Sicurezza e Operatività OT – Soluzione piattaforma OT

Servizi di assessment, implementazione e piattaforma modulare (ACCESS, INSIGHT, RESCUE)

Mashfrog Group

Sommario

Sede legale
Via G. Peroni, 400/402
00131 - Roma
C.F. e P.IVA 02534640905

info@mashfrog.com
www.mashfrog.com

1. Executive Summary

Questo documento descrive le caratteristiche principali della piattaforma OT di Mashfrog. La piattaforma è una **soluzione integrata** e modulare basata su componenti Edge che assicura:

- accesso sicuro agli impianti OT, vincolato all'identità aziendale, a passkey/WebAuthn e a un broker di sessione basato su gateway Edge;
- visibilità passiva e continua sul traffico OT tramite sensoristica di rete e motori DPI, integrati con i sistemi SIEM aziendali;
- protezione e versioning delle configurazioni di PLC, SCADA e apparati di rete, con orchestrazione dei backup, validazione automatica e rollback verificabile.

La modalità standard di implementazione della soluzione si articola in due fasi.

La fase iniziale di **assessment** produce l'inventario degli asset OT e dei sistemi IT correlati, la mappa di siti e reti, la classificazione dei dispositivi e dei protocolli, i flussi di comunicazione e le dipendenze operative; definisce inoltre baseline, criteri di controllo e requisiti di integrazione con IdM/SSO, SIEM, CMDB/ITSM e sistemi di backup esistenti.

A valle dell'assessment viene attivata la piattaforma composta dai moduli ACCESS, INSIGHT e RESCUE: ACCESS implementa il controllo degli accessi privilegiati e la tracciabilità delle sessioni, sfruttando autenticazione forte (SSO, passkey/WebAuthn) e un gateway Edge che apre le sessioni verso gli impianti solo dopo verifiche di identità, contesto e autorizzazione; INSIGHT realizza la visibilità passiva del traffico OT con DPI dei protocolli industriali, arricchimento del contesto (asset, siti, linee) e generazione di eventi/alert integrabili nativamente nei SIEM; RESCUE gestisce l'orchestrazione dei backup, il versioning e la validazione delle configurazioni con workflow di change, approvazione e rollback automatizzabile.

La modularità consente un'adozione selettiva: è possibile implementare uno o più moduli, senza obbligo di attivarli tutti, iniziando ad esempio dal solo controllo accessi remoti o dalla sola visibilità di rete.

L'integrazione dei tre moduli riduce la frammentazione degli strumenti, standardizza interfacce e processi e consente l'adozione di controlli "security by design" all'interno dei processi esistenti (IdM/SSO, SIEM/SOAR, CMDB/ITSM, ticketing). Ne risultano controllo centralizzato, validazione automatizzata delle configurazioni e gestione operativa

Sede legale
Via G. Peroni, 400/402
00131 - Roma
C.F. e P.IVA 02534640905

info@mashfrog.com
www.mashfrog.com

misurabile, con evidenze di audit e un allineamento naturale ai requisiti normativi e di compliance per la sicurezza OT.

2. Contesto e Sfide

Gli ambienti industriali moderni si trovano ad affrontare sfide crescenti legate alla complessità delle reti **OT (Operational Technology)**. La coesistenza di sistemi eterogenei, spesso distribuiti su più siti, rende difficile avere una **visibilità unificata sugli asset** e sui flussi di comunicazione.

In molti casi, gli accessi non sono gestiti in modo centralizzato e mancano processi strutturati di **controllo e tracciabilità** delle operazioni, con il rischio di interventi non autorizzati o non documentati. A questo si aggiunge l'assenza di un **versioning delle configurazioni**, che porta a modifiche manuali non validate e a una scarsa capacità di rollback in caso di errore o guasto.

Queste condizioni comportano rischi concreti:

- **Downtime non pianificato**, con impatti diretti sulla produzione.
- **Superficie di attacco ampliata**, che espone l'infrastruttura a possibili intrusioni o malware.
- **Difficoltà di compliance** con normative di sicurezza e standard industriali.
- **Incremento dei costi operativi**, dovuti a inefficienze e gestione frammentata degli strumenti.

Per affrontare queste sfide è necessario adottare un approccio che unisca **servizi di assessment** e una **piattaforma integrata**, in grado di offrire controllo, automazione e sicurezza by design.

3. Approccio a fasi

L'implementazione della soluzione è concepita per seguire un percorso **graduale e non disruptive**, così da ridurre al minimo l'impatto sugli impianti e garantire un'adozione sicura e progressiva.

La pianificazione temporale è definita congiuntamente in fase di avvio progetto (**kickoff**) e riportata in un Project Plan.

La soluzione prevede la definizione congiunta di un perimetro in un workshop di scoping guidato da **impatto operativo** e **rischio cyber**.

Sede legale
Via G. Peroni, 400/402
00131 - Roma
C.F. e P.IVA 02534640905

info@mashfrog.com
www.mashfrog.com

Insieme identifichiamo gli impianti “tipo” più rappresentativi/critici e verifichiamo i prerequisiti tecnici (SSO/PAM, SPAN/TAP/NetFlow, reachability di management).

Per ciascun impianto compiliamo una scheda con classi di apparati, protocolli, pattern di accesso, tipologie di change, vincoli safety e finestre operative.

Il perimetro viene quindi congelato con stage-gate di ingresso/uscita, RACI e KPI di baseline per misurare valore e **riusabilità** su ACCESS, INSIGHT e RESCUE.

