Admin By Request

PRIVILEGE MANAGEMENT FOR THE MASSES

Endpoint Privilege Manager (EPM) Specifiche | Windows Edition Version 8

Introduzione a Admin By Request

La soluzione EPM potente e altamente compatta per Workstation e Server Windows. Costruita sull'ampia esperienza di FastTrack Software nella scrittura di applicazioni di rete altamente robuste, portatili e potenti, Admin By Request è semplice da implementare, facile da usare ed è adatto ad organizzazioni di tutte le dimensioni. Admin By Request consente ai reparti IT di identificare l'uso dei diritti di amministratore locale, automatizzare la revoca dei diritti e sostituire l'uso permanente non verificato dei diritti di amministratore con un sistema di elevazione dei privilegi semplice da utilizzare su richiesta o con limiti temporali, con un tracciato completo delle attività. Con Admin By Request, i lavoratori in ufficio o remoto possono svolgere in modo sicuro attività che in passato avrebbero richiesto ticket di supporto e prezioso tempo dell'helpdesk. Operazioni con diritti elevati come la configurazione delle stampanti, l'installazione/rimozione di software approvati e la gestione dei plugin possono essere tutte svolte in modo sicuro dagli utenti, massimizzando la produttività pur mantenendo piena conformità al framework di sicurezza.

Cosa è Admin By Request?

Admin By Request EPM è composto da 2 parti:

L' Agent è installato sull' Endpoint in locale (Windows, Mac e Linux). Questo Agent avvia richieste di elevazione ed esegue carichi di lavoro per l'elevazione. Se è Online, l'endpoint comunica le informazioni configurate al portale (ad esempio, log, richieste e impostazioni). Affinchè la soluzione funzioni, la comunicazione con il portale di gestione non è obbligatoria.

Il Portale di gestione: è un ambiente sicuro e gestito, ospitato su Microsoft Azure, in classe enterprise, su cui vengono raccolte le impostazioni degli Agent, l'inventario dei computer e le richieste del Workflow di elevazione. Il portale amministra anche le funzionalità della App mobile e delle API.

Admin By Request non richiede infrastrutture aggiuntive in locale (server, appliance VM, database, ecc.), tutto ciò che devi fare per avviare un POC (proof of concept) è registrarti al nostro piano gratuito, che ti offre una esperienza del prodotto completa per un massimo di 25 endpoint, gratuitamente, per sempre.

FUNZIONALITA' PRINCIPALI

Gestione dei privilegi

- Riduzione della capacità di diffusione di malware e ransomware
- Revoca automatica dei diritti di amministratore locale con esclusioni utente specifiche
- Modalità di elevazione dei privilegi per app o limitate nel tempo
- Modalità selezionabili senza driver o con assistenza del driver per l'elevazione
- Opzioni di elevazione O365/SAML MFA
- Possibilità di bloccare i diritti di amministratore locale per il proprietario del dispositivo, lo stato di conformità di Intune, applicazioni specifiche (posizione del file, certificato del fornitore o checksum del file)
- Integrazione con OPSWAT Meta Defender per il controllo preventivo della reputazione 'in line' prima dell'elevazione
- Funzione 'Break Glass' (soluzione LAPS potenziata). Genera account amministrativi completi a uso singolo e limitati nel tempo con un click.

Controllo e Reportistica

- Soluzione di inventario potente inclusa di serie
- Registro completo delle attività di elevazione dell'utente, accessi amministrativi e installazioni di software
- Generazione di report programmabili sull'attività chiave degli utenti
- Accesso API ai registri di audit, registri delle richieste, codici PIN, eventi di sicurezza e inventario per SIEM e segnalazione esterna
- Registro completo delle impostazioni di tutte le modifiche alla configurazione del portale

