ivanti

Più visibilità, dati chiari, azioni determinanti

Dati IT più completi, risultati aziendali migliori

Sommario

Introduzione

In breve, questo white paper illustra quanto segue:

Una visibilità dettagliata sugli asset, i servizi, il livello di sicurezza, i processi ed i risultati IT offre solide fondamenta che consentono di gestire, proteggere e ottimizzare al meglio il patrimonio IT. Con dati più chiari, potrete intervenire in modo più determinante ed efficace. Di conseguenza, potrete anche ottimizzare i costi e i futuri budget, migliorare l'esperienza dei clienti e degli utenti interni, e mettere in grado il vostro team di lavorare in modo più produttivo ed efficiente.

Sono tutti aspetti di grande interesse, considerando gli attuali settori altamente regolamentati e le esigenze di conformità; la necessità di fornire indicazioni chiare in merito all'applicazione di patch, all'ottimizzazione dei costi, al controllo delle applicazioni e all'ubicazione degli asset; e l'obiettivo dell'IT di diventare un centro di riferimento per l'innovazione all'interno dell'azienda.

Ma è importante comprendere che la visibilità dettagliata si ottiene per gradi, un passo dopo l'altro. Ad esempio:

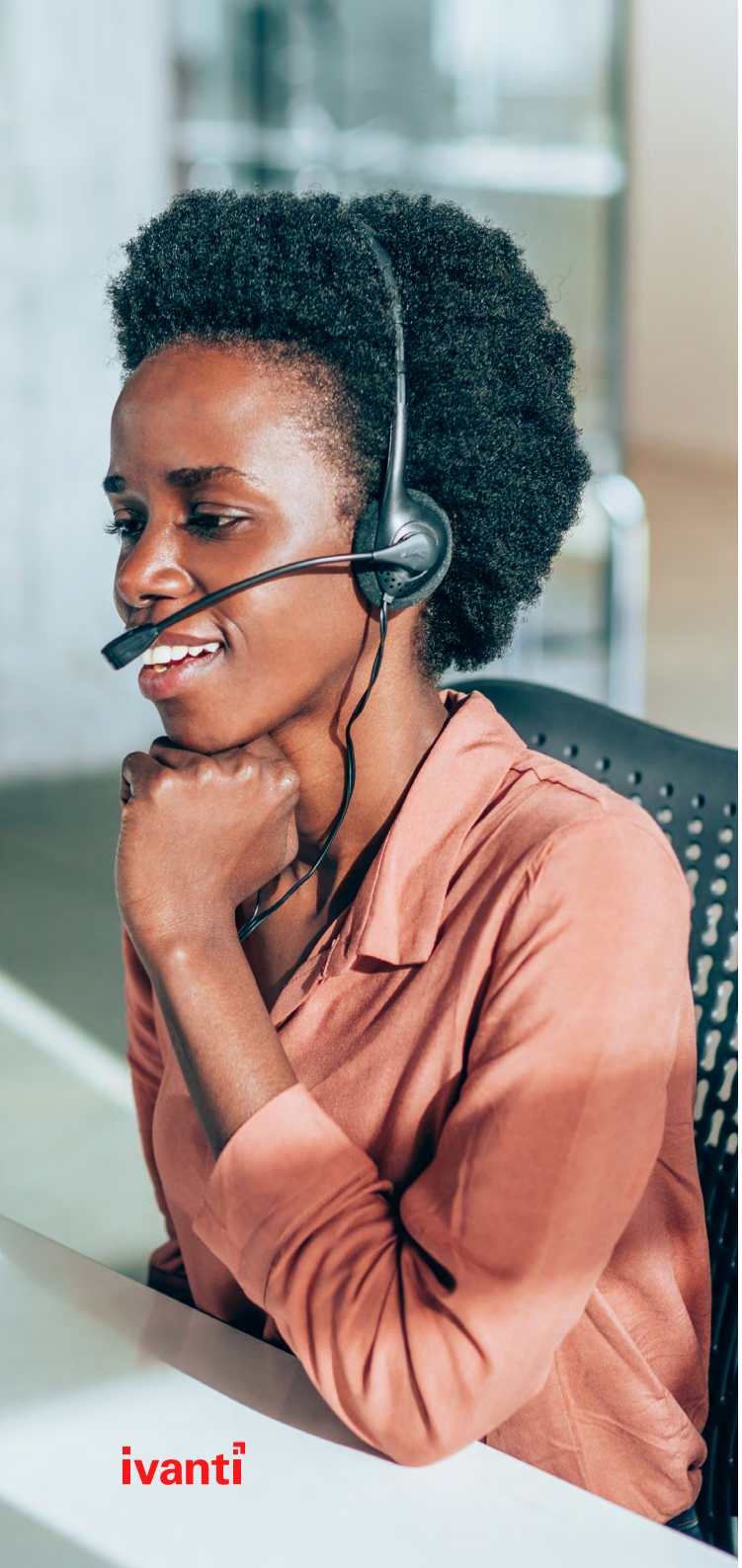
- Se non si definisce la situazione di partenza, non è possibile sapere ciò di cui si dispone dal punto di vista di asset, sicurezza, processi e maturità, né farsi un'idea della mole e del tipo di lavoro che l'IT dovrà gestireComment gérer ce que vous ne connaissez pas dans votre environnement IT ?
- Come si può gestire ciò che non si sa di avere nell'ambiente IT?
- Come si può fornire maggiore valore aziendale con lo stesso budget e le stesse risorse IT?
- Come si può fornire maggiore supporto per una gamma sempre più ampia di tipi di endpoint, con procedure manuali o non evolute che limitano la visibilità sull'intera situazione interna?

