BlackBerry. Intelligent Security. Everywhere.

HOW UES PROTECTS SHIFTING WORK ENVIRONMENTS.

UES REPORT

CONTENTS

EXECUTIVE SUMMARY

The global COVID-19 pandemic has heightened the need for unified endpoint security (UES) solutions that combine incident prevention, detection and response capabilities.

A survey of 300 IT professionals that IDG conducted on behalf of BlackBerry in October–November 2020 shows the shift to a more distributed workforce triggered by the pandemic, which has exposed organizations to new risks from employees accessing the enterprise from insecure home networks. The shift has increased user support requirements and intensified the need for more IT security staff at many organizations.

IT leaders are very concerned about risk to the enterprise from poorly secured desktops, laptops, smartphones and other endpoint devices connecting to their networks. Many are supporting a substantial remote workforce currently and expect to do so over the next six months at least. The survey data shows organizations want technologies that help improve endpoint incident detection. Capabilities that offer better visibility and control over remote desktops, laptops and mobile devices, faster security patching and stronger user authentication and privilege management have become high priorities.

Survey respondents perceived the ability to consolidate endpoint protection, incident detection and response capabilities as key to mitigating attacks, enabling better support and lowering total cost of ownership (TCO). A majority want an endpoint security solution to extend beyond traditional endpoints to the cloud.

DRIVERS FOR CHANGE

Generally, the global pandemic has intensified the need for IT security skills, escalated the risk posed by home networks and increased user support needs.

We asked survey respondents to identify the top challenges that have become apparent or have intensified in the months since the pandemic began. The responses showed that security leaders in the U.S., Canada and the U.K. share many of the same challenges, although the top concerns sometimes tended to vary by region and by industry.

For example, 58% of respondents representing U.S.-based companies and 43% from the U.K. described the pandemic as exacerbating problems caused by skill gaps and security awareness. Nearly three-quarters (74%) of those representing financial organizations, 62% of respondents from the manufacturing sector and 57% from the technology industry expressed the same concern over skills availability and security awareness. The concerns likely stem from the growing pressure on security teams to support a larger distributed workforce while also battling ransomware, distributed denial-of-service (DDoS) attacks and other threats directed at the enterprise network.

CONCERNS ABOUT SKILL GAPS AND SECURITY AWARENESS WERE EXACERBATED BY THE PANDEMIC ACROSS SECTORS

62%

MANUFACTURING

74%

FINANCIAL SERVICES

57%

TECHNOLOGY

Although skills and security awareness are predominant issues for some organizations, security professionals in Canada are mostly concerned about risks to the organization from insecure home routers, modems and other networked components on home networks. In fact, 48% of Canadian-based survey takers identified this as the biggest issue caused by the pandemic. Similarly, nearly three out of four security and risk managers in the healthcare sector (73%) are most concerned about the accelerated migration to the cloud and cloud-hosted services that was prompted by the pandemic.

Our survey also revealed broad concern across all three regions over phishing and smishing attacks and challenges associated with securing personally owned and non-IT-managed endpoint devices.

More than one-third (35%) of respondents were unsure about the ability of the IT infrastructure to securely support a remote workforce.

LONG-TERM SHIFT

Early on in the pandemic there was some anticipation the shift to a remote workforce would be short-lived and temporary. However, that no longer appears to be the case. More than a year into the pandemic, security teams continue to support a substantial proportion of work-from-home and remote employees at a sizable number of organizations. On average, more than 3 in 10 employees at organizations in the U.S., Canada and the U.K. are currently working from home. Organizations in Canada and the U.K. have a substantially higher percentage of their workforce—41% and 38% respectively—working from home compared to U.S.-based entities (19%).

Enterprise security and risk managers expect that requirements to support a widely distributed workforce are likely to remain unchanged in the short term. U.S. organizations expect that nearly one-quarter (23%) of their workers—compared to just 19% now—will be working from home in the next six months. U.K. and Canadian organizations expect a smaller, but still substantial percentage—29% and 32% respectively—of their workers to be home-based in six months. The numbers reflect what some analysts have predicted will be a permanent shift to a remote work environment for at least a subset of workers at many organizations around the world.

A Gartner survey reveals 82% of company leaders plan to allow employees to work remotely some of the time.

THE BYOD CHALLENGE

Adding to the challenges posed by a more distributed endpoint environment is the relatively high use of personally owned devices for work—including PCs, laptops, smartphones and tablets—by employees at many companies.

