



Sicurezza e rapidità grazie all'automazione

Un unico software gestionale per tutti gli endpoint

INDICE

1	Requisiti sempre più complessi: una sfida per i dipartimenti IT.....	2
2	Come automatizzare le attività di routine	4
2.1	La distribuzione di sistemi operativi e applicazioni.....	4
2.2	Individuazione delle vulnerabilità e automazione degli aggiornamenti	6
2.3	L'automazione intelligente: temporizzazione e self-service	10
2.4	Integrazione nell'infrastruttura esistente	10
3	Gestione dei dispositivi mobili	11

© 2025 baramundi software GmbH

Le dichiarazioni relative alle attrezzature e alle funzionalità tecniche non sono vincolanti e hanno uno scopo puramente informativo.

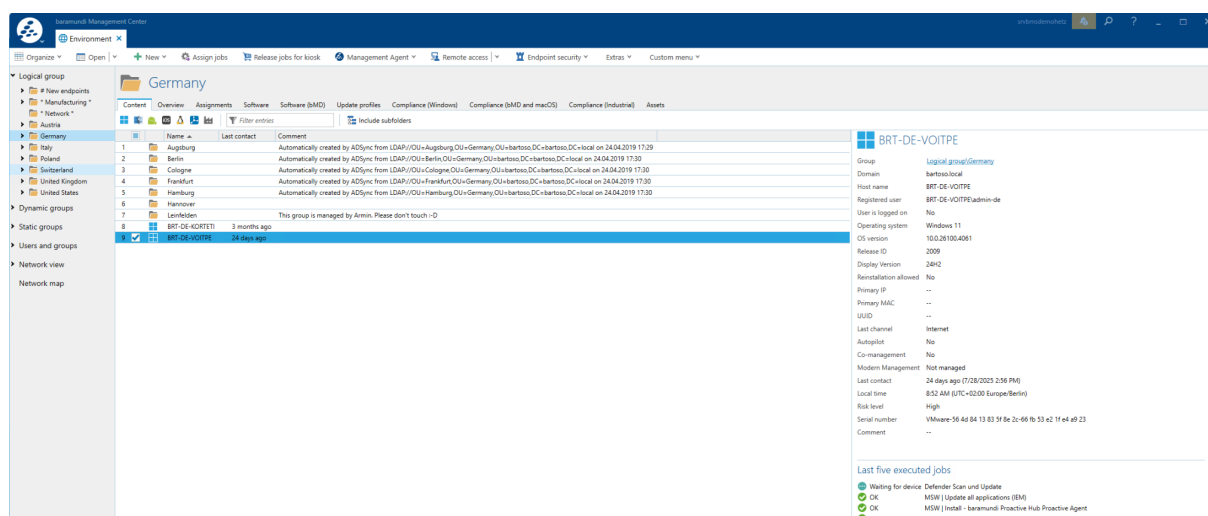
Ci riserviamo il diritto di apportare modifiche. Doc ID WP-201019

1 Requisiti sempre più complessi: una sfida per i dipartimenti IT

Il progresso dell'informatica avviene a un ritmo sempre più rapido: se in passato sono serviti decenni per passare da Zuses Z1 ai primi PC, oggi le novità del settore si presentano a cadenza quasi mensile. E mentre la performance migliora e la varietà dei dispositivi aumenta, le mansioni amministrative diventano sempre più complesse.

Ad esempio, molti utenti non lavorano più unicamente su PC e portatili, ma utilizzano in parallelo o in sequenza anche smartphone e tablet. Si risponde alle e-mail mentre si è in viaggio, e le ricerche possono essere avviate su desktop e proseguite tramite smartphone, mentre le presentazioni vengono controllate con l'ausilio del tablet. I dispositivi mobili impiegano sistemi operativi e applicazioni diversi dagli endpoint tradizionali, ma, richiedendo ugualmente l'accesso ai dati e alle e-mail aziendali, devono essere comunque protetti in modo altrettanto affidabile.

Allo stesso tempo, la linea di confine che separa il mondo dei dispositivi mobili da quello dei PC sta diventando sempre più sfumata: basti pensare ai tablet con funzioni spawn dotati dei sistemi operativi dei PC, o alle applicazioni mobili che funzionano sugli endpoint di Windows. Ecco perché appare sensato accorpate la gestione di tutti gli endpoint utilizzati dagli utenti in-house in un'unica soluzione. Si tratta di un approccio che apre la strada all'introduzione di standard uniformi e all'acquisizione di una panoramica onnicomprensiva dello stato del network e di tutti i dispositivi endpoint. È una soluzione di tipo olistico, che può facilmente integrare nuovi dispositivi futuri.



The screenshot displays the Baramundi Management Center interface. On the left, a sidebar shows a tree view with categories like 'Logical group', 'Dynamic groups', 'Static groups', 'Users and groups', and 'Network map'. The main area is titled 'Germany' and contains a table of endpoints. The table has columns for 'Name', 'Last contact', and 'Comment'. Below the table, there is a detailed view of a specific endpoint named 'BRT-DE-VOITRE'. This view includes various system information such as 'Group', 'Domain', 'Host name', 'Registered user', 'Operating system', 'OS version', 'Release ID', 'Display Version', 'Renewal allowed', 'Primary IP', 'Primary MAC', 'UUID', 'Last channel', 'Autopilot', 'Co-management', 'Modern Management', 'Last contact', 'Local time', 'Risk level', 'Serial number', and 'Comment'. At the bottom, there is a section for 'Last five executed jobs' showing a list of tasks and their status.

