

VOGO DIGITAL

FIȘĂ TEHNICĂ

SECURITATE CIBERNETICĂ GATESCANNER SECURITY DOME TRANSFER ȘI COLABORARE SECURIZATĂ CU SANITIZARE CDR

VERSIUNEA 1.0

Produs	GateScanner Security Dome
Producător	Sasa Software (CAS) Ltd.
Domeniu	Securizarea transferului și partajării fișierelor
Tehnologie	Content Disarm and Reconstruction (CDR)
Interfețe	Web, API REST/OpenAPI, ICAP, extensii și aplicații endpoint
Execuție	On-premises, cloud privat sau SaaS, conform configurației selectate

1. Prezentare generală

GateScanner Security Dome este o platformă pentru transferul, partajarea și colaborarea securizată cu fișiere, bazată pe tehnologia Content Disarm and Reconstruction (CDR). Soluția controlează fluxurile de intrare și ieșire ale fișierelor și livrează utilizatorilor versiuni reconstruite și sanitizate.

Soluția asigură

- Aplică o politică de tip zero-trust tuturor fluxurilor de date bazate pe fișiere care traversează platforma.
- Previne amenințările cunoscute, necunoscute și de tip zero-day fără a depinde exclusiv de detectarea prin semnături.
- Centralizează controlul și vizibilitatea asupra transferurilor de fișiere între furnizori, clienți, departamente, sisteme enterprise și rețele operaționale.
- Integrează într-un singur flux gateway-ul de ingestie, motoarele de sanitizare CDR, livrarea, stocarea și funcțiile de securitate și conformitate.
- Protejează fluxurile de fișiere împotriva malware-ului, ransomware-ului și amenințărilor persistente avansate asociate conținutului transferat.
- Permite utilizatorilor să continue lucrul cu foldere de rețea, browsere, Outlook și medii USB, în timp ce sanitizarea este executată transparent.
- Oferă modele de implementare on-premises, în cloud privat sau ca serviciu SaaS, în funcție de infrastructura și politicile organizației.
- Furnizează un punct unic de administrare pentru politicile aplicate canalelor de transfer și partajare a fișierelor.

2. Beneficii operaționale și de securitate

Platforma reduce expunerea la cod malițios introdus prin documente și arhive și consolidează procesele de transfer într-un serviciu controlat și auditat.

Soluția asigură

- Neutralizează proactiv amenințările din fișiere înainte ca acestea să ajungă în mediile interne sau la destinatarii autorizați.
- Elimină dependența de publicarea unei semnături pentru blocarea unui tipar nou de atac ascuns într-un fișier.
- Permite procesarea volumelor ridicate prin distribuirea sarcinilor între motoarele CDR active.
- Menține continuitatea serviciului în timpul extinderii capacității prin adăugarea de noduri fără oprirea platformei.
- Păstrează experiența normală de lucru a utilizatorilor, oferind fișiere reconstruite după aplicarea politicilor de securitate.
- Reduce numărul soluțiilor punctuale necesare pentru protejarea canalelor web, e-mail, file-share și medii portabile.
- Asigură trasabilitatea acțiunilor asupra fișierelor prin jurnale imuabile și export structurat compatibil cu soluțiile SIEM.
- Sprijină demonstrarea conformității prin păstrarea istoricului de încărcare, descărcare, sanitizare și partajare.
- Separă fișierele primite de versiunile sigure livrate, menținând controlul asupra traseului și destinației.
- Permite alinierea serviciului la politicile organizației prin reguli granulare de eliminare și reconstrucție a conținutului.

3. Arhitectură și flux de procesare

Arhitectura GateScanner Security Dome organizează procesarea în etape distincte, de la ingestie până la livrarea versiunii sanitizate și păstrarea dovezilor operaționale.

Soluția asigură

- Primește fișiere de la furnizori, prestatori de servicii, clienți și alte surse autorizate prin canalele configurate.

