

Schutz vor internem Datenverlust

Tragbare Speichermedien sind überall im Einsatz. Berufstätige und Studenten nutzen sie, und selbst Anwender ohne Vorkenntnisse können diese Medien an einen PC anschließen, auf Ihr Netzwerk zugreifen und potenzielle Schädlinge in Ihre Umgebung einschleusen oder vertrauliche Daten aus dem Netzwerk kopieren. Wissen Sie genau, welche Unternehmensinformationen mit solchen Wechselmedien mitgenommen werden?

Numara[®] FootPrints[®] Device Manager – Vorteile

- ❖ Implementierung und Durchsetzung einer Datenschutzstrategie mit minimalem Aufwand
- ❖ Einschränkung und Kontrolle des Datenzugriffs
- ❖ detaillierte Datenerfassung und Berichterstattung, um Prüfungsstandards zu erfüllen
- ❖ Unterstützung von Upload-/Download-Aktivitäten verschiedenster Geräte

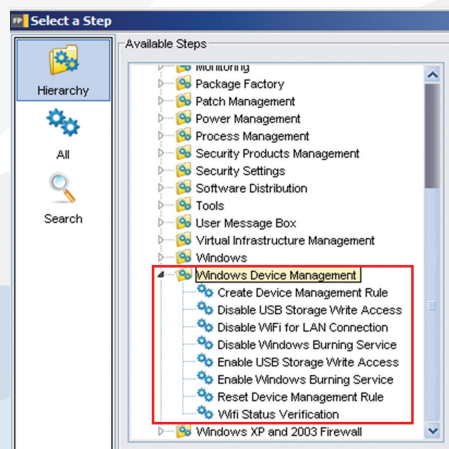
Die meisten Organisationen nutzen Firewalls und Anti-Virus-Software, um sich vor externen Bedrohungen zu schützen. Allerdings wird nun vielen bewusst, dass der Schutz vor internen Bedrohungen ebenso wichtig ist. Der Verlust von sensiblen Daten und geistigem Eigentum kann geschäftsschädigend sein und aus Gründen wie Datenwiederherstellung, Systemausfall, Geschäftsverlust, gesetzlicher Haftung oder Rufschädigung schnell zu einer äußerst teuren Angelegenheit werden.

Mit Numara FootPrints Device Manager kann sich Ihre Organisation besser vor solchen Folgen schützen und Ihr Geschäft absichern, da Risiken in Verbindung mit der unbefugten Verwendung unzulässiger Geräte und Speichermedien minimiert werden. Mit FootPrints Device Manager können Sie Richtlinien definieren, die genau festlegen, welche Geräte zugelassen oder gesperrt sind. Dadurch sinkt die Gefahr, dass Vorschriften nicht eingehalten werden, und es entfällt die manuelle Bearbeitung sowie Lösung von Problemen, die durch die böswillige Verwendung nicht genehmigter Geräte verursacht werden. Über Nutzungsrichtlinien, sogenannte „Betriebsregeln“, können Sie festlegen, welche Geräte von einer bestimmten Richtlinie auf Grundlage von Einzelgeräten in beliebiger Kombination oder von festgelegten Gruppen erfasst werden. FootPrints Device Manager gibt Ihnen also die Möglichkeit, mit minimalem Aufwand Datenschutzmaßnahmen zu konfigurieren und durchzusetzen.

Einhaltung von Vorschriften

FootPrints Device Manager steuert zentral die Upload- und Download-Aktivitäten von Bluetooth[®]-Geräten, CD- und DVD-Laufwerken, Firewire-Geräten, Floppy-Laufwerken, Modems sowie kabellosen und USB-Geräten. Da die Lösung zur Numara Security & Compliance Suite gehört, können Sie alle Ereignisse der Peripheriegeräte über eine Schnittstelle steuern und protokollieren. Wird Datenverlust vermutet, können unerwünschte Aktivitäten einfach geprüft, verfügbare Ereignisprotokolle analysiert und Richtlinien entsprechend angepasst werden.

Bei Compliance ist der Schutz vor Datenverlust für die IT eines der wichtigsten Themen. In den Datenschutz-Rahmenplänen vieler Organisationen sind Wechselmedien gar nicht als Gefahrenquelle aufgeführt. Das Bewusstsein für den Risikofaktor Datenverlust steigt jedoch und eines ist klar: Entweder Sie schützen Ihre sensiblen und vertraulichen Daten oder Sie müssen die mit Sicherheitsverstößen einhergehenden Konsequenzen tragen.



