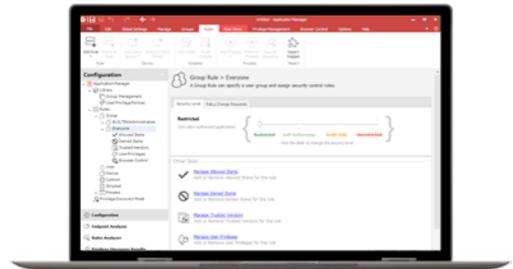


Application Control

Höhere Endpunktsicherheit, niedriger Arbeitsbelastung und Kosten für die IT-Abteilung

Ivanti® Application Control bietet der IT-Abteilung eine nie dagewesene Kontrolle über Endpunkte, reduziert das Sicherheitsrisiko und sorgt zugleich für ein großartiges Nutzungserlebnis in den neuesten Windows-Umgebungen. Abgesehen von der kontextabhängigen Anwendungskontrolle ermöglicht die Lösung eine sichere Windows-Rechteverwaltung, mit der Sie umfassende Administratorrechte von Benutzern entfernen können. Sie verhindert auch, dass nicht autorisierte ausführbare Dateien wie Malware, Ransomware, nicht lizenzierte Software und andere unbekannte Anwendungen installiert oder ausgeführt werden. Mit Application Control 10.1 kann Ihr IT-Team den Anwendungszugriff und die Benutzerrechte für Ihre gesamte Desktop- und Serverlandschaft verwalten.



Volle Unterstützung für Windows Server 2016 und erweiterte Unterstützung für Windows 10

Application Control 10.1 bietet volle Unterstützung für Windows Server 2016 und erweiterte Unterstützung für Windows 10, wobei es dessen Fähigkeiten ausbaut, Ransomware und Malware zu stoppen. Mit den erweiterten granularen Endbenutzer-Kontrollfunktionen dieser neuesten Version können IT-Administratoren die Endbenutzerpersonalisierung und die Endpunktsicherheit verbessern

Trusted Ownership™

Application Control verwendet Trusted Ownership zur Überprüfung der standardmäßigen Endpunktsicherheit. Dabei stützt sich die Lösung auf die Prüfung des NTFS-Besitzers einer Anwendung. Führt ein nicht vertrauenswürdiger Besitzer (z. B. ein Standardbenutzer) eine Anwendung ein, die er folglich „besitzt“, dann wird die Ausführung dieser Anwendung unmittelbar unterbunden.

Wird eine Anwendung jedoch von einem „vertrauenswürdigen Besitzer“ (Trusted Owner) wie einem Administrator oder einem System zur Softwarebereitstellung (z. B. Microsoft SCCM) eingeführt, dann kann jeder Benutzer diese Anwendung ausführen, sofern nicht anders festgelegt. Auf diese Weise wird die Belastung des IT-Teams reduziert, denn es muss keine Positivlisten mehr verwalten, wie sie bei anderen Lösungen zur Anwendungskontrolle beim Patchen von Anwendungs- oder Betriebssysteminhalten zum Einsatz kommen.

Digitale Signaturen

Sie können Anwendungen und Dateien digitale SHA-1-, SHA-256- oder ADLER32-Signaturen zuweisen, um die Integrität von Anwendungen sicherzustellen und die Ausführung von modifizierten oder manipulierten Anwendungen zu verhindern.

Positiv- und Negativlisten

Die IT kann Positiv- und Negativlistenkonfigurationen in Verbindung mit Trusted Ownership zur Kontrolle von bekannten Anwendungen verwenden, die bei der Prüfung des NTFS-Besitzers nicht beanstandet wurden. Anwendungen, auf die Benutzer keinen Zugriff haben sollten, beispielsweise administratoreigene Tools wie cmd.exe oder ftp.exe, werden automatisch verweigert. Sie können aber auch mittels Positivlisten sicherstellen, dass nur bekannte und vertrauenswürdige Anwendungen auf einem System ausgeführt werden können.

Windows-Rechteverwaltung

Werden Benutzern volle Administratorrechte erteilt, kann dies bei Endpunkten zu Anfälligkeiten führen und signifikante Kostensteigerungen bei Sicherheit und Verwaltbarkeit und Produktivitätseinbußen nach sich ziehen, rechtliche und Haftungsfragen aufwerfen und die Compliance erschweren. Indem Sie Benutzern die vollen Administratorrechte entziehen und ihnen erhöhte Rechte genau für diejenigen Anwendungen und Aufgaben erteilen, die sie benötigen, vereinfachen Sie die Endpunktsicherheit, reduzieren die Anzahl der Anrufe beim Support und senken Ihre Gesamtbetriebskosten.

Change-Requests auf Abruf

Mobile Benutzer bzw. Benutzer, die offline arbeiten, müssen unter Umständen auf nicht genehmigte Anwendungen zugreifen. Wird der Zugriff auf diese Anwendungen unterbunden, führt dies zu Produktivitätseinbußen und einem schlechten Erlebnis beim Benutzer. Change-Requests auf Abruf versetzen Endbenutzer in die Lage, eine Noterhöhung ihrer Rechte oder ihres Anwendungszugriffs anzufordern, wenn ihre Produktivität aufgrund der Nichtverfügbarkeit von Anwendungen beeinträchtigt wird.

URL-Umleitung

Verlässt ein Benutzer einen Webbrowser, in dem eine bestimmte Webseite oder Anwendung geöffnet ist, und stellt dann die Verbindung über ein anderes Gerät oder einen anderen Standort wieder her, kann der Browser auf eine vordefinierte sichere Adresse umgeleitet werden.

Archivierung von Anwendungen

Wenn Benutzer versuchen, verbotene Dateien auszuführen, werden diese automatisch kopiert und zur sicheren Analyse in einem gesicherten Repository gespeichert.

Lizenzverwaltung

Microsoft hat Application Control als eine Lösung für die Durchsetzung einer gerätebasierten Softwarelizenzkontrolle anerkannt. Durch die Kontrolle der Benutzer und Geräte, die berechtigt sind, bestimmte Anwendungen auszuführen, können Beschränkungen definiert werden, sei es für die Anzahl der Anwendungsinstanzen, die Geräte oder Benutzer, die zur Ausführung der Anwendung berechtigt sind, oder für die Zeit und die Dauer, zu der bzw. für die Benutzer ein Programm ausführen können.

www.ivanti.de[+49 \(0\)69 941 757-0](tel:+49(0)699417570)contact@ivanti.de