Ivanti Autonomous Endpoint Management

Autonom. Prädiktiv. Sicher. Die Zukunft des Endpoint-Managements beginnt hier.

Unternehmen sehen sich heute mit einer beispiellosen Komplexität von Endgeräten konfrontiert – von Desktops über mobile Geräte und robuste Hardware bis hin zu IoT-Geräten – und müssen gleichzeitig steigende Sicherheitsrisiken und stagnierende IT-Budgets bewältigen. Manuelle Prozesse und fragmentierte Tools machen Endgeräte anfällig und beeinträchtigen Compliance und Mitarbeiterproduktivität. Ivanti Autonomous Endpoint Management (AEM) transformiert Endgeräte-Operationen durch KI-gestützte Automatisierung, risikobasiertes Patching und Self-Healing-Funktionen. Durch die Vereinheitlichung des Managements über alle Geräte und Betriebssystemplattformen hinweg unterstützt AEM IT- und Sicherheitsteams dabei, Risiken zu reduzieren, die Effizienz zu skalieren und reibungslose digitale Erlebnisse bereitzustellen.

Herausforderungen für Kunden

- Sicherheitsrisiken durch ungepatchte Endgeräte: Jedes ungepatchte Endgerät ist eine potenzielle Sicherheitsverletzung, die nur darauf wartet, einzutreten. IT- und Sicherheitsteams befinden sich in einem unmöglichen Wettlauf: Schwachstellen werden täglich entdeckt, Patches werden ständig veröffentlicht, und Exploits mit kritischem Schweregrad werden binnen Stunden für Angriffe ausgenutzt – manchmal noch bevor Patches überhaupt verfügbar sind.
- Begrenzte IT-Ressourcen und stagnierende Budgets: Von IT-Teams wird erwartet, mit weniger mehr zu leisten – und die Lücke wird immer größer. Budgets sind eingefroren oder schrumpfen, während die Anzahl der Geräte wächst, die Erwartungen der Benutzer steigen und die technologische Komplexität zunimmt. Die Rechnung geht einfach nicht auf.
- Mangelnde Transparenz und fragmentierte Tools: IT-Verantwortliche agieren im Blindflug und verwalten eine zunehmend komplexe Umgebung mit unvollständigen, widersprüchlichen Daten, die über nicht verbundene Systeme verstreut sind. Es ist, als würde man versuchen, ein Puzzle zu vervollständigen, bei dem die Hälfte der Teile fehlt und die andere Hälfte aus verschiedenen Schachteln stammt.
- Negative Auswirkungen auf Produktivität und Erlebnis der Mitarbeiter: Ihre Mitarbeiter haben sich bewusst für Ihr Unternehmen entschieden – doch ihre Erfahrung mit der Technologie lässt sie zweifeln. Jeder Reibungspunkt, jede Verzögerung, jede IT-Hürde beeinträchtigt Produktivität, Morale und letztendlich die Mitarbeiterbindung.

Ivanti Autonomous Endpoint Management (AEM) – Lösungsüberblick

Ivanti AEM bietet einen Ansatz der nächsten Generation für Endpoint-Management:

- KI-gestützte Automatisierung: Automatisiert Patching, Compliance-Durchsetzung und Onboarding.
- Einheitliches Management: Unterstützt alle Geräte – Windows, macOS, iOS, Android, ChromeOS, Rugged-Geräte und VR/XR – von einer einzigen Plattform aus.
- Self-Healing & DEX-Optimierung: Löst Probleme proaktiv und verbessert das Mitarbeitererlebnis durch intelligente Workflows.

Zentrale Anwendungsfälle

- Risikobasiertes Patch-Management: Priorisiert und wendet Patches automatisch basierend auf dem Schweregrad der Schwachstelle und der Wahrscheinlichkeit einer Ausnutzung an
- Zero-Touch-Geräte-Onboarding: Vollständig automatisierte Bereitstellung neuer Endgeräte ohne IT-Eingriff
- Self-Healing-Funktionen: Erkennt und behebt Performance- oder Sicherheitsprobleme autonom
- Digital Employee Experience-Optimierung: Nutzt Telemetrie und KI, um Probleme, die Benutzer betreffen, proaktiv anzugehen
- Automatisiertes Software-Lifecycle-Management: Verwaltet Bereitstellung, Updates und Ausmusterung von Anwendungen
- Kontinuierliche Compliance-Durchsetzung: Echtzeit-

Wesentliche Funktionen

- Umfassende Transparenz: Echtzeit-Asset-Discovery und Endgeräte-Sichtbarkeit über alle Geräte und Umgebungen hinweg. Beseitigt blinde Flecken und gewährleistet ein genaues Inventar für Compliance und Optimierung.
- KI-gesteuerte Automatisierung: Self-Healing-Endgeräte, die Probleme automatisch beheben, mit menschlicher Kontrolle, autonomes Patching über Betriebssysteme und Anwendungen hinweg zur proaktiven Risikominimierung.
- Proaktive Risikominimierung: KI-gestützte Bedrohungsprävention, bevor Probleme entstehen. Kontinuierliche Compliance-Überwachung und Behebung von Schwachstellen. Integriertes risikobasiertes Patching und Schwachstellenmanagement.
- Breite Betriebssystem- und Geräteunterstützung: Einheitliches Management für Windows, macOS, Linux, iOS und Android einschließlich Rugged-Geräten und VR/XR.
- Zero-Touch-Bereitstellung & Self-Service: Automatisiertes Geräte-Onboarding und Konfiguration. Self-Service-Funktionen für Endbenutzer zur Reduzierung der IT-Arbeitslast und Verbesserung des Erlebnisses.
- Verbundenes Ökosystem: Einheitliche Plattform, die UEM, DEX und Sicherheitsfunktionen vereint.
- Integriertes ITSM und Sicherheit: Native Integration mit ITSM- und Sicherheits-Workflows. End-to-End ohne Silos, die IT- und Sicherheitsoperationen aufeinander abstimmen.