Für das Windows[®]-Gerätemanagement sind verschiedene Optionen verfügbar. Es besteht die Möglichkeit, benutzerspezifische Regeln zu erstellen, die den Organisationsanforderungen entsprechen.

Dieses gestiegene Bewusstsein hat viele Branchen dazu veranlasst, Vorschriften auszuarbeiten, die Sicherheitsvorkehrungen für gespeicherte personenbezogene oder finanzielle Daten verlangen. Zu den bekanntesten Vorschriften gehören:

- der Payment Card Industry Data Security Standard (PCI DSS) für Organisationen, die Daten von Kreditkarteninhabern erfassen, speichern oder verarbeiten,
- der Gramm-Leach-Bliley Act (GLB) für Organisationen der Finanzwirtschaft,
- der Health Insurance Portability and Accountability Act (HIPAA) für Gesundheitsdienstleister oder Versicherungsunternehmen,
- der Sarbanes-Oxley Act (SOX) für börsennotierte Unternehmen, Wirtschaftsprüfungsgesellschaften und Audit-Unternehmen.

Mit FootPrints Device Manager können Sie viele Aspekte der gängigsten Branchenvorschriften auf einfache Weise kontrollieren. In Verbindung mit leistungsstarken internen Sicherheitsrichtlinien und einer Sensibilisierung der Nutzer hilft Numara Software Ihnen dabei, Risiken einzudämmen und Prüfern die für den Nachweis der Compliance benötigten Informationen bereitzustellen.

Funktionen

- **Unterstützung verschiedener Geräte** – Upload- und Download-Aktivitäten von Bluetooth-Geräten, CD- und DVD-Laufwerken, Firewire-Geräten, Modems sowie kabellosen und USB-Geräten lassen sich zentral steuern.
- **Alternative zur Gruppenrichtlinie** – Richtlinien zur Steuerung von Upload- und Download-Geräteaktivitäten können verwaltet und angewendet werden – ohne die für Gruppenrichtlinien typische Komplexität.
- **Management von Ereignisprotokollen** – Durch die Erfassung von Ereignisprotokollen einzelner Geräte oder Gerätegruppen und die dazugehörigen Berichte können Sie erkennen, gegen welche Richtlinien verstoßen wurde.
- **Betriebsregeln** – Sie können festlegen, welche Geräte von einer bestimmten Richtlinie erfasst werden. Grundlage können Einzelgeräte in einer beliebigen Kombination oder festgelegte Gruppen sein.
- **Sofortige Berichterstellung** – Über Executive Dashboards und umfassende Berichte lassen sich Ergebnisse aufzeigen.

FootPrints family

- FP Incident&ProblemManager
- FP ChangeManager
- FP ConfigurationManager
- FP ServiceCatalogManager
- FP InventoryManager
- FP RemoteManager
- FP DeploymentManager
- FP PatchManager
- FP DeviceManager**
- FP VulnerabilityManager
- FP ComplianceManager
- FP PowerManager
- FP MigrationManager

Die Freiheit, einfach... zu wählen

FootPrints Device Manager ist Bestandteil einer vollständig integrierten IT Operations Management-Lösungsreihe. Die FootPrints-Lösungsfamilie ist modular aufgebaut und dient dazu, verschiedenste komplexe Anforderungen rund um das Servicemanagement, Asset Management sowie PC-Lifecycle-Management zu vereinfachen.

Stellen Sie sich vor... Sie haben folgende Möglichkeiten:

- Entscheiden Sie, welche Komponenten und Produkte für Ihr Unternehmen relevant sind.
- Verwalten Sie unterschiedliche Plattformen von einer einzigen Konsole aus.
- Investieren Sie in ein einziges Produkt, in eine Lösungsfamilie mit mehreren Produkten, oder in die gesamte Suite.
- Kaufen Sie, was Sie benötigen und nicht, was der Anbieter vorschreibt.

Weitere Informationen zu den Mindestanforderungen für die Nutzung von FootPrints Device Manager erhalten Sie online in unserem Dokument „Technische Daten“.

Über uns

Numara® Software wurde 1991 gegründet und ist ein führender globaler Anbieter integrierter Managementlösungen für IT-Abläufe. Numara bietet für physische, virtuelle und mobile Geräte ein Portfolio integrierter Lösungen. Sie unterstützen das Management des Endgeräte-Lifecycles und mobiler Geräte genauso wie Help Desks sowie Service Desks und vereinfachen und optimieren das Management des IT-Betriebs.



freedom
to simply choose
the right solution for you