White Paper

The New Reality:
Bring Order To Chaos With Unified Endpoint Security

Summary

Chaos and confusion dominated the enterprise cybersecurity landscape even before the COVID-19 pandemic. The increasing volume and variety of endpoints in organizations combined with ever-increasing cybersecurity threats put tremendous pressure on IT. When companies implemented security solutions with burdensome requirements, employees often turned to workarounds and shadow IT. Then the pandemic exacerbated all these challenges and revealed serious gaps in organization's preparedness for remote work.

Experts predict that digital transformation and remote work will accelerate in the new normal. So will the need to secure every kind of endpoint and safeguard sensitive corporate data. To succeed in the new reality, solutions must meet the rigorous security requirement of IT leaders while also accommodating users' desire for ease-of-use and mobility.

Unified endpoint security is a modern solution to these modern problems. Leveraging AI, machine learning and automation, it provides next-generation cyber threat prevention and remediation across devices, networks, apps and people – all without interfering with user productivity. Bridging Zero Trust with Zero Touch, unified endpoint security is designed for the future of work.

Table of Contents

The New Cybersecurity Landscape

The COVID-19 pandemic has forced organizations worldwide to rely on technology like never before. Pre-pandemic, businesses were already confronting an increasingly menacing cybersecurity environment and a proliferation of vulnerable endpoints. Now, with the sudden pivot to nearly 100% remote work at many companies, IT leaders face an unprecedented test as cyber criminals across the globe capitalize on the crisis.

The old approaches to defending against cyber threats are simply not up to the task. Businesses need the latest, smartest solutions to defend their employees, clients, sensitive data, and reputations during this crisis and beyond. According to Gartner, CIOs should be reviewing their existing security infrastructure and assessing what employees need to work safely from home, with a particular focus on endpoint security for devices.[1]

Unified endpoint security (UES) is a new, comprehensive approach to meeting today's ever-increasing cybersecurity requirements. Leveraging AI, machine learning, and automation, it's designed to meet the intense security demands of IT leaders while still supporting user productivity.

The Global Attack Surface is Expanding

Easier access to attack toolkits combined with the explosion of connected endpoints has escalated cyber threats across the globe. In 2020, AI and machine learning will be critical for threat prevention and remediation strategies because of the advantages they offer through continuous learning and proactive threat modelling of increasingly complex attacks.

– BlackBerry Cylance 2020 Threat Report

Critical Factors in the Cybersecurity Landscape

In recent years, the cyber environment has been increasingly chaotic, with organizations facing relentless, sophisticated cyber threats while also trying to manage an exponential growth in endpoints. Then, the pandemic created a massive – often inexperienced – remote workforce overnight. Most organizations did not have solutions in place to allow remote employees to access corporate data while keeping it secure. Together, these conditions have put enterprises at serious risk.

Cyber Chaos

A culmination of multiple trends is fueling cyber chaos, including:

- **Acceleration of tech innovation**
  There's a constant flow of new technology, and organizations must constantly adopt new tools to stay competitive.
- **Expanding attack surface**
  Organizations are increasingly reliant on technology – including connected endpoints.
- **Exponential vulnerabilities**
  More endpoints mean more vulnerability.
- **Exponential attackers and attack types**
  Attackers use a multi-pronged approach to target exposed endpoints.
- **Offensive investments**
  Beyond individual attackers, a growing number of nations invest in offensive cyber weapons for profit or national interest.
- **Geopolitical tensions**
  Global geopolitics complicate the already complex cybersecurity environment.
- **Lack of governance**
  There's consensus on the need to improve security in Internet governance, but no agreement on how.

Endpoint Chaos

The time when organizations only had to secure laptops and desktops is long over. The increasing volume and variety of endpoints – ranging from phones and tablets to wearables, and all kinds of IoT and cloud-connected devices – has resulted in higher costs and complexity for IT. Organizations are struggling to cope with a rising number of security vendors, tools, consoles, and threat alerts – not to mention the increased vulnerability to attackers.

