Ivanti Endpunktsicherheit mit Technologie von Heat

Bringen Sie Ihre Endpunkte unter Ihre Kontrolle

Das moderne, sich rasch verändernde IT-Netzwerk ist stärker verteilt und virtualisiert denn je: Immer mehr Daten werden auf remoten Endpunkten wie Laptops und Smartphones gespeichert und der Zugriff darauf erfolgt immer öfter über cloudbasierte kollaborative Anwendungen. Zudem nimmt die Zahl der gezielten Bedrohungen zu. Daher sind Sicherheits-Frameworks mit einer in der Tiefe gestaffelten Verteidigung („Defense-in-Depth“) wichtiger denn je. Unternehmen kämpfen ständig damit, eine Balance zwischen der Notwendigkeit von mehrschichtigen, punktbasierten Technologien zur Unterbindung anhaltender Angriffe und den Budget- und Ressourcenbeschränkungen zu finden.

Unternehmen jedweder Größe sind von gezielten Bedrohungen betroffen:

- 40 % der Unternehmen geben an, dass ihre Endpunkte als Einstiegspunkt für einen APT-Angriff (Advanced Persistent Threat) genutzt wurden.[1]
- Im Visier stehen Unternehmen mit durchschnittlich 2.500 Mitarbeiter, doch am schnellsten wächst das Segment der Unternehmen mit 250 oder weniger Mitarbeitern.[2]

Punktbasierte Technologien für die Endverwaltung und Sicherheit haben die Komplexität und die Kosten der IT-Umgebung vergrößert. Die durchschnittliche Anzahl der Agenten ist in den vergangenen Jahren auf über sieben pro Endpunkt gestiegen. Gleichzeitig hat die durchschnittliche Anzahl der Konsolen zur Verwaltung von grundlegenden Funktionen für die Endpunktsicherheit und den Betrieb auf nahezu sieben pro Unternehmen zugenommen.[3]

Ivanti Endpunktsicherheit bietet:

- Defense-in-Depth-Schutz vor gezielten Bedrohungen, der operative und Sicherheitsfunktionen zur effizienten Reduzierung der Angriffsfläche kombiniert und mehrere Schichten präventiv wirkender Technologien bietet, um die Ausbreitung gezielter Angriffe zu unterbinden.
- Größere Transparenz und Kontrolle durch einen Komplettansatz, der die Anforderungen an den Endpunktbetrieb, die Sicherheit und Compliance sowie das IT-Risikomanagement erfüllen kann.
- Geringere Komplexität und Gesamtbetriebskosten dank einer voll integrierten Architektur, die mit nur einem Agenten und einer einzigen Konsole auskommt. Hierdurch werden eine übermäßig hohe Agentenzahl und Leistungsengpässe verhindert und der Workflow rationalisiert.

Ivanti Endpunktsicherheit geht das Problem des Endpunktschutzes unter operativen und sicherheitsbasierten Aspekten durch die Bereitstellung einer integrierten Plattform an, die nicht nur die Komplexität, sondern auch die Kosten reduziert.

Ivanti bietet einen mehrschichten Schutz im Hinblick auf mehrere Aspekte des Endpunktrisikos. Erreicht wird dies durch die Verkleinerung der bekannten Angriffsfläche von Endpunkten, die Schaffung einer vertrauenswürdigen Anwendungsumgebung, das Blockieren von unbekannter Malware und den Schutz von Daten. Komplexität kann die durchdachtesten Sicherheitsansätze konterkarieren. Daher wurde Ivanti Endpunktsicherheit so konzipiert, dass die Architektur mit einem einzigen Server, einer Datenbank und einer Konsole mit einem modularen Agenten auskommt, was die Verwaltung von tausenden Endpunkten vereinfacht, wo auch immer sich diese befinden.