Semplicità

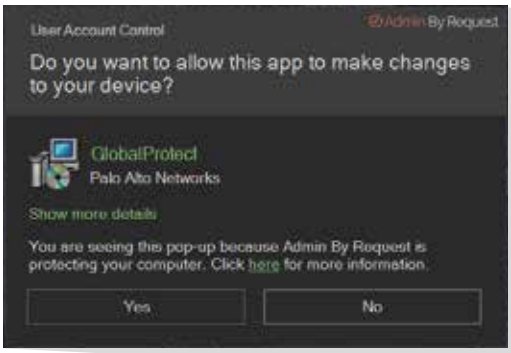
- Supporto simultaneo per endpoint senza AD, multidominio Active Directory e Azure Active Directory
- Non è necessaria un'Appliance o installare software sull'infrastruttura server: la soluzione è basata solo sugli Endpoint
- ZeroConfig, installer su Endpoint inferiore a 2 MB: si installa utilizzando gli strumenti di distribuzione standard (SCCM/Intune)
- Gestione delle richieste di elevazione dei privilegi da smartphone tramite App gratuita.
- Funzionamento sia online che offline (approvazione con codice PIN)

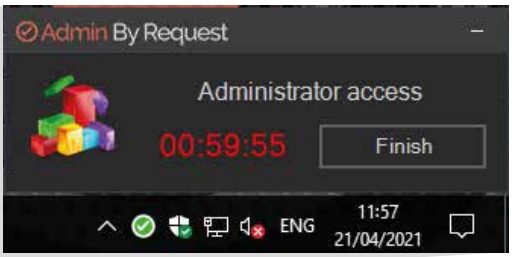
Edizioni del Prodotto

CARATTERISTICHE	SKU	MAX. ENDPOINTS	MODELLO DI LICENZA	SISTEMI OPERATIVI SUPPORTATI	SUPPORTO
Free Plan (solo Workstation)	N/A	25	Gratuito	Windows 7 e succ. Mac O/S 10.8 e succ.. Ubuntu 20.04 LTS / 22.04 LTS e Red Hat Enterprise 9 (RHEL9)	No
Admin By Request Workstation	ABR-WKS	Illimitato	Sottoscrizione annuale	Windows 7 e succ. Mac O/S 10.8 e succ.. Ubuntu 20.04 LTS / 22.04 LTS e Red Hat Enterprise 9 (RHEL9)	Incluso
Admin By Request Server	ABR-SRV	Illimitato	Sottoscrizione annuale	Windows Server 2008R2 e succ.	Incluso

'Run as admin' per app in Sandbox Elevazione dei Privilegi

Con la modalità di elevazione "Run As Admin", gli utenti possono avviare singole applicazioni e eseguirle con diritti elevati su richiesta o con approvazione manuale, se necessario. Quando un'applicazione avviata viene elevata, il resto del sistema rimane in uno stato di non elevazione. Poiché le richieste vengono elaborate una alla volta, questa modalità è più adatta per gli utenti che necessitano di elevazioni ad hoc per un tempo limitato. Poiché la modalità "Run As Admin" viene attivata facendo clic destro su un'applicazione e selezionando "Run As Admin", ciò riproduce il comportamento standard di Windows e quindi non richiede alcuna formazione aggiuntiva per gli utenti.





Elevazione dei permessi in una sessione a Tempo

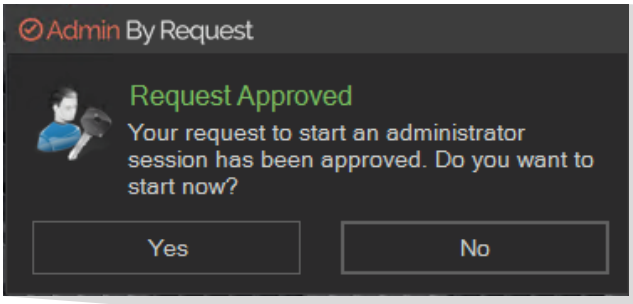
La modalità sessione amministrativa viene attivata selezionando "Richiedi accesso amministratore" tramite l'icona di controllo a forma di spunta di Admin By Request presente nella barra delle applicazioni (Windows) o nel Menù (Mac).
Con l'approvazione abilitata, un amministratore del portale deve elaborare la richiesta di sessione amministrativa come parte del flusso di elevazione.
Con l'approvazione disabilitata, l'utente può avviare automaticamente la sessione amministrativa e diventare un amministratore a tempo limitato con un registro completo delle azioni. La modalità sessione amministrativa è ideale per utenti come sviluppatori che necessitano della libertà di eseguire più applicazioni elevate entro un determinato periodo di tempo. Una volta che l'utente interrompe il timer o il tempo scade, i dettagli relativi alla sessione (processi eseguiti, software installato/rimosso) vengono trasferiti e sono visibili sul portale.

