Securing your remote workforce

BlackBerry Enterprise Software

Contents

Securing your workforce at home

BlackBerry has a long history as a leader in helping people work securely when they are out of the office. The world is facing an unprecedented situation and many governments, organizations, and companies have quickly transitioned to having the majority of employees at home rather than in the office. The new reality presents a very real challenge for organizations that were not already equipped to support a large, secure remote workforce.

BlackBerry has made several of our industry-leading software products free for a period of time to help organizations manage this transition. This document will help you figure out which BlackBerry products meet your organization's needs and point you towards the information you need to get started using them.

What products can help me?

BlackBerry offers a wide array of products to help secure your vital communications when employees are out of the office. The following selection of products can play a vital role in securing your data when employees work from home.

To learn more about starting a free trial, visit the BlackBerry Web site.

Product	Description
BlackBerry Desktop	BlackBerry Desktop is an easy-to-deploy solution that gives employees remote access to their work email and calendars and your organization's intranet and web-based applications, including Cisco WebEx, Zoom, and Salesforce, from Windows 10 and macOS devices, without requiring a VPN.
BlackBerry UEM	BlackBerry UEM is a full featured solution for securing and managing your workforce's mobile devices. BlackBerry UEM Cloud is hosted on BlackBerry servers, minimizing the amount of software to be installed and allowing you to get it up and running quickly. With BlackBerry UEM, you can fully manage devices or simply provide support for installing and setting up secure productivity apps like BlackBerry Desktop and BBM Enterprise.
CylancePROTECT	CylancePROTECT enhances the security of Android and iOS devices managed with BlackBerry UEM.
BlackBerry 2FA	BlackBerry 2FA provides two-factor authentication for users logging into your network from a remote location. Users can provide a second factor to verify their identity simply by responding to a notification on their mobile device.
BBM Enterprise	BBM Enterprise allows users to send encrypted instant messages, have encrypted group conversations, and host secure voice and video conferences with up to 15 participants using iOS, Android, Windows 10, and macOS devices.
BlackBerry SecuSUITE	SecuSUITE provides NIAP and CSfC certified security for text messaging and voice calls on iOS and Android devices.

About BlackBerry Desktop

BlackBerry Desktop combines BlackBerry Access and BlackBerry Work to allow users to access their work email and calendar and your organization's intranet and business applications through the work firewall, without using a VPN, on Windows 10, and macOS devices.

BlackBerry Access and BlackBerry Work are part of the suite of BlackBerry Dynamics mobile productivity apps. You deploy and manage BlackBerry Desktop using BlackBerry UEM.

BlackBerry Access provides the following features:

Feature	Description
Secures data	BlackBerry Access secures work web apps in containers, ensuring that data is protected and never leaves your organization's control.
User authentication	BlackBerry Access leverages standard user authentication methods, including SSL, NTLM, and TLS, and supports credential persistence. BlackBerry Access also supports single sign-on with Kerberos Constrained Delegation across realms and RSA soft token generation.
App deployment	BlackBerry Access supports pop-ups that streamline the deployment of web apps, including Cisco WebEx, Zoom, Salesforce, and custom-developed apps. You can deploy your organization's HTML5 desktop apps securely, and you can provide users with offline access to those apps.
Remote commands	If a user's device is compromised (for example, it's lost or stolen), you can remotely delete browser data, lock the app, or wipe device data.

BlackBerry Work provides the following features:

Feature	Description
Work email	Users can securely access work email. View, send, and edit attachments. Be instantly notified of key messages, and manage your inbox with smart folders and more
Personal and shared calendar management	Users can manage and schedule meetings, check availability, attach files to invitations, and quickly join conference calls and web conferences. They can quickly pull up all their obligations for the day with agenda view.
One-click communication	Users can see mobile presence and then reach colleagues using the best way, whether by phone, text message, instant message, or email.
Document access and editing	Users can access documents while they're on the go from native Microsoft Office Web Apps, Microsoft SharePoint, or other popular cloud storage options within the app.

For more information, see the BlackBerry website and the BlackBerry Access and Work for Windows or BlackBerry Access and Work for macOS content.

About BlackBerry UEM

To put it simply, BlackBerry UEM allows you to manage what users can do on their mobile devices when they are using them for work. You can manage apps on the device, secure communication between devices and your work servers, ensure work data on the device stays secure, and disable features on devices that your organization controls. You set the level of control you have over each device, so you can choose to secure and control only work data on a device the employee owns, allow users to have personal apps and data on a work device, or maintain full control over work-owned devices that employees can only use for work purposes.