Ivanti fa luce in ogni angolo dell'ambiente IT

L'acquisizione di una maggiore visibilità deve diventare una pratica di base e le soluzioni comprovate di Ivanti fanno luce su ogni aspetto dell'ambiente IT aziendale. Con un approccio IT unificato, i vari team dedicati a IT Service Management, IT Asset Management, gestione della protezione degli endpoint e gestione degli utenti e dell'area di lavoro sono tutti organizzati come pilastri di Enterprise Service Management e Unified Endpoint Management. Una maggiore chiarezza e visibilità porta a una migliore sincronia con gli utenti, i servizi e gli asset nell'intera azienda, nonché con il panorama IT, la sicurezza, i processi e i dati. Inoltre, permette di raggiungere meglio gli obiettivi strategici.

Informazioni su questo white paper

Questo white paper illustra sei brevi casi d'uso e punti derivanti da ricerche per aiutarvi a valutare le aree in cui l'organizzazione IT potrebbe acquisire maggiore chiarezza e visibilità, e vi invita a considerare le soluzioni Ivanti in grado di aiutare le organizzazioni a fare proprio questo.



Carenza di visibilità: sei casi d'uso

Considerate le sei situazioni descritte di seguito, e le difficoltà tipicamente associate alla carenza di visibilità:

1 Laptop troppo lenti

Un agente dell'help desk rileva un aumento di chiamate in merito a problemi di lentezza dei laptop. Dopo aver seguito diverse segnalazioni di questo tipo, l'agente viene a conoscenza del fatto che un dirigente è rientrato da una conferenza con una nuova app e ne ha incoraggiato il download dalla sua chiavetta USB, riutilizzando così la stessa licenza. Da ulteriori indagini emerge poi che questa app richiede molte risorse, e non è chiaro su quanti laptop sia stata installata.

Molte organizzazioni IT ancora oggi seguono procedure manuali o non evolute che limitano la visibilità sull'intera situazione interna. È quindi molto difficile rilevare, gestire e proteggere hardware e software, nonché gestire in modo efficace l'utilizzo del software.

Questo scenario solleva diverse incognite:

- Rischio di mancata conformit√† per via di software utilizzato senza licenza.
- Shadow IT, con l'installazione di software non autorizzato.
- Numero di laptop potenzialmente interessati.
- Numero totale di chiamate all'assistenza derivanti dal problema primario.
- Rischi alla sicurezza derivanti dall'installazione e dall'utilizzo di software non autorizzato.
- Rischi associati all'allineamento di licenze ignote.

Reiterando il fatto che non si può gestire, proteggere e ottimizzare ciò che non si vede e non si sa di avere, in un white paper pubblicato da Ernst & Young (EY) dal titolo "Data Validation the Best Practice for Data Quality in Fixed Asset Management" si legge che il 56% delle aziende verifica l'ubicazione degli asset fissi una volta all'anno, mentre tra il 10% e il 15% non controlla i propri asset da oltre cinque anni.

