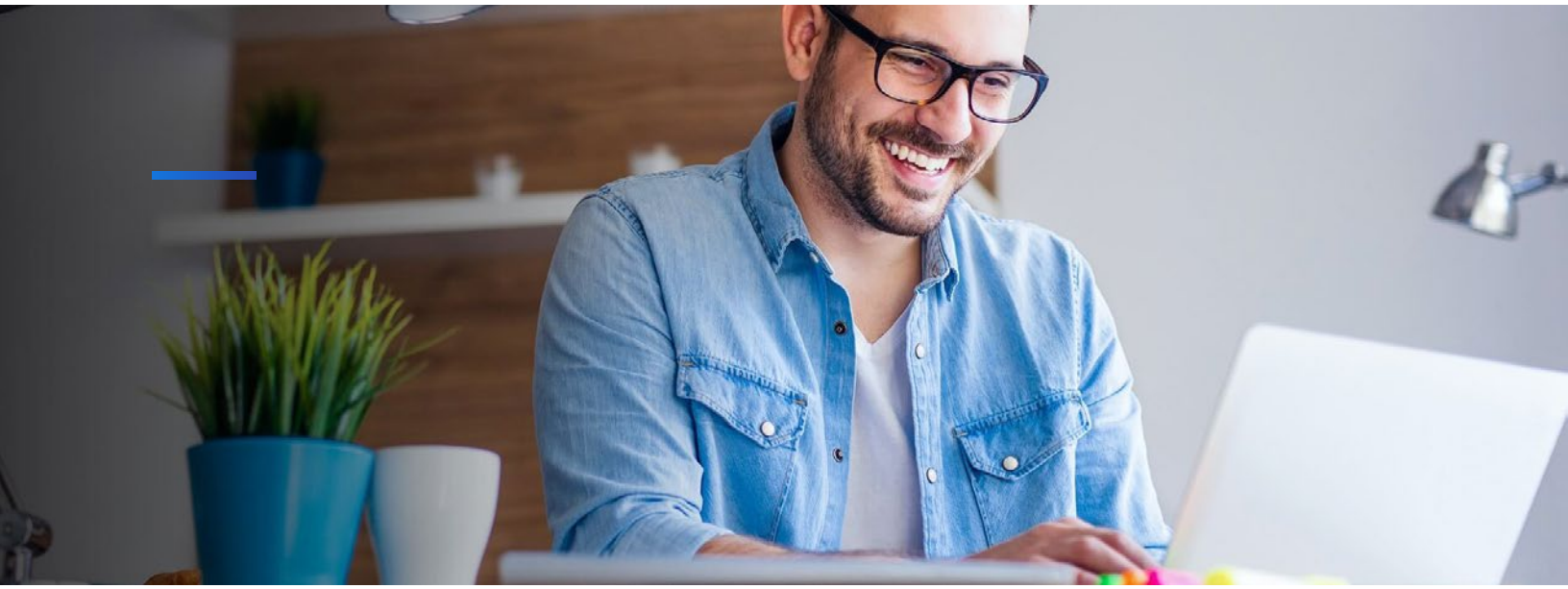


Don't Compromise on Security in a Crisis

A flash survey conducted by law firm Seyfarth Shaw LLP[1] between March 12th and March 16th found that 85% of the 550 responding companies were actively encouraging employees to work from home, a trend that organizations large and small are adopting quickly in the wake of the COVID-19 pandemic. How prepared these organizations are to function safely in this environment, however, is very much open to question.

Adversaries are already moving swiftly to exploit the situation. More than a third (36%) of respondents to a recent CNBC survey[2] reported that cyber threats had increased since employees began working from home.

Organizations cannot afford to compromise on security at this critical time. They also can't afford to stifle productivity when business continuity depends on employees being able to perform their duties without unnecessary obstacles to success.