The BYOD model is being put to the test globally during the pandemic. Organizations that already supported BYOD have an advantage, but not many companies had a 100% remote workforce. Now, IT leaders are struggling not only to manage huge numbers of endpoints, but many unmanaged devices within those numbers.

Lack of Preparedness for a Remote Workforce

Few, if any, organizations were fully prepared for the scale of disruption that came with the COVID-19 pandemic and the necessity of remote work. Many companies did not have enough corporate devices to equip the entire workforce. They also lacked solutions to enable employees to access corporate data and resources behind the firewall. Most important, they had no infrastructure to ensure data, device, and app security.

IT leaders everywhere had to rethink their cybersecurity strategies amid global reports of heightened cyber attacks. An alert from the U.S. Department of Homeland Security early in the pandemic warned that cyber criminals were targeting individuals, small and medium enterprises, and large organizations with COVID-19-related scams, malware attacks, weaponized websites, and phishing emails.[2] The Wall Street Journal cautioned that these attacks, and the resulting chaos and confusion, have created costly long-term security risks.[3]

Many Organizations Were Not Ready for a 100% Remote Workforce

In a PwC survey of finance leaders worldwide at the start of the pandemic, the respondents said "productivity loss due to lack of remote work capabilities" would be their top challenge.[4]

The Human Response To Cybersecurity Chaos, and Why It's Dangerous

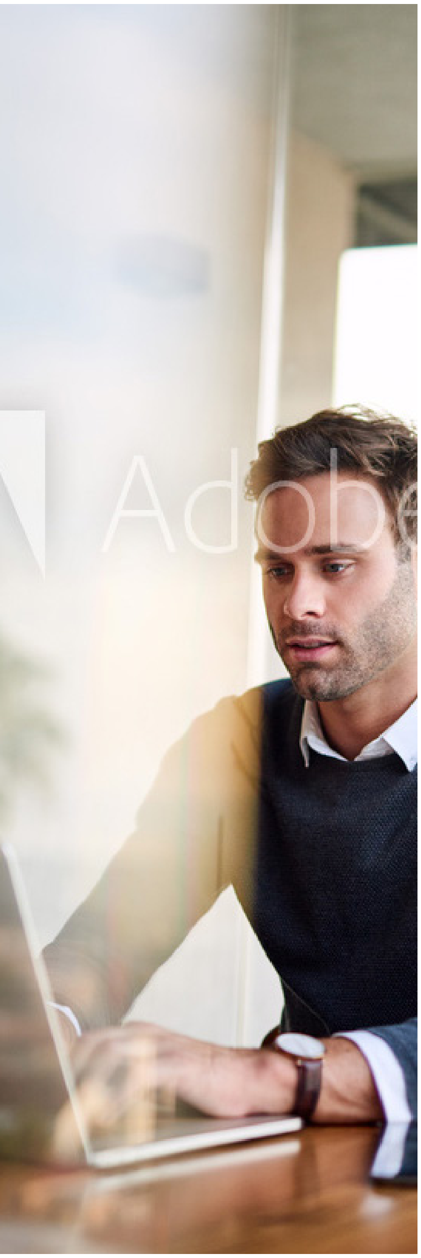
Even prior to the pandemic, the chaotic cybersecurity environment had pushed many employees to the brink of frustration. Onerous authentication processes, clunky interfaces, endless alerts, ineffective and costly signature-based security measures, and other irritations led people to use security workarounds and shadow IT. While the intention to simplify and preserve productivity is understandable, the resulting data breaches could be harmful – even disastrous – to organizations.

With the sudden, sharp increase in remote workers during the COVID-19 outbreak, the threats to data security are at an all-time high. A CNBC flash survey of tech executives in the early weeks of the pandemic found 36% believe cyber threats increased as a majority of their employees shifted to working from home.[5]

Similarly, the National Law Review reported an upswing in phishing attacks that preyed on people's fear and need for health, safety, and financial information.[6] With employees under pressure to get work done from home – even if they've never done so in the past – security workarounds and susceptibility to scams are an urgent problem for organizations.

