Secure UEM Solution Plans

Introduction

Everywhere Work has brought on a rush of IT challenges. Organizations now must manage and secure a variety of devices, requiring them to gain complete visibility on device compliance issues even while rolling out apps and standardizing processes for all users, whether in-office or remote.

Beyond this, they have to provide great onboarding experiences for remote workers while ensuring secure and reliable access to corporate data and applications. They need to support bring-your-own-device (BYOD) initiatives yet still protect corporate data and user privacy.

Finally, it's vital for organizations to stay in step with the latest cloud security trends and technologies to maintain cybersecurity. All of these require the right tools and processes to ensure a secure and efficient work environment.

Solution Packages

Secure UEM Professional	Secure UEM Professional Plus	Secure UEM Premium
Provide complete endpoint management to improve digital employee experience and IT efficiency. **Key Capabilities** ■ Discover and inventory all devices on your network and gain complete visibility into IT assets. ■ Support modern and client management. ■ AI-driven self-healing automation with OOTB* and build-your-own bots. ■ Centralized visibility into device, people and organizational DEX** scores. ■ App distribution. ■ Remote control. ■ Software asset intelligence and management. ■ Partner conditional access.*** *Out of the box **Digital employee experience ***Conditional access integration with Microsoft AAD and Google BeyondCorp	Support breadth of use cases, especially for mobile and frontline workers. **Key Capabilities** ■ Includes all the key capabilities from Secure UEM Professional, plus advanced mobile security capabilities. ■ Provide secure network connectivity and dynamic access control for cloud and on-prem applications. ■ Secure applications for mobile devices and users. ■ Provide secure communications and data loss prevention (DLP) capabilities.	Deliver a comprehensive UEM solution with integrated endpoint security. **Key Capabilities** ■ Includes all the key capabilities of Secure UEM Professional Plus, and comprehensive cloud-native patch management. ■ Prioritize and remediate vulnerabilities. ■ OS and third-party app patching. ■ Risk-based cloud patch management. ■ Patch reliability insights. ■ Autonomous patch configurations.

IT challenges in the Everywhere Work environment

- Using multiple tools to discover, manage and secure all types of devices.
- Not having complete visibility on device compliance status or issues.
- Difficulty rolling out apps and standardizing processes across the organization.
- Supporting BYOD initiatives to protect corporate data and user privacy at the same time.
- Providing great onboarding experiences for hybrid/remote workers.
- Optimizing usage and cost of resources.
- Reducing friction in digital tech to improve user productivity and IT efficiency.

Discover, manage, secure and heal all your devices — no matter where they are

Secure UEM solutions are powerful tools that help IT teams gain a comprehensive understanding of their endpoint environment by providing a unified view of all endpoints, including desktops, laptops, mobile devices and other internet-connected devices. By enabling IT teams to discover, manage and secure all endpoints, it provides actionable insights — including real-time intelligence into the health, security and performance of all devices — they can use to quickly and efficiently detect and remediate any device issues or security vulnerabilities.

With Secure UEM solutions, IT teams can accurately pinpoint any issues or vulnerabilities and take immediate action to prevent harm. Because it includes comprehensive device management capabilities, they can provision, deploy and configure devices quickly and easily. Finally, by monitoring and controlling user activity on their devices, IT teams ensure compliance with organizational policies and best practices.

Thanks to powerful contextual insights and intelligent automation, IT teams can now proactively detect and resolve any IT and security issues. This proactive approach means potential problems get identified before they cause any disruption to the digital employee experience or business outcomes. Automating mundane and repetitive tasks frees up staff time to focus on more complex and higher-value activities.

With Secure UEM solutions:

- Manage any device securely, from mobile to traditionally managed devices, on your network to cloud and edge.
- Provide a complete view of all devices in your IT estate to discover, manage and secure all types of devices.
- Enable robust endpoint management and security capabilities to ensure only compliant and authorized devices connect to business resources.
- Improve IT efficiency and optimize resources by automating routine tasks and offering actionable and contextual insights.
- Deliver highly secure, contextualized, personalized and productive digital employee experiences without overburdening your IT team.
- Contain risks by effectively assessing, prioritizing and remediating vulnerabilities.
- Resolve endpoint issues before employees report them or see any impact on their productivity.

Choose the option that fits your needs

Organizations can choose from **three recommended solution packages**, depending on their endpoint management needs and maturity:

Secure UEM Professional offers comprehensive endpoint management capabilities such as asset discovery and inventory, device enrollment, app distribution, configuration management, application management, remote control, software spend optimization and partner conditional access (integration with Microsoft AAD, Google BeyondCorp). Furthermore, it equips IT teams with AI-driven automation bots and real-time insights, helping them detect and resolve device issues and IT service degradations quickly, thereby improving IT efficiencies and employee productivity.