Una panoramica uniforme di tutte le tipologie di dispositivo/piattaforma

Una soluzione di unified endpoint management consente inoltre di automatizzare le mansioni di routine, che possono essere portate a termine in modo più semplice, rapido e ottimizzato. Oltre a fornire la visione d'insieme necessaria, questo approccio permette anche di migliorare il livello di sicurezza del network aziendale. Il presente documento fornisce una panoramica delle mansioni amministrative che dovrebbero essere automatizzate, indipendentemente dalle circostanze.

2 Come automatizzare le attività di routine

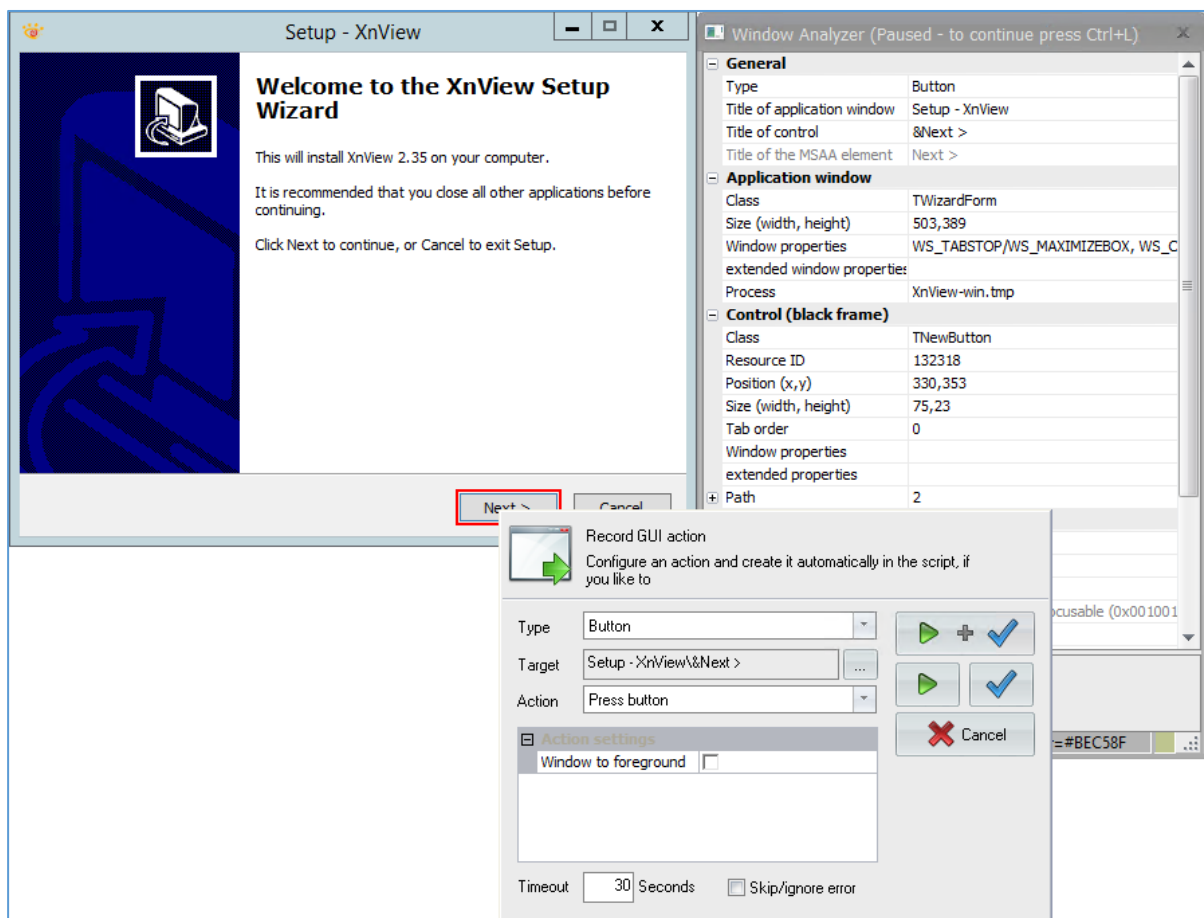
2.1 La distribuzione di sistemi operativi e applicazioni

Un nuovo collaboratore è stato assunto in azienda. Questo significa che il dipartimento IT dovrà occuparsi di allestire una postazione di lavoro dotata di computer o laptop. La re-installazione del sistema operativo e di tutte le applicazioni necessarie all'interno di un computer - ad inclusione di tutte le opportune operazioni di riavvio, della selezione dei driver appropriati, ecc. - può richiedere molte ore di lavoro. Con l'adozione di una soluzione gestionale, al contrario, basteranno pochi clic del mouse per completare l'operazione.

Invece di effettuare il setup manualmente o tramite script, il nuovo dispositivo sarà automaticamente individuato all'interno del network. In questo modo, con un'unica operazione sarà possibile preparare l'hard disk per l'uso e assegnare i driver necessari. Le soluzioni intelligenti si affidano al metodo di installazione nativa del produttore del sistema operativo e potranno quindi anche beneficiare di una garanzia completa. Grazie al servizio Wake-on-LAN, vi è la possibilità di re-installare i computer durante le ore notturne. Anche il software potrà essere distribuito automaticamente.

