Meta title: How to Keep Endpoints Secure during COVID-19?
Meta description: The COVID-19 pandemic rages on and employees are working from home. This creates new endpoints and vulnerabilities. Can BlackBerry UEM keep them safe?
Meta tags: blackberry UEM

How to Keep Your Endpoints Secure During the COVID-19 Epidemic

Image text: Endpoint security
Alt text: Data breaches
Image description: Online security.

Many businesses are now implementing social distancing measures to curb the spread of the novel coronavirus. This means transitioning to digital media platforms to keep their employees safe and minimizing the resulting disruption due to work-from-home measures.

Because of this new situation, organizations are now experiencing a new paradigm shift that will severely impact the security of their operations.

Since employees are no longer within their corporate borders, it has become easier for hackers to exploit new vulnerabilities in the endpoints used by remote workers. While cybersecurity breaches aren't a new thing - hundreds of millions of records are compromised every year - the stakes are much higher during the COVID-19 pandemic.

Cybercriminals will be targeting individual users who will lure end-users to take actions on emails and links shared by them via social media. They will mostly try to capitalize on their concern during the pandemic.

Cybersecurity breaches can have a devastating effect on organizations. This has been demonstrated time and again in recent cases such as the Capital One event where a hacker gained access to 100 million credit card applications and accounts. The 2017 Equifax data breach exposed the personal information of 147 million people. And just recently, the Marriot Data Breach of 2020 resulted in 5.2 million guest records being stolen. The list just goes on.

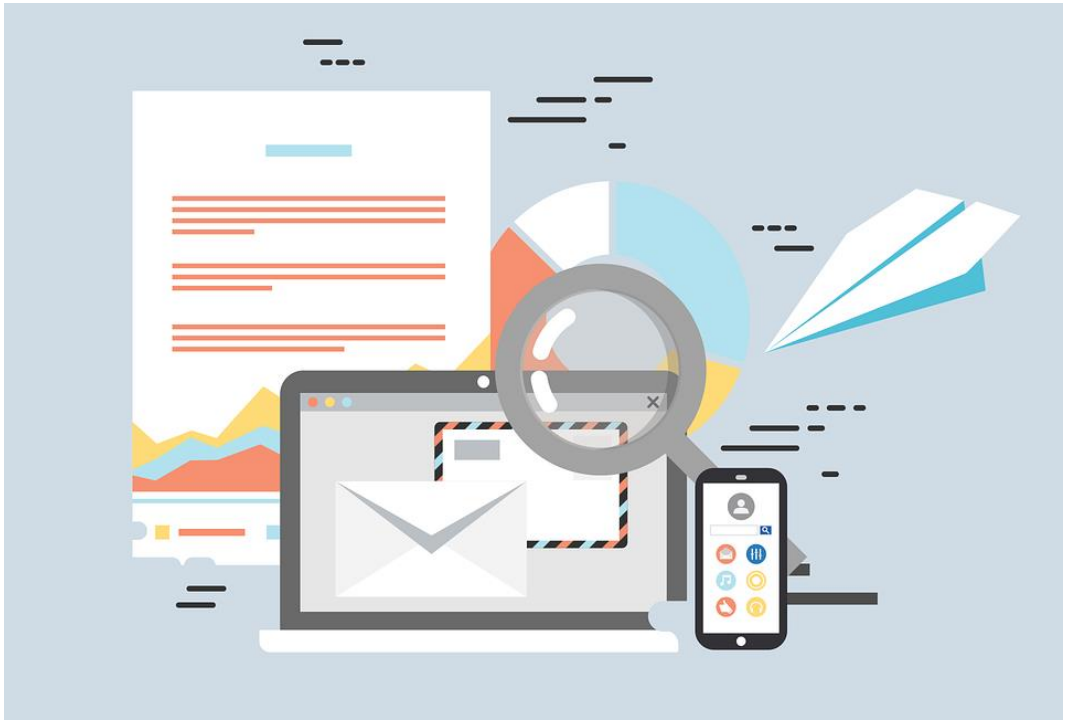
Endpoint security is a critical concern for many organizations because most of them take place at the end-user level. The challenges facing IT teams because of COVID-19 now include:

- The use of personal devices while accessing critical business data
- Making appropriate configurations of business servers for use by remote users
- Securing corporate virtual private networks
- Using advanced authentication methods such as two-factor authentication

How to Keep End-points Secure?

Many organizations are now turning to BlackBerry UEM, Blackberry's advanced endpoint protection solution. Unlike traditional software that exclusively relies on malware signatures, BlackBerry UEM utilizes a rare combination of artificial intelligence and machine learning to identify malicious code. This is shown to be extremely effective because it evolves as rapidly as the attack vectors used by hackers to propagate security breaches.

Key features of BlackBerry UEM:



- ✓ True zero day prevention
- ✓ AI powered malware detection and prevention
- ✓ Application control
- ✓ Easy distribution and configuration
- ✓ Low hardware resources consumption
- ✓ Single solution for device and app management
- ✓ Support for multiple platforms including Windows, iOS, macOS, Android, and more

Easily Manage Remote Devices with UEM

During these troubling times when employees are asked to work from home, BlackBerry UEM can prove to be monumental in securing access to the organization's resources such as file shares and intranet. BlackBerry UEM can give IT teams complete control over the entire setup, nothing can leave or enter the company's corporate data without the admins knowing it.

More importantly, it does not allow sensitive data to be accessed by third-party apps such as Facebook and Messenger unless specified by the administrator.

To make remote working more secure, BlackBerry UEM builds a unique signature for compliant devices and apps. The moment an unauthorized or rogue signature is detected, its connection is blocked and alerts are sent to administrators.

All of these features make BlackBerry UEM one of the best endpoint protection solutions that are currently available in the market.