BlackBerry UEM has both an on-premises solution and a cloud-based solution. Both versions offer trusted end-to-end security and provide the control that organizations need to manage all endpoints and ownership models.

Benefits of BlackBerry UEM include:

Feature	Benefit
Low total cost of ownership	BlackBerry UEM on-premises reduces complexity, optimizes pooled resources, ensures maximum uptime and helps you achieve the lowest total cost of ownership for an on-premises solution. BlackBerry UEM Cloud reduces the cost of ownership by removing the need to install, manage, and update services.
Single web-based interface	You can manage iOS, macOS, Android, Windows 10, and BlackBerry 10 devices plus additional BlackBerry Secure UEM & Productivity Suite services all from a single management console.
Flexible ownership models	BlackBerry UEM provides a set of customizable policies and profiles to manage BYOD, COPE, and COBO devices, and protect business information.
User and device reporting	You can manage fleets of devices using comprehensive reporting and dashboards, dynamic filters, and search capabilities.
Simple user setup and enrollment	Users can activate their own devices with BlackBerry UEM Self-Service.
Industry-leading mobile security	BlackBerry UEM leverages the BlackBerry Infrastructure to ensure data security across all devices.
High availability	You can configure high availability for BlackBerry UEM on-premises to minimize service interruptions for device users or rely on BlackBerry to maintain BlackBerry UEM Cloud and maximize uptime for you.

For more information, see the BlackBerry UEM content.

About CylancePROTECT

CylancePROTECT is a suite of features that enhances the ability of BlackBerry UEM to detect, prevent, and resolve security threats without disrupting the productivity of your workforce. CylancePROTECT establishes a secure ecosystem where data is protected and malicious activities are identified and eliminated proactively.

CylancePROTECT is integrated with BlackBerry UEM, so no additional software or user actions are required to benefit from it. Your data and resources are protected continuously without intruding on the daily activity of your device users.

Feature	Platform	Description
Malware detection for internally deployed apps	Android	When you upload a hosted app to UEM to deploy it to your users, UEM scans the app and detects potential malware.
Detecting malware on devices	Android	The UEM Client or a BlackBerry Dynamics app uploads app files to CylanceINFINITY to identify whether malicious apps are present on a user's device. If a malicious app us found, UEM can take a compliance action that you specify.
Detecting sideloaded apps	iOS	UEM, the UEM Client, and BlackBerry Work can detect sideloaded apps on iOS devices and take a compliance action that you specify.
Safe browsing with BlackBerry Dynamics apps	Android iOS	When a user navigates to a URL in a BlackBerry Dynamics app, the app sends the URL to CylanceINFINITY in real-time to determine if it is safe. You can choose the user experience when a user tries to navigate to an unsafe URL.
App integrity checking	iOS	UEM can leverage the Apple DeviceCheck framework to verify the integrity of BlackBerry or ISV authored BlackBerry Dynamics apps. UEM also supports partial integrity checking for custom BlackBerry Dynamics apps, based on the Apple team ID that is associated with the app.
Hardware certificate attestation	Android	CylancePROTECT extends security patch level enforcement to BlackBerry Dynamics apps. If the security patch level is not satisfied, UEM takes a compliance action that you specify.

For more information, see the CylancePROTECT content.

About BlackBerry 2FA

BlackBerry 2FA provides users with two-factor authentication to your organization's resources. It allows you to use your users iOS and Android devices as the second factor of authentication to verify their identity when they connect to your organization's resources.

If you're new to thinking about this type of security, two-factor authentication simply means that you require a second type (factor) of authentication from users in addition to a password when they connect remotely. This type of authentication is commonly used when you have a VPN. Users log into the VPN on their laptop with a password. After the password is verified, BlackBerry 2FA sends a notification to the user's iOS or Android device. The user must tap Allow on the device within a number of seconds or the connection is terminated. Users don't need to open an app or take actions on their mobile device before logging into the VPN, they just need to respond to the device notification when it is received.

You manage BlackBerry 2FA from the BlackBerry UEM management console. You can also install a BlackBerry 2FA server on your network. The BlackBerry 2FA server allows you to leverage services such as a VPN gateway or REST endpoint to provide users with access to those resources.

For more information, see the BlackBerry 2FA content.

About BBM Enterprise

BBM Enterprise uses a FIPS 140-2 validated cryptographic library to provide end-to-end encryption for individual and group chats. BBM Enterprise is available for iOS, Android, Windows 10, macOS, and BlackBerry 10 devices. Your organization owns the encryption keys, and no one else, not even BlackBerry, can access them to read messages between your employees.

BBM Enterprise also provides secure voice and video conferencing for up to 15 users, allowing teams to have secure meetings while everyone is out of the office.