Il piano si articola in tre fasi principali:

➤ **Fase 1 – Assessment**

- **Rilievo dei siti, delle reti e dei dispositivi OT/IT/IoT:** Un team di esperti conduce un'analisi completa per identificare e mappare i siti, le reti e tutti i dispositivi OT/IT/IoT, inclusi i protocolli industriali in uso.
- **Popolamento del database degli asset con informazioni strutturate e correlate**: I dati raccolti verranno inseriti in un database centrale per creare un inventario strutturato e dinamico degli asset, completo di informazioni sui rischi e le vulnerabilità.
- **Definizione di una baseline operativa come punto di riferimento per le fasi successive:** è stabilita una "baseline" operativa, fornendo un punto di riferimento per le prestazioni normali del sistema e per il monitoraggio futuro.

➤ **Fase 2 – Implementazione Edge**

- **Installazione e configurazione dell’Edge nei siti pilota:** Installazione e configurazione dei dispositivi Edge nei siti pilota (nel caso di modulo INSIGHT o ACCESS), che agiranno come gateway per la raccolta dei dati industriali.
- **Integrazione dei protocolli standard e proprietari**: si implementa l'integrazione con protocolli standard (come Modbus, OPC-UA) e proprietari per avviare la raccolta del traffico di rete e garantire piena visibilità operativa.
- **Attivazione della raccolta del traffico** di rete per consentire visibilità e monitoraggio.

➤ **Fase 3 – Operatività**

- **Attivazione progressiva dei moduli ACCESS, INSIGHT e RESCUE**: I moduli sono attivati e configurati progressivamente per il sito pilota, rendendo la soluzione pienamente operativa.

Sede legale
Via G. Peroni, 400/402
00131 - Roma
C.F. e P.IVA 02534640905

info@mashfrog.com
www.mashfrog.com

- **Abilitazione** del **tracciamento** e **controllo centralizzato** degli **accessi**: abilitazione della gestione centralizzata degli accessi privilegiati. Ogni sessione di controllo e modifica è tracciata e monitorata in tempo reale.
- **Monitoraggio continuo del traffico OT con generazione di alert e reportistica:** La piattaforma inizia a monitorare il traffico OT, identificando anomalie e generando alert e reportistica dettagliata per una risposta tempestiva.
- Implementazione del **versioning delle configurazioni**, con processi di validazione e rollback in caso di anomalie: si implementa il versioning automatico delle configurazioni degli apparati. Questo include l'abilitazione di processi di validazione (approvazione delle modifiche) e la possibilità di **rollback** immediato a una versione precedente e sicura in caso di problemi, garantendo la continuità operativa.

4. La Piattaforma

4.1 Panoramica Generale

La nostra piattaforma rappresenta una **dashboard unica** e centralizzata per la gestione integrata degli ambienti **OT, IT e IoT**. Attraverso un'unica interfaccia, è possibile consolidare e gestire dati critici come l'inventario degli asset, gli utenti e i loro profili di accesso, le sessioni e i log di attività, e le configurazioni dei dispositivi.

Questo approccio elimina la frammentazione degli strumenti e garantisce una **visibilità completa sull'intero ecosistema tecnologico**, migliorando l'efficienza operativa, la postura di sicurezza e la governance complessiva. La piattaforma funge da "singola fonte di verità" per tutti i dati di sicurezza e operatività, consentendo una gestione proattiva e un'analisi olistica dei rischi.

Sede legale
Via G. Peroni, 400/402
00131 - Roma
C.F. e P.IVA 02534640905

info@mashfrog.com
www.mashfrog.com

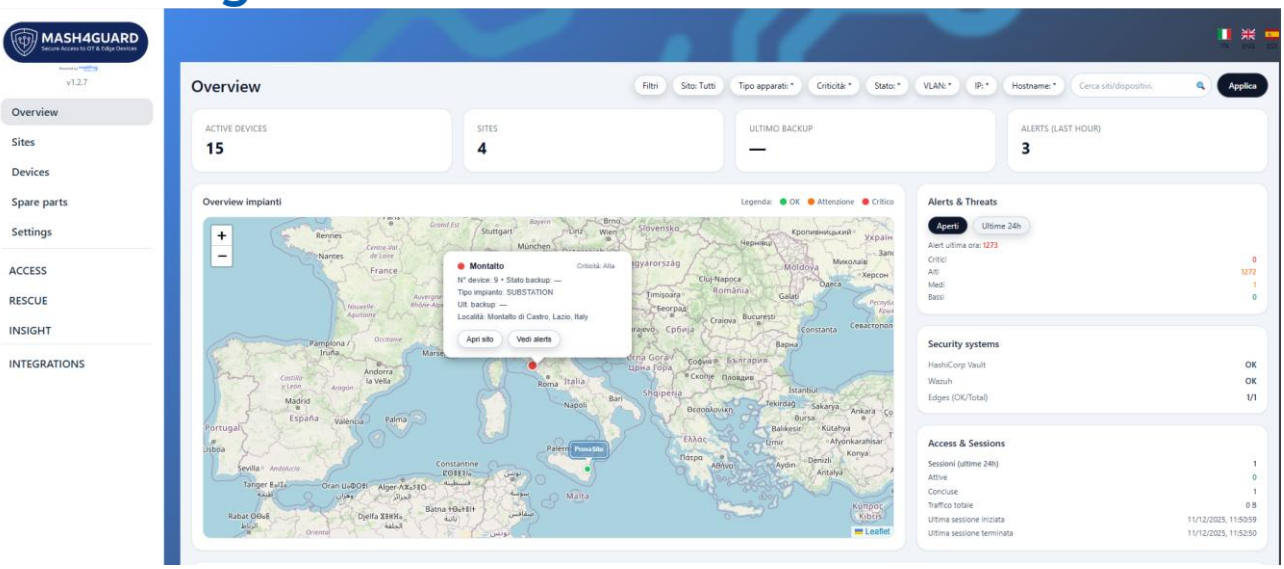

Figura 1- Dashboard Unificata

4.2 Modulo ACCESS

Il modulo **ACCESS** si occupa della gestione sicura degli accessi privilegiati agli impianti e ai sistemi OT, fungendo da punto di ingresso unico per operatori interni, manutentori e fornitori esterni. Si integra nativamente con i principali servizi di identità e directory come Active Directory, LDAP ed Entra ID, sfruttando SSO aziendale, autenticazione a più fattori e passkey/WebAuthn per legare ogni accesso a una identità forte e verificata.

