Application Control for Windows Servers

Schutz für Windows-Server mit rollenbasiertem Benutzerzugriff

Mit Ivanti® Application Control for Windows Servers können Sie den Zugriff auf Server kontrollieren und das Risiko reduzieren, indem Sie die administrativen Rechte von Benutzern beschränken, die sich zur Erledigung bestimmter arbeitsbezogener Aufgaben bei einem Server anmelden müssen. Dies ist insbesondere bei einem Mehrzweckserver (z. B. SQL und IIS) mit mehreren Administratorbenutzern vorteilhaft oder wenn ein Unternehmen Auflagen erfüllen muss, die Sicherheitspraktiken für die EDV-Infrastruktur vorgeben.

Mit Application Control for Windows Servers kann die IT administrative Rechte auf bestimmte Konsolen, Anwendungen, Services und Befehle beschränken.

Beschränken Sie Benutzer bei der Serveranmeldung auf die Durchführung bestimmter Tasks

Mit Ivanti Application Control for Windows Servers kann die IT die administrativen Rechte auf bestimmte Konsolen, Anwendungen, Services und Befehle beschränken und dadurch das Risiko reduzieren, dass Administratoren Malware einschleppen, die wichtige Services zum Erliegen bringen oder die Erbringung von unternehmenskritischen Services beeinträchtigen.

Erhöhung von Rechten

Erhalten Benutzer, die nicht als IT-Systemadministratoren geschult sind, volle Administratorrechte, bringt dies mehrere Risiken mit sich, z. B. das Starten oder Stoppen von Services oder die versehentliche Installation oder Deinstallation von Software. Dies kann das Sicherheitsrisiko und die Kosten der Verwaltbarkeit erhöhen, die Produktivität beeinträchtigen, rechtliche und Haftungsfragen aufwerfen und die Erfüllung von Compliance-Anforderungen erschweren. Indem Sie Benutzern die vollen Administratorrechte entziehen und ihnen erhöhte Rechte genau für diejenigen Tasks erteilen, die sie für ihre Arbeit benötigen, können Sie die Endpunktsicherheit vereinfachen, die Anzahl der Anrufe beim Support reduzieren und Ihre Gesamtbetriebskosten senken.

Application Control

Ivanti Application Control for Windows Servers gewährt autorisierten Zugriff auf Serveranwendungen, Services und Komponenten basierend auf Positivlisten für Anwendungen. Mit Application Control kann die IT die Datenintegrität durch Zuweisung einer digitalen SHA-1, SHA-256 oder ADLER32-Signatur sicherstellen. Zusätzlich kann die IT die Metadaten von Dateien prüfen (z. B. Anbieter, Zertifikat, Herausgeber, Version und mehr), um die Integrität von Anwendungen, Komponenten und Skripts sicherzustellen und die Ausführung von modifizierten oder manipulierter Anwendungen zu verhindern.

Schutz durch Systemkontrollen

Setzen Sie Systemkontrollen ein, um den Zugriff auf bestimmte Services zu beschränken, das Entfernen oder Ändern von Serveranwendungen und -prozessen sowie das Löschen von bestimmten Ereignisprotokollen zu verhindern.

Negativliste der Anwendungen

Implementieren Sie kurzerhand Negativlisten, um den Administratorzugriff auf kritische Anwendungen und Komponenten des Serverbetriebssystems zu kontrollieren. Negativlisten verhindern, dass wichtige Serverressourcen modifiziert werden, und erhöhen den Serverschutz im Rechenzentrum.

Befehlszeilenvergleich

Mit Application Control for Windows Servers können Sie Sicherheitsrichtlinien auf den Start von Anwendungen und die zugehörigen Befehlszeilenargumente anwenden. Bei Anwendungen wie Windows PowerShell in Serverumgebungen können Sie den Administratorzugriff auf den Start von bestimmten Dateien und Skripten beschränken bzw. die Ausführung der Anwendung nur unter bestimmten Bedingungen erlauben.

Kontrolle des Netzwerkzugriffs von Anwendungen

Diese Funktion verhindert den Netzwerkzugriff ohne Einsatz von komplexen Kontrollmechanismen wie Routern, Switches und Firewalls. Sie kann Sicherheitsrisiken beseitigen, die durch IT-Administratoren verursacht werden, die über bestimmte Server Zugriff auf geschützte Rechenzentren oder Netzwerkressourcen erhalten.

Kontextabhängige Kontrolle

Für die Verwaltung des Zugriffs auf Serverressourcen nimmt Application Control eine umfangreiche Prüfung von Bedingungen basierend auf dem Kontext des angemeldeten Benutzers vor. Sie können den Kontext anhand von Bedingungen wie u. a. folgenden bewerten: Benutzer, Gruppen- oder OU-Mitgliedschaft, Gerätename, Geräte-IP- oder MAC-Adresse, Informationen zum vermittelnden Client, Betriebssystem, Site-Mitgliedschaft, Datum und Uhrzeit oder sogar benutzerdefinierte Regeln, die mit PowerShell, VBScript oder JScript erstellt wurden. Darüber hinaus stellt die vollintegrierte Unterstützung für Microsoft RDSH, Citrix XenApp, Citrix XenServer und VMware sicher, dass Sicherheitslinien auch auf Remotesitzungen angewendet werden können.

www.ivanti.de

+49 (0)69 941 757-0

contact@ivanti.de