43%

delle organizzazioni intervistate utilizza fogli di lavoro.

50%

usa una soluzione per la gestione degli endpoint.

45%

usa strumenti di inventario come una delle risorse impiegate.

In assenza di un programma formale di IT Asset Management (ITAM), i team spesso si avvalgono solo di Active Directory o di informazioni di inventario di base fornite da soluzioni per la gestione degli endpoint. Per quanto riguarda il tracciamento degli asset, dalla ricerca basata sul sondaggio ITXM commissionato da Ivanti a dicembre 2019 emergono i dati seguenti. Nota - Gli intervistati potevano scegliere più opzioni tra quelle elencate di seguito:

La necessità di combinare dati da origini diverse, ad esempio dati ITSM, ITAM e SAM, rallenta l'acquisizione delle informazioni e riduce la visibilità complessiva. Secondo una ricerca condotta da Enterprise Management Associates (EMA), il 50% delle organizzazioni dispone di almeno 12 strumenti per rilevamento e/o inventario, e l'11% di oltre 30 strumenti. In media, le organizzazioni dedicano 10 ore alla settimana alla risoluzioni di problemi di accuratezza dei dati; il 32% vi dedica più di 25 ore alla settimana.

In breve, la carenza di visibilità conduce all'impossibilità di gestire, proteggere e ottimizzare ciò che non si sa di avere e che non è chiaramente visibile. Le soluzioni Ivanti usano potenti capacità di importazione dei dati che consentono di combinare insieme dati provenienti da diverse origini (fogli di calcolo, strumenti per inventario, lettori di codici a barre, servizi di rilevamento, ecc.) per confrontare i dati effettivi con quelli rilevati e segnalare eventuali discrepanze. Con questo tipo di informazioni, i decision maker possono verificare la validità delle stime e garantire che le informazioni sugli asset siano sempre aggiornate e accurate.

2 Consegna di una partita di router

> Il team dedicato alla rete riceve una chiamata dall'ufficio degli approvvigionamenti. È appena arrivato un pallet di nuovi router. I tecnici iniziano a configurare i nuovi router per sostituire quelli esistenti, prima di rendersi conto che nessuno aveva ordinato i nuovi router.

La carenza di visibilità comporta numerose incognite. Quali sono i dati cronologici degli ordini? Quali sono i fornitori e i percorsi di approvvigionamento preferiti? Quali potenziali rischi alla sicurezza comporta la connessione di un hardware non autorizzato alla rete aziendale?

Nel sondaggio commissionato da Ivanti sull'ITXM (dicembre 2019), già citato, è stato chiesto in che modo le organizzazioni tengono traccia e monitorano i dati di acquisto, i contratti e i dati delle garanzie per gli asset IT. Ecco i risultati. Anche in questo caso era possibile scegliere più opzioni:

39%

degli intervistati usa più sistemi e archivi.

38%

tiene traccia degli asset manualmente, con i fogli di calcolo dell'inventario.

37%

tiene traccia degli asset mediante un archivio o database di gestione degli asset.

22%

sa un sistema dedicato per la gestione dei contratti.

Una maggiore visibilità sui dati e sulle origini dei dati (e la possibilità di sapere di quali dati si dispone e di averli tutti in un unico luogo) può ridurre notevolmente tutte queste difficoltà, con dati coerenti, accurati e affidabili.

Come accennato nell'introduzione, quando Enterprise Service Management e Unified Endpoint Management sono allineati, integrati e automatizzati, si può usufruire dei seguenti vantaggi:

- È possibile usare informazioni sul rilevamento degli asset a scopo predittivo e per intraprendere azioni basate sui tipi, i modelli e i fornitori degli asset problematici.
- Si trae vantaggio da informazioni approfondite che aiutano a migliorare la gestione dei fornitori, lo stato di conformità e l'ottimizzazione delle garanzie.
- Lo staff IT, libero dalle attività di tipo reattivo o non necessarie, può dedicare più tempo e risorse a progetti di maggior valore strategico.
- I rischi alla sicurezza vengono ridotti grazie alla certezza che vengono usati solo hardware autorizzati.
- Si può lavorare in modo più efficiente, con costi e carico amministrativo ridotti al minimo e fornendo più valore aziendale.

