BlackBerry. Intelligent Security. Everywhere.

TODAY'S RANSOMWARE WON'T BE STOPPED BY YESTERDAY'S TECHNOLOGY

BUSINESS BRIEF

Ransomware is having a banner year in 2021. Successful attacks against Kaseya, Colonial Pipeline, JBS meat packing, and Acer made headlines, while several lesser-known attacks netted high profits for threat actors. In fact, ransomware has not achieved so many high-profile victories since the WannaCry and NotPetya attacks of 2017. Fast-forward four years, and the world is yielding to another onslaught of ransomware attacks, which begs the question: *How is this happening again?*

The simple answer is that many industries are still using the same technology and strategies that failed in 2017 and are likewise failing them now. Many organizations still use outdated antivirus (AV) approaches, perform work on unpatched systems, and hope short-staffed or overwhelmed security teams will keep them safe. Organizations often rush to react to the last ransomware attack, yet do nothing to prevent the next one. This reactive dynamic means threat groups will always achieve some measure of success, so it is unsurprising that ransomware attacks are steadily increasing YOY.

PERCENTAGE OF ORGANIZATIONS VICTIMIZED BY RANSOMWARE ATTACKS WORLDWIDE 2018-2021

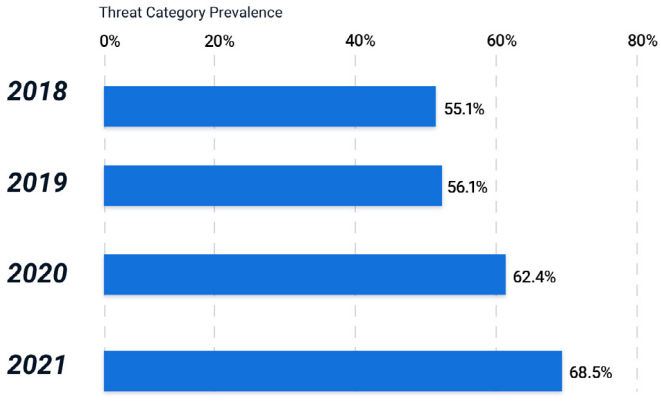

Figure 1: Ransomware attacks are affecting more organizations around the world every year.[1]

1 https://www.statista.com/statistics/204457/businesses-ransomware-attack-rate/

If organizations want to achieve effective security, they cannot respond to the ransomware attacks of 2021 the same way they did in 2017. Organizations need a forward-looking solution that stops known threats in their tracks, but also detects and prevents attacks that will be launched in the future. This may seem like an unobtainable level of cybersecurity, but it is not. BlackBerry® cybersecurity solutions, powered by Cylance® AI, prevent known, unknown, and zero-day attacks — with an average threat prediction timeframe of 25 months before they occur.

HOW BLACKBERRY ACCURATELY PREDICTS THE UNKNOWN

The predictive capabilities of artificial intelligence (AI) are a familiar force in our daily lives, although many people might not realize this. When a search engine returns a page of desired results, predictive AI is responsible. When a smartphone successfully recognizes and tags faces in a photo album, predictive AI is operating behind the scenes. How does AI know to identify and separate useful data from an astronomical pool of unwanted information?

Long-term training on massive, relevant data sets is a key factor in creating effective and mature AI math models. Mathematical models are designed to find specific features and patterns in data and return intelligently selected results. The performance, or fitness, of an AI model is determined by the accuracy of its results. After training, the AI is adjusted, the entire process repeats, and the cycle continues until the fitness of the model is maximized. This process of graduated improvement teaches AI to predict things — like who appears in a photo, which products you may want to buy a week from now, or navigating a safe path through traffic for an autonomous vehicle.

BlackBerry trains AI to predict cyber threats. The Cylance AI engine was created in 2015 and is the most mature cybersecurity AI on the market, with six years of continuous

learning under its belt. Years of training and real-world experience allow BlackBerry AI-driven solutions to stop major malware families before they are unleashed on the world. Predictive advantage measures the timeframe between the ability to stop a particular threat and the date when the attack eventually occurred (see Figure 2 for an example of the BlackBerry predictive advantage).

The Cylance AI engine has been trained on over 2.8 billion code samples and recognizes approximately 1.4 million threat features. It operates with unparalleled precision, preventing 99.1% of existing and never-before-seen malware.

THE BLACKBERRY DIFFERENCE

Many organizations react to headline-grabbing cyberattacks by modifying or adding security layers to address the specific malware currently threatening them. This approach to cybersecurity guarantees at least one organization will fall victim to an attack before others respond to the danger. Once the crisis subsides, organizations are still vulnerable to the next attack, which will claim new victims before the cycle repeats, often via a different variant of the same malware. This dynamic means threat groups enjoy a strategic advantage over their targets. They can always rely on achieving some measure of success before organizations implement effective countermeasures.

BlackBerry cybersecurity products are trained to identify and prevent threats before they execute or cause damage. This approach does not require one or more organizations to suffer successful attacks before an effective response is determined and deployed. BlackBerry threat detection models can reside directly on endpoints, securing devices regardless of their Internet connectivity status. Protected endpoints enjoy continuous security, share contextual threat information with the environment, and perform lightning-fast response actions that occur in milliseconds.