The bring-your-own-device (BYOD) challenge is significant. Nearly one in five employees (18%) at the average organization in the U.S., Canada and the U.K. are using a personal PC to access corporate data, and 20% use a personal smartphone for that purpose. Our survey data showed the use of personally owned devices such as PCs and mobile devices at work to be more prevalent in Canada and the U.K. than in the U.S. Of Canadian and U.K. workers represented in the survey, 17% and 23% respectively described themselves as using a personal PC for work compared to 14% in the U.S. The same was true of personally owned smartphones, with 20% and 26% respectively of Canadian and U.K. workers using a personal smartphone compared to 16% in the U.S.

The risks to enterprise security posed by personally owned and unmanaged PCs, smartphones and other endpoint devices have been well chronicled over the past decade. But the shift to a more remote and hybrid work environment appears to be driving renewed focus on the issue. Personally owned endpoint devices such as PCs, laptops and smartphones often have little of the protection found on IT-managed systems and are harder to patch and protect because they are not centrally managed. As a result, corporate data on these systems is more vulnerable to data theft and leaks than data on IT-owned and IT-managed endpoints.

Vulnerable and unapproved applications running on these devices often can heighten these risks. Personally owned devices are also attractive targets for attackers because they can serve as an entry point to the broader enterprise network. However, personally owned PCs and smartphones are not the only issue. Home wireless networks, modems, routers, printers and other devices typically tend to lack the same level of protection as components on a corporate network and are therefore more vulnerable to attack and exploitation.

Concerns are also high over the security status of the PCs, laptops, smartphones and tablets employees will bring back with them to the office after using them on a home network for months without proper supervision or control.

Consequently, a majority or plurality of respondents across all three regions in the survey said they either planned on quarantining PCs upon arrival or scanning and installing patch updates on them before allowing users to connect them to the corporate network. Scanning and patch updates are the primary choice in Canada and the U.K. In the U.S., a majority of organizations appear to consider quarantining as a safer first option.

The data suggests the responsibility for key decisions on how to protect remote access continues to rest outside of the IT security department at many companies, even as the work environment itself has shifted to an increasingly remote or hybrid model.

THE ENDPOINT SECURITY MANAGEMENT LANDSCAPE

Weighted data from across all three survey regions shows the IT networking team is typically responsible for managing remote access and has primary decision-making responsibility for the function in the U.S. and Canada. A reported 50% of U.S. respondents and 40% in Canada identified the network team as the decision-maker on remote access matters. In the U.K., 46% identified the IT infrastructure team as being responsible for the function.