3 Riduzione dei costi

Il CIO invita il personale a ridurre i budget per l'anno in corso. Il Responsabile delle Operation vuole capire se è possibile rimandare il ciclo di aggiornamento dei laptop, ma non sa con esattezza quanti laptop e quali dipendenti sarebbero interessati, quali potenziali problemi potrebbero verificarsi e a quanto ammonterebbe la riduzione dei costi.

In questo caso d'uso emergono diverse problematiche associate alla visibilità: l'assenza di dati storici relativi ai fornitori e agli incidenti per tipo di laptop, l'assenza di un sistema di monitoraggio dell'intero ciclo di vita degli asset per determinare lo stato e le prestazioni dei vari tipi di laptop, e l'assenza della cronologia relativa alle pach. Inoltre, non si sa quali dipendenti verrebbero interessati.

Disponendo invece di dati affidabili, un cliente Ivanti è stato in grado di estendere i cicli di aggiornamento dei dispositivi di 6-12 mesi, generando un risparmio iniziale per il reparto IT di 1,5 milioni di dollari senza alcun impatto negativo né sul tasso di incidenti né sulla qualità del servizio erogato agli utenti finali.

Inoltre, dal sondaggio ITXM di dicembre 2019 emerge quanto segue:

La capacità di comprendere i cicli di vita degli asset, le loro prestazioni, lo stato di compliance e le implicazioni a livello di costi è particolarmente importante per le aziende che operano in settori altamente regolamentati. Si pensi ad esempio al settore dei dispositivi medici e ai regolamenti Mobile Device Regulation (MDR) e European Database on Medical Devices (EUDAMED).

28%

ei professionisti IT intervistati dedica diverse ore alla settimana al supporto di asset che non sono più coperti da garanzia o che non rientrano più nella politica di supporto.

20%

di essi indica inoltre di non disporre di informazioni sugli asset non aggiornati.

4 E-mail troppo lenta

Una mattina il personale dell'help desk viene subissato di chiamate. L'e-mail "non funziona", "è lentissimo". Dopo numerose chiamate ad altri team IT, il personale IT Operations capisce che qualcuno, durante la notte, ha aggiornato l'applicazione e-mail e il server corrente non può gestire le modifiche di configurazione, con conseguenti problemi di prestazioni. Non è immediatamente chiaro se dispongono dell'hardware necessario per alleviare i problemi.

A causa della carenza di visibilità, in questa situazione non è possibile ottenere una cronologia affidabile in merito alla modifica e alla configurazione, non si possono prevedere le modifiche future, non è possibile eseguire un'analisi dell'impatto e dei rischi associati alla modifica, e non si conosce lo stato dell'inventario hardware.

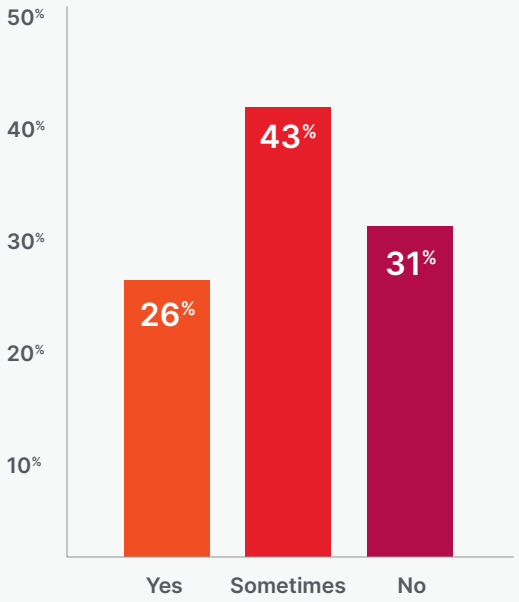
Le organizzazioni sviluppano obiettivi IT per migliorare l'attuale livello di maturità e si avvalgono dell'automazione per ottimizzare l'efficienza. Eppure molti si dimenticano del primo indispensabile passaggio: definire la linea di partenza. Per definire la linea di partenza, è necessario: 1) ottenere piena visibilità su processi e sulle azioni che interessano i servizi chiave e sugli asset sottostanti, ad esempio la gestione delle modifiche; e 2) comprendere appieno i pattern al verificarsi di incidenti, le cause alla base di sistemi non disponibili e così via, per poter determinare lo stato iniziale dal quale avviare le iniziative di miglioramento.