L'accesso agli impianti non avviene più tramite connessioni dirette o credenziali condivise, ma attraverso un gateway Edge che agisce come session broker: l'utente si autentica sulla piattaforma, richiede l'accesso a uno specifico asset OT e, solo in caso di autorizzazione positiva, viene aperta una sessione controllata (es. RDP, SSH, VNC, accesso web) dall'Edge verso il dispositivo. Le credenziali tecniche restano gestite e custodite dalla piattaforma, evitando la loro esposizione a operatori e terze parti e riducendo il rischio di uso improprio.

Il controllo è granulare e basato sui ruoli (RBAC), con possibilità di definire scope temporali, finestre di manutenzione, separazione dei compiti (SoD) e, ove richiesto, workflow di approvazione (es. apertura accessi solo se associati a un ticket o a un change autorizzato). Ogni sessione può essere tracciata e, dove previsto, registrata, generando log dettagliati su chi ha fatto cosa, quando e su quali apparati.

Il valore principale risiede nella possibilità di avere sempre un quadro chiaro e centralizzato degli accessi agli impianti OT, riducendo drasticamente il rischio di accessi non autorizzati o

Sede legale
Via G. Peroni, 400/402
00131 - Roma
C.F. e P.IVA 02534640905

info@mashfrog.com
www.mashfrog.com

non tracciati. Un sistema di logging e audit robusto fornisce inoltre le evidenze necessarie per la compliance e per la rendicontazione verso auditor interni ed esterni.

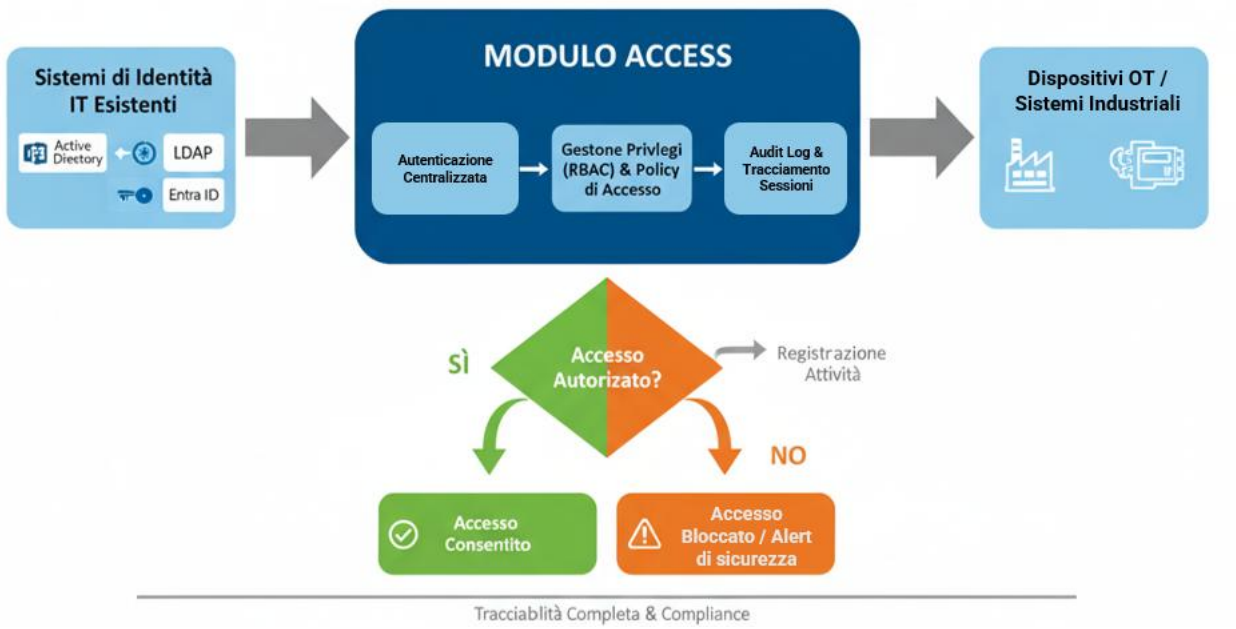

Figura 2 – Access process

4.3 Modulo INSIGHT

Il modulo **INSIGHT** raccoglie e analizza in tempo reale il traffico delle reti OT, fornendo una visibilità profonda sui flussi di comunicazione tra PLC, SCADA, HMI, apparati di rete e sistemi di supervisione. La soluzione si basa su sensoristica passiva installata sugli Edge Device, che sfrutta motori di ispezione avanzata (DPI) – come Suricata, Zeek e parser specifici per protocolli industriali – per decodificare i principali protocolli OT (es. Modbus, OPC-UA, Ethernet/IP, ecc.) e arricchire gli eventi con contesto operativo.

INSIGHT permette di costruire una mappa dinamica degli asset e delle loro relazioni, identificando quali dispositivi parlano con chi, su quali protocolli e con quali pattern di traffico. Su questa baseline vengono generati eventi e alert in caso di anomalie (nuovi device non censiti, variazioni improvvise dei flussi, comandi fuori standard, tentativi di accesso anomali) che possono essere filtrati e correlati per ridurre il rumore e concentrarsi sui fenomeni realmente significativi.