36%

of tech executives believe cyber threats have increased due to employees working from home.[5]



Security Designed for Humans

Before, during, and after the pandemic, any security solution that hopes to tame the chaos must also accommodate human nature and human error. In the new security landscape, cyber threats can come from both outside and inside.

In a recent IDG survey of global IT professionals, 95% of respondents said that employee mistakes present a data security risk for their organization. Most respondents felt that increased security has negatively affected productivity, yet 58% still prioritize strict security controls over ease-of-use and convenience for employees.[7]

Organizations should consider whether solutions are designed to:

- Accommodate users' drive for simplicity, efficiency, and ease
- Mitigate unintentional mistakes
- Thwart malicious actions by disgruntled employees

The latest generation of smarter security reconciles the priorities of the two main stakeholders in enterprise IT:

- IT and business leaders, who want maximum security
- Users/employees, who want maximum ease-of-use, functionality and mobility

58%

of IT professionals still prioritize strict security controls over ease-of-use and convenience for employees.[7]

Zero Trust vs. Zero Touch

Zero Trust has become a buzzword in cybersecurity circles, but the true value of Zero Trust for security teams depends on whether it can also enable Zero Touch for users/employees. If creating a Zero Trust environment produces excessive security hurdles and inconvenience for users, they will try to circumvent the system and render it useless. Striking a balance between continuous threat protection and user productivity is key.

Zero Trust Means…

Users cannot access anything on any device until they prove who they are, that their access is authorized, and that they're not acting maliciously. They must continually earn this trust across endpoints.

Zero Touch Delivers…

Immediate productivity with instant access to corporate resources, without the hassle of passwords, timeouts, special permissions, or multiple authentications.

When Zero Trust solutions provide a path to Zero Touch, organizations get the best of both worlds: security they can trust to defend against emerging cyber threats and a positive user experience that fosters productivity.

Defenses at Human Speed vs. Computer Speed: The AI Advantage

The cybersecurity tools of the past operated at human speed. As each new cyber attack emerged, vendors analyzed the threat and issued virus definitions via subscription to identify known malware as a rearward-looking defense solution. It was a time-consuming process that couldn't keep pace with the onslaught of increasingly advanced threats.

Today's cyber criminals use AI to maximize the reach and impact of their attacks, so today's solutions must also exploit the power of machine learning and automation. Only with advanced AI-based security tools can organizations gain the predictive time advantage they need.

The WannaCry Ransomware Attack

On May 12, 2017 at 7:44 AM, the ransomware known as WannaCry started its rampage around the world, attacking hospitals, manufacturers, telecommunications, and more. It ultimately affected devices across 150 countries. Traditional security tools couldn't stop this novel and fast-spreading malware that signaled a new era of cyber warfare. Ultimately, a new AI-powered tool contained the threat.

A New Approach for the New Reality: Unified Endpoint Security

50%

of organizations will have mobile threat defense in place by 2023.[8]

Modern problems require modern solutions. The next generation of cybersecurity consolidates the best available AI-driven tools for detecting, protecting against, and remediating threats to every type of endpoint. Unified endpoint security takes a comprehensive approach to taming the chaotic cybersecurity environment.

The Gartner Predicts 2020 Mobile and Endpoint Technologies report notes the trend toward consolidating mobile threat defense (MTD) offerings with endpoint detection and response (EDR) and endpoint protection.[8] It recommends that organizations adopt security tools, such as MTD, to close gaps in existing security infrastructure capabilities, rather than fundamentally change security capabilities. The report also forecasts that 50% of organizations will have MTD in place by 2023, up from fewer than 20% of organizations in 2020.