Purtroppo, nonostante il grande impegno del personale IT, spesso le attività di servizio e supporto sono limitate alla reattività a causa di sistemi inadeguati e carenza di risorse. Risulta quindi difficile adottare un approccio sistematico per andare oltre i risultati a breve termine, e i problemi vengono risolti man mano che si presentano. Inoltre:

- Molti processi sono spesso manuali e non seguono flussi di lavoro o standard IT coerenti.
- La visibilità dello stato attuale o dell'impatto lascia a desiderare e le capacità di reporting sono minime, se non addirittura assenti.
- I costi continui e i rischi sono elevati, i tempi di risoluzione troppo lunghi e la qualità dei servizi scadente.
- I dirigenti potrebbero non essere a conoscenza dell'impatto che può avere il team addetto ai servizi, e solo raramente supporta ulteriori investimenti nell'IT.
- Klaren und unterstützt größere Investitionen nur selten.

Sondaggio: L'impatto dell'allineamento dei processi di IT Service Management e IT Asset Management

I vostri processi di Service Management e le service request hanno automaticamente visibilità sulle informazioni e le relazioni tra gli asset?



I dati riportati di seguito, tratti dal sondaggio ITXM di dicembre 2019, illustrano in quale misura i processi di gestione dei servizi e i flussi di lavoro per le richieste possono attingere direttamente ai dati sugli asset e le loro interrelazioni.

Meno di un terzo degli intervistati ha indicato di disporre di informazioni sugli asset, mentre per i restanti due terzi tale visibilità è parziale o non esistente.

Secondo lo stesso sondaggio, i professionisti IT si aspettano di vedere i seguenti miglioramenti derivanti dall'integrazione di processi e dati tra gestione dei servizi e gestione degli asset IT:

- Migliore visibilità sul patrimonio IT: 63 %
- Maggiore produttività del personale IT: 59 %
- Ottimizzazione dei costi: 54 %
- Migliore fornitura di servizi: 53 %

5 Laptop bloccato

Un commerciale chiama l'help desk dicendo di non poter accedere al suo laptop, e un messaggio lo sollecita a chiamare un numero per sbloccarlo. Riferisce anche che, prima del blocco, aveva fatto clic su un collegamento in una mail che pensava provenisse da un partner con cui ha lavorato in passato. Non è chiaro, ma è possibile che anche altri dipendenti abbiano ricevuto la stessa mail.

In questo caso, i potenziali problemi derivanti da una carenza di visibilità comprendono: impossibilità di sapere se altri dipendenti abbiano ricevuto la stessa mail; impossibilità di avere un quadro aggiornato sullo stato attuale di applicazione delle patch; impossibilità di sapere chi disponga di autorizzazioni di livello amministratore per i computer; e impossibilità di sapere quanti dispositivi sono stati infettati e il loro stato.

Nel 2019 Ivanti ha sponsorizzato un sondaggio su Windows 10, da cui emerge che una delle questioni di sicurezza prioritarie riguarda il rischio di violazioni di dati (41%), seguita dal timore di ransomware/malware (20%). Un altro sondaggio sponsorizzato da Ivanti e pubblicato nell'aprile del 2019 rileva che il 70% delle organizzazioni vorrebbe soprattutto conoscere l'effettivo livello di sicurezza del proprio ambiente, e quasi il 60% vorrebbe visibilità sui dati delle applicazioni.

Dal punto di vista della gestione unificata degli endpoint, la carenza di visibilità aumenta il tempo necessario ad affrontare i problemi di sicurezza. Aumenta anche il rischio che un incidente si tramuti in una violazione che possa compromettere i dati dell'organizzazione; mette sotto pressione i team già sovraccarichi; e riduce il livello di fiducia nell'organizzazione. Tutto questo può risultare da visibilità limitata o dalla mancanza di dati integrati, determinando conflitti nei dati sugli asset e nelle informazioni sulla sicurezza, lacune di visibilità e difficoltà di reazione.

Al contrario, potendo contare su informazioni accurate sullo stato delle patch e sugli accessi degli utenti, è possibile reagire tempestivamente a eventuali attacchi proteggendo la rete; debellare minacce ransomware e interromperne la diffusione; e prepararsi ad affrontare eventuali attacchi futuri.