Solitamente, ciò implica la definizione di una configurazione standard per un profilo di utilizzo. Se necessario, l'amministratore IT potrà installare il pacchetto software sul sistema target con un clic del mouse - anche in parallelo su più dispositivi, ad inclusione delle necessarie procedure di riavvio e assicurando un'ottimale qualità di installazione utilizzando metodi originali di setup. La soluzione automatizzata fornisce anche un feedback sullo stato dell'installazione e su eventuali errori verificatisi in qualsiasi fase della procedura. Una volta definiti, i task potranno essere riutilizzati in qualsiasi momento nel caso in cui un nuovo collega sia assunto nei mesi successivi o qualora si renda necessaria la sostituzione di un dispositivo. Allo stesso tempo, l'automazione dell'installazione aiuta a garantire configurazioni standardizzate del computer e minimizzare il numero degli errori.

Spesso si rende necessaria l'installazione del software senza i pacchetti di installazione standardizzata del produttore. In questo caso, gli strumenti integrati nel software gestionale comune possono essere utilizzati per creare in modo semplice e intuitivo gli script necessari per l'automazione di superficie. Anche le impostazioni più complesse possono essere installate a livello centrale e in modo automatico utilizzando la procedura di setup indicata dal produttore del software. In questo modo, la garanzia rimarrà pienamente valida.



Automazione di superficie basata su procedura guidata con baramundi Automation Studio

Il software gestionale non è solo in grado di distribuire le applicazioni, ma anche di rimuoverle dall'endpoint. Nella scelta di una soluzione, occorre accertarsi che questo sia possibile anche per i programmi che non sono stati installati tramite il software gestionale. Di conseguenza, per esempio, le applicazioni che gli utenti hanno installato sul proprio computer senza autorizzazione possono essere efficacemente rimosse.

Anche gli amministratori IT e gli utenti finali potranno beneficiare dell'installazione delle applicazioni e dei sistemi operativi secondo questa modalità centralizzata e automatizzata: nel caso in cui si verifichino problematiche di rendimento o errori persistenti, la re-installazione della postazione di lavoro potrà avvenire comodamente durante le ore notturne, invece di dover procedere alla ricerca della causa degli inconvenienti. Questo significa anche che l'amministratore potrà disporre il più rapidamente possibile, e riducendo al minimo i tempi di inattività, di un dispositivo perfettamente funzionale. È inoltre possibile ricorrere all'automazione in caso di necessità di effettuare procedure di migrazione su numerose postazioni di lavoro, per passare, ad esempio, a un nuovo sistema operativo come Windows 11 o a una nuova versione di Office.

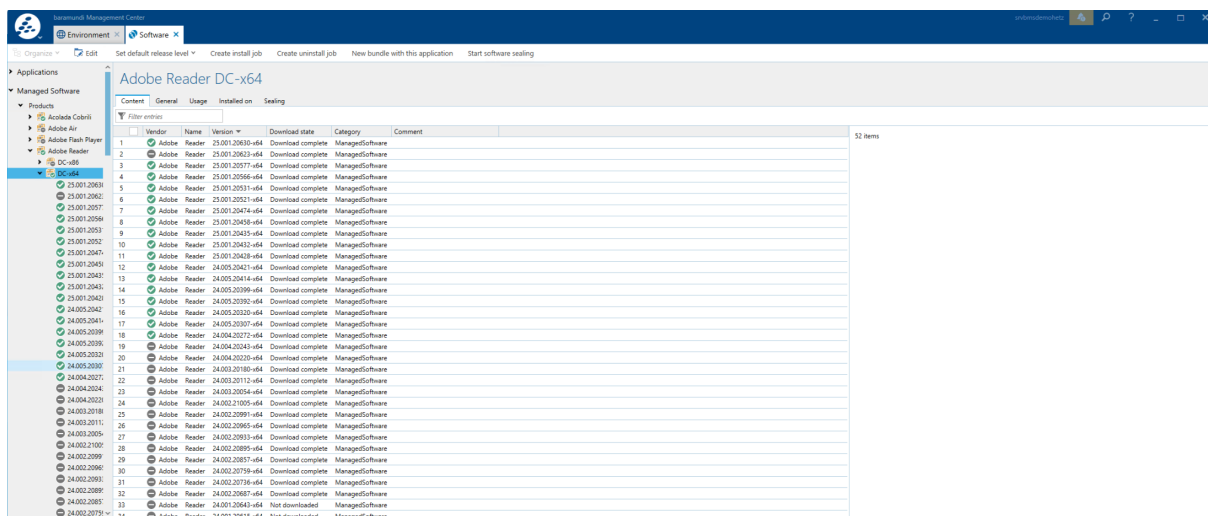
2.2 Individuazione delle vulnerabilità e automazione degli aggiornamenti

Dopo le operazioni di installazione e completamento, il lavoro è finito? Purtroppo no. Gli aggiornamenti per le applicazioni e i sistemi operativi si presentano a cadenza regolare, e devono essere installati su tutti i dispositivi target al più presto possibile. Non si tratta solo di una questione di nuove funzionalità, ma soprattutto di sicurezza: le nuove versioni e patch proteggono i punti deboli del sistema, prevenendo così eventuali attacchi informatici che potrebbero infiltrarsi nel network aziendale e causare seri danni. Le conseguenze di questi attacchi spaziano da danni di immagine e dalla divulgazione di informazioni aziendali riservate a problematiche legali causate da qualsiasi furto di dati dei clienti e violazioni delle leggi di protezione dei dati stessi.