OPSWAT MetaDefender completamente integrato

Questa innovativa funzione consente un controllo prima di elevare i permessi, per le modalità di elevazione "Run As Admin" e "Admin Session". Quando questa funzione è attivata, la reputazione dei file assicura che tutte le operazioni di elevazione dell'utente, sia con che senza approvazione, vengano verificate attraverso oltre 20 motori di Antivirus di fornitori leader di settore, in linea e in tempo reale.
Se i punteggi dei controlli risultano sospetti o dannosi, la richiesta di elevazione viene negata direttamente o posta in quarantena per la revisione del tuo team di sicurezza.
La funzione OPSWAT MetaDefender è completamente integrata all'interno dell'agente di Admin By Request e non interferisce in alcun modo con i tuoi prodotti di sicurezza degli endpoint esistenti.

Modalità di approvazione

Le richieste di elevazione possono essere approvate tramite il portale di gestione, l'app mobile o addirittura tramite API se abilitata. Quando una richiesta viene gestita selezionando il pulsante Approva o Nega, l'utente richiedente riceverà l'esito della richiesta tramite e-mail e/o notifica desktop.
Le integrazioni out-of-the-box con MS Teams, Slack, ServiceNow e Jira consentono l'invio di notifiche di approvazione a gruppi utilizzando applicazioni alternative di collaborazione o di ticketing.



Approvazione Automatica per applicazioni specifiche (pre-approvazione)

Per situazioni in cui desideri richiedere l'approvazione per le applicazioni sconosciute ma vuoi attivare l'elevazione automatica per applicazioni specifiche, puoi utilizzare la funzionalità di "pre-approvazione".
Con la pre-approvazione delle applicazioni, un amministratore del portale può impostare delle politiche generali o per Gruppo di utenti, basate su diversi tipi di regole, come la posizione dei file (condivisione di rete), il certificato del fornitore sull'applicazione o controlli specifici. Le regole delle applicazioni possono anche essere configurate per richiedere all'utente di fare clic su una casella "sì/no" durante l'elevazione, oppure senza conferma dell'utente, il che consente l'elevazione dell'utente "non assistita". La modalità di elevazione non assistita può essere utile in situazioni in cui le applicazioni necessitano di elevazione senza l'input dell'utente, come durante l'avvio del sistema o per uno script eseguito dall'utente.
Le elevazioni per le applicazioni pre-approvate non vengono inviate attraverso il sistema opzionale di controllo della reputazione OPSWAT MetaDefender.