- Direcționează fișierele către gateway-ul de ingestie înainte de accesul în zonele protejate ale organizației.
- Distribuie procesarea către o grilă de motoare CDR active pentru sanitizare paralelă și disponibilitate ridicată.
- Reconstruiește fișierele conform politicilor și livrează rezultatul către departamente, sisteme enterprise sau rețele operaționale.
- Integrează stocarea și protejarea fișierelor în același circuit cu sanitizarea și livrarea.
- Oferă un tablou de bord de administrare pentru vizibilitate asupra procesării și a politicilor de securitate.
- Separă funcțiile de ingestie, sanitizare, workflow și livrare pentru dimensionare și administrare controlată.
- Permite reutilizarea fișierelor sanitizate din zona de stocare și integrare, conform drepturilor și politicilor aplicabile.
- Aplică același control asupra fluxurilor de intrare și ieșire, inclusiv pentru partajarea internă și externă.

4. Motorul Content Disarm and Reconstruction

Motorul CDR analizează structura fișierului, elimină elementele care încalcă politica și reconstruiește un rezultat utilizabil, fără executarea conținutului potențial periculos în mediul destinatarului.

Soluția asigură

- Utilizează tehnologie CDR independentă de detectare pentru prevenirea amenințărilor transportate prin fișiere.
- Aplică reguli granulare pentru eliminarea macrocomenzilor din documentele procesate.
- Elimină scripturile și alte componente active interzise de politica organizației.
- Controlează obiectele încorporate și păstrează numai elementele permise în fișierul reconstruit.
- Poate elimina hyperlinkurile și alte elemente considerate riscante conform politicii configurate.
- Procesează recursiv fișierele încorporate pentru ca obiectele atașate să fie supuse acelorași controale.
- Procesează arhivele în profunzime și aplică sanitizarea conținutului identificat în interiorul acestora.
- Acceptă arhive protejate cu parolă, în condițiile și prin mecanismele prevăzute de configurația produsului.
- Livrează o versiune reconstruită a fișierului după eliminarea elementelor nepermise.
- Aplică politici diferențiate în funcție de canal, tipul fișierului, sursă, destinație și cerințele organizației.
- Menține procesarea deterministă, astfel încât rezultatul să reflecte politica definită pentru conținutul analizat.

5. Tipuri de fișiere și controale asupra conținutului

Soluția acoperă o gamă extinsă de formate utilizate în activitatea curentă și în schimburile cu partenerii externi.

Soluția asigură

- Suportă peste 300 de tipuri de fișiere.
- Procesează documente Microsoft Office și formate asociate activităților de birou.
- Procesează documente PDF și controlează elementele active sau încorporate conform politicii.
- Procesează imagini și formate grafice incluse în fluxurile de transfer.
- Procesează arhive și conținutul acestora prin analiză și sanitizare recursivă.
- Acoperă formate specializate menționate în catalogul de suport al produsului.
- Acceptă fișiere de dimensiune nelimitată la nivel declarativ, limita efectivă fiind determinată de politica și infrastructura implementării.
- Permite definirea elementelor acceptate, eliminate sau reconstruite pentru fiecare categorie de fișier.
- Aplică aceleași politici conținutului transferat individual și loturilor de fișiere.
- Păstrează pentru audit rezultatul procesării și acțiunile efectuate asupra fișierului, conform configurației.

6. Disponibilitate, scalabilitate și performanță

GateScanner Security Dome utilizează o grilă de procesare CDR Active-Active pentru distribuirea sarcinii și menținerea serviciului disponibil.

Soluția asigură

- Rulează motoarele de sanitizare într-o arhitectură Active-Active.
- Distribuie fișierele între nodurile disponibile pentru procesare paralelă.
- Permite scalarea orizontală prin adăugarea dinamică a nodurilor de procesare.
- Menține funcționarea platformei în timpul extinderii capacității, fără oprire planificată pentru adăugarea nodului.
- Asigură procesare batch paralelă pentru volume ridicate de fișiere.
- Utilizează mecanisme de coadă adaptate procesării concurente a sarcinilor.
- Separă capacitatea de ingestie, sanitizare și livrare pentru dimensionarea componentelor în funcție de volum.
- Permite adaptarea infrastructurii la creșterea numărului de utilizatori, fluxuri și canale protejate.
- Centralizează monitorizarea activității de procesare prin tabloul de bord al platformei.