For more information about BBM Enterprise, see the BBM Enterprise content.

About SecuSUITE

SecuSUITE is a software-based solution that provides secure calling and text messaging for iOS, Android, and BlackBerry 10 devices. SecuSUITE technology was designed to protect national security: It is NIAP and CSfC certified and has been chosen by national governments and NGOs to protect their communications against electronic eavesdropping and third-party attacks.

For more information, see the SecuSUITE information on the BlackBerry web site.

Legal notice

WERE FORESEEN OR UNFORESEEN, AND EVEN IF BLACKBERRY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW IN YOUR JURISDICTION, BLACKBERRY SHALL HAVE NO OTHER OBLIGATION, DUTY, OR LIABILITY WHATSOEVER IN CONTRACT, TORT, OR OTHERWISE TO YOU INCLUDING ANY LIABILITY FOR NEGLIGENCE OR STRICT LIABILITY.

THE LIMITATIONS, EXCLUSIONS, AND DISCLAIMERS HEREIN SHALL APPLY: (A) IRRESPECTIVE OF THE NATURE OF THE CAUSE OF ACTION, DEMAND, OR ACTION BY YOU INCLUDING BUT NOT LIMITED TO BREACH OF CONTRACT, NEGLIGENCE, TORT, STRICT LIABILITY OR ANY OTHER LEGAL THEORY AND SHALL SURVIVE A FUNDAMENTAL BREACH OR BREACHES OR THE FAILURE OF THE ESSENTIAL PURPOSE OF THIS AGREEMENT OR OF ANY REMEDY CONTAINED HEREIN; AND (B) TO BLACKBERRY AND ITS AFFILIATED COMPANIES, THEIR SUCCESSORS, ASSIGNS, AGENTS, SUPPLIERS (INCLUDING AIRTIME SERVICE PROVIDERS), AUTHORIZED BLACKBERRY DISTRIBUTORS (ALSO INCLUDING AIRTIME SERVICE PROVIDERS) AND THEIR RESPECTIVE DIRECTORS, EMPLOYEES, AND INDEPENDENT CONTRACTORS.

IN ADDITION TO THE LIMITATIONS AND EXCLUSIONS SET OUT ABOVE, IN NO EVENT SHALL ANY DIRECTOR, EMPLOYEE, AGENT, DISTRIBUTOR, SUPPLIER, INDEPENDENT CONTRACTOR OF BLACKBERRY OR ANY AFFILIATES OF BLACKBERRY HAVE ANY LIABILITY ARISING FROM OR RELATED TO THE DOCUMENTATION.

Prior to subscribing for, installing, or using any Third Party Products and Services, it is your responsibility to ensure that your airtime service provider has agreed to support all of their features. Some airtime service providers might not offer Internet browsing functionality with a subscription to the BlackBerry® Internet Service. Check with your service provider for availability, roaming arrangements, service plans and features. Installation or use of Third Party Products and Services with BlackBerry's products and services may require one or more patent, trademark, copyright, or other licenses in order to avoid infringement or violation of third party rights. You are solely responsible for determining whether to use Third Party Products and Services and if any third party licenses are required to do so. If required you are responsible for acquiring them. You should not install or use Third Party Products and Services until all necessary licenses have been acquired. Any Third Party Products and Services that are provided with BlackBerry's products and services are provided as a convenience to you and are provided "AS IS" with no express or implied conditions, endorsements, guarantees, representations, or warranties of any kind by BlackBerry and BlackBerry assumes no liability whatsoever, in relation thereto. Your use of Third Party Products and Services shall be governed by and subject to you agreeing to the terms of separate licenses and other agreements applicable thereto with third parties, except to the extent expressly covered by a license or other agreement with BlackBerry.

The terms of use of any BlackBerry product or service are set out in a separate license or other agreement with BlackBerry applicable thereto. NOTHING IN THIS DOCUMENTATION IS INTENDED TO SUPERSEDE ANY EXPRESS WRITTEN AGREEMENTS OR WARRANTIES PROVIDED BY BLACKBERRY FOR PORTIONS OF ANY BLACKBERRY PRODUCT OR SERVICE OTHER THAN THIS DOCUMENTATION.

BlackBerry Enterprise Software incorporates certain third-party software. The license and copyright information associated with this software is available at http://worldwide.blackberry.com/legal/thirdpartysoftware.jsp.

BlackBerry Limited
2200 University Avenue East
Waterloo, Ontario
Canada N2K 0A7

BlackBerry UK Limited
Ground Floor, The Pearce Building, West Street,
Maidenhead, Berkshire SL6 1RL
United Kingdom

Published in Canada