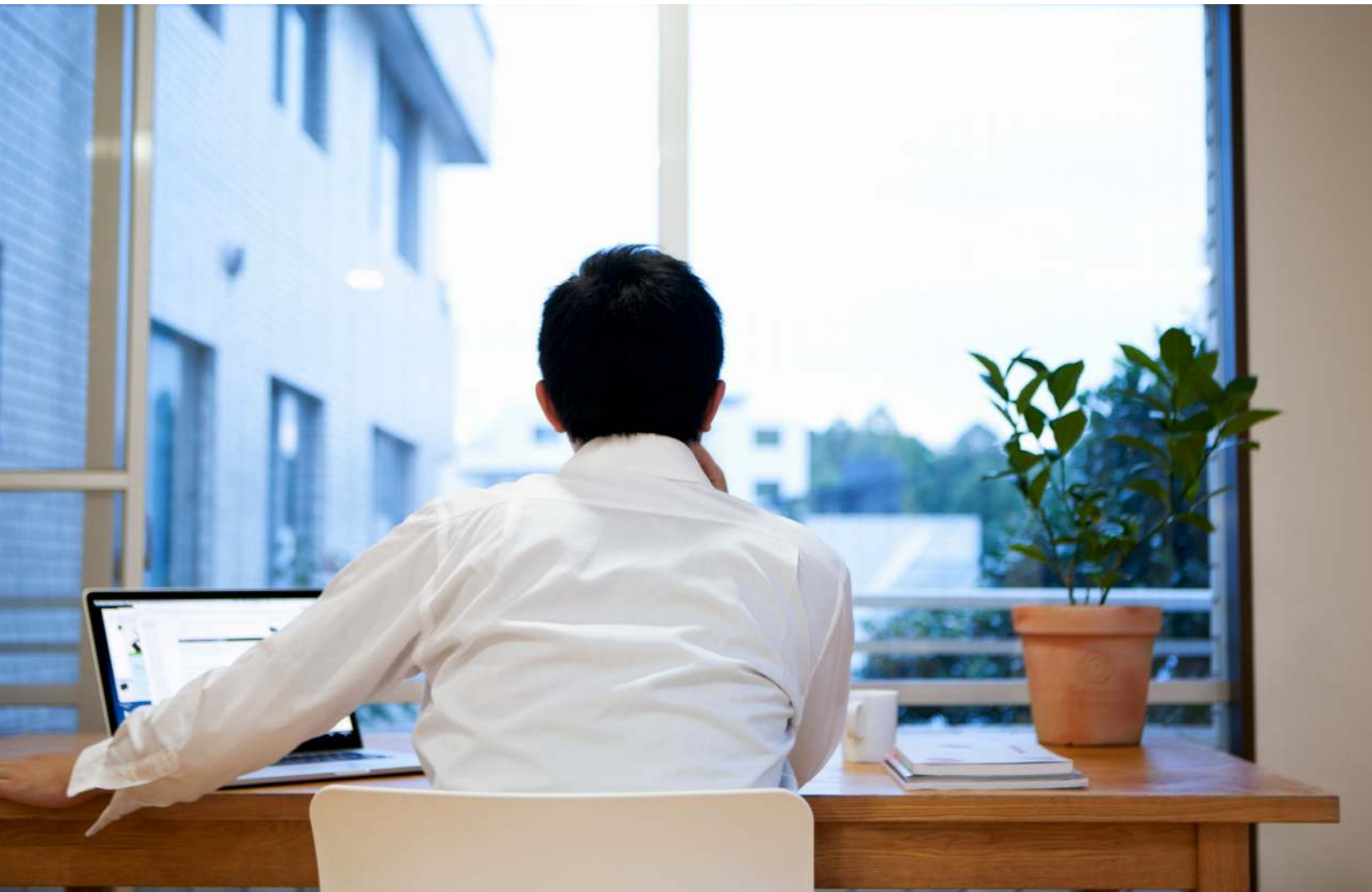
Notably, the IT security team is a decision-maker in less than one-quarter of organizations across all three of our survey regions. Just 24% of U.S.- and Canadian-based respondents and an even smaller 20% of U.K. survey takers described the IT security team as being responsible for the remote access function.

ENDPOINT SECURITY CONTROLS

What controls have organizations currently deployed—or what are they planning to deploy—to protect endpoint devices connecting to the enterprise network? Our data revealed they are using—or plan to use—a combination of endpoint protection mobile threat detection (MTD) and endpoint detection and response (EDR) technologies.

Interest in EDR in particular appeared to be quite high across all three surveyed regions. EDR technologies help organizations continuously monitor, collect and analyze data from endpoint devices to help detect suspicious behavior, block malicious activity and provide rule-based remediation guidance. Security analysts consider the capabilities offered by EDR tools as key to being able to quickly detect and mitigate threats to PCs, laptops and mobile devices at a time when many attackers have begun leveraging legitimate admin tools and processes to carry out malicious activities.

Nearly one-third (32%) of organizations across the U.S., Canada and the U.K. have already implemented the technology, 21% plan to implement it and 31% are evaluating EDR. More organizations in the U.S. have deployed endpoint detection and response capabilities and appear interested in it than entities in Canada and the U.K. Its biggest fans appear to be financial services companies and organizations in the manufacturing and technology sectors.



Interest in mobile threat detection tools appears to be quite high as well. Although fewer organizations (16%) have currently deployed MTD compared to EDR, 28% said they plan to do so and another 31% are currently evaluating the technology. Like EDR, MTD tools are designed to protect mobile devices, networks and applications by continuously monitoring for threats and signs of suspicious behavior. Security analysts consider the technology useful especially in helping organizations establish some level of security over personally owned mobile devices in work environments. Our survey data suggests fairly substantial interest in the technology among organizations in the healthcare, financial services, retail and manufacturing sectors in particular.

Organizations are not just focused on after-the-fact detection and response to threats on desktop PCs, laptops and mobile devices. Many remain committed to protecting these devices from compromise in the first place. Nearly 3 in 10 (29%) described their organization as continuing to have a separate endpoint protection capability, 22% have plans to implement it and 30% are evaluating the capability.