7. Transfer securizat și automatizarea fluxurilor

Funcțiile Managed File Transfer conectează surse și destinații eterogene și automatizează mutarea controlată a fișierelor prin circuitul CDR.

Soluția asigură

- Conectează directoare și partajări de rețea prin protocoale SMB și CIFS.
- Conectează surse și destinații prin SFTP pentru schimburi securizate de fișiere.
- Conectează servicii FTPS acolo unde acest protocol este utilizat de organizație sau parteneri.
- Integrează stocare compatibilă Amazon S3 pentru preluarea și livrarea fișierelor.
- Integrează Azure Blob Storage ca sursă sau destinație pentru fluxurile configurate.
- Permite utilizarea stocării locale, a căilor de rețea UNC și a serviciilor cloud declarate de produs.
- Execută fluxuri programate la intervalele stabilite de administrator.
- Execută fluxuri declanșate de evenimente sau de apariția fișierelor în endpointurile monitorizate.
- Transferă fișiere între endpointuri definite, cu sanitizarea inclusă în circuitul operațional.
- Permite procesarea loturilor și livrarea rezultatelor către destinația configurată.
- Păstrează trasabilitatea operațiunilor de transfer, sanitizare și livrare.

8. Seif de colaborare și partajare

Componenta de colaborare oferă un spațiu controlat pentru încărcarea, sanitizarea, descărcarea și partajarea fișierelor.

Soluția asigură

- Controlează accesul prin roluri și politici RBAC.
- Integrează identități și grupuri din Active Directory și LDAP.
- Permite autentificare federată prin SAML 2.0.
- Permite autentificare OpenID Connect pentru scenariile configurate.
- Oferă legături de partajare protejate prin parolă.
- Permite limitarea în timp a legăturilor de partajare.
- Oferă foldere partajate pentru colaborarea controlată între utilizatorii autorizați.
- Jurnalizează încărcările, descărcările, sanitizările și partajările efectuate în seif.
- Integrează sanitizarea înaintea distribuirii fișierului către destinatar.

- Permite înlocuirea atașamentelor de mari dimensiuni cu legături către fișiere sanitizate.

9. Identitate, audit și conformitate

Mecanismele de identitate și audit controlează cine poate opera cu fișierele și păstrează dovezile necesare analizelor de securitate și conformitate.

Soluția asigură

- Aplică autorizarea pe roluri prin mecanisme RBAC.
- Integrează serviciile de director AD și LDAP pentru administrarea identităților.
- Acceptă SAML 2.0 și OpenID Connect pentru autentificare unică.
- Înregistrează acțiunile de încărcare, descărcare, sanitizare și partajare.
- Păstrează jurnale declarate de producător ca imuabile pentru acțiunile asupra fișierelor.
- Exportă evenimente structurate în formate compatibile cu platformele SIEM.
- Sprijină investigațiile prin corelarea acțiunii cu utilizatorul, fișierul și momentul operațiunii.
- Oferă vizibilitate centralizată asupra canalelor și operațiunilor protejate.
- Permite demonstrarea aplicării politicilor de sanitizare în cadrul controalelor și auditurilor.
- Menține separarea accesului între organizații și domenii în configurațiile multi-tenant.

10. Multi-tenancy și modele de implementare

Platforma poate fi configurată pentru organizații segmentate și furnizori de servicii care administrează mai multe domenii sau entități.

Soluția asigură

- Oferă suport multi-tenant pentru separarea logică a organizațiilor administrate.
- Oferă suport multi-domain pentru medii cu domenii distincte de identitate și acces.
- Susține scenarii MSSP în care un furnizor operează servicii pentru mai mulți clienți.
- Permite implementare on-premises sub forma unui appliance virtual.
- Declară suport pentru VMware vSphere în scenariul appliance-ului virtual.
- Declară suport pentru Microsoft Hyper-V în scenariul appliance-ului virtual.
- Permite implementare în cloud privat pe AWS, Microsoft Azure sau Google Cloud Platform.
- Este disponibilă și o variantă SaaS administrată în cloud de furnizor.
- Permite alegerea modelului de implementare în funcție de cerințele de control, integrare și operare ale organizației.
- Păstrează aceleași funcții de bază pentru sanitizare și control al fluxurilor, adaptate modelului de implementare selectat.

