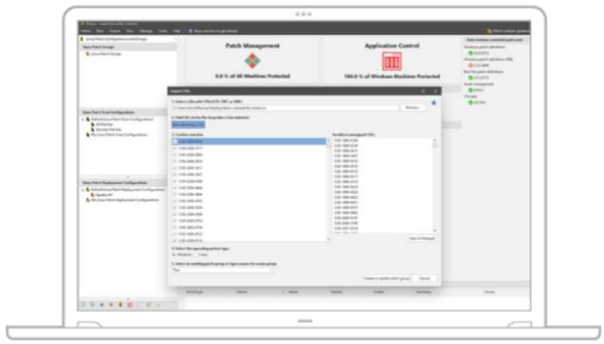
Ivanti Security Controls

I team IT dedicano troppo tempo a gestire la sicurezza per un numero sempre crescente di dispositivi, ed i team Security hanno risorse limitate. Ivanti semplifica la sicurezza con una soluzione unificata che contrasta i maggiori vettori di attacchi. Ivanti Security Controls (evoluzione di Ivanti Patch for Windows) riunisce strumenti di sicurezza che gli esperti in tutto il mondo riconoscono essere in grado di contrastare al meglio gli attacchi informatici di nuova generazione. Tali strumenti permettono di rilevare i software autorizzati e non autorizzati nell'ambiente aziendale; gestire le patch in ambienti eterogenei e per applicazioni di terze parti; abilitare il whitelisting dinamico; e gestire le autorizzazioni in modo granulare. Comprendono inoltre strumenti per patch aggiuntivi grazie ai quali i team IT e Security possono collaborare con maggior efficienza per meglio proteggere l'azienda.

Patch per sistemi Windows e Linux

Ivanti Security Controls è una singola soluzione per la gestione automatizzata delle patch, non solo per i server Windows fisici e virtuali, ma anche per le workstation. Alla soluzione leader per il patching Windows, abbiamo aggiunto il supporto delle patch per Red Hat Enterprise Linux.

- **Patch per server virtuali.** Potete rilevare workstation e server sia online che offline, analizzare i sistemi, individuare le patch mancanti ed implementarle. Quindi potete gestire le patch di sistemi operativi ed applicazioni, VM e persino l'hypervisor ESXi, grazie all' integrazione con VMware. Anche le immagini virtuali offline possono essere mantenute sempre aggiornate e pronte all'implementazione, evitando così di dover creare una VM, e successivamente applicarvi le patch. Mantenendo sempre aggiornati i modelli offline, potrete implementare una VM senza correre il rischio che non disponga di tutte le ultime patch.



- **Patch senza agenti.** Grazie alla tecnologia priva di agenti, potete valutare e distribuire le patch ai computer e server collegati in rete, con un impatto minimo sul vostro team e sul carico dei sistemi. In alternativa, potete usare l'agente per creare criteri diversi in base alle esigenze di gestione della rete. Potrete così operare con maggiore flessibilità ed accuratezza negli ambienti in cui i dispositivi non sono sempre connessi alla rete, assegnando configurazioni agente differenti ai diversi dispositivi utilizzati nell'azienda.
- **Patch per computer Windows e Linux.** Scegliete un software consolidato per la gestione delle patch in ambienti eterogenei. È indispensabile poter estendere la gestione delle patch oltre il mondo Windows. E con uno strumento efficiente, automatizzato e con una singola interfaccia, si liberano le risorse IT e si riduce il potenziale di errori, oltre a ottimizzare la protezione.
- **Patch per le applicazioni.** Le applicazioni e gli add-on per browser più sfruttati dagli hacker sono prodotti di terze parti come Adobe Acrobat, Flash e Reader, Google Chrome, Mozilla Firefox e Oracle Java.

  Offriamo il più esteso catalogo di patch per applicazioni di terze parti, ed il nostro team addetto ai contenuti sottopone tutte le patch a rigorosi test grazie ai quali potrete risparmiare tempo prezioso da dedicare piuttosto agli obiettivi aziendali più strategici.