Grazie alla sua architettura aperta, INSIGHT si integra facilmente con i principali sistemi di **SIEM** già presenti in azienda (es. Wazuh, Splunk, QRadar, Microsoft Sentinel), permettendo di correlare gli eventi OT con quelli IT in un'unica vista. In questo modo, il team di sicurezza ottiene una comprensione completa del panorama delle minacce e può adottare use case e

Sede legale
Via G. Peroni, 400/402
00131 - Roma
C.F. e P.IVA 02534640905

info@mashfrog.com
www.mashfrog.com

playbook specifici per l'ambiente industriale (es. rilevazione di scanning su porte OT, comandi potenzialmente distruttivi, propagazione laterale da IT a OT).

INSIGHT diventa così il componente NDR/visibility della piattaforma OT: consente di passare da una visibilità parziale e frammentata a un monitoraggio continuo, strutturato e allineato ai requisiti di rilevazione, analisi e risposta previsti dagli standard di sicurezza per l'OT.

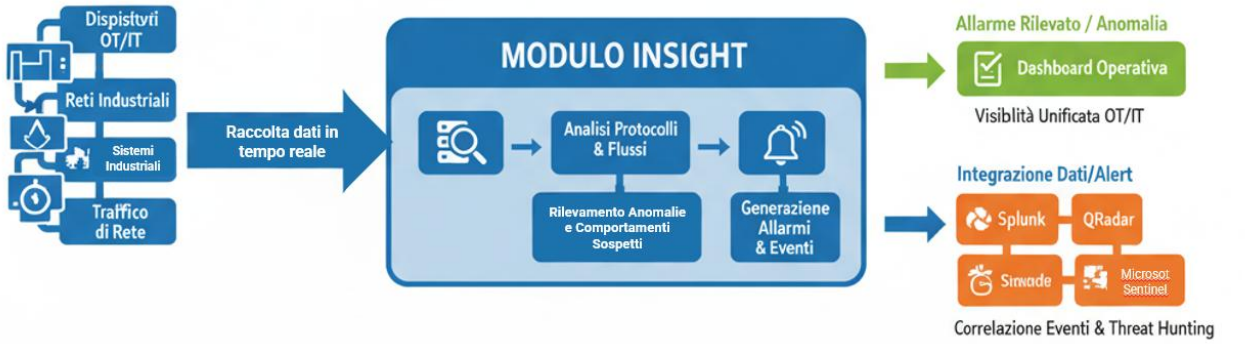

Figura 3 – Inspection Process

4.4 Modulo RESCUE

Il modulo **RESCUE** introduce un livello avanzato di gestione e protezione delle configurazioni, portando nell'ambiente OT i principi di Change Management, versioning e validazione continua tipici dei processi CI/CD del mondo IT. Il suo obiettivo è garantire la continuità operativa e la coerenza delle configurazioni su PLC, RTU, HMI, apparati di rete e sistemi di supervisione, prevenendo errori umani e modifiche non conformi che potrebbero compromettere la produzione. Il modulo nasce da un requisito cyber (integrità, tracciabilità, separazione dei compiti) che genera un impatto diretto e misurabile sulle operations (qualità dei change, tempi di ripristino, riduzione degli errori).

RESCUE agisce come orchestratore centrale di backup e configurazioni OT: le configurazioni vengono estratte in modo strutturato dagli apparati, archiviate in un repository versionato, correlate agli impianti e ai change associati. Questo consente di sapere in ogni momento quale versione di configurazione è in produzione, chi l'ha approvata e quali controlli sono stati eseguiti prima del rilascio.

Sede legale
Via G. Peroni, 400/402
00131 - Roma
C.F. e P.IVA 02534640905

info@mashfrog.com
www.mashfrog.com

Le principali funzionalità includono:

- **Editor di Regole e Policy**: definizione di criteri di configurazione standardizzati e policy di conformità per tutte le classi di dispositivi. Le regole agiscono come un processo di Change Management digitale, strutturando le modifiche prima che vengano applicate e garantendo che ogni operazione sia allineata con gli standard di sicurezza e operatività aziendali.
- **Gestione di Variabili e Range Consentiti**: ogni parametro configurabile (indirizzi IP, subnet, porte, time-out, settaggi di sicurezza, ecc.) può essere definito con valori ammessi o range numerici/logici. Questo assicura che tutte le impostazioni siano coerenti e compatibili, eliminando il rischio di configurazioni rischiose o non standard.
- **Validazione Automatica e Deployment Controllato**: prima dell'applicazione, ogni modifica viene automaticamente verificata rispetto alle regole definite. In caso di non conformità, il sistema blocca la modifica, genera un alert e mantiene attiva la configurazione precedente, prevenendo impatti negativi sull'operatività. La stessa logica abilita rollout progressivi (per linea, sito, cluster di apparati) con controlli pre e post change.

RESCUE trasforma la gestione delle configurazioni da attività manuale a processo controllato: ogni modifica è versionata, "lintata" da un Modulo di Validazione Sintattica dedicato, approvata da terza parte e rilasciata con evidenze firmate. In caso di anomalia o incidente, è disponibile un rollback sicuro alla baseline e, se necessario, il ripristino rapido di backup noti e validati.

In questo modo, RESCUE non agisce solo come un sistema di backup, ma come un vero e proprio Element Manager OT: l'Operatore lavora più veloce e con meno errori, l'ICT ottiene controllo e prove di conformità. Stesso processo, due benefici: continuità e controllo.