11. Integrarea cu browserele web

Extensia GateScanner pentru browsere redirecționează descărcările către Security Dome pentru aplicarea obligatorie a sanitizării CDR.

Soluția asigură

- Este disponibilă ca extensie pentru Google Chrome.
- Este disponibilă ca extensie pentru Microsoft Edge.
- Este disponibilă ca extensie pentru Mozilla Firefox.
- Interceptează descărcările de fișiere inițiate din browser.
- Redirecționează fișierele către Security Dome pentru sanitizare obligatorie.
- Livrează utilizatorului versiunea sigură și reconstruită a fișierului.

- Păstrează experiența de descărcare transparentă pentru utilizator, în limitele politicilor aplicate.
- Neutralizează conținutul malițios transportat prin descărcări web și scenarii de tip drive-by download.
- Extinde controlul CDR asupra unui canal utilizat frecvent pentru introducerea fișierelor în organizație.

12. Integrarea cu Microsoft Outlook

Add-in-ul VSTO pentru Outlook oferă un circuit controlat pentru încărcarea, sanitizarea și transmiterea atașamentelor.

Soluția asigură

- Permite încărcarea atașamentului în seiful Security Dome printr-o acțiune din Outlook.
- Înlocuiește atașamentul cu o legătură către versiunea sanitizată, conform fluxului configurat.
- Permite transferul fișierelor de mari dimensiuni fără a depinde de limita serverului de e-mail.
- Poate utiliza funcția SMTP integrată pentru expedierea controlată direct din Security Dome.
- Menține controlul end-to-end al fluxului de atașamente transmis prin mecanismul platformei.
- Contribuie la prevenirea introducerii atașamentelor malițioase în mediul organizației.
- Contribuie la controlul ieșirii datelor prin canalul de e-mail, în limitele politicilor și configurației implementate.
- Păstrează în audit acțiunile de încărcare, sanitizare și partajare asociate fișierului.

13. Stația virtuală pentru medii USB

GateScanner Virtual USB Kiosk transformă un endpoint într-o stație controlată pentru introducerea fișierelor de pe medii portabile.

Soluția asigură

- Oferă o aplicație endpoint dedicată importului securizat de pe medii detașabile.
- Afișează într-un mod de browser dedicat numai interfața necesară încărcării fișierelor.
- Impune un flux unic de selectare, trimitere către Security Dome și sanitizare.
- Reduce posibilitatea ocolirii circuitului de securitate la importul fișierelor de pe USB.
- Livrează către mediul intern numai rezultatul procesat de motoarele CDR.
- Controlează poarta fizică de transfer al datelor dintre mediile portabile și rețelele organizației.
- Poate fi utilizat pentru scenarii în care rețelele operaționale necesită un punct dedicat de introducere a fișierelor.
- Integrează operațiunile stației în vizibilitatea și auditul central al Security Dome.

14. API și integrarea cu ecosistemul de securitate

Interfețele de integrare permit conectarea Security Dome cu aplicații, platforme de orchestrare și servicii de securitate.

Soluția asigură

- Furnizează un API REST pentru integrarea operațiunilor platformei.
- Documentează API-ul prin OpenAPI Specification și interfață Swagger.
- Permite integrarea cu platforme SOAR pentru orchestrarea fluxurilor și acțiunilor de securitate.
- Declară suport pentru protocolul ICAP în scenariile de integrare compatibile.
- Exportă jurnale și evenimente în formate structurate compatibile cu soluțiile SIEM.
- Integrează depozite locale, căi de rețea și servicii cloud ca surse sau destinații.
- Permite automatizarea fluxurilor pe baza programărilor, declanșatorilor și evenimentelor.
- Centralizează aplicarea politicii CDR indiferent de aplicația sau canalul care inițiază transferul.
- Oferă organizației posibilitatea de a include sanitizarea în procese automate, fără operațiuni manuale pentru fiecare fișier.