Whitelisting e gestione delle autorizzazioni

Ivanti Security Controls offre un'opzione di whitelisting più dinamica, basata su modelli di attendibilità anziché elenchi, con chiari vantaggi: maggiore rapidità di implementazione, minori costi di gestione una volta implementata, e minor impatto sulle prestazioni, mantenendo sempre un elevato livello di sicurezza. Non occorre più assegnare i diritti di amministratore a tutti, e gli utenti potranno comunque accedere alle risorse di cui hanno bisogno. Inoltre, risulterà più facile aggiungere ulteriori autorizzazioni ove necessario.

- **Whitelisting più semplice.** È possibile rilasciare le autorizzazioni di accesso per applicazioni, servizi e componenti, senza che l'IT debba gestire manualmente lunghi elenchi né imporre vincoli agli utenti. Trusted Ownership™, ad esempio, permette di definire il proprietario NTFS di un file per semplificare il processo di whitelisting. Utilizzando alcuni account affidabili per definire la proprietà di file attendibili si semplifica l'implementazione di una white list, nonché l'aggiunta e l'aggiornamento continuo delle applicazioni tramite i sistemi di gestione. I proprietari affidabili infatti sono gli account che eseguono le operazioni di installazione ed aggiornamento.
- **Controllo delle "chiavi del regno".** Esistono numerose vulnerabilità che, se sfruttate, offrono agli hacker le stesse autorizzazioni di accesso dell'utente attuale. Un hacker potrà così utilizzarne le credenziali e i diritti di amministratore per accedere a dati e sistemi e penetrare ulteriormente nella rete. Quando si concedono agli utenti i diritti di amministratore per un server, si introducono anche altri rischi, come la possibilità di avviare o interrompere dei servizi nonché di installare o rimuovere accidentalmente un software.

  Alcune aziende possono applicare un blocco rigoroso delle autorizzazioni degli utenti, ma in genere gli utenti devono poter accedere a specifici dati o sistemi e questo inevitabilmente porta all'assegnazione di privilegi per amministratori. Microsoft offre solo due livelli di controllo: utente o amministratore. Vi sono alcune varianti, ma non sono sufficienti per offrire una buona esperienza sia agli utenti che agli amministratori.

  Le nostre soluzioni si basano sugli approcci Just Enough Administration (JEA) e Just-in-Time Administration (JIT). Potrete così revocare i diritti di amministratore ma consentire comunque agli utenti di accedere ai dati e servizi necessari per il loro lavoro, semplificando il processo di escalation o aggiungendo ulteriori permessi ove necessario. Ora si può scegliere. Invece di assegnare agli utenti i diritti di amministratore, potete fornire loro i normali diritti di utente con la possibilità di usufruire di diritti più elevati quando se ne presenta la necessità, ad esempio per installare un'applicazione o una stampante, usare PowerShell o accedere a specifici dati. Sempre entro quanto previsto dal suo ruolo. Oppure potete assegnare i diritti di amministratore, rimuovendo però l'accesso ad alcuni elementi non pertinenti. Ad esempio, potete rimuovere PowerShell o l'accesso a specifiche capacità. Potete limitare i privilegi di amministratore a particolari console, applicazioni, servizi e comandi, riducendo il rischio di introdurre malware, interrompere servizi fondamentali o compromettere le prestazioni di servizi mission-critical.

Altri strumenti utili per risparmiare tempo e denaro

Ivanti Security Controls include inoltre le seguenti funzionalità con cui i team Security e IT Ops possono proteggere l'organizzazione in modo più efficiente.

- **Integrazione ed automazione oltre le soluzioni Ivanti.** Grazie alle API REST, Security Controls può integrarsi con altri prodotti, automatizzare i processi condivisi e fornire funzioni di controllo ed accesso in remoto.
- **Colmare il gap tra Security e IT Ops con la creazione di elenchi di patch da CVE.** Ivanti Security Controls può basarsi su una valutazione delle vulnerabilità generata dal fornitore scelto dall'organizzazione per individuare tutte le patch relative a tali CVE (Common Vulnerabilities and Exposures), e creare quindi un gruppo di aggiornamenti che possono essere rapidamente approvati ed implementati nell'ambiente. Un enorme risparmio di tempo rispetto all'attuale procedura manuale.

Ulteriori informazioni

www.ivanti.it
+39 02 8734 3421
contact@ivanti.it