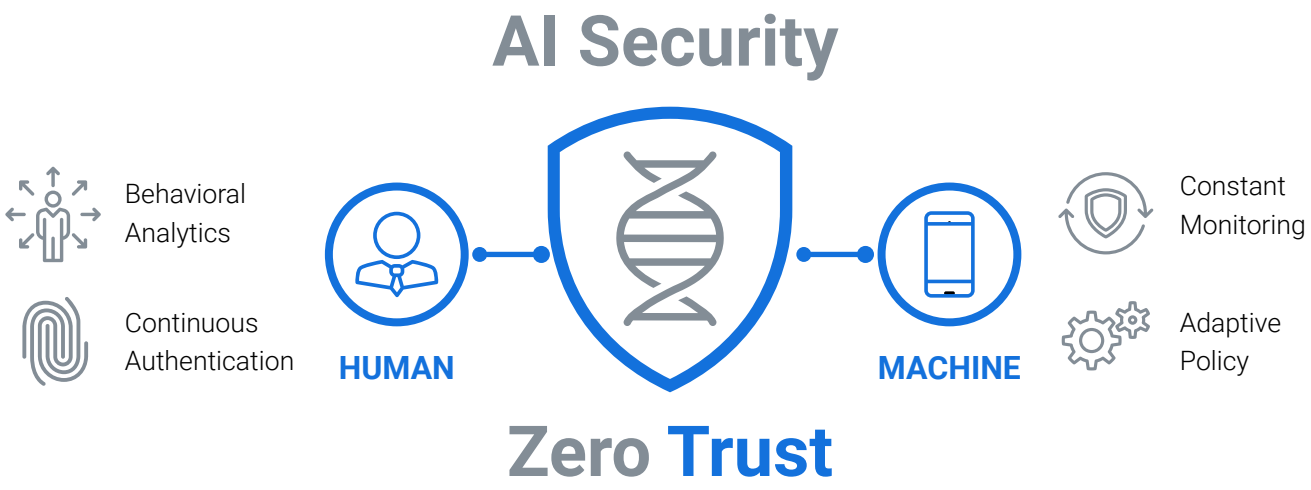
1 COVID-19 Employer Flash Survey Results
2 Phishing scams, spam spike as hackers use coronavirus to prey on remote workers, stressed IT systems

Some providers of cybersecurity products are treating the current crisis as a gold rush, releasing so-called specially packaged versions of endpoint protection products that were never designed to secure a mobile workforce. Watered-down, fractional offerings like these can undermine an organization's security posture and introduce significant regulatory risks.

Companies offering these feature-poor products spin their dependence on the cloud as a benefit. In reality, the inherent latency introduced by a cloud-dependent architecture is an obstacle to providing proactive prevention. This is particularly true for large mobile deployments that are often subject to connectivity challenges. The effectiveness of an organization's endpoint security should never be dependent on Internet connection speeds.

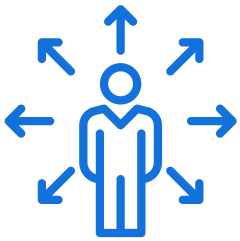
When vendors like these claim that their cloud-based analytics provide increased visibility into events, what they are actually revealing is that their threat detection methods are inherently reactive, occurring too late to prevent a breach or minimize the impact of a breach in progress. This is especially true for their minimalist home-use versions, which do not provide real-time response or network containment capabilities.

By contrast, BlackBerry's prevention-first agent supports a Zero Trust architecture and resides locally on the endpoint with zero reliance on a cloud connection. Consequently, automated prevention occurs at the endpoint in real time, where the battle to protect the device and the network is taking place. The ability to proactively interdict the kill chain locally at machine-speed makes all the difference when defending a distributed network of mobile devices outside of the network firewall.



Don’t Be Forced To Choose Between Privacy and Efficacy

Products that are cloud-dependent can also force customers to choose between product efficacy and data privacy. This issue is compounded with remote work scenarios when considering the sensitive nature of corporate data and the concerns employees may have when using their personal devices for work.



Lightweight versions of cloud-dependent security products being offered for home use may claim to minimize collection of personally identifiable information (PII). By their very design, however, they cannot work without sending detection-related event data to the cloud for analysis. If you inquire about data privacy, the vendor will likely tell you that the only information they collect is merely metadata. However, this metadata can include a wealth of personal information, including account usernames, filenames, file paths on the device, specific device identifiers, and more. Much of this data is protected by strict regulatory mandates, so your organization will be required to obtain explicit consent from employees before the product is put into use, a significant obstacle to ease of deployment at scale.

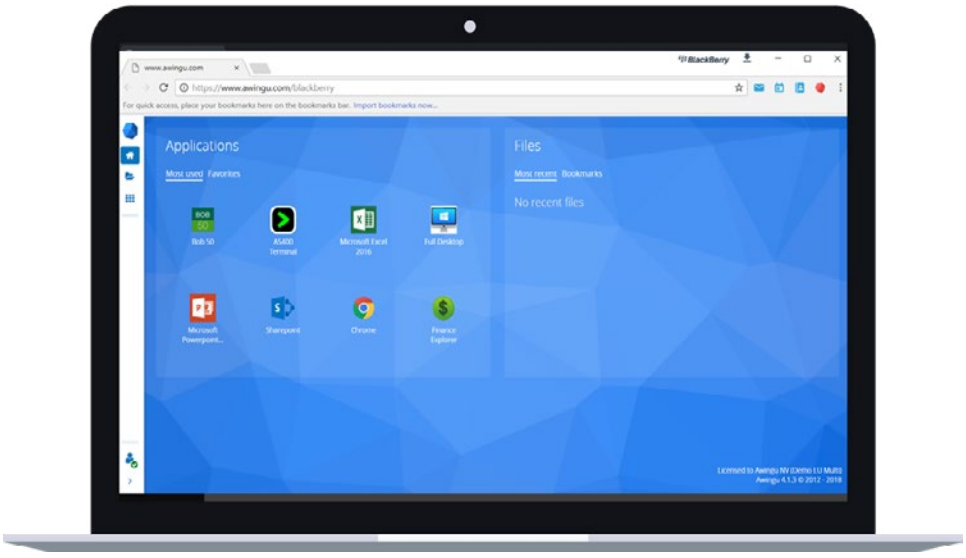
BlackBerry® products and services, in contrast, are designed to offer customers a granular level of control regarding data collection for forensic examination. We go to great lengths to ensure privacy-by-design in the architecture of our endpoint agent, and we never treat our customers’ data as something to be profited from. Trust is paramount for BlackBerry, and we will continue our legacy of earned trust in how we approach the security and privacy of our valued customers.