SECURITY PROFESSIONALS WANT MORE

IT leaders expect more from endpoint security technologies. In recent years, attackers have heavily targeted users and user devices such as PCs, laptops and smartphones via phishing and malware attacks designed to gain a foothold in enterprise networks. Enterprise mobility initiatives have led to an increase in the use of smartphones, tablets and other mobile devices in work environments and expanded the attack surface at many companies. With a large number of breaches resulting from attacks on user devices, IT leaders appear to be looking for new ways to bolster endpoint protection.

Our survey showed that specifically, organizations want technology that improves visibility and control over PCs, laptops and mobile devices—including personally owned devices—that are being used to access corporate systems. With users accessing enterprise assets from inside the network and from remote locations using a variety of corporate and personally owned devices, security professionals say improved visibility can help speed endpoint threat detection. They perceive better endpoint visibility as helping mitigate risks related to home networks, address risks posed by personally owned endpoint devices and enable stronger user authentication and patching.

When we asked survey respondents to identify the capabilities they considered most essential to future endpoint security, some 50% pointed to the ability to detect threats when a device is offline or not connected to the corporate network.

The top cited potential benefit of better endpoint visibility varied a bit by country. A reported 45% of U.S. respondents and 40% in the U.K. described faster threat detection as the top benefit, while 46% of Canadian respondents pointed to stronger user authentication and privilege management.

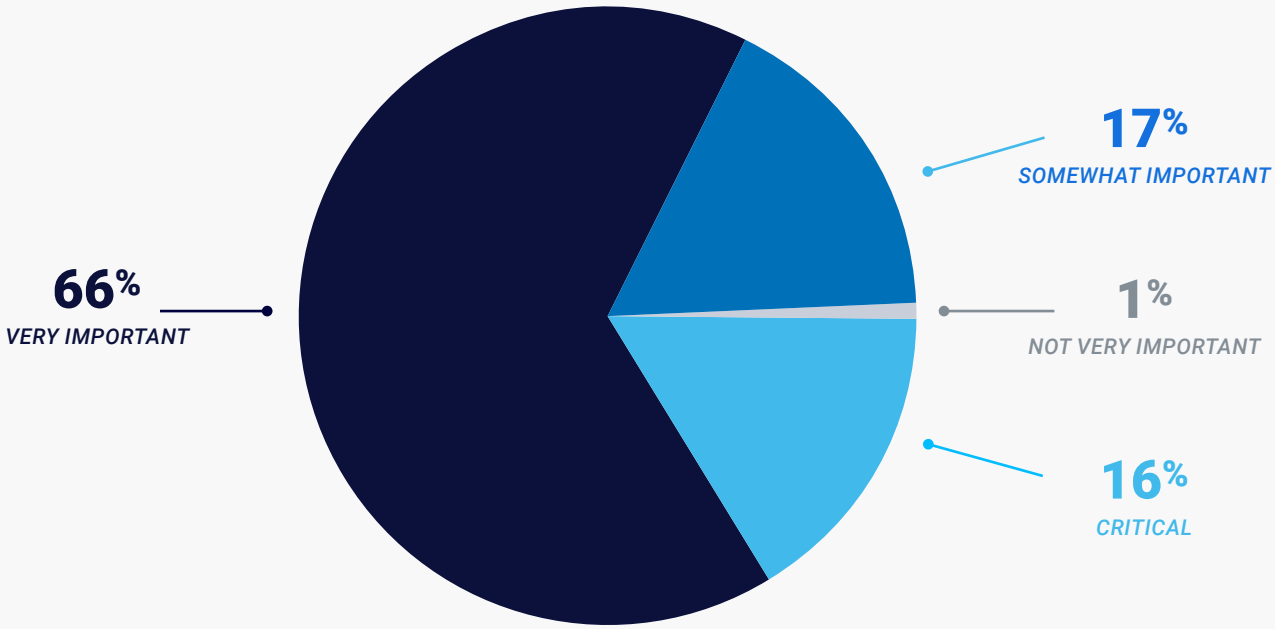
Meanwhile, more than 8 in 10 organizations (82%) want their current or future EDR technology to support both traditional endpoint devices as well as mobile devices. That sentiment likely is tied to the pandemic-related shift to remote working and the resulting increase in the use of mobile endpoint devices—both corporate and personally owned—to access enterprise data and network assets. The data suggests organizations are looking for technologies that can help consolidate and centrally manage endpoint and mobile device security in a unified manner.