La carenza di visibilità, inoltre, non consente di gestire in maniera efficiente le esigenze di re-imaging a supporto delle attività di recupero in seguito a situazioni come quella appena descritta.

La visibilità completa sugli asset presenti nell'ambiente aziendale, con dati relativi a dove si trovano, come vengono utilizzati e da chi, senza dover ricorrere a complicati fogli di calcolo, è fondamentale per l'efficienza operativa degli analisti del service desk e per consentire loro di risolvere rapidamente i problemi che si verificano. In questo caso d'uso, una maggiore visibilità sulla potenziale minaccia veicolata da una mail sospetta consente anche di intervenire e porvi rimedio più rapidamente.

6 Il grande ignoto

Un analista IT sta valutando la sicurezza dell'ambiente aziendale e si rende conto di una grande incognita: quanti computer ci sono realmente e come vengono gestiti? Solo il 75% dell'ambiente è realmente noto. In seguito ad aggiornamenti ed altri interventi, molti computer escono dal ciclo di gestione. Per quanto riguarda i server, sono state create macchine virtuali prive di informazioni di configurazione adeguate e che ormai non sono più aggiornate con le ultime patch.

In questo caso, la carenza di visibilità sugli endpoint e sui server presenti nell'ambiente determina anche la mancanza di informazioni sui sistemi a cui sono sono state applicate le patch a livello di produzione. La capacità di sapere sempre dove si trovano tutti gli asset dell'azienda non è fondamentale solo dal punto di vista del supporto, ma anche in termini di sicurezza. Gli asset non gestiti e privi delle ultime patch rappresentano un rischio per l'integrità dei dati e lo stato di conformità. E dato il numero sempre crescente di vulnerabilità IT, è imperativo poter tenere traccia di ogni dispositivo.

Nel white paper pubblicato da Ernst & Young precedentemente citato, dal titolo "Data Validation the Best Practice for Data Quality in Fixed Asset Management", si legge che il 30% degli asset IT fissi sono risorse "fantasma" che non possono essere reperite. La visibilità degli asset è un aspetto fondamentale, in quanto il patrimonio IT effettivo è spesso sottostimato. Quando un'organizzazione avvia un'iniziativa di IT Asset Management, può trovare tra il 20% e il 30% di dispositivi in più rispetto a quelli che si aspettava. Non è possibile gestire ciò che non si sa di avere, e i dispositivi non gestiti rappresentano un notevole rischio alla sicurezza.

Con soluzioni Unified Endpoint Management, si può ottenere visibilità completa e controllo sugli endpoint, e quindi proteggere ogni asset ed evitare le minacce derivanti da dispositivi non protetti e non gestiti. I team IT possono adottare una strategia di provisioning automatizzato con analisi in tempo reale e riconciliazione dei dati relativi a utenti e ubicazione. Per evitare il dilagare di server virtuali, è importante poter controllare chi dispone di autorizzazioni di livello amministratore, e consentire ad altri gruppi IT di generare macchine virtuali sicure a livello di produzione. Ma anche così facendo sarà importante poter rilevare tali nuovi server e aggiungerli ai gruppi appropriati, affinché vengano inclusi nella successiva finestra di manutenzione.

Inoltre, gli asset devono essere gestiti durante il loro intero ciclo di vita. Monitorandone le prestazioni, i problemi, le correzioni, le patch, i contratti e le licenze, si avrà la certezza di ricavare il massimo dagli investimenti software e hardware in termini di prestazioni e produttività degli utenti.

Ivanti : visibilità a 360 gradi

Nel loro ruolo di leadership e responsabilità, i CIO, CISO e VP non possono permettersi problemi di visibilità nell'ambito IT . Le nostre soluzioni Unified Endpoint Management e Enterprise Service Management offrono la visibilità necessaria per completare i dati del settore e supportare sia i vostri obiettivi sia la missione e la vision della vostra azienda.

Scoprite come Ivanti può migliorare la visibilità IT nella vostra organizzazione, consentendovi di intervenire in modo decisivo, offrire agli utenti un'esperienza IT ottimizzata e incrementare sia l'efficienza organizzativa sia la produttività. Per saperne di più, non esitate a contattarci.

ivanti

ivanti.it
+33 (0)1 76 40 26 20
contact@ivanti.it