BlackBerry: Comprehensive Endpoint Security for Your Remote Workforce

BlackBerry offers a comprehensive solution to secure remote worker devices, with AI-powered prevention capabilities against zero-day malware, file-based and fileless attacks, memory-based exploits, malicious scripts, and compromised devices. This prevention-first protection is effective regardless of whether the devices are connected or offline, fixed or mobile, corporate-managed or BYO. BlackBerry products also provide a containerized, encrypted communications channel for securely connecting to the enterprise network while respecting the privacy of the device owner.

BlackBerry allows organizations to maintain continuous operations at scale while allowing security teams to optimize the productivity of remote workers on their personal devices, thereby assuring effective controls for the organization. Our solutions do not require the complexities and high costs of traditional VPNs or virtual desktop infrastructure (VDI), and enable administrators to reach more endpoints faster with turnkey access to quickly onboard or offboard users.

BlackBerry offers more than a simplified home use version of our solutions by providing true enterprise-level security that was designed to work anywhere and offers broad OS support for Windows®, Mac®, Linux®, Android™, iOS®, and Chrome OS™. BlackBerry solutions also offer the benefits of configurable, adaptive security policies and open APIs for SIEM and other enterprise security integrations where other whittled-down offerings for home use do not.



Secure Productivity Suites: More Than Just Endpoint Defense

Today's mobile workforce is often a mix of full-time employees, contractors, seasonal workers, and partners, so organizations need a way to enable this wider range of users to easily access firewall-protected business resources using either company-managed or personal devices.

And while security is critical with regard to managing a mobile workforce, it is often the single most significant barrier to business-critical workflows when it is bolted-on instead of baked-in. BlackBerry provides a mature platform for maintaining critical business operations with secure productivity and collaboration solutions that work with the most popular business applications and operating systems from within or outside the network.

BlackBerry's secure, browser-based Internet gateway interface allows users unfettered access to email, calendars, contacts, documents, Microsoft® Office 365® apps, intranet sites, cloud-based business apps, and more without the need for IT to actively manage individual devices or cumbersome VPNs that diminish performance and the user experience. BlackBerry solutions also allow IT teams to easily wipe all corporate data from devices without having to maintain a complex enrollment and deprovisioning process, saving time and budget.

BlackBerry. Intelligent Security. Everywhere.

Remote, anywhere, anytime access to company resources and data is what empowers a productive mobile workforce to be successful. Ensuring they can do this securely with the least complexity is what enables organizations to thrive. BlackBerry provides intelligent solutions based on a Zero Trust model that combines the right tools for the modern enterprise and a mobile workforce.

BlackBerry is trusted as the secure mobility solution of choice by world leaders and governments, the largest global banks, law firms, managed healthcare providers, investment services, and oil and gas companies. This is because we deliver smarter solutions that require fewer resources to support, in turn producing a better return on investment for our customers.

Contact BlackBerry today to find out how we can empower your organization to securely meet the productivity needs of your mobile workforce.

Keep Mobile Staff and Their Devices Secure

Make sure your mobile workers are staying secure and sustaining their levels of productivity. Learn more at https://www.blackberry.com/us/en/solutions/business-continuity

About BlackBerry

BlackBerry (NYSE: BB; TSX: BB) provides intelligent security software and services to enterprises and governments around the world. The company secures more than 500M endpoints including 150M cars on the road today. Based in Waterloo, Ontario, the company leverages AI and machine learning to deliver innovative solutions in the areas of cybersecurity, safety and data privacy solutions, and is a leader in the areas of endpoint security management, encryption, and embedded systems. BlackBerry's vision is clear — to secure a connected future you can trust.

BlackBerry. Intelligent Security. Everywhere.

For more information, visit BlackBerry.com and follow @BlackBerry.