

Windows Security

Going Back To Basics

WHITE PAPER





Initially, security was not a priority to Microsoft, due to the low number of successful public breaches when the operating system was first released.

Background

According to Statista's January 2019 Report¹, Microsoft Windows leads the global operating systems (OS) market share for desktop PCs by 75.4% while Mac OS and Linux place a distant second and third, respectively. As a matter of fact, Microsoft Windows became and stayed a dominating presence in the desktop operating system market since its debut in 1985.

Initially, security was not a priority to Microsoft, due to the low number of successful public breaches when the operating system was first released. The original versions of Windows were open and never limited users from accessing personal data. Linux and Mac, on the other hand, focused on limiting unauthorized access from their very first days.

Although Windows 3.1, 95, and 98 seemed like advanced operating systems, they were based on the disk operating system (DOS) initially released in 1981. It was a single-user design without segregation of user accounts and permissions. DOS did not offer security restrictions or adequate file permissions to protect the data and the OS from intrusions. There was no primary need for it anyway, so it took time before the company turned its consideration towards strengthening security measures.

¹ <https://www.statista.com/statistics/218089/global-market-share-of-windows-7/>

The result was Windows NT, which became Microsoft's substance for later more widespread and popular versions such as Windows 2000, XP, Vista, 7, 8, and now their latest flagship product, Windows 10. These are modern multi-user platforms that include security features to restrict unauthorized entry.

Today, Microsoft is offering a lot more security features than ever before. It is the duty of security practitioners to adapt to Microsoft's security best practices while also enhancing them with advanced security tools.

Windows 10

Windows 10 drastically improved a lot of elements in a traditional Windows Operating System. The fast evolution of malware alongside advanced attacks in recent years has made security a vital concern, not only to IT professionals, but home users as well.

According to Microsoft, Windows 10 delivers comprehensive, built-in, and ongoing security protections you can trust – including Windows Defender Antivirus, firewall, and more. These features defend against software threats like viruses, malware, and spyware across email, apps, the cloud, and the web.

There have also been some new additions to Windows 10 Security, including:

- Windows Hello
- Windows Sandbox
- Device Guard
- Credential Guard

Windows Hello

Windows Hello allows users to use a digital wristband, smartwatch, phone, and other companion devices to quickly unlock a Windows PC without a password. By certifying a user's identity, these devices provide another choice for quick, secured sign-ins.

Passwords are asymmetric keys, which means a server keeps of a copy of the password. Windows Hello PIN is not. Windows Hello protects a user's key in the TPM (Trusted Platform Module). Even if the keys/passwords server gets hacked, the user's PIN and access are unaffected.

Windows Hello PIN is tied locally to the device, is backed by hardware, can be complex, and uses biometrics for an additional security factor and recovery solution.

Windows Sandbox

Windows Sandbox offers an isolated, temporary, desktop environment where you can run untrusted software without the fear of harming the user's PC. Any software installed in Windows Sandbox stays only in the sandbox and cannot affect the host. Once Windows Sandbox is closed, all the software, files, and states are permanently deleted.

Windows Sandbox creates a secure Windows 10 instance within a running Windows 10 virtual machine environment. It uses hardware-based virtualization for kernel isolation, which relies on Microsoft's hypervisor to run a separate kernel for Windows Sandbox. The sandbox also uses the integrated kernel scheduler, smart memory management, and virtual GPU.

Users can copy and paste executables and files into the sandbox and run them to observe their behavior. They can also browse to unknown websites to test their maliciousness within a closed and safe environment.


Device Guard

Device Guard relies on hardware and software, including Windows 10's virtualization-based security, to lock down the machine so it only runs trusted applications. Applications must have a valid cryptographic signature from specific software vendors, or Microsoft, to execute.

Device Guard isolates Windows services that verify whether drivers and kernel-level code are legitimate in a virtual container. Even if malware infects the machine, it cannot access that container to bypass the checks and execute a malicious payload. Device Guard goes beyond the older AppLocker feature, which could be accessed by attackers with administrative privileges. Only an updated policy signed by a trusted entity can change the app control policy that has been set on the device.

This feature eliminates the risk of being infected by unsophisticated malware. Having said that, Device Guard does not protect against Just-In-Time (JIT) compiled applications, or code running in documents, such as macros in Microsoft Office tools.

It is the duty of security practitioners to adapt to Microsoft's security best practices while also enhancing them with advanced security tools.



While Windows 10 is a significant improvement from a security standpoint, the new exciting features come with a lot of challenges.

Credential Guard

Credential Guard protects corporate identities by isolating them in a hardware-based virtual environment. Microsoft isolates critical Windows services in the virtual machine to block attackers from tampering with the kernel and other sensitive processes. The new features rely on the same hypervisor technology already used by Hyper-V.