Sede legale
Via G. Peroni, 400/402
00131 - Roma
C.F. e P.IVA 02534640905

info@mashfrog.com
www.mashfrog.com

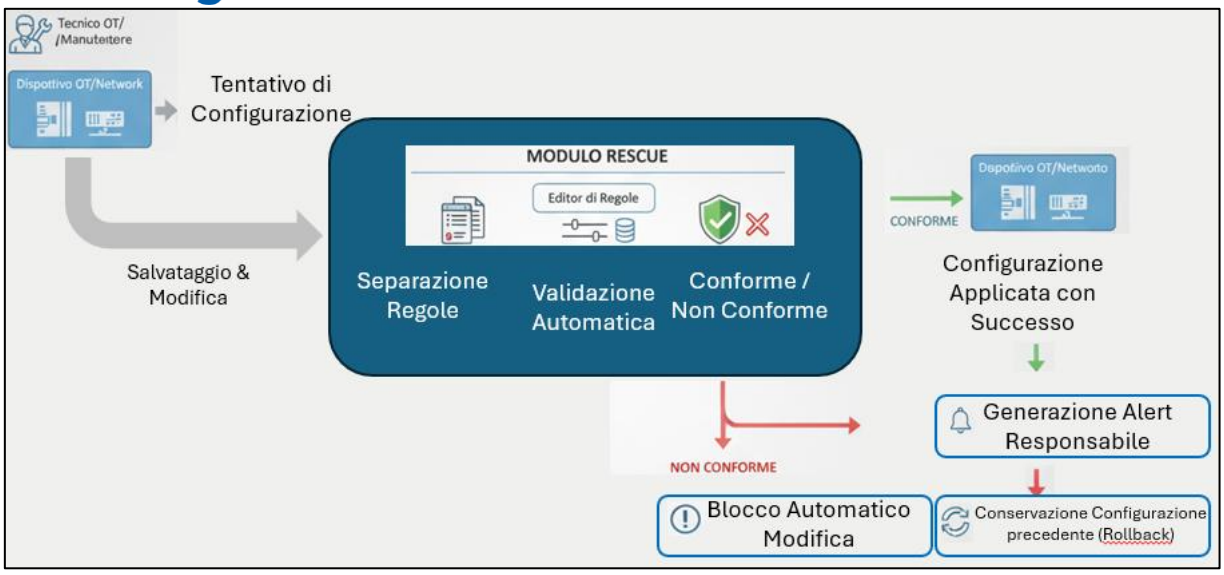

Figura 4 – Configuration/Versioning Management process

RESCUE è l'**Element Manager OT** che porta la disciplina di CI/CD alle configurazioni d'impianto: l'Operatore lavora più veloce e con meno errori, l'ICT ottiene controllo e prove di conformità. Stesso processo, due benefici: continuità e controllo.

5. Integrazione con sistemi esterni

La nostra piattaforma è progettata con un'architettura aperta e modulare, che non mira a sostituire i sistemi esistenti, ma a potenziarli e a estenderne le funzionalità. Grazie all'uso di **API** e connettori standard, la soluzione si integra in modo nativo e bidirezionale con gli strumenti già presenti nell'ecosistema IT e OT. Questo approccio permette di massimizzare il valore gli investimenti pregressi e di abilitare flussi di lavoro più sicuri, coerenti ed efficienti.