I firewall e gli antivirus sono componenti essenziali di un efficace concetto di sicurezza, ma diventano praticamente inutili se le lacune non vengono colmate con l'installazione delle patch. Se il computer di un collaboratore viene forzato a stabilire una connessione con il server di controllo degli aggressori, in quello che viene chiamato attacco a connessione inversa, che sfrutta una vulnerabilità del sistema, il firewall solitamente non riesce a intervenire, perché il contatto viene stabilito in forma crittografata su canali standard di provenienza aziendale. Ecco perché è fondamentale monitorare le vulnerabilità di ogni singolo endpoint, colmando le lacune di sicurezza il prima possibile, a seconda del grado di suscettibilità.

Tuttavia, sono circa 100 le nuove vulnerabilità che vengono individuate e documentate ogni settimana, come riportano le statistiche del National Vulnerability Database di US-CERT. In questo ambito, il software gestionale può supportare gli amministratori IT effettuando scansioni automatiche e regolari di tutti gli endpoint e i server. Successivamente, l'amministratore riceve delle liste chiare che indicano le principali vulnerabilità all'interno del network aziendale o gli endpoint più esposti. A questo punto, tutte le lacune potranno essere rettificare, in ordine di priorità.

Se la soluzione include un sistema di gestione delle update unitamente alla scansione delle vulnerabilità, qualsiasi problematica riscontrata potrà essere risolta automaticamente a livello centralizzato. Oltre alle patch di Microsoft, la soluzione di management dovrebbe, come minimo, distribuire anche gli aggiornamenti per applicazioni di uso frequente, come Adobe Reader, Java o Firefox, automaticamente e in modo centralizzato, data la loro ampia diffusione e la corrispondente popolarità tra gli hacker. Gli attuali pacchetti software per numerose applicazioni sono resi disponibili anche come Managed Software dal produttore dell'UEM. In accordo con le linee guida in-house, il rilascio è possibile anche per un uso produttivo o per il testing.



Vendor	Name	Version	Download state	Category	Comment
Adobe	Reader	25.001.20630-x64	Download complete	ManagedSoftware	
Adobe	Reader	25.001.20623-x64	Download complete	ManagedSoftware	
Adobe	Reader	25.001.20771-x64	Download complete	ManagedSoftware	
Adobe	Reader	25.001.20566-x64	Download complete	ManagedSoftware	
Adobe	Reader	25.001.20531-x64	Download complete	ManagedSoftware	
Adobe	Reader	25.001.20521-x64	Download complete	ManagedSoftware	
Adobe	Reader	25.001.20474-x64	Download complete	ManagedSoftware	
Adobe	Reader	25.001.20438-x64	Download complete	ManagedSoftware	
Adobe	Reader	25.001.20432-x64	Download complete	ManagedSoftware	
Adobe	Reader	25.001.20432-x64	Download complete	ManagedSoftware	
Adobe	Reader	25.001.20428-x64	Download complete	ManagedSoftware	
Adobe	Reader	24.005.20471-x64	Download complete	ManagedSoftware	
Adobe	Reader	24.005.20414-x64	Download complete	ManagedSoftware	
Adobe	Reader	24.005.20399-x64	Download complete	ManagedSoftware	
Adobe	Reader	24.005.20392-x64	Download complete	ManagedSoftware	
Adobe	Reader	24.005.20330-x64	Download complete	ManagedSoftware	
Adobe	Reader	24.005.20307-x64	Download complete	ManagedSoftware	
Adobe	Reader	24.004.20272-x64	Download complete	ManagedSoftware	
Adobe	Reader	24.004.20244-x64	Download complete	ManagedSoftware	
Adobe	Reader	24.004.20220-x64	Download complete	ManagedSoftware	
Adobe	Reader	24.003.20180-x64	Download complete	ManagedSoftware	
Adobe	Reader	24.003.20112-x64	Download complete	ManagedSoftware	
Adobe	Reader	24.003.20054-x64	Download complete	ManagedSoftware	
Adobe	Reader	24.002.21005-x64	Download complete	ManagedSoftware	
Adobe	Reader	24.002.20991-x64	Download complete	ManagedSoftware	
Adobe	Reader	24.002.20965-x64	Download complete	ManagedSoftware	
Adobe	Reader	24.002.20933-x64	Download complete	ManagedSoftware	
Adobe	Reader	24.002.20895-x64	Download complete	ManagedSoftware	
Adobe	Reader	24.002.20857-x64	Download complete	ManagedSoftware	
Adobe	Reader	24.002.20758-x64	Download complete	ManagedSoftware	
Adobe	Reader	24.002.20736-x64	Download complete	ManagedSoftware	
Adobe	Reader	24.002.20687-x64	Download complete	ManagedSoftware	
Adobe	Reader	24.001.20647-x64	Not downloaded	ManagedSoftware	
Adobe	Reader	24.001.20611-x64	Not downloaded	ManagedSoftware	