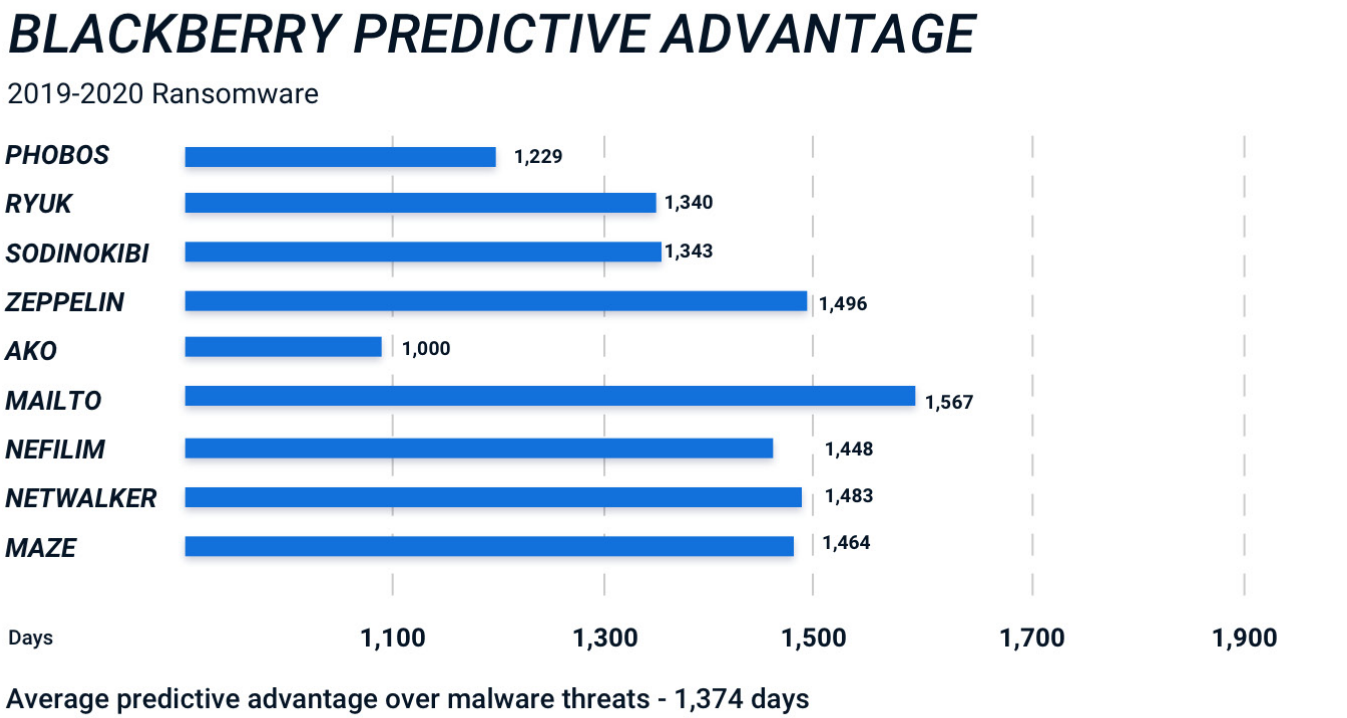

Figure 2: BlackBerry solutions, powered by Cylance AI, can stop threats years before the first attack occurs.

More importantly, BlackBerry cybersecurity offers proactive protection. It can prevent known, unknown, and zero-day threats. BlackBerry customers have been safe from recent high-profile cyberattacks for years, including those by:

- **DarkSide** - the ransomware gang behind the Colonial Pipeline attack
- **Nobelium** - the infamous threat group behind the SolarWinds attack
- **REvil** - the group behind the attacks on Kaseya, JBS meat packing, and Acer

BlackBerry solutions offer a prevention-first approach to security. The Cylance AI engine identifies fundamental features common to cyber threats and stops them before they execute.

DETECTION AND PREVENTION

Ransomware attacks have surged in 2021 and are meeting with considerable success. The criminal groups are likely to exceed the estimated $350 million USD[2] they took in ransom payments last year. The continued success of these attacks relies on organizations clinging to the reactive security policies of the past. When organizations merely respond to the current crisis, they remain vulnerable to the next one.

BlackBerry uses highly trained AI to detect and prevent ransomware attacks before they can execute. Predictive AI does not need an organization to succumb to a new variant of ransomware before it can offer protection. By understanding the core features of a malware threat, BlackBerry solutions protect organizations from known, unknown, zero-day, and future ransomware attacks.

BlackBerry® Cyber Suite and the BlackBerry portfolio of consulting services solutions help organizations minimize their risks of a ransomware breach by transitioning from a reactive to a prevention-first security posture.

2 https://abcnews.go.com/Politics/dhs-secretary-warns-ransomware-attacks-rise-targets-include/story?id=77512872

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**.*