Credential Guard addresses an essential aspect of enterprise security. It stores domain credentials within a virtual container, away from the kernel and user mode operating system. This way, even if a machine is compromised, the credentials are not available to the attacker.

Advanced persistent attacks rely on the ability to steal domain and user credentials to move around the network and access other computers. Typically, when users log in to a computer, their hashed credentials are stored in the operating system's memory. Previous versions of Windows stored credentials in the Local Security Authority, and the operating system accessed the information using remote procedure calls. Malware or attackers lurking on the network were able to steal these hashed credentials and use them in the prevalent pass-the-hash attacks that were originally published by Paul Ashton in 1997.

A typical example is Mimikatz, which is a widely used tool that enables the viewing of credential information from the Windows Lsass (Local Security Authority Subsystem Service). Using its sekurlsa module, which includes plaintext passwords and Kerberos tickets, allows threat actors to execute pass-the-hash and pass-the-ticket attacks. Before Credential Guard, an attacker could leverage easy-to-use tools to dump all passwords from memory.

Windows 10 – Security Challenges

While Windows 10 is a significant improvement from a security standpoint, the new exciting features come with a lot of challenges. For example, Device Guard and Credential Guard are intended for business systems and are available only in Windows 10 Enterprise and Windows 10 Education. The hardware needed to add all the new security features is substantial, hard to implement, and requires significant infrastructure changes. The built-in Windows Defender is undoubtedly an improvement to Windows 10. However, it remains a signature-based antivirus that suffers from the ills common to that approach - friction for security content updates, possible content corruption, and dependence on network/cloud lookups and communications.

User Account Control

While this Windows security feature has been around since Windows Vista, it has not yet been fully adopted. A lot of enterprises and government entities allow regular users to have local administrative rights.

For many years, organizations have been giving normal users administrative privileges for several reasons, including:

- Legacy software requiring administrative rights to run.
- Software installation and updates, especially on laptops or portable devices.
- IT personnel, especially developers, to increase their overall productivity and development experience.
- Lack of information security culture. Some organizations are not fully aware of the challenges around information security in general, and users' access in particular.

Why Giving Normal Users Administrative Access Is Dangerous

While giving a user access to install a new printer might not seem that risky, the same access rights allow malicious execution to happen and also spread across an entire network.

Adversaries have been focusing in the last few years on users more than systems and servers. Systems and servers, for the most part, are usually well maintained, patched, and protected by several firewalls and intrusion detection systems. They are also highly and frequently audited by IT and Security teams. Users, on the other hand, can perform very inconsistently and make much better targets for attackers.

Malware Spread

People are the weakest link in information security. Many online users are easily deceived into visiting legitimate-looking fake sites or opening unknown emails, making them vulnerable to threat actors. Adversaries find it easy to steal unsuspecting user's credentials and access their systems with their designated privileges.

According to Verizon's 2018 Data Breach Investigations Report (DBIR)², 92.4% of malware is delivered by email as users continue to be deceived by phishing attempts, social engineering, and malicious attachments made to look legitimate.

Lateral Movement

Lateral movement is a technique used by adversaries to move through a network in search of data or assets to exfiltrate.

Adversaries use different tools and methods to get higher privileges and access, allowing them to move laterally across the network. If the attacker secures administrative privileges, lateral movement can be challenging to detect, as it may appear like legitimate network traffic to security analysts.

Insider Threats

A Crowd Research Partners survey shows that careless users are the most significant insider threat concern for organizations³. And they should be, considering that many high-profile breaches happen as a result of inadequate access management practices and unintentionally exposed administrative credentials.

People are the weakest link in information security. Many online users are easily deceived into visiting legitimate-looking fake sites or opening unknown emails, making them vulnerable to threat actors.

² https://enterprise.verizon.com/resources/reports/DBIR_2018_Report.pdf

³ <http://crowdresearchpartners.com/wp-content/uploads/2017/07/Insider-Threat-Report-2018.pdf>