Secure UEM Professional Plus includes all the key capabilities from Secure UEM Professional and additionally provides enhanced mobile application security, connectivity and access control for cloud and on-premises applications. This package provides secure communications and data loss prevention (DLP) capabilities to effectively secure access to business essential apps such as email, contacts and calendar so employees can work securely and productively.

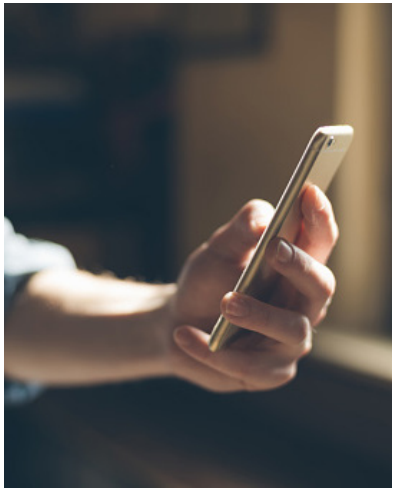
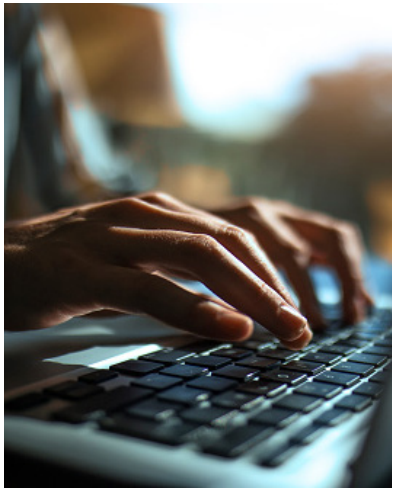
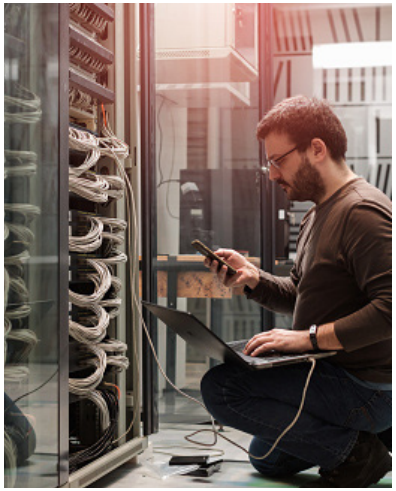
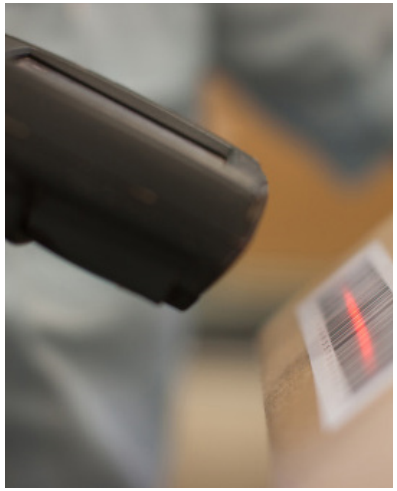
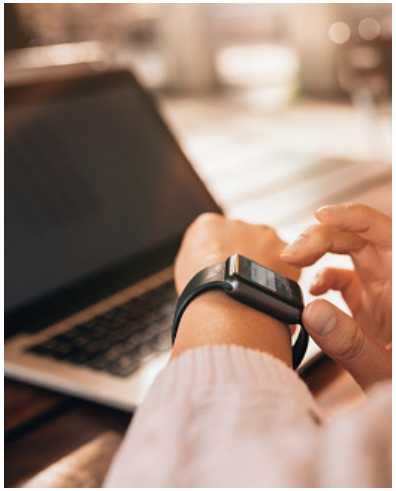
Secure UEM Premium is a comprehensive solution that includes all the essential features of Secure UEM Professional Plus as well as risk-based cloud patch management. Designed to secure and manage your IT infrastructure, your teams can identify and address device issues and security vulnerabilities before they cause harm to users and the environment.

Solution plans

- Secure UEM Professional
- Secure UEM Professional Plus
- Secure UEM Premium

Key benefits

- Gain complete visibility into IT assets by discovering all devices on your network.
- Manage all types of devices across the entire lifecycle from onboarding to retirement.
- Improve security posture by securing all your endpoints and environment.
- Provide all users with secure and seamless access to the corporate network.
- Deliver exceptional digital employee experience and improve employee productivity.
- Increase IT efficiency and productivity via AI-powered automation.
- Optimize IT spending and resources to focus on strategic initiatives.
- Prevent security vulnerabilities by regularly patching and updating software and hardware.
- Reduce attack surface to prevent data breaches and ransomware attacks and their negative effects (e.g., system downtime, diminished reputation, customer turnover).
- Maintain compliance with visibility into devices nearing SLA.
- Facilitate data and risk conversations between security and IT operations through operational collaboration.
- Improve operational efficiencies by eliminating the need to jump between siloed patch management solutions.

