

SOLUSI PERLINDUNGAN DATA OLEH SEARCHINFORM:

Modul Komprehensif dan Deskripsi Terperinci

Untuk informasi lebih lanjut, silakan merujuk pada deskripsi	TimeInformer	DLP	Risk Monitor	FileAuditor
 Forensic	✗	✗	✓	✗
 M365	✗	✓	✓	✓
 MailController	✗	✓	✓	✗
 IMController	✗	✓	✓	✗
 DeviceController	✗	✓	✓	✗
 CloudController	✗	✓	✓	✗
 HttpController	✗	✓	✓	✗
 FtpController	✗	✓	✓	✗
 PrintController	✗	✓	✓	✗
 MonitorController + Keylogger	✓	✗	✓	✗
 Watermarks on screenshots	✓	✗	✓	✗
 MicrophoneController	✓	✗	✓	✗
 ProgramController	✓	✗	✓	✗
 Data Classification	✗	✗	✗	✓
 Files activities monitoring	✗	✗	✗	✓
 Files access rights audit	✗	✗	✗	✓
 Watermarks in files	✗	✗	✗	✓

Forensic DataBase menyimpan semua peristiwa “mentah” (raw events), yang menjadi dasar bagi sistem untuk mendeteksi insiden. Misalnya, versi asli email, pesan obrolan Telegram, pesan suara di WhatsApp, dokumen yang diunggah ke cloud, dan lain sebagainya. Data disimpan tanpa batas waktu dan terlepas apakah ditemukan pelanggaran kebijakan keamanan di dalamnya atau tidak. Forensic DataBase menawarkan pencarian informasi berbasis konten, serta kemampuan untuk menerapkan kebijakan keamanan pada arsip komunikasi.

M365 adalah integrasi dengan Microsoft 365 melalui API milik sendiri. Untuk DLP dan RM, integrasi ini memungkinkan perlindungan komunikasi (lampiran, chat, teks) di Teams Online dan Exchange Online, terlepas dari apakah pengguna mengakses platform 365 melalui browser web atau aplikasi desktop. Untuk FA, integrasi ini memfasilitasi kategorisasi terhadap setiap data yang diunggah atau diproses oleh pengguna.

MailController – pengumpulan, kategorisasi, dan karantina email. Melindungi email perusahaan maupun email publik (seperti Gmail dan lainnya). Melindungi klien email dengan protokol klasik (IMAP, MAPI, SMTP) serta email yang diakses melalui browser.

IMController – pengumpulan, kategorisasi, dan pemblokiran pesan, panggilan, serta file yang dikirim melalui messenger perusahaan maupun messenger publik, termasuk WhatsApp dan Telegram.

DeviceController – pengumpulan, kategorisasi, pemblokiran, dan enkripsi paksa terhadap file yang ditransmisikan melalui port input/output pada perangkat penyimpanan data.

CloudController – pengumpulan, kategorisasi, dan pemblokiran file yang ditransmisikan ke layanan cloud atau perangkat lunak kolaborasi (misalnya, Zoom).

HttpController – pengumpulan, kategorisasi, dan pemblokiran terhadap lalu lintas browser acak apa pun yang tidak dikumpulkan oleh pengendali lainnya.

FtpController – pengumpulan, kategorisasi, dan pemblokiran lalu lintas FTP.

PrintController – pengumpulan, kategorisasi, dan pemblokiran file yang dikirim untuk dicetak.

MonitorController + Keylogger – membuat tangkapan layar dan merekam layar pengguna, mengambil foto atau membuat rekaman video melalui webcam, serta mengaudit input keyboard. Mendeteksi pemotretan monitor dan memastikan identifikasi biometrik karyawan melalui pengenalan wajah.

Watermarks on screenshots – menampilkan informasi pada monitor untuk melindungi dari pengambilan tangkapan layar atau pemotretan monitor.

MicrophoneController – melakukan perekaman audio dari mikrofon PC dengan konversi dan pengenalan audio ke teks secara berkelanjutan.

ProgramController – memperkirakan waktu yang dihabiskan untuk bekerja di program dan browser. Mengevaluasi produktivitas serta menelusuri aktivitas pengguna selama investigasi internal perusahaan.

Data Classification – klasifikasi file berbasis konten yang disimpan di PC, LAN, dan dalam Sistem Manajemen Basis Data (Database Management System). Sistem menambahkan label khusus yang dapat digunakan baik untuk audit maupun sebagai kriteria pemblokiran akses ke file.

File activity monitoring – pencatatan aktivitas operasi file lokal dan jaringan, bekerja pada level driver dan tidak memerlukan aktivasi log bawaan sistem operasi.

File access rights audit – audit terhadap hak akses saat ini, serta mendeteksi perubahan hak akses terhadap objek pada sistem file lokal dan jaringan.

Watermarks in files – menambahkan teks atau simbol pada dokumen tertentu untuk menandai tingkat kerahasiaannya.