Endpunktbetrieb

Patchmanagement: Reduziert das Betriebsrisiko und optimiert den IT-Betrieb, indem es die Anfälligkeiten von Betriebssystemen und Anwendungen über alle Endpunkte und Server hinweg eliminiert. Unterstützt mehrere Betriebssysteme (z. B. Windows, Linux, UNIX und OSX) und Drittanbieteranwendungen (z. B. Adobe Acrobat Flash und Reader, Google Chrome, Mozilla Firefox und Oracle Java).

Inhalts-Assistent: Bietet kundespezifische Erweiterbarkeit durch Tools mit Assistentenfunktion für das Bereitstellen und Entfernen von Software, die Reparatur von Konfigurationen, die Durchführung von Systemverwaltungsaufgaben und die Bereitstellung von benutzerdefinierten Patches.

Reporting Services: Bieten integrierte, vorkonfigurierte und zentralisierte Business Intelligence, die ganz auf die Bedürfnisse des Unternehmens zugeschnitten werden kann.

40 % der Unternehmen geben an, dass ihre Endpunkte als Einstiegspunkt für einen APT-Angriff (Advanced Persistent Threat) genutzt wurden.

Endpunktsicherheit

Anwendungskontrolle: Definiert und setzt die Nutzung von vertrauenswürdigen Anwendungen mittels Whitelist-Richtlinien durch, um sicherzustellen, dass nur explizit autorisierte oder vertrauenswürdige Anwendungen ausgeführt werden können. Umfasst Advanced Memory Protection zum Schutz vor ausgeklügelten Speicherinjektionsangriffen.

Antivirus: Bietet Blacklist-Schutz und ermöglicht das Entfernen aller Arten von Malware, einschließlich Viren, Würmern, Trojanern und Adware.

Gerätesteuerung: Setzt Nutzungsrichtlinien für Geräte und Ports durch und bietet zugleich Datenverschlüsselung für Wechselmedien, um Datenverlust bzw. -diebstahl zu verhindern.

Hauptmerkmale

- Modulare, erweiterbare Architektur mit einem einzigen robusten Agenten: Eine erweiterbare Plattform, die mit einem einzigen Agenten anstatt einer ganzen Sammlung von Agenten auskommt.
- Rollenbasierte Zugriffskontrolle: Bietet eine granulare Kontrolle von Gruppen und Domänen, um sensible Informationen wirksam zu schützen und Benutzerfehler durch nicht autorisierten Zugriff zu verhindern.
- Active Directory-Integration und Synchronisierung: Unterstützt in Active Directory eingerichtete Domänen, Benutzergruppen und einzelne Benutzer und stellt die AD-Synchronisierung sicher, um Setup- und Wartungsaufwand zu reduzieren.
- Erweiterte Asseterkennung und Agentenbereitstellung: Durchsucht die Umgebung nach Endpunkten, um die Transparenz von verwalteten und nicht verwalteten Systemen sicherzustellen und stellt automatisch oder nach Zeitplan Agenten für nicht verwaltete Systeme bereit.
- Schnelle Richtlinien-Updates und Aktionen: Liefert Richtlinien und Ereignis-Updates in Echtzeit ohne hierzu auf Push-Technologie zurückgreifen zu müssen.
- Virtuelle Infrastruktur im Blick: Identifiziert alle virtuellen Systeme in der Umgebung, um die Verwaltung von physischen und virtuellen Systemen mit einer einzigen Lösung zu ermöglichen.
- Berichterstattung: Eine ganze Palette von Management- und Betriebsberichten mit kritischem Feedback für das Unternehmen bieten umfassende Einblicke in die Endpunktumgebung.
- Erweitertes Wake-on-LAN: Stellt sicher, dass Computer im Offlinezustand aktiviert werden können, damit sie kritische Patches und Softwareupdates erhalten, und sorgt für eine maximale Energieeffizienz beim Einsatz in Verbindung mit Energierichtlinien über den Inhalts-Assistenten.

1 Ponemon Institute, 2014 State of Endpoint Risk
2 Symantec, Internet Security Threat Report vol. 17
3 Ponemon Institute, 2015 State of Endpoint Risk

www.ivanti.de
+49 (0)69 941 757-0
contact@ivanti.de