Sede legale
Via G. Peroni, 400/402
00131 - Roma
C.F. e P.IVA 02534640905

info@mashfrog.com
www.mashfrog.com

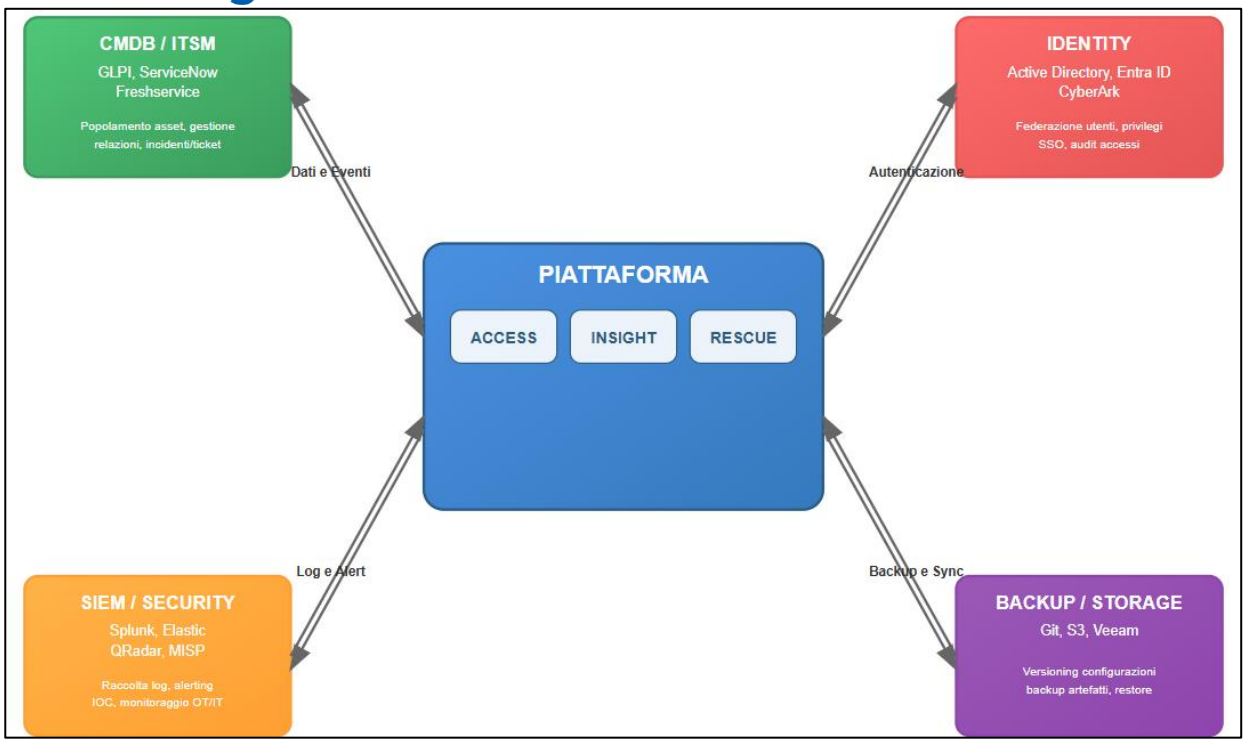

Figura 5- Integrazione con i sistemi esterni

Il punto di forza della nostra architettura risiede nella sua capacità di agire come un ponte tra mondi tecnologici diversi. In questo modo si permette l'utilizzo di strumenti già in essere, arricchendo i flussi di lavoro con dati specifici dell'ambiente OT. Tutto questo avviene tramite **API standard**, **webhook** e **connettori nativi**, garantendo che i flussi operativi esistenti non vengano interrotti.

L'integrazione con sistemi esterni, come i CMDB/ITSM, consolida l'inventario degli asset e automatizza i processi di gestione. Allo stesso modo, la connessione ai sistemi di Identity Management e SIEM potenzia la postura di sicurezza complessiva, fornendo visibilità unificata e controllo centralizzato. Infine, l'integrazione con i sistemi di Backup e Storage assicura la resilienza e la continuità operativa, elementi cruciali in qualsiasi ambiente industriale.

6. Deliverable

Al completamento dell'implementazione saranno consegnati i deliverable tecnici e operativi previsti (documentazione, configurazioni, runbook ed evidenze di collaudo), necessari a una gestione autonoma e sicura dell'ambiente OT.

Sede legale
Via G. Peroni, 400/402
00131 - Roma
C.F. e P.IVA 02534640905

info@mashfrog.com
www.mashfrog.com

Deliverable	*Descrizione*
Report di Assessment e Inventario Asset	Documento dettagliato che evidenzia lo stato attuale degli asset OT/IT/IoT, la loro classificazione, le vulnerabilità riscontrate e le raccomandazioni per il miglioramento.
Dashboard Operativa Funzionale	Un'interfaccia attiva e popolata con i dati in tempo reale del sito pilota, pronta per il monitoraggio, l'analisi e la gestione centralizzata.
Piattaforma e Moduli Operativi	La piattaforma completa, con i moduli **ACCESS**, **INSIGHT** e **RESCUE**, implementata e collaudata sul sito pilota, pronta per l'uso quotidiano.
Report di Validazione Configurazioni	Un resoconto che certifica l'efficacia del processo di versioning e validazione (tipo CI/CD), dimostrando la sicurezza e la coerenza delle configurazioni applicate.
Training Operativo e Manuale d'Uso	Sessioni di formazione dedicate per il personale IT e OT, accompagnate da un manuale dettagliato per garantire una piena autonomia nell'utilizzo della piattaforma.