15. Specificații tehnice declarate de producător

Specificațiile de mai jos reproduc capabilitățile publicate în materialul GateScanner Security Dome furnizat ca sursă pentru această fișă.

Soluția asigură

- Tipuri de fișiere suportate: peste 300, inclusiv Microsoft Office, PDF, imagini și arhive.
- Dimensiunea maximă a fișierului: nelimitată la nivel de produs, dependentă de politica și infrastructura implementării.
- Depozite suportate: stocare locală, căi de rețea UNC și servicii cloud precum AWS S3, Azure Storage și OneDrive.
- Protocoale de integrare declarate: RESTful API documentat prin OpenAPI și ICAP.
- Mecanisme de autentificare declarate: AD/LDAP, SAML 2.0 și OpenID Connect.
- Jurnalizare și raportare: export compatibil SIEM și trasee complete de audit.
- Canale MFT declarate: SMB/CIFS, SFTP, FTPS, Amazon S3 și Azure Blob Storage.
- Modele de implementare declarate: appliance virtual on-premises, cloud privat și SaaS administrat.
- Componente endpoint declarate: extensie de browser, add-in Outlook și aplicație Virtual USB Kiosk.

16. Politici de securitate aplicate canalelor de fișiere

Politicile GateScanner permit aplicarea acelorași principii de sanitizare în mod diferențiat, în funcție de canalul prin care fișierul intră, este partajat sau părăsește organizația.

Soluția asigură

- Asociază fiecărui canal un circuit de ingestie, sanitizare și livrare controlată.
- Aplică reguli de eliminare a macrocomenzilor, scripturilor, obiectelor încorporate și hyperlinkurilor în funcție de politica selectată.
- Permite diferențierea politicilor pentru descărcările web, atașamentele e-mail, partajările de rețea și mediile portabile.
- Direcționează către motoarele CDR fișierele interceptate înainte de livrarea către utilizator sau sistemul destinatar.
- Aplică procesarea recursivă atunci când fișierele conțin obiecte încorporate sau arhive.
- Păstrează rezultatul reconstruit ca versiune sigură destinată utilizării operaționale.
- Permite menținerea unui control unitar asupra fișierelor provenite de la parteneri, clienți și furnizori.
- Extinde același control asupra fișierelor distribuite către departamente, sisteme enterprise și rețele operaționale.
- Leagă decizia de procesare de tipul fișierului, endpoint, sursă și destinație.
- Păstrează în jurnal acțiunile efectuate asupra fișierului pe parcursul circuitului configurat.
- Permite administrarea centralizată a politicilor, în locul unor reguli independente pentru fiecare aplicație utilizatoare.
- Asigură aplicarea politicii înainte ca fișierul să fie pus la dispoziția destinatarului autorizat.

17. Administrare și vizibilitate operațională

Funcțiile de administrare oferă vizibilitate asupra canalelor, nodurilor de procesare, fluxurilor și acțiunilor executate asupra fișierelor.

Soluția asigură

- Centralizează administrarea componentelor de ingestie, sanitizare, workflow, livrare și stocare.
- Oferă un tablou de bord pentru supravegherea funcționării platformei și a procesării fișierelor.
- Permite urmărirea fluxurilor programate, declanșate și bazate pe evenimente.

- Prezintă activitatea motoarelor CDR din grila Active-Active.
- Sprijină dimensionarea capacității prin observarea volumelor procesate pe canalele configurate.
- Permite adăugarea nodurilor de procesare în timpul funcționării platformei.
- Oferă control unitar asupra endpointurilor locale, de rețea și cloud utilizate în transferuri.
- Permite administratorilor să gestioneze rolurile și accesul prin integrarea cu serviciile de identitate declarate.
- Consolidează jurnalele operaționale necesare analizelor de securitate și conformitate.
- Permite separarea administrativă a clienților și domeniilor în configurațiile multi-tenant și multi-domain.
- Menține vizibilitatea asupra fișierelor încărcate, sanitizate, descărcate și partajate.
- Oferă un punct central pentru integrarea evenimentelor cu SIEM și a fluxurilor cu platformele SOAR.

