PRODUCT BRIEF

LEVELBLUE ENDPOINT SECURITY

Defend Your Mobile Endpoints

Now you can get enterprise-grade mobile management and security for businesses of all sizes—all in one affordable package.

With Ivanti Blue, You Don't Have to Choose Between Mobile Security and Mobile Productivity

Cybercriminals and hackers have set their sights on mobile devices. Why? These endpoints hold the keys to all kinds of data valuable to your business. And they can be the entry point to the rest of your network.

With mobile phishing attacks and other mobile threats on the rise, it's time for a mobile security solution designed for anyone to use—and at a price that's friendly to the bottom line.

With Ivanti Blue, you get cloud-based mobile threat protection that's always on and continuously updated without interrupting users. Mobile Threat Defense (MTD) is fully integrated with its Unified Endpoint Management (UEM) client so it doesn't require any actions from an end user to activate. This drives a 100% adoption rate.

Best of all, it's fully deployed and supported by world-class support from LevelBlue so you don't have to worry about updating complicated software on all your devices. Just activate it and go—it's really that easy.

What is Blue?

Ivanti Blue is an integrated bundle. You get both Ivanti Neurons for MDM and Ivanti Mobile Threat Defense—all at one low monthly rate.

Mobile Threat Defense—Continuous protection against mobile phishing and malicious threats across all managed iOS and Android devices.

Neurons for MDM—Device management features for Android and iOS. You can quickly set up and enroll new devices with company email, passcode requirements, Wi-Fi settings, and other configurations right out of the box.

Benefits

- Help manage multiple endpoints from a single console
- Improve user productivity with easy-to-use app management and content integration
- Protect against the latest cyberthreats to improve your security posture

Features

- Self-service app portal for end users
- Web browser designed for remote workforce
- Detect and remediate malicious threats with no action required by end user

Mobile Threat Defense

You can rest easy knowing that Mobile Threat Defense continuously scans managed devices for threats and provides immediate notification and threat remediation when it detects a high level of risk.

- Always on—No Wi-Fi or cellular connection required
- Integrated into Ivanti Neurons for MDM
- Easy, automated deployment
- Protect and remediate against mobile phishing attacks at the device, network, and application levels
- Mobile threat detection through machine learning
- On-device threat notification and remediation
- Real-time insight into the apps installed on user devices
- Improve IT decision-making using analytics and detailed reports that provide threat assessment scores, explanation of risks, and implications

Device Management

Managing mobile devices is a challenge for companies of all sizes. Ivanti Blue allows you to easily configure native email, apps, and device and security policies based on each user's role.

- Apple iOS and Google Android support
- Provide comprehensive audit trails
- Integrate with OS device enrollment program (ABM and Zero Touch)
- Native email configuration

Device Security

Ivanti Blue makes it easy to set up device configurations that help prevent your apps and data from falling into the wrong hands. You can remotely enforce passcode requirements and other security policies.

- Deploy configurations
- Lock and wipe data from lost, stolen, or retired devices
- Set passcodes and restrictions
- Enforce security policies and compliance
- Protect data in motion with WiFi and VPN configuration

2-in-1 Solution So You Can…

- Defend against phishing, network, app, and device attacks—even when device is offline
- Set role-based policies
- Administer apps and configure settings remotely
- Install and update through a single app
- Wipe data from the device instantly
- Update without user interruption

App Management

Ivanti Blue also makes it easy to administer an enterprise app store. You can deploy in-house, public, and web apps to users based on their roles and responsibilities.

- Manage public, web, and internal apps
- Encrypt applications
- Blacklist apps (to restrict access on devices)
- Instantly update apps on devices without any manual intervention
- If users change roles, you can instantly wipe those apps from their devices

LevelBlue Professional Services

Purchase of a professional configuration and training package is required for the initial purchase of Ivanti Blue. LevelBlue Professional Services include configuration and training as well as the LevelBlue customer support desk (CSD).

Why LevelBlue

Technology is complex. Transformation is fast. With experience across all industries, we bring a rich understanding of how to support your teams that depend on mission-critical mobile devices. No matter the size of your business, we'll deliver the right insights, guidance, and solutions.

Important information

General: Ivanti Neurons for MDM (fka MobileIron Cloud) as described in this product brief (the "Solution") is available only to eligible Customers with a qualified LevelBlue agreement ("Qualified Agreement"). The Solution is subject to (a) the terms and conditions found at https://www.ivanti.com/company/legal/eula ("Additional Product Terms"); (b) the Qualified Agreement; and (c) applicable Sales Information. For government Customers, any Additional Product Terms not allowable under applicable law will not apply, and the Qualified Agreement will control in the event of any material conflict between the Qualified Agreement and the Additional Product Terms.

A minimum of 20 Solution subscriptions are required for initial purchase. The Solution's functionality is limited to certain mobile devices and operating systems. A list of supported operating systems can be obtained by contacting an LevelBlue Account Executive. Not all features are available on all devices. All amounts paid for the Solution are non-refundable.
Billing begins as of Effective Date of applicable order. User subscriptions may download licensed Software onto a maximum of 5 devices. If any user exceeds the 5 device limit per license, an additional monthly license fee will be charged.

