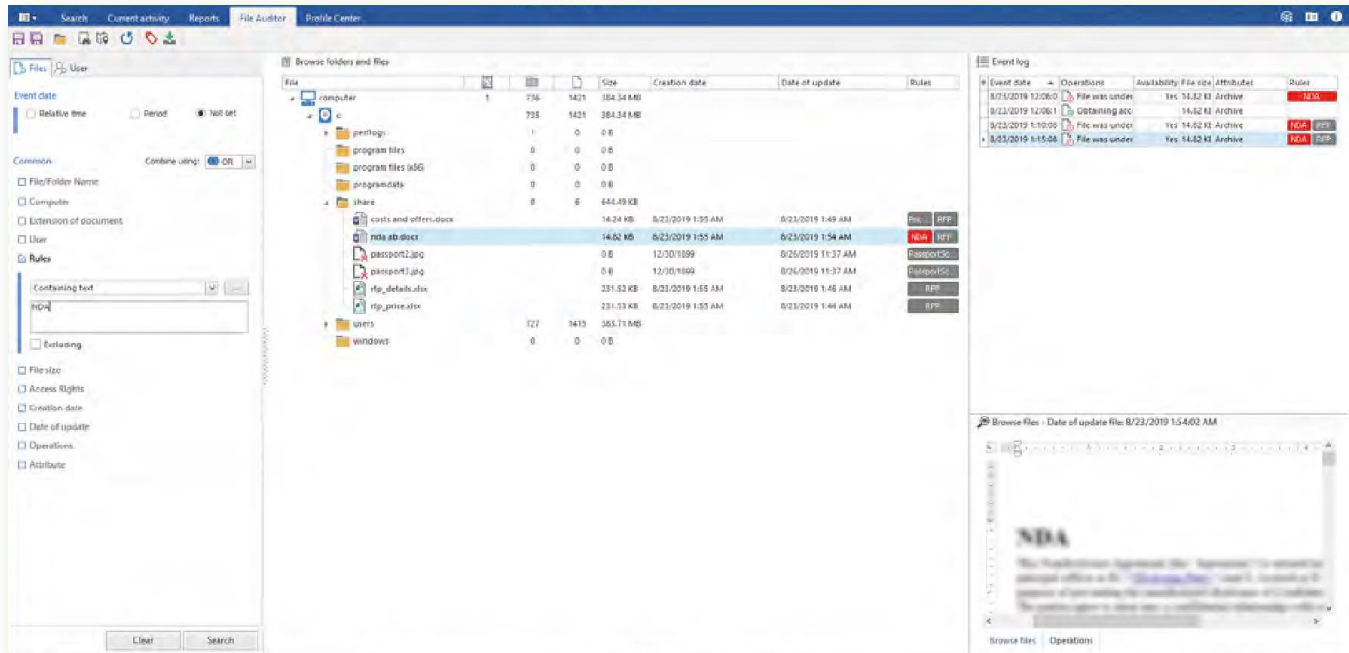
ANALISIS DATA

TKMT Risk Management DLP memvisualisasikan hasil pemindaian sistem file sesuai dengan aturan yang ditentukan. Program ini menunjukkan:

- Setiap direktori atau berkas memiliki tempatnya dalam tata letak yang jelas, dengan aturan hak akses yang dapat dimengerti.
- Aktivitas pada berkas, seperti kapan dibuat dan dimodifikasi, dicatat untuk memudahkan pemantauan.
- Berkas diberi label berdasarkan jenisnya, misalnya perjanjian rahasia, data pribadi, atau laporan keuangan, untuk kemudahan pengidentifikasian dan pengelolaan.
- Jumlah berkas penting dihitung di setiap disk atau folder, memberikan gambaran seberapa banyak informasi krusial yang tersimpan.

TKMT Risk Management DLP

Informasi yang dikumpulkan oleh agen dan modul pemindaian jaringan ditulis ke database yang menjalankan Microsoft SQL Server, dan salinan file penting disimpan dalam repositori. Begitulah cara dokumen tersedia bahkan setelah penghapusan.



Topologi dengan penandaan dokumen sensitif.

KEUNTUNGAN

- Integrasi solusi DCAP yang mulus ke dalam TKMT Risk Management DLP secara signifikan memperluas fungsionalitas sistem untuk mitigasi risiko
- Perubahan yang dilakukan pada file dapat dilacak hampir seketika - sistem menyimpan sejumlah revisi file tertentu yang membantu selama penyelidikan internal
- Pengaturan aturan yang dapat disesuaikan menyelamatkan spesialis dari pekerjaan yang tidak perlu, memungkinkan mereka untuk fokus pada pemantauan hanya data penting

KEMAMPUAN ANALITIS

Produk ini dapat dibandingkan dengan filter yang dilalui semua kueri pengguna dan respons server SQL. Monitor Database mengindeks kueri database secara otomatis membuatnya tersedia untuk pencarian dan analisis. Sistem ini mengintegrasikan berbagai jenis algoritma pencarian (berdasarkan frasa, berdasarkan atribut database dan pengguna, dengan ekspresi reguler, berdasarkan jenis kueri basis data, dll.), Yang dapat digabungkan menjadi kueri kompleks, menentukan kondisi pencarian.

TKMT Risk Management DLP



SPESIFIKASI TEKNIS

Fitur aplikasi	Deskripsi Keunikan Fitur
Automatic Classification	Automatic data classification based on file attributes such as content, file name, and file size.
Manual Classification	Users can classify files manually.
Data Backup	Back up classified data or files.
Data Versioning	Stores up to 99 versions of changes to data or files, including before and after changes.
File Monitoring	Log changes to files, such as file name changes or file deletions.
Keylogger	Recording keyboard activity, including recording passwords typed by users.
Camera Controller	Automatically capture or record the camera according to security policies when users open risky sites.
Monitor Controller	Automatically screenshot or record screens according to security policies when users open risky sites.
Microphone Controller	Automatically record sound on the microphone according to security policies when users open risky sites.
Program Controller	Records program usage activities and can block certain programs.
Cloud Controller	Monitor data activity and prevent important data leaks through cloud services such as Google Drive, One Drive, etc.
Print Controller	Monitor data activity and prevent important data leaks through printing physical documents.
HTTP/S Controller	Monitors HTTP/S activity and prevents users from accessing or sending critical data to risky sites.
Mail Controller	Monitor email activity and prevent important data leaks through email services like Gmail, Outlook, etc.
Instant Messenger Controller	Monitor instant messaging activities and prevent important data leaks through platforms like Whatsapp, Telegram, etc.
Device Controller	Monitor data and prevent data leaks via external devices such as flash disks, external HDDs and USB mobile devices. And can encrypt files sent to external devices.
FTP Controller	Record all file movement activities sent or received via the FTP protocol.
OCR (Optical Character Recognition)	Uses OCR technology to monitor and prevent the sending of scanned photos or documents.
Alert Notification	Provide warnings when users violate established security policies.
Audit Detail	Carefully audit all devices installed by SearchInform, including installed, attached, or removed hardware and software.
Report	Provide reports regarding violations of security policies and KPI reports as well as efficient use of employee devices.

Contacts:

www.tkm-teknologi.id

Email : support@tkm-teknologi.com

+62 811-1552-270