18. Trasabilitatea fișierului și dovezile de audit

Circuitul controlat al fișierului produce evenimente verificabile pentru operațiunile principale și permite exportul lor către sistemele organizației.

Soluția asigură

- Înregistrează încărcarea fișierului și identitatea asociată operațiunii.
- Înregistrează sanitizarea și aplicarea circuitului de procesare configurat.
- Înregistrează descărcarea versiunii sigure de către utilizatorul autorizat.
- Înregistrează partajarea prin legături și foldere controlate.
- Păstrează evenimentele într-un jurnal declarat de producător ca imuabil.
- Exportă evenimentele într-un format structurat compatibil cu soluțiile SIEM.
- Permite corelarea dovezilor GateScanner cu evenimentele colectate din alte sisteme de securitate.
- Sprijină verificarea traseului dintre sursa fișierului, procesarea CDR și destinația finală.
- Oferă informații utilizabile pentru investigații privind încărcarea, descărcarea, sanitizarea și partajarea.
- Permite demonstrarea faptului că fișierele au traversat circuitul obligatoriu de sanitizare.
- Contribuie la pregătirea dovezilor solicitate în controale și audituri de conformitate.
- Păstrează separarea jurnalelor și accesului în scenariile cu organizații sau domenii distincte.

19. Scenarii de utilizare și integrare

Componentele GateScanner pot fi combinate pentru a proteja scenarii distincte de schimb de fișiere, păstrând același motor CDR și aceeași administrare centrală.

Soluția asigură

- Protejează descărcările din Chrome, Edge și Firefox prin redirectionarea obligatorie către Security Dome.
- Protejează trimiterea atașamentelor din Outlook prin încărcarea în seif și distribuirea unei legături către fișierul sanitizat.
- Permite transferul fișierelor mari fără utilizarea atașamentului clasic și fără dependența de limita serverului de e-mail.
- Controlează importul de pe medii USB printr-o stație dedicată și un flux unic de selectare și sanitizare.
- Automatizează preluarea din directoare SMB/CIFS și livrarea către destinațiile autorizate.
- Automatizează schimburile cu partenerii prin endpointuri SFTP și FTPS.
- Integrează fluxuri cu depozite Amazon S3 și Azure Blob Storage.
- Permite colaborarea prin foldere partajate și legături protejate prin parolă și limitate în timp.
- Integrează sanitizarea în aplicații și procese prin REST API documentat prin OpenAPI.
- Integrează platforma cu ecosistemul de securitate prin ICAP, export SIEM și orchestrare SOAR.
- Susține scenarii pentru rețele operaționale care necesită o poartă controlată de transfer al fișierelor.

- Susține operarea pentru mai multe organizații prin capabilitățile multi-tenant și multi-domain declarate.
- Permite alegerea între appliance virtual on-premises, cloud privat și serviciu SaaS administrat.
- Menține același principiu de livrare a unei versiuni reconstruite și sanitizate indiferent de canalul de origine.

20. Componente și responsabilități în soluție

Componentele platformei au responsabilități distincte în circuitul fișierului și sunt administrate ca parte a aceleiași soluții de securizare și transfer.