That requirement is likely driven by concerns over enterprise data being increasingly scattered across remote PCs, laptops, smartphones and tablets, including personally owned devices with little protection.

Security professionals also want endpoint technologies to support the ability to dynamically adapt security policy based on user location, device and other factors. The most anticipated benefits of the ability to dynamically adapt security policy include an enhanced user experience and less friction (44%), continuous authentication (43%) and reduced remediation cost (43%). More than half (53%) of respondents from the technology sector say endpoint technologies that support adaptive security policies will help reduce the cost of issue remediation and 56% from the financial services sector believe it will help them use security staff more productively.

Consolidation of incident detection and response across all endpoint platforms is another major requirement. A reported 43% expect consolidating incident detection and response to help lower TCO (42%), enable broader device support (41%) and stop the spread of attacks (40%). More than 80% consider these capabilities as essential or critical requirements for future endpoint security products.

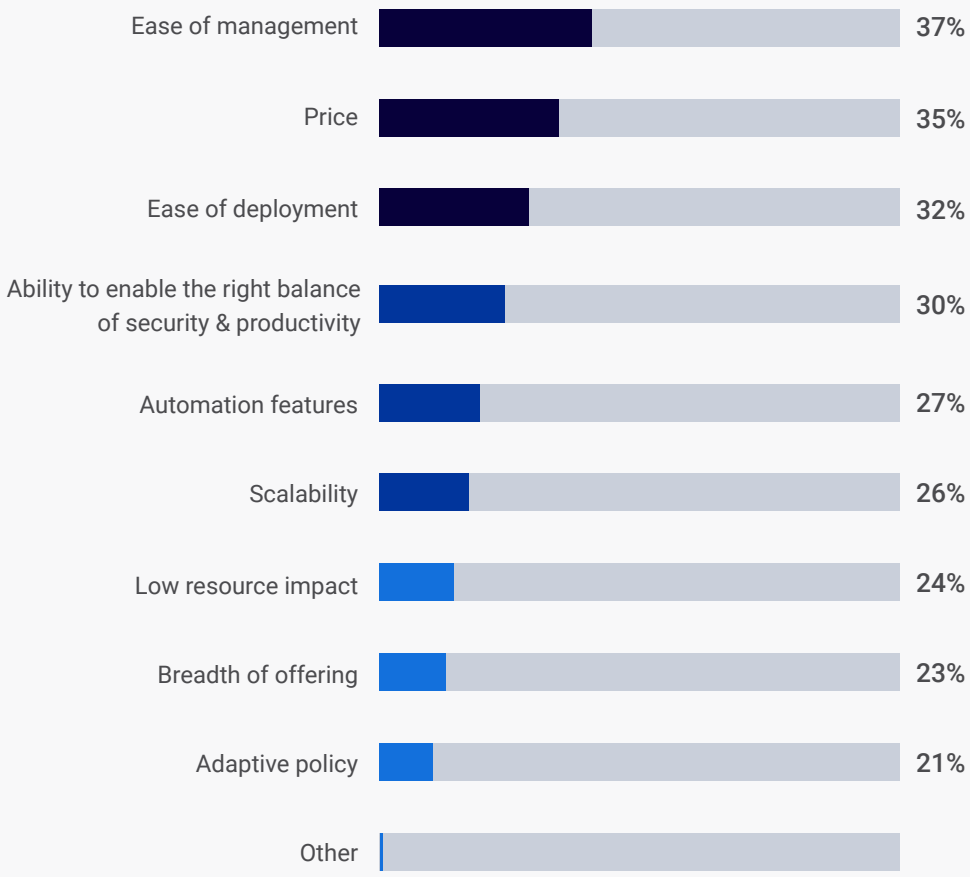
EIGHT IN TEN RESPONDENTS (82%) CONSIDER IT HIGHLY IMPORTANT THAT THEIR CURRENT OR FUTURE EDR SOLUTION CAN EXTEND BEYOND TRADITIONAL ENDPOINTS TO MOBILE DEVICES



When evaluating endpoint security tools, organizations consider ease of management, price and ease of deployment to be the most critical attributes. Eight in 10 respondents (82%) consider it highly important that their current or future EDR solution can extend beyond traditional endpoints to mobile devices. Here again, the attributes survey respondents considered the most important varied a bit by region. Canadian- and U.S.-based respondents identified ease of management to be the most critical attribute (42%) and automation features topped the list in the U.K. (34%).