Pacchetti software pronti per la distribuzione con diversi livelli di rilascio

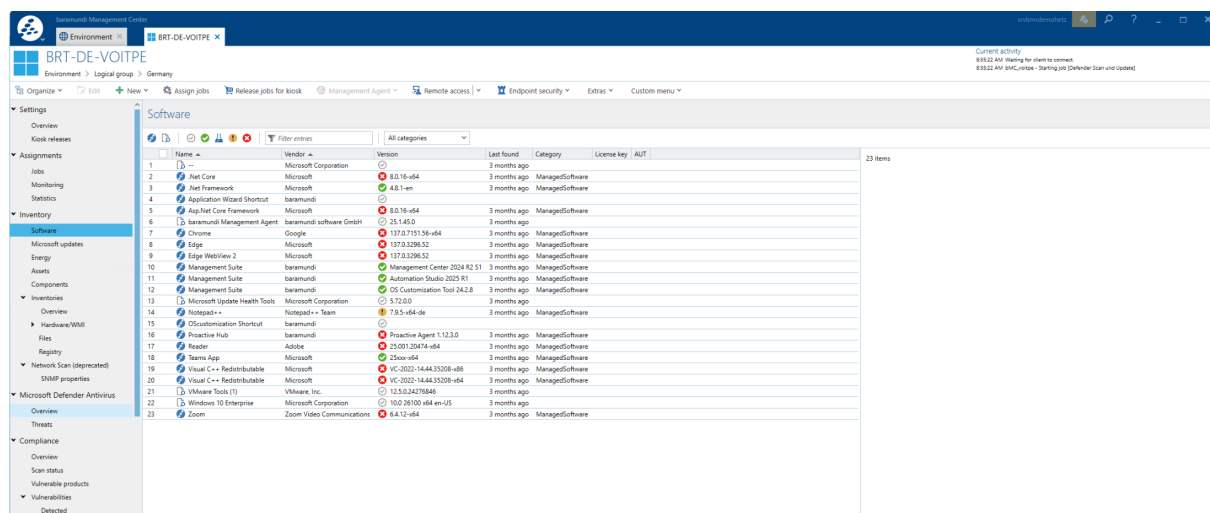
Un'efficace gestione delle vulnerabilità, tuttavia, richiede più della semplice consapevolezza delle lacune e dell'avvio dell'installazione di una patch. Ogni dispositivo collegato in rete dovrebbe essere sottoposto regolarmente a inventario per la rilevazione di nuovi software. È importante che l'inventario o la scansione delle vulnerabilità siano effettuati con continuità, e non vengano lasciati al caso. Ecco perché è essenziale sapere quali dispositivi siano effettivamente presenti in azienda. Questo accorgimento è valido sia per l'area dell'ufficio che per i dispositivi in rete della produzione. Come requisito minimo, il dipartimento IT dovrebbe sempre disporre di una lista aggiornata di tutti i dispositivi.

Gli aggiornamenti (incluse le patch di sicurezza) dovrebbero inoltre essere distribuiti a intervalli regolari. Un esempio ben noto è il patch day di Microsoft, ogni secondo martedì del mese. Partendo da questo punto di riferimento, gli amministratori IT possono impostare un calendario di distribuzione delle nuove patch per ogni singolo caso.

La soluzione di automazione qui descritta si basa su due processi indipendenti, e offre quindi un livello di sicurezza molto elevato:

- **automatismo di aggiornamento:** nell'ambito dei processi di update management, si procede ad installare gli aggiornamenti software forniti dal produttore sui dispositivi endpoint. La procedura si basa sulla fiducia accordata al produttore del software e al meccanismo di aggiornamento.
- **automazione delle vulnerabilità:** la scansione delle vulnerabilità è indipendente da questo procedimento da un punto di vista tecnico. Qui, viene effettuato l'accesso ai cataloghi indipendenti dai produttori del software e si impiegano metodi ugualmente distinti per la ricerca dei programmi o dei loro componenti. Grazie all'algoritmo separato, questo fornisce una seconda prospettiva indipendente sulla sicurezza dei dispositivi. Inventario di hardware e software, gestione delle licenze

Una panoramica completa non è importante solo per individuare le vulnerabilità e garantire la sicurezza. I manager IT devono anche essere in grado di stilare resoconti sull'utilizzo dell'hardware e del software o, in caso di un audit sulle licenze da parte di un produttore di software, poter dimostrare la corretta gestione delle licenze stesse. Da un punto di vista dei costi, è inoltre importante individuare il software inutilizzato sugli endpoint, che comporta comunque elevati costi di licenza.



	Name	Vendor	Version	Last found	Category	License key	AUT
1	...	Microsoft Corporation	...	3 months ago	ManagedSoftware		
2	.Net Core	Microsoft	6.0.16-x64	3 months ago	ManagedSoftware		
3	.Net Framework	Microsoft	4.8.1-en	3 months ago	ManagedSoftware		
4	Application Wizard Shortcut	baramundi		3 months ago	ManagedSoftware		
5	AspNet Core Framework	Microsoft	6.0.16-x64	3 months ago	ManagedSoftware		
6	baramundi Management Agent	baramundi software GmbH	25.1.45.0	3 months ago	ManagedSoftware		
7	Chrome	Google	117.0.1915.16-x64	3 months ago	ManagedSoftware		
8	Edge	Microsoft	117.0.2296.52	3 months ago	ManagedSoftware		
9	Edge WebView 2	Microsoft	117.0.2296.52	3 months ago	ManagedSoftware		
10	Management Suite	baramundi	Management Center 2024 R2 S1	3 months ago	ManagedSoftware		
11	Management Suite	baramundi	Automation Studio 2025 R1	3 months ago	ManagedSoftware		
12	Management Suite	baramundi	OS Customization Tool 24.2.8	3 months ago	ManagedSoftware		
13	Microsoft Update Health Tools	Microsoft Corporation	5.72.0.0	3 months ago	ManagedSoftware		
14	Notepad++	Notepad++ Team	8.5.5-x64-de	3 months ago	ManagedSoftware		
15	OSCustomization Shortcut	baramundi		3 months ago	ManagedSoftware		
16	Proactive Hub	baramundi	Proactive Agent 1.12.3.0	3 months ago	ManagedSoftware		
17	Reactor	Adobe	55.001.22474-x64	3 months ago	ManagedSoftware		
18	Teams App	Microsoft	25x64-x64	3 months ago	ManagedSoftware		
19	Visual C++ Redistributable	Microsoft	VC-2022-14.44.35208-x66	3 months ago	ManagedSoftware		
20	Visual C++ Redistributable	Microsoft	VC-2022-14.44.35208-x64	3 months ago	ManagedSoftware		
21	VMware Tools (1)	VMware, Inc.	12.5.5.24278646	3 months ago	ManagedSoftware		
22	Windows 10 Enterprise	Microsoft Corporation	100.26100-x64-en-US	3 months ago	ManagedSoftware		
23	Zoom	Zoom Video Communications	6.4.12-x64	3 months ago	ManagedSoftware		