Was Ivanti AEM anders macht

Alles sehen, nichts verpassen

Ihre IT-Umgebung entwickelt sich ständig weiter – neue Geräte, Schatten-IT, Remote-Mitarbeiter. Ivanti AEM bietet Echtzeit-Transparenz über jeden Endpunkt, jedes Betriebssystem und jeden Standort hinweg. Keine blinden Flecken mehr, die Sie anfällig oder nicht-konform machen. Sie erhalten ein vollständiges, genaues Bild Ihrer gesamten IT-Infrastruktur, sodass Sie fundierte Entscheidungen mit Zuversicht treffen können.

IT, die sich selbst repariert

Warum auf Tickets warten, wenn sich Probleme selbst lösen können? Die KI-gesteuerte Automatisierung von Ivanti AEM erkennt und behebt Probleme, bevor Benutzer sie überhaupt bemerken – Patching von Schwachstellen über Betriebssysteme und Anwendungen hinweg erfolgt autonom. Ihr Team wechselt von der Problembekämpfung zur Innovation, während sich Ihre Sicherheitslage kontinuierlich verbessert.

Bedrohungen stoppen, bevor sie entstehen

Sicherheitsteams können es sich nicht mehr leisten, reaktiv zu sein. Ivanti AEM nutzt KI, um Bedrohungen vorherzusagen und zu verhindern, bevor sie sich materialisieren. Mit kontinuierlicher Compliance-Überwachung, intelligenter Behebung von Schwachstellen und risikobasiertem Patching, die Hand in Hand arbeiten, sind Sie Angreifern immer einen Schritt voraus – nicht hinterher.

Eine Plattform, jedes Gerät

Windows-Laptops, MacBooks, Linux-Server, mobile Geräte, sogar robuste Handhelds und VR-Headsets – Ihre Benutzer arbeiten mit allem. Ivanti AEM verwaltet alles über eine einzige zentrale Oberfläche. Endlich einheitliche Kontrolle ohne die Komplexität, mehrere Tools oder Plattformen jonglieren zu müssen.

Benutzer ermächtigen, IT entlasten

Niemand möchte warten, bis die IT sein Gerät einrichtet oder grundlegende Probleme behebt. Mit Zero-Touch-Bereitstellung und intelligentem Self-Service sind neue Mitarbeiter vom ersten Tag an produktiv, und erfahrene Benutzer lösen ihre eigenen Probleme sofort. Ihr IT-Team gewinnt jede Woche Stunden zurück, um sich auf strategische Initiativen statt auf Routineanfragen zu konzentrieren.

Silos aufbrechen

Wenn UEM, Digital Experience Monitoring und Sicherheit isoliert arbeiten, fallen Probleme durchs Raster. Ivanti AEM verbindet alles – native Integration mit Ihren ITSM-Workflows bedeutet, dass IT und Sicherheit endlich die gleiche Sprache sprechen. Ein Ökosystem, eine einzige Quelle der Wahrheit, ein optimierter Betrieb.

IT und Sicherheit, endlich aufeinander abgestimmt

Die Zeiten, in denen IT und Sicherheit mit gegensätzlichen Zielen arbeiteten, sind vorbei. Ivanti AEM integriert sich nahtlos in Ihre bestehenden Sicherheits- und Service-Management-Tools und schafft End-to-End-Workflows, in denen Transparenz, Maßnahmen und Governance natürlich fließen. Operationen werden schneller, intelligenter und deutlich sicherer.

Über Ivanti

Ivanti baut Barrieren zwischen IT und Sicherheit ab, damit Everywhere Work gedeihen kann. Ivanti hat die erste speziell entwickelte Technologieplattform für CIOs und CISOs geschaffen – die IT- und Sicherheitsteams umfassende Softwarelösungen bietet, die mit den Anforderungen ihrer Organisation skalieren, um die Erlebnisse der Mitarbeiter zu ermöglichen, zu sichern und zu verbessern. Die Ivanti-Plattform wird von Ivanti Neurons angetrieben – einer intelligenten Hyperautomatisierungsebene in Cloud-Umfang, die proaktive Fehlerbehebung, benutzerfreundliche Sicherheit im gesamten Unternehmen ermöglicht und ein Mitarbeitererlebnis bietet, das Benutzer begeistert. Über 40.000 Kunden, darunter 85 der Fortune 100, haben sich für Ivanti entschieden, um mit seinen End-to-End-Lösungen Herausforderungen direkt anzugehen. Bei Ivanti streben wir danach, eine Umgebung zu schaffen, in der alle Perspektiven gehört, respektiert und geschätzt werden, und setzen uns für eine nachhaltigere Zukunft für unsere Kunden, Partner, Mitarbeiter und den Planeten ein. Weitere Informationen finden Sie unter ivanti.com und folgen Sie @GoIvanti.

ivanti

Erfahren Sie mehr unter Autonomous Endpoint Management Solutions oder kontaktieren Sie noch heute Ihren Ivanti-Ansprechpartner.