Sede legale
Via G. Peroni, 400/402
00131 - Roma
C.F. e P.IVA 02534640905

info@mashfrog.com
www.mashfrog.com

7. Architettura logica e diagramma high-level

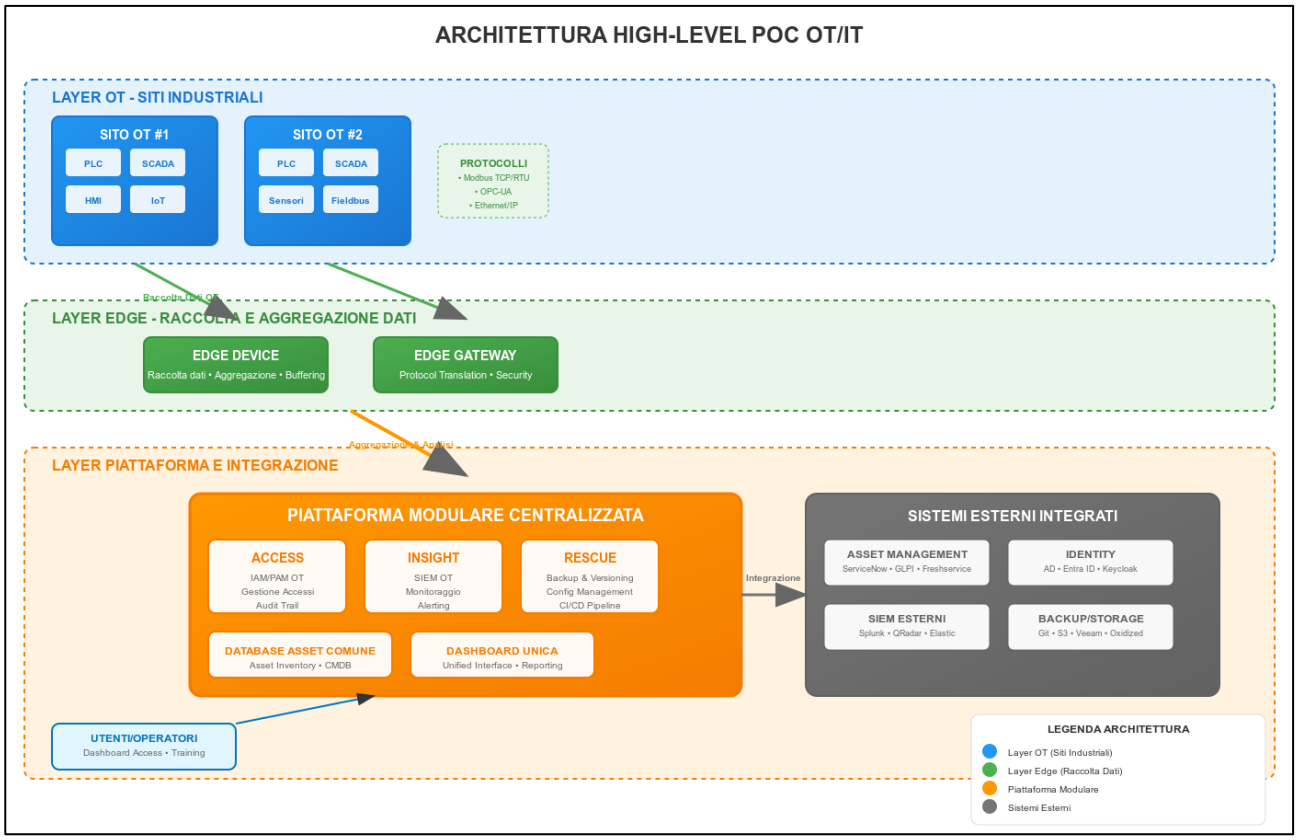

Figura 6 – High-Level Diagram

Il diagramma mostra come la soluzione mediante la nostra piattaforma OT/IT opera direttamente sul sito industriale. Nei **siti OT** (layer **blu**), le macchine, i PLC, gli SCADA e i sensori IoT generano dati costantemente durante le operazioni quotidiane.

Questi dati vengono raccolti dagli **Edge Device** (layer **verde**), dispositivi posizionati localmente che aggregano il traffico dei macchinari, traducono i protocolli industriali (come Modbus e OPC-UA) e garantiscono che le informazioni siano sicure e pronte per l'elaborazione.

Dal layer Edge, i dati vengono inviati alla **Piattaforma Modulare centrale** (layer **arancione**), dove i moduli ACCESS, INSIGHT e RESCUE permettono rispettivamente di gestire gli accessi, monitorare l'infrastruttura OT, applicare backup e versioning delle configurazioni.

La piattaforma dispone di un **database comune degli asset** e di una **dashboard unica**, che offre agli operatori una visione completa e aggiornata dello stato degli impianti. Infine, la piattaforma si integra con **sistemi esterni** come strumenti di gestione degli asset, identità, SIEM o soluzioni di backup, consentendo sincronizzazione e interoperabilità con l'IT aziendale.

Sede legale
Via G. Peroni, 400/402
00131 - Roma
C.F. e P.IVA 02534640905

info@mashfrog.com
www.mashfrog.com

In pratica, il flusso operativo è chiaro: i dati nascono nel sito OT, vengono raccolti e preparati dall'Edge, analizzati e gestiti dalla piattaforma, e infine integrati con i sistemi esterni, permettendo agli operatori e ai responsabili di avere sempre informazioni affidabili, in tempo reale, senza interrompere la produzione.

8. Roadmap

La piattaforma implementata definisce la baseline tecnica per la gestione della sicurezza e dell'operatività dell'ambiente OT. Gli esiti della fase pilota abilitano l'estensione a un modello multi-sito, con applicazione uniforme delle policy, standardizzazione dei processi e visibilità centralizzata sull'insieme degli impianti.

Le evolutive previste comprendono l'estensione multi-sito con scalabilità dei collector e templatizzazione delle policy; l'automazione dei change (canary deploy, progressive rollout); l'ampliamento della libreria di regole DPI con supporto a protocolli aggiuntivi (TBD); l'evoluzione dell'API alla versione 2 con meccanismi di subscription, query avanzate ed export in formati aggiuntivi; e il miglioramento di HA/DR con riduzione di RPO/RTO e ottimizzazione dello storage.

La nostra roadmap futura prevede:

- **Espansione Multi-sito**: Replicare il modello di successo in altri siti produttivi.
- **Evoluzione a Soluzione di Produzione**: Transizione del sistema verso un'infrastruttura di produzione completa, con un piano di manutenzione e aggiornamento continuo.
- **Supporto Continuativo**: Offerta di servizi di supporto tecnico e consulenza per massimizzare il ritorno sull'investimento nel lungo termine.

Figura 7 - Prossimi Passi & Benefici

Sede legale
Via G. Peroni, 400/402
00131 - Roma
C.F. e P.IVA 02534640905

info@mashfrog.com
www.mashfrog.com

9. Allineamento normativo (NIS 2 / IEC 62443)

La piattaforma OT proposta è progettata per supportare concretamente l'adozione delle principali normative e linee guida in ambito industriale:

- la Direttiva NIS 2 e il relativo recepimento nazionale, con particolare riferimento agli obblighi di gestione del rischio, controllo degli accessi, monitoraggio continuo e gestione degli incidenti;
- le serie di standard IEC 62443, che definiscono requisiti per sistemi di automazione e controllo industriale, con focus su gestione degli accessi, protezione delle comunicazioni, gestione delle configurazioni e capability di ripristino.

Il contributo della piattaforma è organizzato attorno ai tre moduli ACCESS, INSIGHT e RESCUE, che fungono da "mattoni" tecnologici a supporto dei controlli richiesti dalle normative.

9.1 Approccio generale

Dal punto di vista normativo, la piattaforma non si limita a introdurre nuove tecnologie, ma struttura i processi OT in chiave "cyber by design":

- governance: tracciabilità di accessi, modifiche configurative e attività manutentive su impianti e reti OT;
- misure tecniche: autenticazione forte, segregazione dei percorsi di accesso, monitoraggio passivo, gestione centralizzata dei backup e delle configurazioni;
- evidenze e audit: produzione automatica di log, report e baseline che costituiscono la base documentale per audit interni, ispezioni e verifiche di conformità.

Ne deriva un allineamento naturale ai requisiti di NIS 2 e ai principi IEC 62443 relativi a gestione del rischio, defence in depth e separazione tra control plane e data plane.