Access To Sensitive Information

Recommendations and Best Practices

- Choose a strong password and enforce a strong password security policy in enterprise environments.
- Require passwords to be frequently changed.
- Enable multi-factor authentication.
- Enable logging and auditing.
- Disable local administrator accounts.
- Enforce an account lockout policy to prevent unlimited attempts to access a machine. The threshold for locking out accounts does not need to be overly restrictive to be effective. For example, a limit of three incorrect attempts, with a reset period of 10 minutes for the lockout counter will prevent any brute force attempt but allow a legitimate user to enter their password incorrectly a few times.
- Adapt to the principle of least privilege access, removing administrative rights and allowing them purely on demand.
- Enable disk encryption to protect against data loss following physical theft.
- Enable Windows Hello for Business and allow the user to log in with a PIN code that can be the same as the one used to authenticate to BitLocker.
- When possible (Windows 10), enable secure boot. A UEFI password can make it more difficult for an attacker to modify the boot process.
- Configure Windows Update to automatically download and install updates as soon as possible.
- Disable PowerShell everywhere possible. Blocking PowerShell across endpoints eliminates the risk of a whole class of cyber attacks.
- Disable Command Prompt access or the ability to execute batch files and scripts.
- Applications that have any built-in security functionality should be enabled and appropriately configured along with unrequired functionality disabled. For example, Microsoft Office by default should be used to block untrusted macros in Office documents from automatically executing without user interaction.
- Limit credential caching to one login and don't allow storage of passwords and credentials for network authentication.
- Enable Early Launch Anti-Malware (ELAM) to be used in conjunction with Secure Boot. An ELAM driver can be registered as the first non-Microsoft driver that will be initialized on a workstation as part of the boot process, thus allowing it to verify all subsequent drivers before they are initialized. Only known good drivers should be allowed to be initialized during the boot process.
- Uninstall unneeded built-in Microsoft applications and always use the latest possible version of web browsers.
- Use a 64-bit architecture whenever possible as it has additional security functionality that the x86 (32-bit) versions lack.
- Centrally manage and deploy patches and driver updates and ensure they are installed in an appropriate timeframe (as determined by the severity of the security vulnerability and any mitigating measures already in place). This can be achieved using Microsoft System Center Configuration Manager (SCCM) and Windows Server Update Services (WSUS).
- Antivirus software should be installed. It is actually recommended to use more than an antivirus as they may only cover attacks that have been previously defined. Adapt to the new era of endpoint security by introducing an artificial-intelligence-based approach and leverage cloud-based services when beneficial.
- Disable Autoplay and AutoRun functionality and restrict USB devices to trusted ones.
- Disable Remote Desktop Services. If necessary, configure Remote Desktop Services as secure as possible and only for the machines and users with the specific need.
- Disable Safe Mode as *Safe Mode with Networking* or *Safe Mode with Command Prompt*. These options may allow attackers to bypass system protections.
- Enable session locking. An adversary with physical access to an unattended workstation may attempt to inappropriately access other users' sessions to misuse their credentials. They may seek to obtain sensitive information or ruin someone's reputation by engaging in malicious or suspicious communications.
- Configure and enforce a secure Windows Remote Management and Disallow WinRM from storing RunAs credentials.
- Disable Remote Shell Access as it can allow an adversary to remotely execute scripts and commands.

How Can BlackBerry Cylance Help?

Today’s advanced cyber threats target every computer, mobile device, and enterprise endpoints, especially those related to critical infrastructure like industrial control systems (ICS). The modern computing landscape consists of a complex array of physical, mobile, cloud, and virtual computing, creating a vast attack surface. Meanwhile, the cybersecurity industry is prolific with defense-in-depth security technologies, despite a threat landscape that remains highly dynamic, sophisticated, and automated.

BlackBerry Cylance takes a different, innovative approach of using real-time, machine learning threat analysis to solve this problem for organizations, governments, and end-users worldwide — demonstrating its leadership as a global cybersecurity solutions provider.

BlackBerry Cylance uses artificial intelligence (AI) to deliver prevention-first, predictive security solutions that change how organizations, governments, and end-users approach endpoint security. BlackBerry Cylance’s security solutions combine AI-driven predictive prevention with dynamic threat detection and response to deliver full spectrum threat prevention and threat visibility across the enterprise.

Pre-Execution Prevention

BlackBerry Cylance’s next-generation antivirus product, CylancePROTECT®, delivers industry-leading malware prevention powered by AI, combined with application and script control, memory protection, and device policy enforcement to prevent successful cyber attacks.

Without the use of signatures or the need to stream data to the cloud, CylancePROTECT combats common threats such as malware, ransomware, fileless malware, malicious scripts, weaponized docs, and many other attack vectors, no matter where the endpoint resides. With unmatched effectiveness, ease of use, and minimal system impact, CylancePROTECT is the best way to prevent both known and unknown attacks before they can execute.

Malware Execution Control



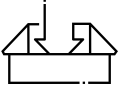
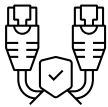
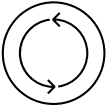

Malware Execution Control is the core protection technology of CylancePROTECT. This technology leverages AI and machine learning to detect and prevent malware on Windows, Mac, and Linux environments before it executes. This revolutionary approach provides effectiveness far beyond traditional signature-based approaches. The CylancePROTECT agent architecture consists of a lightweight agent installed on the host and managed by a BlackBerry® Cylance® console.