Pre-approvazione tramite Machine Learning per applicazioni specifiche

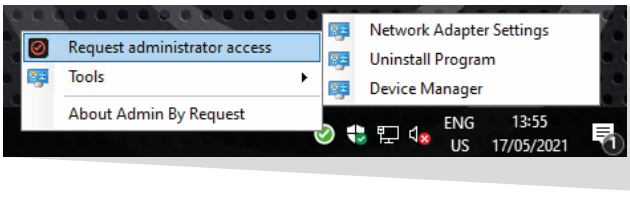
Quando sia l'Approvazione che il Machine Learning sono abilitati, l'amministratore del portale può definire una soglia sopra la quale le applicazioni approvate manualmente vengono apprese automaticamente. Ad esempio, impostando la soglia di Machine Learning su 'tre' fa in modo che un'applicazione debba essere approvata manualmente per tre volte: dalla quarta richiesta di elevazione non è più necessaria l'approvazione manuale.
Il Machine Learning, come la Pre-Approvazione, è una funzione configurata come Gruppo, il che significa che possono essere configurate diverse soglie di Machine Learning.
Le applicazioni apprese possono in seguito essere individualmente "dimenticate" se non si desidera più consentire agli utenti di ottenere l'approvazione automatica.
Nota: A differenza delle applicazioni Pre-Approvate, quelle apprese tramite Machine Learning sono comunque soggette a regole di blocco OPSWAT e di blocco dell'applicazione.

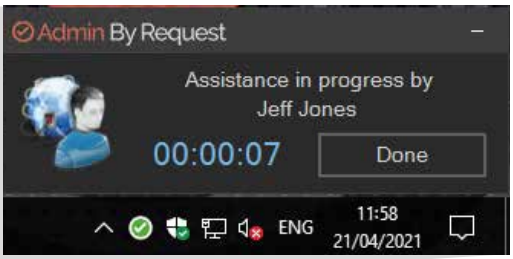
Approvazione pre-appresa tramite AI: intelligenza artificiale per applicazioni che superano i punteggi dell'applicazione o del venditore.

A tutte le applicazioni elevate con Admin By Request vengono assegnati sia un Punteggio di Popolarità dell'Applicazione, che un Punteggio di Popolarità del Fornitore. L' Approvazione tramite Intelligenza Artificiale consente all'amministratore del portale di impostare soglie, per Gruppi, sopra le quali le applicazioni possono essere elevate automaticamente a seconda del punteggio specifico dell'applicazione o del punteggio del fornitore. Abilitando sia le soglie dell'applicazione che del fornitore verrà considerata la più bassa delle due.
Come le regole di Machine Learning, le Approvazioni tramite Intelligenza Artificiale sono comunque soggette a regole di blocco OPSWAT e di blocco dell'applicazione.

Tray Tools

I componenti del pannello di controllo di Windows 10 come Gestione dispositivi, Configurazione di rete e Guida Aggiungi Stampante possono essere eseguiti con privilegi elevati utilizzando la nostra funzione Tray Tools, con la quale gli utenti possono eseguire operazioni comuni di configurazione di sistema come cambiare l'indirizzo IP, senza la necessità di fornire diritti elevati all'intero sistema.





Assistenza al Supporto (solo edizione Workstation)

La funzione di Assistenza al Supporto consente a un utente con diritti superiori di Admin By Request e accesso alle funzionalità, di eseguire un aggiornamento temporaneo dei diritti di Admin By Request. Ad esempio, se a un utente non è stata data l'autorizzazione ad elevare i file di sistema di Windows con Admin By Request, o se non è stato concesso il diritto di avviare una sessione amministrativa completa senza richiedere l'approvazione manuale, un utente del servizio di assistenza IT potrebbe trovare la configurazione dell'utente troppo restrittiva per lavorare e risolvere i problemi di sistema.
Utilizzando la funzione di Assistenza al Supporto di Admin By Request, l'utente del servizio di assistenza IT può temporaneamente trasferire i propri diritti di Admin By Request all'utente connesso, consentendo quindi di elevare i file di sistema e avviare sessioni senza dover attendere l'approvazione. Le sessioni di Assistenza al Supporto sono "registrate congiuntamente" nel portale, quindi i dettagli sia dell'utente (proprietario) del sistema che i dettagli dell'utente che ha avviato la sessione di Assistenza, sono mostrati insieme nel registro degli eventi. Perché l'Assistenza al Supporto funzioni appieno, lo staff dell'Helpdesk non dovrebbe essere autorizzato permanentemente come amministratori (ad esempio, facendo parte degli amministratori di dominio). La modalità di Assistenza al Supporto è progettata per essere utilizzata da utenti non privilegiati. Ciò consente di revocare non solo i diritti di amministratore agli utenti, ma anche allo staff dell'Helpdesk.