Elenco del software installato

Il software gestionale può essere utilizzato per generare un inventario automatizzato utile a evidenziare, in modo rapido e chiaro, quali hardware e software vengono impiegati all'interno del network aziendale. Ciò significa che un database aggiornato sarà sempre a disposizione per una valutazione gestionale. Con riguardo a volumi e upgrade delle licenze, l'obiettivo di un monitoraggio completo è una vera e propria sfida. In risposta a questa esigenza, una soluzione di gestione delle licenze fornisce una chiara panoramica e assicura la compliance.

Vi è inoltre la possibilità di rilevare l'uso effettivo di un programma, per eliminare tutti i costi superflui. A questo scopo, si procede a registrare l'avvio di un'applicazione sui singoli dispositivi. Questa procedura permette di individuare i computer sui quali un programma rimane inutilizzato per determinato periodo di tempo - e, di conseguenza, quali costi di licenza possono essere risparmiati. Importante: la soluzione adottata deve essere conforme alla normativa internazionale sulla protezione dei dati e non consentire il monitoraggio del comportamento dei singoli dipendenti.

Anche l'assistenza IT potrà beneficiare dell'inventario automatizzato: le soluzioni integrate di helpdesk supportano lo staff, in caso di richieste, nella rapida acquisizione delle informazioni sulle dotazioni hardware e software della postazione di lavoro. Essere in possesso dei dati corretti sul dispositivo terminale in questione è essenziale per evadere le richieste in modo veloce e competente.

2.3 L'automazione intelligente: temporizzazione e self-service

Molte aziende hanno delle "finestre temporali" di manutenzione, in base alle quali le mansioni amministrative su certi computer possono essere effettuate solo in momenti specifici. Pertanto, un efficiente software gestionale apre la strada alla temporizzazione delle attività. Rende inoltre possibile, ad esempio, l'installazione di una patch su un dispositivo specifico entro un determinato periodo.

I task legati agli eventi, al contrario, alleviano il carico di lavoro degli amministratori IT in caso di necessità di risposta a singoli episodi. Per esempio: il gioco XY dovrebbe essere rimosso automaticamente nel caso in cui sia rilevata la sua presenza su un endpoint durante l'inventario. Invece di dover intervenire ogni volta che il gioco viene rilevato, l'amministratore IT riceve esclusivamente un report sull'avvenuta disinstallazione.

Gli amministratori IT e gli utilizzatori apprezzeranno la comodità di poter mettere a disposizione, all'interno di un chiosco self-service, procedure di installazione già predisposte. Ciò consente una gestione più semplice e rapida di richieste standard, come ad esempio l'installazione di Firefox – proprio quando l'utente lo desidera e necessita di un'operatività impeccabile. Allo stesso tempo, la mole del lavoro di assistenza si riduce, in quanto le mansioni vengono portate a termine in modo completamente automatico e on demand. L'amministratore dovrebbe inoltre essere in grado di monitorare le installazioni self-service con regolarità.

Un software gestionale dall'elevata performance consente di coinvolgere gli utenti nei processi di installazione, permettendo allo stesso tempo agli amministratori di mantenere il controllo. Ad esempio, l'utente può essere autorizzato a posticipare, nell'ambito di una determinata finestra temporale, l'installazione di una patch che richiede un reboot. Questo aiuta a evitare interruzioni nel flusso di lavoro dei colleghi, con possibilità, ad esempio, di programmare l'installazione durante la pausa caffè. Al tempo stesso, però, ci si assicura che la distribuzione di una patch di importanza critica non sia eccessivamente rimandata.