9.2 Contributo del modulo ACCESS

ACCESS indirizza i requisiti relativi a identità, accessi privilegiati e tracciabilità:

- Autenticazione e gestione delle identità degli utilizzatori
  - integrazione con IdM/SSO aziendale (AD, Entra ID, LDAP);
  - uso di passkey/WebAuthn e MFA per gli accessi agli impianti;
  - riduzione delle credenziali locali sugli asset OT a favore di un access broker centralizzato.

Sede legale
Via G. Peroni, 400/402
00131 - Roma
C.F. e P.IVA 02534640905

info@mashfrog.com
www.mashfrog.com

- Gestione e registrazione degli accessi remoti privilegiati sugli asset
  - session broker basato su gateway Edge, che apre le sessioni solo dopo verifica di identità e autorizzazioni;
  - binding tra sessione, identità, asset coinvolti e motivazione (ticket, change, intervento manutentivo).
- Separazione dei ruoli e dei compiti (SoD)
  - definizione di ruoli distinti per operatori, manutentori, amministratori OT/IT e service provider;
  - possibilità di introdurre approvazioni a più livelli per gli accessi più critici.
- Logging, advisory e gestione delle vulnerabilità
  - generazione di log di accesso completi, esportabili verso SIEM e sistemi di audit;
  - integrazione con strumenti di ticketing/ITSM per collegare accessi e change a piani di remediation e gestione vulnerabilità.

In questo modo **ACCESS** contribuisce in modo diretto ai controlli su gestione identità e accessi, logging e accountability richiesti da NIS 2, ACN e IEC 62443.

9.3 Contributo del modulo INSIGHT

INSIGHT risponde ai requisiti di monitoraggio, rilevazione delle minacce e logging centralizzato:

- Monitoraggio continuo degli asset OT e dei flussi di comunicazione
  - sensoristica di rete passiva basata su motori DPI, installata sugli Edge;
  - discovery e mappatura dinamica di dispositivi, linee, celle e protocolli industriali.
- Registrazione ed analisi dei log e degli eventi OT
  - normalizzazione degli eventi di rete OT e invio verso SIEM;
  - correlazione con eventi IT per una vista integrata delle minacce;
  - costruzione di baseline comportamentali con cui confrontare nuove attività.
- Rilevazione delle minacce e meccanismi di alert
  - regole e use case specifici per l'OT (comandi anomali, scanning, nuovi device, deviazioni dai flussi attesi);
  - alert verso SOC/CSIRT o verso i referenti OT per azioni di risposta coordinate.

Sede legale
Via G. Peroni, 400/402
00131 - Roma
C.F. e P.IVA 02534640905

info@mashfrog.com
www.mashfrog.com

INSIGHT abilita il passaggio da un monitoraggio manuale e parziale a un sistema strutturato di logging e detection, in linea con i requisiti di NIS 2 e ACN su monitoraggio continuo, rilevazione degli incidenti e segnalazione tempestiva, e con i requisiti IEC 62443 relativi alla protezione delle comunicazioni e al rilevamento di condizioni anomale.

9.4 Contributo del modulo RESCUE

RESCUE copre i requisiti relativi a gestione delle configurazioni, integrità e capacità di ripristino:

- Backup centralizzato delle configurazioni OT
  - estrazione e archiviazione delle configurazioni di PLC, RTU, HMI, switch, firewall, ecc.;
  - repository versionato, con tracciabilità di chi ha effettuato l'ultima modifica e quando.
- Ottimizzazione del change management
  - workflow strutturati di proposta, validazione, approvazione e deployment delle modifiche;
  - controlli automatici di conformità rispetto a regole e policy aziendali prima dell'applicazione dei change.
- Preservazione dell'integrità delle configurazioni
  - validazione sintattica e logica (linting) delle configurazioni;
  - separazione dei compiti tra chi propone, chi approva e chi applica le modifiche;
  - evidenze storiche che consentono di dimostrare che la configurazione "in produzione" è nota e sotto controllo.
- Soluzioni di ripristino (recovery)
  - possibilità di rollback rapido a una configurazione baseline nota in caso di errore o incidente;
  - supporto ai piani di continuità operativa e disaster recovery per l'ambiente OT.

Queste funzionalità rispondono direttamente ai requisiti di NIS 2 e ACN su backup, continuità operativa e gestione delle configurazioni, e agli obiettivi IEC 62443 relativi a gestione del ciclo di vita degli asset, security levels e protezione contro modifiche non autorizzate.

Sede legale
Via G. Peroni, 400/402
00131 - Roma
C.F. e P.IVA 02534640905

info@mashfrog.com
www.mashfrog.com

9.5 Sintesi di copertura

In sintesi:

- **ACCESS** fornisce il “pilastro identità e accessi”, rendendo gli accessi remoti OT fortemente autenticati, autorizzati, tracciati e riconducibili a persone e processi aziendali.
- **INSIGHT** realizza il “pilastro visibilità e monitoraggio”, garantendo logging, detection e capacità di analisi dei flussi OT integrata con il SOC aziendale.
- **RESCUE** introduce il “pilastro configurazioni e resilienza”, trasformando backup e change OT in processi controllati, versionati e verificabili.

L’adozione congiunta dei tre moduli permette all’organizzazione di dimostrare un livello di maturità coerente con i requisiti di NIS 2, con le misure tecniche e organizzative indicate da ACN e con i principi di sicurezza descritti nella serie IEC 62443, costruendo un framework di sicurezza industriale solido, sostenibile e auditabile.

Sede legale
Via G. Peroni, 400/402
00131 - Roma
C.F. e P.IVA 02534640905

info@mashfrog.com
www.mashfrog.com