Break Glass (LAPS potenziato)

La funzionalità Break Glass, integrata in Admin By Request, in modo semplice e con singolo Click, rende disponibile per qualsiasi Endpoint, un utente amministratore locale completo, a tempo limitato e ad uso singolo. Essendo un utente amministratore locale, gli account Break Glass non dipendono da un'AD funzionante o da una registrazione di Entra ID. La generazione degli account Break Glass viene registrata nel portale e tutti i processi elevati con un account Break Glass vengono anche registrati negli audit log.
lo scenario d'uso tipico per l'utilizzo della funzione Break Glass è se un utente risulta disconnesso/deregistrato da una directory senza più un account amministratore abilitato sull'endpoint.

Pre-Revoca: log per gli utenti amministratori

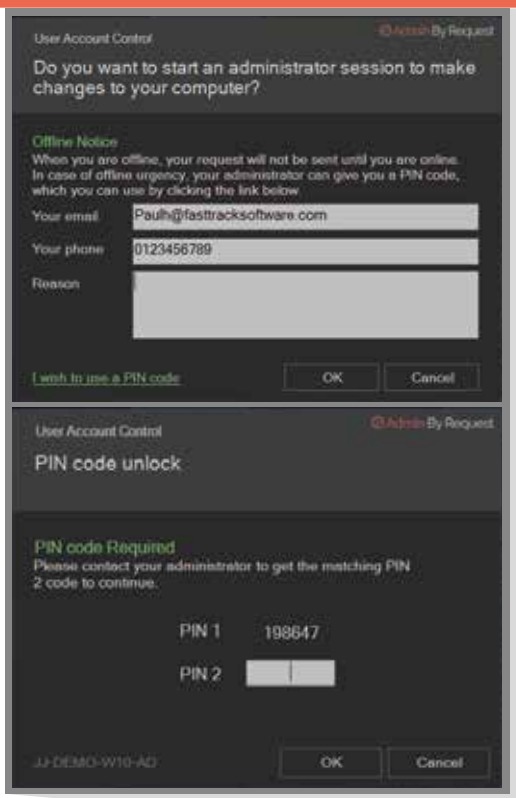
Implementare Admin By Request per gli utenti che sono amministratori permanenti, senza abilitare la funzione di revoca, consentirà di registrare l'attività di elevazione senza modificare l'esperienza dell'utente nell'uso del computer come amministratore. L'utente non noterà alcuna differenza nell'utilizzo del suo computer come amministratore e non vedrà alcuna richiesta di Admin By Request. Utilizzare il logging di Pre-Revocation è una tecnica ideale per la fase iniziale di implementazione/ricerca in ambienti in cui non si sa cosa stiano facendo gli utenti con i loro attuali diritti amministrativi. Una volta che l'attività di elevazione delle applicazioni è "registrata", le applicazioni possono essere facilmente pre-approvate, importate nel database di Machine Learning o bloccate. Un rapporto di tutta l'attività di elevazione è anche facilmente esportabile per scopi di audit.

Segmentazione degli Asset e delega del Flusso di Lavoro

All'interno del portale è possibile raggruppare e filtrare gli asset per dipartimento al fine di delegare l'elaborazione delle richieste. Gli endpoint di Admin By Request che richiedono impostazioni diverse (rispetto alle impostazioni predefinite globali) possono essere raggruppati in un numero illimitato di "Sub Settings" configurati nel portale. Ad esempio, diversi dipartimenti possono essere impostati con diversi destinatari di posta elettronica per le richieste di elevazione.
Il portale può essere configurato con diversi account amministrativi con la possibilità di settare dei limiti in modo che ogni utente amministrativo possa visualizzare solo gli asset per lui rilevanti.