IDC Survey Finds Organizations Struggle To Balance Flexibility and Security

A pre-pandemic IDC survey found more than 60% of organizations have trouble balancing employee flexibility (increasing remote work, agility, and consumer-like digital experiences) with security requirements. IDC predicts that the pandemic experience will prompt many organizations to closely examine and upgrade policies, processes, and technologies related to remote work at an accelerated pace.[9]

A Total Solution for Today: BlackBerry UES

Gartner research predicts that by 2024,

70%

of organizations will have a unified console.[10]

BlackBerry® Unified Endpoint Security (UES) is a security solution designed for the new reality. While other vendors address parts of the cyber threat problem, BlackBerry UES provides a true AI-powered solution for Zero Trust with full coverage across the spectrum of devices, networks, apps, and people. The outcome of this Zero Trust approach is a Zero Touch experience, which improves security without interrupting user productivity.

BlackBerry Spark

The BlackBerry® Spark Suite is a one-stop shop and the gold standard for unified endpoint security (UES) and unified endpoint management (UEM). It supports all device types and ownership models.

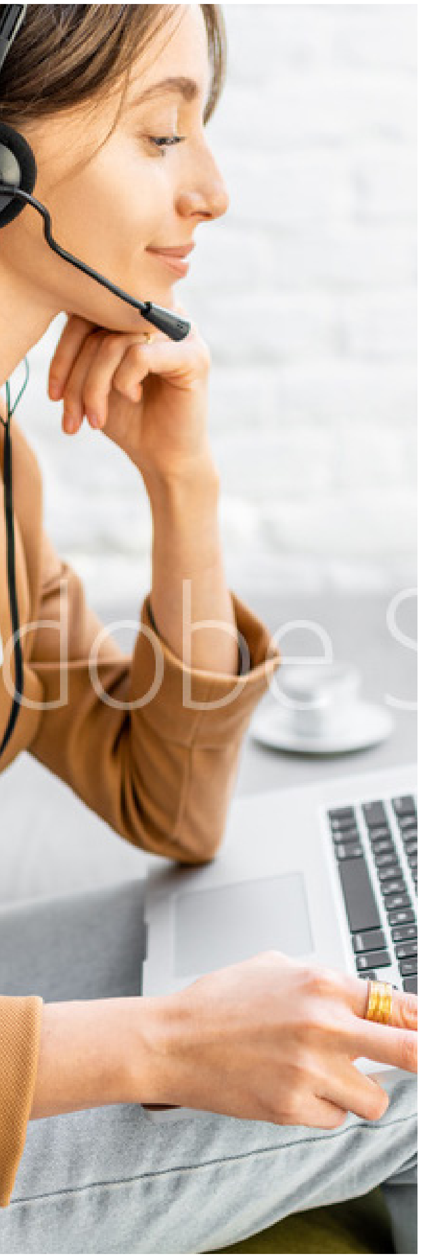
Leveraging AI, machine learning and automation, BlackBerry UES provides improved cyber threat prevention and remediation while offering improved visibility across all endpoints and simplified administration.

Zero Trust To Zero Touch

BlackBerry UES is built to meet the most stringent security requirements of organizations coping with today's cyber chaos, yet is also designed for humans. Instead of requiring users to constantly re-authenticate, BlackBerry UES relies on AI to maintain dynamic trust across devices, networks, data, users, and apps.

BlackBerry UES Prevents IcedID Banking Trojan

First identified in 2017, IcedID (originally known as BokBot) is malware with information-stealing capabilities. By training AI agents for threat detection using millions of safe and unsafe files, BlackBerry UES prevents IcedID and similar malware from executing based on the detection of several malicious file attributes. With this predictive advantage, organizations can take a prevention-first security posture to protect against unknown and emerging threats.



Trusted Productivity Apps for the New Mobile Workforce

The AI-driven threat protection at the heart of BlackBerry UES is built directly into BlackBerry mobile apps, so users and admins don't have to install or manage third-party apps that are specifically built for mobile threat detection.

It's a mobile threat defense (MTD) solution that constantly scans mobile apps for malware, stopping attacks before they can start. Organizations can rest assured that the critical business apps used by their remote workforce – and the vital data within those apps – are protected.

Six Technologies Working Together To Reduce Cyber Threats

BlackBerry UES offers the broadest set of security capabilities and visibility through six interconnected technologies, or pillars. These pillars work in tandem to calculate risk, share data, and enable better policy controls.