2.4 Integrazione nell'infrastruttura esistente

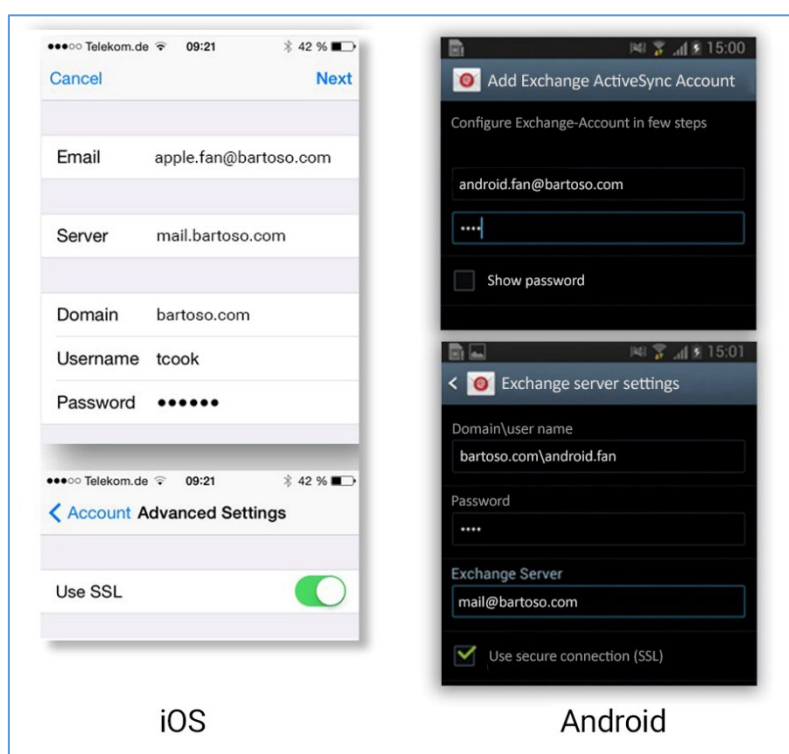
È inoltre auspicabile evitare di considerare il software gestionale come un nuovo elemento a sé stante all'interno dell'infrastruttura esistente. Per un'integrazione perfetta, occorre che il software gestionale disponga di moderne interfacce. Questo è l'unico modo per poter automatizzare anche altri processi organizzativi. Ad esempio, dopo che il nuovo PC è stato registrato nel sistema ERP, un endpoint con tutti i dati essenziali - come numero di inventario, centro di costo, ecc. - può essere creato automaticamente nella soluzione di management e fornito immediatamente completo di software e configurazioni.

L'integrazione nel sistema di ticketing esistente è altrettanto facile! Grazie a questa procedura, lo staff di supporto riceve in ogni momento le informazioni più aggiornate sul software e sull'hardware utilizzati nell'endpoint, e le nuove installazioni possono essere avviate in base alle necessità.

3 Gestione dei dispositivi mobili

L'utilizzo degli apparecchi mobili è ormai una consuetudine in numerose aziende, e molti collaboratori richiedono di accedere ai dati aziendali dai propri dispositivi. Questo può comportare alcuni vantaggi per l'azienda, ma i manager IT devono comunque essere consapevoli dei rischi. Un'efficace protezione e un inventario aggiornato sono i requisiti di base necessari per integrare in sicurezza computer portatili, tablet e smartphone nel mondo professionale. Idealmente, la gestione dei dispositivi mobili dovrebbe essere integrata nella soluzione UEM, in quanto in questo ambito molte mansioni possono essere ugualmente automatizzate.

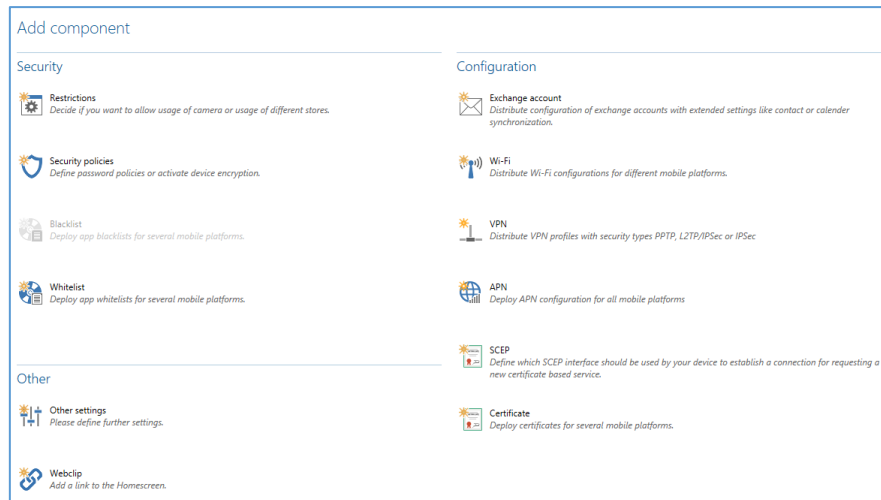
Effettuando un confronto tra le due piattaforme mobili più comuni – iOS e Android – risulta evidente come gli stessi parametri – nome, indirizzo e-mail, server, dominio e crittografia per l'impostazione degli exchange account - debbano essere inseriti in diversi punti. In termini pratici, questo si traduce in un'enorme mole di lavoro, che richiede la conoscenza da parte dell'amministratore di tutte le maschere di input. Questo flusso di lavoro può essere notevolmente semplificato utilizzando moduli di profilo multipiattaforma e una gestione centralizzata dei dispositivi.



Configurazione Exchange su diverse piattaforme mobili

Lo smartphone o il tablet dovranno essere inseriti, una sola volta, nella soluzione di management ("registrazione"), utilizzando ad esempio l'Apple Device Enrollment Program (DEP) o la scansione di un codice a barre. Lo step successivo prevede l'implementazione,

attraverso la soluzione, dei task gestionali - l'esempio riportato mostra la configurazione exchange - a livello centralizzato. Le impostazioni necessarie vengono configurate in un'interfaccia uniforme e multiplatforma, per poi essere trasferite nei dispositivi gestiti.



Moduli di profilo multiplatforma per la configurazione di dispositivi mobili

I vantaggi sono evidenti: l'amministratore non ha più necessità di sapere dove e su quale dispositivo mobile vengono inserite le singole impostazioni, dato che il punto di partenza è sempre costituito dall'interfaccia nota della sua console di gestione centralizzata. Questo semplifica, accelera e migliora ulteriormente l'accuratezza del processo. È poi importante sottolineare come questo tipo di procedura aumenti il grado di sicurezza.