Computer Offline

Admin By Request funziona allo stesso modo sia che il computer sia online che offline. Le impostazioni del portale vengono memorizzate nella cache sul client, quando il computer è offline i log di elevazione vengono memorizzati localmente sul client e sincronizzati con il portale quando il client è nuovamente online. Se un utente richiede un'approvazione manuale e il suo computer è offline, può ottenere un codice PIN temporaneo specifico per un'azione contattando un amministratore IT o un utente di help desk che abbia l'accesso al portale di generazione dei codici.. Ogni codice PIN è univoco e valido per una sola richiesta offline. E' possibile utilizzare una funzione API per abilitare la richiesta personalizzata di codici PIN e l'emissione tramite servizio REST. Quando l'utente torna online, i log di audit di qualsiasi attività di elevazione offline vengono sincronizzati nuovamente con il portale di gestione, garantendo che non vi siano interruzioni nell'auditing per mantenere la piena conformità.



Audit & asset tracking

Viene fornita una potente soluzione di tracciatura, Audit e Inventario, senza la necessità di ulteriori configurazioni.
Il sistema di Inventario fornisce una vista filtrabile di tutti i dispositivi dotati di Admin By Request, fornendo un report centralizzato di: software installati, hardware, utenti AD/AAD, gruppi di appartanenza.e utenze amministrative e relativi gruppi. I dati dell'inventario possono essere esportati tramite semplici pulsanti, oppure tramite API, nei formati PDF, XLS e CSV.

Prevenire gli abusi

Admin By Request è dotato di diverse funzionalità avanzate anti-manomissione per prevenire abusi e utilizzi impropri del prodotto. Una volta installato, Admin By Request è l'unico mezzo tramite il quale un utente può ottenere l'elevazione dei privilegi.
Come supplemento all'anti-manomissione, abilitiamo anche la presentazione di un messaggio di codice di condotta personalizzabile che può informare gli utenti della politica aziendale e che le loro azioni vengono verificate.
Non è possibile per l'utente disinstallare Admin By Request semplicemente utilizzando Admin By Request per ottenere pieni diritti amministrativi. La funzione di Proprietario del Dispositivo, quando configurata per il blocco, limita l'uso di Admin By Request specificamente al "proprietario" designato di quell' Endpoint.
Similmente alla funzione di Proprietario del Dispositivo, il blocco di conformità Intune impedisce all'utente di utilizzare Admin By Request se tale endpoint non è conforme, a seconda di come è stata configurata la conformità di Intune o in base a cosa costituisce la conformità per quell'Endpoint.

Disinstallazione con codice PIN

Admin By Request non può essere semplicemente disinstallato utilizzando i diritti amministrativi che il prodotto stesso concede. In una situazione in cui un utente deve rimuovere Admin By Request, la funzione di disinstallazione tramite codice PIN assicura che ciò possa essere fatto rapidamente, con un registro di verifica di chi ha emesso il codice di disinstallazione e quando il prodotto è stato disinstallato.
Per gli utenti Locali e di Azure AD, se Admin By Request è stato responsabile della revoca dei diritti di amministratore locale per l'utente, questi diritti vengono automaticamente ripristinati alla disinstallazione del prodotto.