Key capabilities

Effectively discover and inventory all your endpoints

- Instantly detect new and unknown devices on your network via active and passive scanning and third-party connectors.
- Enjoy an out-of-the-box normalization and reconciliation engine.
- Automatically deliver accurate IT asset data in minutes instead of days.

Efficiently manage and secure all your devices across the entire lifecycle

- Manage all your endpoints – including iOS, iPadOS, macOS, Android, ChromeOS, Windows, Zebra, Oculus devices and wearables – and support both modern and client management.
- Secure access to data and apps on any device across your Everywhere Work – by enabling IT teams to easily identify and monitor BYOD/COBO/COPE devices and customize authentication paths.
- Automate endpoint lifecycle management – from onboarding and provisioning to configuration and retirement.

Deliver AI-driven self-healing and self-service capabilities

- Provide a 360-degree view of devices, users, applications and services, with real-time, contextualized insights.
- Automate workflow management and enable both standard and custom actions.
- Proactively diagnose and remediate issues on all endpoints.

Improve endpoint performance and operational costs

- Gather real-time insights from all devices by using natural language processing (NLP).
- Deliver real-time IT intelligence across the enterprise in seconds or minutes, not days.

Robust application management and deployment

- Deploy applications and manage updates with a single, intuitive tool.
- Roll out apps quickly and easily to users' devices, streamlining access while reducing IT management and deployment time.
- Interact with users, provide feedback and collect information in one place.

Optimize software spending via asset intelligence and management

- Provide comprehensive software overviews including software inventory status, reports on end-of-life licenses, upgrades and risks associated with apps, etc.
- Get a detailed analysis within minutes, presented in engaging dashboards of your licenses, purchases and instances so you can more effectively track your purchase history, upcoming license renewals, contract expirations and ongoing spend.
- Improve operational speed, asset visibility and utilization while reducing costs and risks.

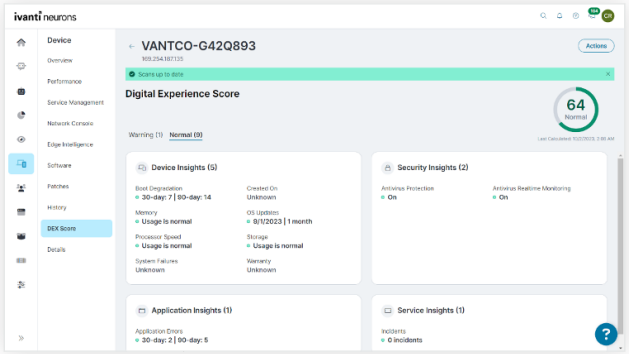


Figure 1 Device DEX score

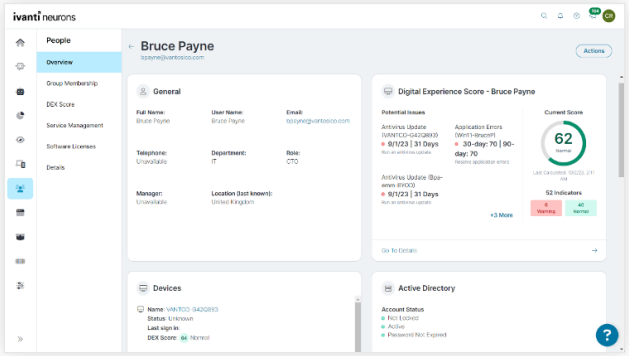


Figure 2 People DEX score

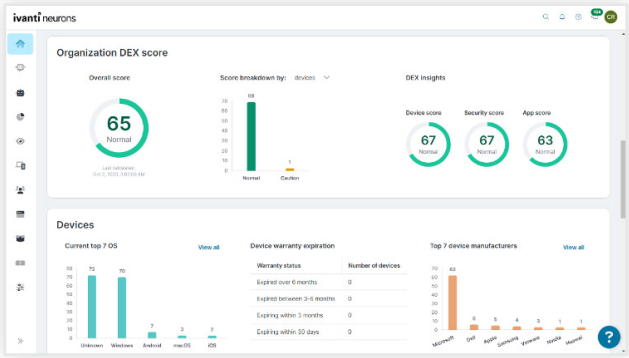


Figure 3 Organization DEX score

Comprehensive risk-based cloud patch management

- Streamline vulnerability remediation processes with a risk-based patch management approach.
- Efficiently prioritize and remediate vulnerabilities based on adversarial risk.
- Save time and reduce patch deployment failures with patch reliability insights from crowdsourced social sentiment data and anonymized patch deployment data.