Automation features, scalability, breadth of offerings and support for adaptive policies are other factors organizations consider when evaluating or procuring products for securing PCs, laptops, smartphones and other endpoints.

MOST IMPORTANT ATTRIBUTES WHEN CONSIDERING ENDPOINT SECURITY TECHNOLOGY



THE USE CASE FOR UES

Data from the BlackBerry/IDG survey clearly shows IT security professionals perceive UES technology that consolidates incident prevention, detection, response and data loss prevention (DLP) across all endpoints offers several significant benefits over current endpoint protection products.

The most anticipated benefits include better detection of both known and unknown threats, the ability to manage the endpoint environment via a single console, lower operational expenses and better integration with endpoint management tools.

Security professionals also perceive UES technology as helping them align better with enterprise Zero Trust initiatives. The Zero Trust security model emphasizes the notion of all devices and users being granted access to the enterprise network only after they have been fully authenticated and vetted for security issues each time. Among other things, the model is designed to address security issues caused by adversaries using valid credentials to access and traverse enterprise networks. Interest in Zero Trust models has increased recently with the adoption of remote and hybrid work environments at many organizations.

Nine in 10 IT leaders are familiar with UES platforms that combine the main features of an endpoint protection platform (EPP), EDR and MTD. They view such platforms as a single console with threat analysis across all endpoint devices offering the ability to detect previously undiscoverable threats through cross-data analysis.

Despite enthusiasm for the technology, relatively few organizations have implemented a UES solution. Just 11% have deployed UES currently although our data suggests many more organizations will likely implement it over the next year or so. More than one in four respondents (27%) said their organization planned to implement UES and 37% are currently evaluating the technology.

In considering UES products, IT security leaders appear to have a clearly defined set of expectations for the technology. For example, 63% wanted their UES platform to incorporate EDR capabilities as well, 59% wanted it to include an EPP capability and 50% wanted it to support mobile threat detection. The data reflects the desire for a consolidated endpoint threat detection and response capability across desktop and mobile environments that respondents expressed elsewhere in the survey.

Opinion appears divided on whether to source UES components from a single vendor or from multiple vendors. A reported 43% expressed a preference for sourcing UES components from a single vendor compared to 40% who said they preferred assembling the capability using multiple vendors. ***Those who preferred a single-vendor solution felt the approach would help better detect endpoint threats.*** Other cited benefits of a single-vendor solution included access to a single console and lower operational expenses.

At the same time, however, a majority of organizations view outsourcing as the best approach to addressing UES requirements. More than three-quarters of respondents (76%) said they were highly likely to deploy UES as a managed service.

BETTER DETECTION IS RANKED AS THE NUMBER ONE BENEFIT LIKELY TO INCREASE INTEREST IN A SINGLE UES SOLUTION

	ALL	OVERALL SCORE	SINGLE-VENDOR PREFERENCE	MULTIPLE-VENDOR PREFERENCE
Better detection (finding threats you didn't know existed)	*#1*	*1,165*	*1*	*1*
Single console	*#2*	*902*	*3*	*2*
Lower OpEx (less management)	*#3*	*895*	*2*	*3*
Alignment with Zero Trust strategy	*#4*	*805*	*5*	*4*
Integration with endpoint management tools	*#5*	*760*	*4*	*5*

*Ranks are determined by creating an overall score for each benefit ((#1 rankings x 5)+(#2 rankings x 4)+(#3 rankings x 3)+(#4 rankings x 2)+(#5 rankings 1) = Overall score)

CONCLUSION

New challenges stemming from the global pandemic have heightened requirements for a UES solution at many organizations. Organizations that have deployed endpoint protection, EDR and MTD tools want increased visibility over the PCs, laptops, smartphones and tablets being used to access their network. They want a better way to address risks tied to the shift to a remote or hybrid work environment at organizations around the world. A substantial percentage of security professionals in the U.S., Canada and the U.K. view a UES capability as critical to their ability to detect and respond to threats on traditional endpoints and increasingly on mobile devices as well.

BlackBerry Intelligent Security. Everywhere.

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 175M 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.

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