For example, the endpoint detection and response (EDR) solution leverages endpoint protection and mobile threat detection (MTD) technologies to block malware and phishing attacks – which *PC Magazine* reports are on the rise at organizations worldwide.[11] Continuous authentication uses data from EDR, EPP, and MTD to refine behavioral profiles and close the gap between Zero Trust and Zero Touch.

1. **Endpoint Protection**

   Automated malware prevention powered by AI, combined with application and script control, memory protection, and device policy enforcement to predict and prevent cyber attacks

2. **Endpoint Detection and Response (EDR)**

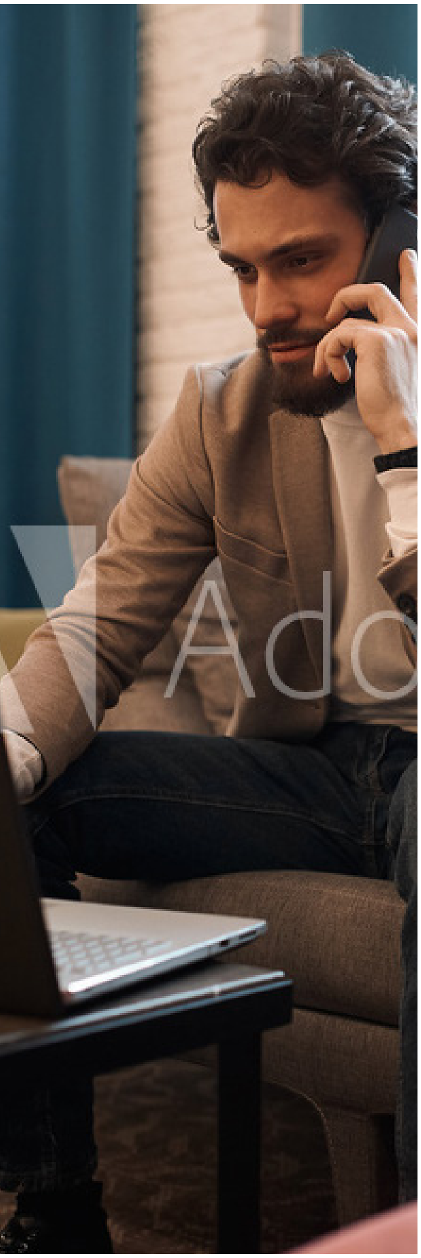
   AI-based, prevention-first endpoint detection and response stops attacks before they can execute, and automates investigation and response with playbook-based workflows

3. **Mobile Threat Defense (MTD)**

   Leverages AI to monitor mobile devices and the apps running on them for any new or known threats (including malicious URLs and phishing) and takes appropriate action to remediate

Report Warns of Skyrocketing Mobile Malware

Even prior to the COVID-19 pandemic, attacks on mobile devices were pervasive and prolific, according to the recent BlackBerry Mobile Malware and Advanced Persistent Threat Espionage report. The findings showed that mobile malware, often used in combination with traditional desktop malware, has been used by state-backed groups in ongoing surveillance campaigns far more than previously estimated.[12]



4. Continuous Authentication

Assesses a user's ongoing interaction and behavior with their device (combining biometric, app usage, network, and process invocation patterns across mobile and desktop) to authenticate and dynamically grant them access to corporate data, significantly reducing administration overhead

5. Data Loss Prevention (DLP)*

Combines core BlackBerry technologies such as digital rights management (DRM) and machine learning to establish Zero Trust between users and data

6. Secure Web Gateway*

Provides several capabilities to meet the Zero Touch objective of instant, secure, and VPN-less mobile access on any device:

- Continuous and contextual authentication
- Traffic segmentation
- Threat prevention
- Reporting and analysis

* Future release

Key Benefits of BlackBerry UES

Delivers Better Cybersecurity Threat Prevention and Remediation

BlackBerry UES eliminates the hassle of multiple vendors, the noise of excessive alerts, and the uncertainty of securing organizations in the new reality. Using the latest in AI-driven threat prevention, detection, continuous authentication, and response, it matches and exceeds the sophistication of today's attackers. BlackBerry UES works across organizations' expanding attack surface to address the unprecedented vulnerability in the global remote workforce.