Endpoint Privilege Manager (EPM) Specifiche
Windows Edition Version 8

IMPLEMENTAZIONE E DISTRIBUZIONE

IMPLEMENTAZIONE E DISTRIBUZIONE	DESCRIZIONE FUNZIONALITA'
Agent Thin (dimensione totale inferiore a 2 MB)	Implementazione semplice e rapida, ridottissime richieste di risorse
Interfaccia Endpoint Multilingua	Rilevamento automatico della lingua per Inglese, Francese, Tedesco, Spagnolo, Norvegese, Svedese e Danese.
Altamente Scalabile	Implementazione di oltre 80.000 endpoint
Personalizzazione dell' Endpoint	Logo aziendale e reparto sulla interfaccia dell'Endpoint
Zero Config con singolo file MSI	L'Agent si configura automaticamente per una semplice implementazione
Gestione basata su Servizio SaaS	Nessun impatto sulla infrastruttura / gestione centralizzata
Interfaccia di gestione intuitiva e facile da usare	Registra, implementa e utilizza in meno di 5 minuti.
Supporto nello stesso Tenant per Workgroup, AD, AZURE AD	Diverse opzioni di implementazione per tutte le situazioni
Nessuna Appliance richiesta	Minori apparecchiature da gestire e da considerare per l'alta disponibilità
Nessun software richiesto sui server di Dominio	nessuna modifica richiesta alla architettura del Server AD
Nessuna esigenza di esporre o gestire password	Ideale per elevati requisiti di sicurezza
Agent 'Learning Mode'	Ricerca trasparente e invisibile sull'uso delle elevazioni delle applicazioni prima della revoca dei diritti
Supporto mondiale incluso in tutti i piani a pagamento	Nessun costo aggiuntivo per il supporto
Repository sicuro della documentazione nel portale ABR	Tutto ciò di cui ha bisogno il DPO, il CISO o l'auditor esterno per la documentazione di conformità in un unico posto

ELEVAZIONE DEI PRIVILEGI E REVOCA

ELEVAZIONE DEI PRIVILEGI E REVOCA	DESCRIZIONE FUNZIONALITA'
Architettura globale/settoriale	Applica impostazioni predefinite globali e/o gruppi illimitati di impostazioni
Sistema di revoca dei diritti ed esclusione dell'account	Revoca gli utenti dal gruppo Amm. locali/esclusioni specifiche da non revocare
Modalità di elevazione assistita dal driver	Conferma semplice Sì/No sull'elevazione dell'applicazione
Modalità di elevazione nativa UAC	Elevazione UAC senza driver Win con ri-autentic. sull'elevaz dell'applicazione
Supporto Windows Hello per l'elevazione nativa UAC	Autenticazione dell'elevazione con Windows Hello
Modalità di elevazione non interattiva (senza prompt)	Elevare le applicazioni senza interazione dell'utente (avvio/login etc)
Modalità di elevazione MFA	Richiede Entra ID / Office 365 / MFA SAML per l'elevazione
Verifica stati elevazione in tempo reale nel portale/app	Mantieni il controllo di tutti gli utilizzi di elevazione in tempo reale
Modalità di elevazione per processo	Elevazione sandbox per processo / approvazione su base per applicazione
Modalità di elevazione della Sessione Amministrativa	Elevazione limitata nel tempo a livello di sistema
Chiusura forzata al termine Sessione Amministrativa	Chiusura forzata al termine della modalità di sessione amministrativa: le applicazioni vengono chiuse forzatamente alla scadenza della sessione
Assistenza al Supporto IT	Aggiornamento nel profilo di elevazione per il personale dell'helpdesk
Codice PIN per l'uso offline	Consente l'approvazione manuale per gli utenti offline

AUMENTO DELLA SICUREZZA

AUMENTO DELLA SICUREZZA	DESCRIZIONE FUNZIONALITA'
Controllo malware OPSWAT in tempo reale	Controllo pre-elevazione su oltre 20 fornitori di antivirus che garantisce l'elevazione solo di file affidabili
Rilevamento automatico di soluzioni Proxy e VPN	Soluzioni come Z-Scaler e Pulse Secure sono rilevate automaticamente e supportate
Schermate di istruzioni utente personalizzabili	Messaggi personaliz. 'regolamenti aziendali' agli utenti prima di elevazione
Blacklist applicazioni (posizione/cert.fornitore/checksum)	Nega l'elevazione di specifiche applicazioni / fornitori
Codice PIN per la revoca della Blacklist	Approvazione manuale per la revoca delle applicazioni dalla blacklist
Modalità Desktop sicuro UAC	Opzione della modalità nativa UAC per utilizzare la modalità Desktop sicuro (oscura la schermata sulla richiesta UAC)
Funzionalità anti-manomissione multiple	rimozione agent negata, monitoraggio processi, anti-manomissione servizi
Registro attività impostazioni del portale	Traccia tutte le modifiche alle impostazioni del portale: chi, quando, impostazione precedente, nuova impostazione