Soluția asigură

- Gateway-ul de ingestie primește fișierele din sursele și canalele autorizate.
- Grila de motoare CDR execută sanitizarea și reconstrucția conținutului procesat.
- Componenta de workflow și livrare transmite rezultatul către destinația configurată.
- Zona de stocare și integrare păstrează și protejează fișierele utilizate în fluxurile autorizate.
- Tabloul de bord de administrare oferă vizibilitate asupra activității platformei.
- Funcțiile de securitate și conformitate gestionează politicile și dovezile asociate procesării.
- Componenta MFT conectează endpointurile de rețea, SFTP, FTPS și stocare cloud.
- Seiful de colaborare gestionează încărcarea, descărcarea, folderele partajate și legăturile temporare.
- Serviciile de identitate aplică rolurile și autentificarea integrată prin mecanismele declarate de producător.
- Exportul SIEM transmite evenimentele structurate către platforma de monitorizare a organizației.
- API-ul REST documentat prin OpenAPI permite integrarea operațiunilor în aplicații și automatizări.
- Interfața ICAP permite conectarea cu sisteme compatibile din ecosistemul de securitate.
- Extensia de browser protejează canalul de descărcare a fișierelor de pe web.
- Add-in-ul Outlook protejează circuitul atașamentelor și al transferurilor de mari dimensiuni.
- Virtual USB Kiosk protejează introducerea fișierelor de pe medii detașabile.
- Arhitectura Active-Active distribuie procesarea între nodurile CDR disponibile.
- Funcțiile multi-tenant și multi-domain separă clienții, organizațiile sau domeniile administrate.
- Modelele on-premises, cloud privat și SaaS permit alegerea amplasării operaționale a serviciului.
- Jurnalele imuabile declarate de producător păstrează istoricul acțiunilor asupra fișierelor.
- Politicile CDR leagă tipul fișierului și canalul de setul de elemente eliminate sau reconstruite.

21. Producător și delimitarea informațiilor comerciale

GateScanner Security Dome este un produs Sasa Software (CAS) Ltd. Informațiile comerciale din acest capitol sunt atribuite explicit producătorului și provin din broșura furnizată.

Soluția asigură

- Producătorul declară că Sasa Software a fost înființată în anul 2013.
- Producătorul declară utilizarea suitei GateScanner de către peste 400 de organizații la nivel mondial.
- Domeniile menționate de producător includ apărare, administrație publică, sănătate, finanțe, energie și infrastructură critică.
- Producătorul declară că organizația are sediul central în Israel.
- Producătorul declară certificarea ISO 27001.
- Materialul furnizorului menționează recunoașteri Gartner din 2020 și Frost & Sullivan din 2017.
- Materialul furnizorului menționează integrarea cu Microsoft 365 pentru schimbul securizat de fișiere.
- Datele comerciale, certificările și recunoașterile trebuie reconfirmate cu producătorul la momentul ofertării sau contractării.

- GateScanner este identificat ca produs Sasa Software și poate fi inclus ca tehnologie specializată într-o soluție oferită și integrată de VOGO.

22. Parametri de configurare pentru implementare

Configurația finală se stabilește pentru mediul beneficiarului prin selectarea canalelor, politicilor, integrărilor și modelului de implementare dintre opțiunile declarate de produs.

Soluția asigură

- Se selectează modelul de implementare: appliance virtual on-premises, cloud privat sau serviciu SaaS administrat.
- Se dimensionează grila Active-Active în funcție de volumele de fișiere și canalele care necesită procesare.
- Se definesc sursele și destinațiile locale, UNC, SMB/CIFS, SFTP, FTPS și cloud utilizate de fluxuri.
- Se configurează politicile CDR pentru tipurile de fișiere și elementele active acceptate sau eliminate.
- Se stabilesc regulile de procesare recursivă pentru arhive și fișiere încorporate.
- Se selectează integrările de identitate AD/LDAP, SAML 2.0 sau OpenID Connect aplicabile organizației.
- Se configurează rolurile RBAC pentru administrare, încărcare, descărcare, sanitizare și partajare.
- Se aleg componentele endpoint necesare: extensii de browser, add-in Outlook și Virtual USB Kiosk.
- Se definesc fluxurile programate, declanșate sau bazate pe evenimente pentru transferurile automatizate.
- Se configurează exportul jurnalelor către SIEM și, unde este aplicabil, integrarea cu platforma SOAR.
- Se stabilesc regulile pentru legăturile protejate prin parolă, perioadele de valabilitate și folderele partajate.
- Se verifică prin testare traseul complet dintre ingestie, sanitizare, livrare, stocare și audit pentru fiecare canal activat.