Un altro vantaggio, infine, consiste nella possibilità di completare i task "over the air" tramite il software gestionale, eliminando così la necessità dell'assunzione del controllo del dispositivo da parte dell'amministratore. Ad esempio, se un utente avvia un nuovo dispositivo iOS in una postazione remota, questo viene automaticamente registrato nel sistema gestionale tramite Apple DEP. L'amministratore potrà così impostare le ulteriori configurazioni. I processi e i task impiegati possono anche essere preparati e riutilizzati più volte, anche simultaneamente per un grande numero di dispositivi.

I dispositivi mobili sono anche più soggetti ad andare perduti rispetto ai PC: da qui la necessità di adottare le necessarie precauzioni. Le opzioni includono un blocco automatico quando lo schermo è spento, la possibilità di cancellare il profilo assegnato da remoto e l'adozione di password sicure.

È inoltre necessario garantire che l'amministratore conservi una visione d'insieme dei dispositivi in ogni momento e possa essere informato in caso di compromissione del sistema operativo da parte di un utente. Per questo motivo, qualsiasi soluzione gestionale dovrebbe includere la possibilità di definire regole di compliance, che saranno poi controllate automaticamente e costantemente. In caso di violazioni, l'amministratore viene informato e

ha la possibilità di intraprendere le appropriate contromisure, dall'invio di una email all'utente fino alla cancellazione del dispositivo da remoto. Un tempestivo aggiornamento del firmware, non appena disponibile la nuova versione del produttore, è importante quanto la prevenzione delle manomissioni. Di norma, questo consente non solo l'introduzione di nuove funzioni, ma aiuta anche a eliminare le vulnerabilità. Gli upgrade possono già essere controllati da remoto su moderne piattaforme.

Per prevenire l'avvio di applicazioni pericolose o per fornire una selezione di app di fiducia dell'azienda, la soluzione dovrebbe supportare processi di blocklisting o allowlisting. L'amministratore può quindi prevenire l'installazione o l'esecuzione di applicazioni indesiderate sui dispositivi mobili compatibili. Un approccio di "whitelisting", al contrario, autorizza esplicitamente la definizione delle applicazioni consentite, e impedisce l'installazione o l'esecuzione di app indesiderate.

L'amministratore potrà optare per l'adozione di un approccio di allowlisting o blocklisting per ciascun endpoint. Una volta scelto il tipo di lista, le app corrispondenti vengono aggiunte all'elenco e poi trasferite sul dispositivo mobile come profilo.

Come membro attivo della AppConfig Community, un'iniziativa di produttori leader di EMM, baramundi è impegnata nella semplificazione della distribuzione e della configurazione delle app utilizzando risorse native dei produttori dei sistemi operativi. La suite offre un'ampia gamma di funzionalità per il Mobile Device Management (MDM) e il Mobile Application Management (MAM), ed è integrata da app idonee di terze parti dall'ambiente Document Management Systems (DMS)/Personal Information Management (PIM) con funzioni di Mobile Content Management (MCM). Queste aree sono collegate attraverso gli standard di configurazione a livello di iOS e AppConfig; ciò significa che la soluzione gestionale offre anche una comoda distribuzione e configurazione delle funzionalità MCM, mentre le funzioni di contenuto, come la sincronizzazione e l'elaborazione dei dati, sono riservate alle app di terze parti.

L'integrazione dell'Enterprise Mobility Management in una suite software per la gestione degli endpoint consente non solo di risparmiare tempo e ridurre la complessità delle operazioni durante le procedure di setup e manutenzione e nel corso dell'operatività, ma rende anche possibile gestire i dispositivi mobili e i PC in gruppi condivisi e unità organizzative, e l'introduzione di standard uniformi. Si tratta, probabilmente, anche di un approccio più orientato al futuro, dato che è possibile introdurre più facilmente nuove classi di dispositivi all'interno di una soluzione integrata.

baramundi software GmbH

baramundi software sviluppa l'Unified Endpoint Management per la gestione centralizzata di PC, dispositivi mobili e server. Automatizza la distribuzione del software, semplifica la gestione delle patch e favorisce la trasparenza del network: baramundi apporta un contributo significativo alla sicurezza IT e libera risorse.

www.baramundi.com

Sei pronto a dare uno sguardo più approfondito alla baramundi Management Suite?

Scopri come utilizzare la baramundi Management Suite per gestire e mettere in sicurezza i tuoi PC client, i server e i dispositivi mobili partecipando a uno dei nostri webinar live o on-demand su:

www.baramundi.com/it-training/

Non vediamo l'ora di conoscerti!

Contattaci!



baramundi software GmbH
Forschungsallee 3
86159 Augsburg, Germany

 +49 821 5 67 08 - 380
request@baramundi.com
www.baramundi.com

 +44 2071 93 28 77
request@baramundi.com
www.baramundi.com

 +48 735 91 44 54
request@baramundi.com
www.baramundi.com

 +49 821 5 67 08 - 390
request@baramundi.com
www.baramundi.com

 +43 19 28 01 36 00 10
request@baramundi.com
www.baramundi.com

 +39 340 8861886
request@baramundi.com
www.baramundi.com

 +41 77 280 49 79
request@baramundi.com
www.baramundi.com

baramundi software USA, Inc.
30 Speen St, Suite 501
Framingham, MA 01701, USA

 +1 508-861-7561
requestUSA@baramundi.com
www.baramundi.com