Supports Productivity By Bridging Zero Trust and Zero Touch

BlackBerry UES continuously monitors all endpoints to learn how users interact with devices, apps, and networks. With this information, AI automatically determines whether users can be trusted with instant access to enterprise resources from any device, at any time, from any location, over any network. This smart, AI-powered approach optimizes legitimate users' experience while thwarting attacks and preventing data loss.

Offers Comprehensive Coverage

By working across all endpoint types, BlackBerry UES ensures complete coverage and better insight into trusted user behavior. It provides continual authentication that spans devices, networks, apps, and people, along with visibility across the entire ecosystem. In the pandemic enterprise landscape, BlackBerry UES offers a clear line of sight across organizations' expanding attack surface.

Becomes Smarter with Time and Use

BlackBerry UES is built on a proven AI-ML engine with years and multiple generations of threat detection and threat modelling. It's continuously learning as the environment changes with new users, new devices, new applications, and new technologies. So, the longer an organization uses BlackBerry UES, the smarter it gets.

Simplifies Administration

As organizations confront unexpected financial challenges and complex restructuring to ensure business continuity during and after the pandemic, BlackBerry UES delivers stronger and *simpler* cybersecurity. It's easy to manage, saves time and money spent on multiple vendors, reduces the burden on IT, and frees resources for more strategic priorities.

* Future release

Preparing for the Future of Work

The COVID-19 pandemic changed how people work in a sudden and dramatic way. When – or whether – things will ever return to the status quo is unknown, and experts predict an acceleration of digital transformation and remote work. Unfortunately, cyber criminals worldwide thrive on the attack opportunities presented by the wide variety of endpoints used by a massive remote workforce.

By closing the gap between Zero Trust and Zero Touch with the latest AI, BlackBerry UES allows organizations to safeguard their data while empowering employees to get work done from anywhere, at any time, on any device or app. It’s a complete solution for the new reality.

* Future release

About BlackBerry

BlackBerry (NYSE: BB; TSX: BB) is a trusted security software and services company that provides enterprises and governments with the technology they need to secure the Internet of Things. Based in Waterloo, Ontario, the company is unwavering in its commitment to safety, cybersecurity, and data privacy, and leads in key areas such as artificial intelligence, endpoint security and management, encryption, and embedded systems. For more information, visit BlackBerry.com and follow @BlackBerry.

[1] https://www.gartner.com/smarterwithgartner/coronavirus-cio-areas-of-focus-during-the-covid-19-outbreak/
[2] https://www.us-cert.gov/ncas/alerts/aa20-099a
[3] https://www.wsj.com/articles/coronavirus-cybersecurity-fallout-might-not-be-felt-for-weeks-or-longer-11585128601
[4] https://www.pwc.com/us/en/library/covid-19/pwc-covid-19-cfo-pulse-survey-global.html
[5] https://www.cnbc.com/2020/03/20/phishing-spam-spike-as-hackers-use-coronavirus-to-hit-remote-work.html
[6] https://www.natlawreview.com/article/working-remotely-and-cyber-security-during-covid-19-outbreak
[7]
[8] https://www.gartner.com/en/documents/3980406/predicts-2020-mobile-and-endpoint-technologies
[9] https://blogs.idc.com/2020/03/16/remote-work-in-the-covid-19-era-are-we-ready/
[10] https://www.gartner.com/en/documents/3980406/predicts-2020-mobile-and-endpoint-technologies
[11] https://www.pcmag.com/news/phishing-attacks-increase-350-percent-amid-covid-19-quarantine
[12] https://www.blackberry.com/uk/en/company/newsroom/press-releases/2019/blackberry-cylance-releases-mobile-malware-report-reveals-pervasive-mobile-malware-dimension-in-cross-platform-advanced-persistent-threat-espionage-campaigns