

SAM

SECURITY ADMINISTRATION MANAGEMENT



TANTE SOLUZIONI IN UN'UNICA PIATTAFORMA

- Stai controllando le **attività sui tuoi sistemi critici**?
- Stai monitorando l'**accesso dei fornitori** ai tuoi sistemi IT?
- Sei organizzato per gestire i fenomeni di **Data Breach**?
- Sei protetto da possibili **esfiltrazione dei dati** dalla tua Azienda?
- Stai utilizzando una piattaforma sicura per lo smart working?
- Riesci a rilevare tempestivamente i **tentativi di accesso non autorizzati**?





FUNZIONALITÀ DELLA PIATTAFORMA

Access Control: per tracciare gli accessi degli operatori ai dispositivi ed alle applicazioni che essi gestiscono;

Video Management: ogni operazione viene monitorata attraverso la produzione di sessioni video che memorizzano le operazioni eseguite, i video sono protetti da crittografia e gestiti secondo la Separation of Duty. Queste registrazioni sono considerate prove forensi inalterabili e inoppugnabili.

Event Management: vengono registrati i movimenti del cursore, i tasti digitati sulla tastiera ed i file originali trasferiti in upload/download.

Accesso remoto sicuro: la connessione verso i Sistemi Aziendali avviene tramite SAM su protocollo HTTPS bloccando malware, virus e attacchi man-in-the-middle.

Strong Authentication: SAM include un sistema nativo di OTP (one time password) che aggiunge un ulteriore livello di sicurezza al login applicativo. La piattaforma supporta anche sistemi di autenticazione multifattore terze parti, come Google Authenticator.

Intrusion Detection: Nuova funzione Agentless introdotta per identificare tentativi di accesso ai target non veicolati da SAM, compresi eventuali attacchi hacker.

Password Vault: Registrazione e modifica automatica delle password attraverso SAM, l'utente conosce solo la password che gli è stata assegnata non quella dei target che viene gestita esclusivamente dalla piattaforma. In combinazione con il sistema di Intrusion Detection garantisce che l'accesso ai target solo via SAM.

Badge virtuale: SAM integra una funzione nativa per la gestione delle timbrature elettroniche, migliorando ulteriormente la sua applicazione in ambito smart working.

A graphic at the bottom of the page features the word 'Security' in a large, blue, pixelated font. To the left is a circular logo with a shield and a key. Below the text, a hand is shown pointing at a screen, suggesting digital interaction. The background is dark with a grid pattern.

Security



SICUREZZA MADE IN ATLANTICA



SAM è una piattaforma per la gestione delle attività degli utenti privilegiati e non per l'accesso alle risorse aziendali critiche.

SAM è riconosciuta tra le piattaforme più evolute di Privilege Access Management sul mercato.

SAM è un ambiente sicuro e controllato per lo Smart Working che impedisce il trasferimento di virus sui sistemi aziendali.

SAM è una soluzione on top agentless e clientless che si integra facilmente nell'infrastruttura IT dei clienti.

LA SICUREZZA DI SAM

La Piattaforma garantisce il rigoroso rispetto delle normative italiane, internazionali e delle best practices in materia di:

Separazione dei compiti tra utenti e revisori

Controllo delle attività degli utenti privilegiati e non

Non-ripudio dei log generati

Registrazione e gestione degli accessi

Designazioni individuali degli utenti privilegiati

Rilevamento in tempo reale di possibili frodi

Gestione smart delle password

Identificazione accessi non autorizzati





PRIVACY & COMPLIANCE

In conformità al **GDPR**, il regolamento dell'Unione Europea sulla protezione dei dati, SAM tutela le informazioni e i dati raccolti garantendone la correttezza e la trasparenza del trattamento.

In conformità con i requisiti imposti da  **AgID** la piattaforma SAM prevede le seguenti soluzioni:

Uso appropriato dei privilegi di amministratore: In conformità con il requisito **ABSC 5 (CSC 5)**;

Difese contro i malware: In conformità con il requisito **AGID ABSC 8 (CSC 8)**;

Protezione dei dati: Nel rispetto delle indicazioni in conformità del requisito **AGID ABSC 13 (CSC 13)**;

Inventario dei dispositivi autorizzati e non autorizzati: Supporta il processo di adeguamento al requisito **ABSC 1 (CSC 1)**;

Proteggere le configurazioni di hardware e software dei dispositivi: Garantisce la protezione delle configurazioni permettendo la conformità con il requisito **AGID ABSC 3 (CSC 3)**.

SMART WORKING CON

SAM per le sue caratteristiche di sicurezza e flessibilità è la piattaforma ideale per lo Smart Working

Profilazione utenti

Crea un ambiente completamente personalizzabile per ogni singolo utente che acceda all'infrastruttura on site o da remoto.

Definizione aree

Ogni singolo utente potrà accedere esclusivamente alle aree a lui destinate.

Nessun virus

Impedisce il trasferimento di qualsiasi malware tra client e Sistemi Aziendali.

Protocolli sicuri

Prevede le trasmissioni tra computer remoto e azienda su protocollo crittografato e protetto da certification authority. Impedisce attacchi «Man in the middle».

Timbratura elettronica

Include una funzionalità per le timbrature elettroniche di inizio e termine delle attività lavorative dei dipendenti. Amministrazione dei log delle presenze.