The Solution is available for use with a Qualified Agreement and multiple network service providers. Customer Responsibility Users ("CRUs"), Individual Responsibility Users ("IRUs") and Bring Your Own Device ("BYOD") users are eligible to participate in the Solution. With respect to users subscribed to an AT&T wireless service, activation of an eligible AT&T data plan on a compatible device with short message service ("SMS") capabilities is required. With respect to use of the Solution with devices subscribed to non-AT&T wireless providers, Customer is responsible for ensuring that its applicable end users and the Solution comply with all applicable terms of service of such other wireless carrier(s). All associated voice, messaging and data usage will be subject to the applicable rates and terms of such other wireless carrier(s). Refer to applicable wireless carrier(s) for such rates, terms and conditions.
A compatible device with SMS capabilities is required.

The Solution's administrative interface is accessed via a Web portal and requires a PC with internet connection. The Solution may be used as a tool to configure and customize certain settings and features and perform software updates only for compatible devices. Improper or incomplete configuration and/or downloads performed by Customer may result in service interruptions and/or device failures. LevelBlue does not guarantee compliance with such customized settings and/or updates.

Customer must accept the Additional Product Terms as the party liable for each CRU, and agrees in such case that the CRU will comply with the obligations under the Additional Product Terms, including but not limited to the limitations of use in certain countries. See your account representative for additional information regarding use of the Solution outside the U.S. Customer is responsible for providing each CRU of an enabled mobile device with a copy of the Additional Product Terms. The Customer and the CRU are individually and jointly liable under the Additional Product Terms. With regard to use of the Solution by residents of countries other than the U.S., Customer agrees to comply with the additional terms and conditions of use located in the Country Specific Provisions portion of the Ivanti Blue Cloud Service Guide located at serviceguidenew.att. com. Not all optional features are available in every country.

Data privacy: Customer Personal Data: Customer Personal Data may be transferred to or accessible by (i) LevelBlue personnel around the world; (ii) third parties who act on behalf of LevelBlue or LevelBlue supplier's behalf as subcontractors; and (iii) third parties (such as courts, law enforcement or regulatory authorities) where required by law. Customer will only provide or make Customer Personal Data accessible when Customer has the legal authority to do so and for which it has obtained the necessary consents from its end users, and will camouflage or securely encrypt Customer Personal Data in a manner compatible with the Solution. The term Customer Personal Data includes, without limitation, name, phone number, email address, wireless location information or any other information that identifies or could reasonably be used to identify Customer or its end users. Customer is responsible for providing end users with clear notice of LevelBlue's and Customer's collection and use of Customer Personal Data obtained via the Solution, including, without limitation, end user device location information, and for obtaining end user consent to that collection and use. Customer may satisfy its notification requirements as to LevelBlue by advising end users in writing that LevelBlue and its suppliers may collect and use Customer Personal Data by providing for end user review the relevant links to the Product Brief or other sales information that describes the Solution and to LevelBlue Privacy Policy at https://www.att.com/gen/privacy-policy?pid=2506. Customer is responsible for notifying end users that the Solution provides mobile device management (MDM) capabilities and allows Customer to have full visibility and control of end users' devices, as well as any content on them.

Professional Services: Upon completion of Professional Services, Customer must either sign the acceptance document LevelBlue presents or provide within five business days of the service completion date written notice to LevelBlue identifying any nonconforming Professional Services. If Customer fails to provide such notice, Customer is deemed to have accepted the Professional Services. Customer acknowledges that LevelBlue and Customer are independent contractors. Customer will in a timely manner allow LevelBlue access as reasonably required for the Professional Services to property and equipment that Customer controls. The Professional Services provided shall be performed Monday through Friday, 9:00 a.m. to 5:00 p.m., local time. The mandatory software installation and configuration is estimated to take two days and must be completed within 45 days of order placement. If Customer's acts or omissions cause delay of installation and configuration beyond 45 days of order placement, LevelBlue will invoice Customer for the installation and configuration charges after the 45th day. If the Professional Services provided in connection with the Solution are more complex than those described in this Product Brief, then a separate statement of work describing the activity and related terms and pricing will be executed. If impediments, complications or Customer-requested changes in scope arise (Changes), the schedule, Solution and fees could be impacted. In the event any Change(s) affect the Solution or fees, the parties will modify Customer's order (or statement of work, if applicable) accordingly by executing a change order.

As between LevelBlue and the Customer, the Solution is provided "AS IS" with all faults and without warranty of any kind. LEVELBLUE HAS NO DEFENSE, SETTLEMENT, INDEMNIFICATION OR OTHER OBLIGATION OR LIABILITY ARISING FROM THE ACTUAL OR ALLEGED INFRINGEMENT OR MISAPPROPRIATION OF INTELLECTUAL PROPERTY BASED ON THE SOLUTION.

LevelBlue reserves the right to (i) modify or discontinue the Solution in whole or in part and/or (ii) terminate the Solution at any time without cause. LevelBlue reserves the right to conduct work at a remote location or use, in LevelBlue's sole discretion, employees, contractors or suppliers located outside the United States to perform work in connection with or in support of the Solution.

Exclusive Remedy: Customer's sole and exclusive remedy for any damages, losses, claims, costs and expenses arising out of or relating to use of the Solution will be termination of service.

LevelBlue

About LevelBlue

We simplify cybersecurity through award-winning managed security services, experienced strategic consulting, threat intelligence and renowned research. Our team is a seamless extension of yours, providing transparency and visibility into security posture and continuously working to strengthen it.

We harness security data from numerous sources and enrich it with artificial intelligence to deliver real-time threat intelligence. This enables more accurate and precise decision making. With a large, always-on global presence, LevelBlue sets the standard for cybersecurity today and tomorrow. We easily and effectively manage risk, so you can focus on your business.

Cybersecurity. Simplified.

Discover how to manage and secure your endpoint devices.