GESTIONE

GESTIONE	DESCRIZIONE FUNZIONALITA'
Aggiornamento Agent tramite LAN	Aggiornamento automatico dell'agent tramite condivisione di rete
Aggiornamento Agent tramite Internet	Singolo pulsante per Aggiornamento automatico dell'agente tramite Internet
Distribuzione tramite Intune e SCCM	Distribuzione semplice con il sistema di gestione del software esistente
App Mobile (Android e Apple)	Approvazioni dei processi e revisione dei log lontano dal tuo PC
Registro delle attività e impostazioni del portale	Registro completo di tutte le modifiche delle impostazioni nel portale (chi, quando, precedente impostazione , nuova impostazione)
Report schedulati tramite Email	Invio schedulato tramite email di vari report predefiniti dal portale
Inventario di sistema (Software installato / AD / Gruppi AAD / Amministratori locali)	Visibilità dello stato del sistema migliorata
Conservazione dei dati configurabile sul portale	Minimo 3 mesi, massimo 5 anni
Utenti del portale illimitati	Nessun limite sul numero di amministratori del portale
Configurazione utente del portale basata sui ruoli	Assegna agli utenti l'accesso condizionale al portale in base al loro ruolo
Filtro dati portale in base ai permessi degli utenti	Limitare gli utenti del portale alla gestione di specifici utenti / gruppi
Impostazioni secondarie illimitate (impostazioni specifiche per gruppi)	Nessun limite sul numero di gruppi di impostazioni

INTEGRAZIONI

INTEGRAZIONI	DESCRIZIONE FUNZIONALITA'
API REST per integrazioni esterne	Tramite le API (per Log di Audit, Sistema di Richieste e Inventario) è possibile leggere i dati per archiviazione e reportistiche esterne
MS Teams, Slack, ServiceNow e Jira	Ricevono le notifiche di approvazione e le gestiscono tramite integrazioni
Integrazione SCIM con OKTA e Azure AD	Popola e sincronizza gli utenti del portale da AAD o OKTA
AAD SSO / O365 / SAML per Login al Portale	Utilizzo dell'aut, SSO aziendale per l'accesso trasparente al portale di ABR
Integrazione al sistema di Ticketing	Integra richieste e stato di approvazione nel sistema di ticketing esistente

Admin By Request
By FastTrack Software

Permessi Admin Locali, Gestiti.

Una potente soluzione di Gestione degli Accessi Privilegiati (PAM) basata su SaaS progettata per gestire gli account degli amministratori degli endpoint e l'elevazione in modo sicuro, efficiente e user-friendly.

Pieno Controllo a tua disposizione

App Elevation
Eleva le applicazioni senza elevare l'Utente

Break Glass/LAPS
Fornisce account amministrativi locali temporanei.

Malware Detection
Scansione multipla, con oltre 35 motori AV.

Endpoint MFA/SSO
Policy aziendali con MFA/SSO prima dell'elevazione.

Machine Learning
Auto-approvazioni dopo N approvazioni manuali.

GDPR Compliance
Assicura che tutti i dati sensibili siano protetti.

Multi Piattaforma
Versioni per Windows, macOS,

AI Approval
Consente al nostro motore AI di auto-approvare le richieste di elevazione.

Integrazioni
Teams, Slack, ServiceNow, Sentinel, Intune e altro ancora.

Applicazione Mobile
Accedi alla gestione del Portale tramite il tuo Smartphone

emea-sales@fasttracksoftware.com

Installa subito il Piano Gratuito per iniziare:

www.adminbyrequest.com/freeplandownload

Segui Admin By Request su LinkedIn per News, aggiornamenti e promozioni.