Foundation for mobile device security via integrated mobile threat defense* (MTD) (*MTD: Add-on SKU)

- Protect against all known and unknown threats on Android and iOS devices across all mobile attack vectors – including device-level, network-level, application-level and phishing attacks.
- Remediate threats via on-device detection, even if the device is not connected to a Wi-Fi or cellular network.
- Automatically remediate threats based on access policies.

What sets Ivanti Secure UEM solutions apart?

- Continual, automated discovery for all devices. Provides a gap analysis of management and security coverage without manual effort.
- Complete UEM solution with client and modern management. Supports all devices, use cases and deployment scenarios across all OS platforms.
- Support breadth of use cases. Manages and protects any employee device, from knowledge workers to frontline workers.
- Secure application connectivity. Provides secure network connectivity and dynamic access control for cloud and on-prem applications. Allows IT to authorize specific mobile apps to access corporate resources behind the firewall without requiring any user interaction.
- AI-powered self-healing and self-service for endpoints. Provides IT with real-time intelligence and contextualized insights that help reduce routine tasks and time on troubleshooting.
- Improve the digital employee experience (DEX). Aggregates device details and scores end-user experience with devices to improve both IT and end-user experience and productivity.
- Software asset intelligence. Provides comprehensive software overviews that help reduce security risks and improve IT spending.
- Mobile threat defense (MTD) and risk-based vulnerability management (RBVM). Easily integrates with other security solutions* to provide IT teams with actionable insights and reduced overhead, enabling greater levels of compliance with security mandates. (*Ivanti security solutions such as: MTD and/or RBVM can be integrated with the purchase of an add-on SKU.)

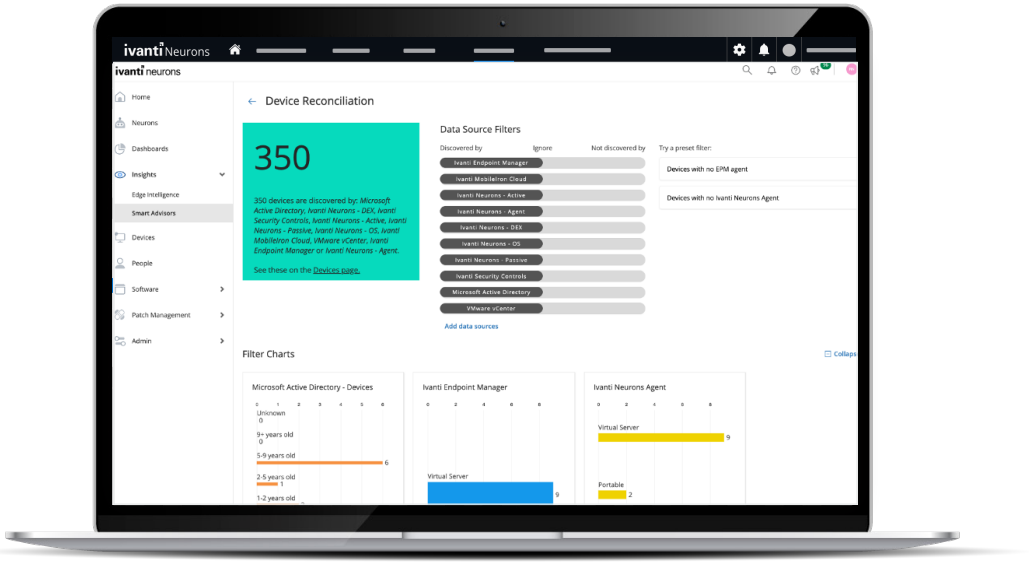


Figure 4 Device Reconciliation Smart Advisor

About Ivanti

Ivanti elevates and secures Everywhere Work so that people and organizations can thrive. We make technology work for people, not the other way around. Today's employees use a wide range of corporate and personal devices to access IT applications and data over multiple networks to stay productive, wherever and however they work. Ivanti is the only technology company that finds, manages and protects every IT asset and endpoint in an organization. Over 40,000 customers, including 88 of the Fortune 100, have chosen Ivanti to help them deliver an excellent digital employee experience and improve IT and security team productivity and efficiency. At Ivanti, we strive to create an environment where all perspectives are heard, respected and valued and are committed to a more sustainable future for our customers, partners, employees and the planet. For more information, visit ivanti.com

ivanti

For more information, or to contact Ivanti, please visit ivanti.com