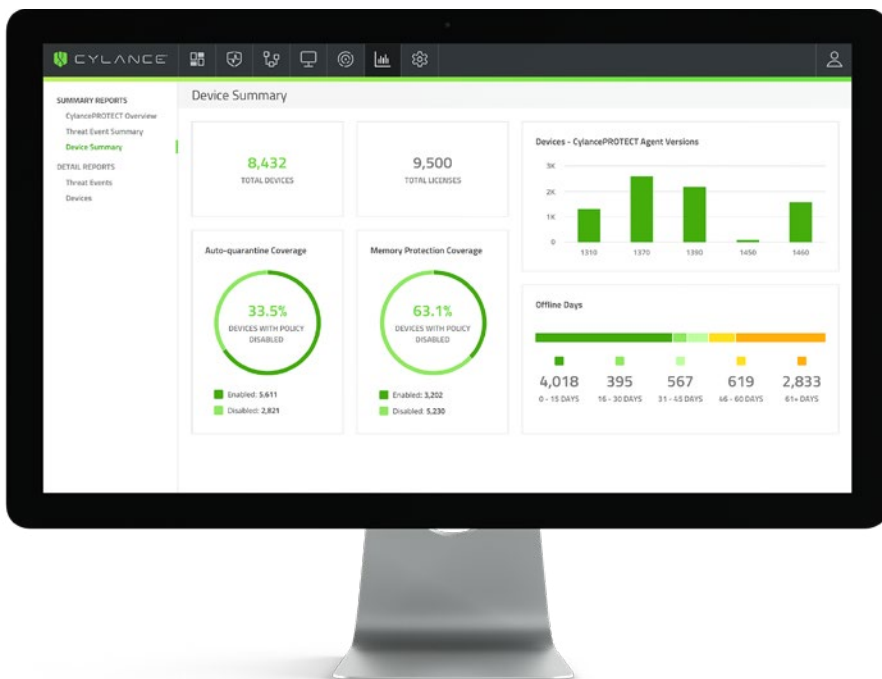
One of the key capabilities of CylancePROTECT is malware execution control, which will detect and prevent malware using tested mathematical models on the host, independent of cloud connectivity, signatures, trust-based systems, or behavioral analysis. It is capable of detecting and quarantining malware in both open and isolated networks without the need for continual updates, rendering malware, ransomware, fileless attacks, bots, and future variants useless.

Script Control

CylancePROTECT offers integrated script control to assist its superior AI-based malware execution prevention technologies, giving administrative control over when, where, and how scripts are used in an environment. This ultimately reduces the attack surface on which a threat actor may distribute malware.

CylancePROTECT Script Control protects users from malicious scripts running on their devices by injecting itself into a script interpreter (responsible for the execution of scripts) to monitor and safeguard against scripts running in an environment. The agent is then able to detect the script and script path before the script is executed. Depending on the policy set for script control (alert or block), the agent will allow or block the execution of the script.

Past	Present				Future
					
AV	HIPS / Anti-Exploitation	Sandboxing	Isolation	EDR	AI
Humans Needed	Specialized Humans Needed Post-Execution: REACTIVE				No Humans Pre-Execution: PREDICTIVE



CylancePROTECT detects and prevents file exploitations from delivering their malicious payloads in both the operating system (OS) and memory layers.

Memory Defense

CylancePROTECT detects and prevents file exploitations from delivering their malicious payloads in both the operating system and memory layers.

CylancePROTECT memory protection abilities are similar to those found in modern host intrusion prevention systems, but without the configuration complexity. Memory protection adds an additional layer of security and strengthens the OS's basic protection features, such as data execution prevention, address space layout randomization, and enhanced mitigation experience toolkit.

In many breach events, a benign process is initially exploited by malicious payload code. The most common incidents involve a user browsing to a malicious website or a user executing malicious macros in documents. When this occurs, the attacker's payload code executes in the memory of the browser or application without attempting to create or execute a new malicious executable. When deployed on servers, CylancePROTECT's memory protection capabilities prevent the exploitation of many of the most common classes of vulnerabilities, such as exploits for buffer overflows and use-after-free.

CylancePROTECT's memory protection module is comprised of an agent dynamic-link library loaded into each protected process, and a service component to supply configurations, receive information, and respond to events. The agent hooks various user-mode application program interface (API) functions to maintain a secure state and watch for specific hard-coded behaviors indicative of a compromise. Whenever such a behavior is detected, an event is communicated to the service before the hooked API function is allowed to complete.

CylancePROTECT Memory Exploit Prevention Stops:

- Memory misuse
- Exploitation
- Process injection
- Privilege escalation
- Payload termination

Device Control

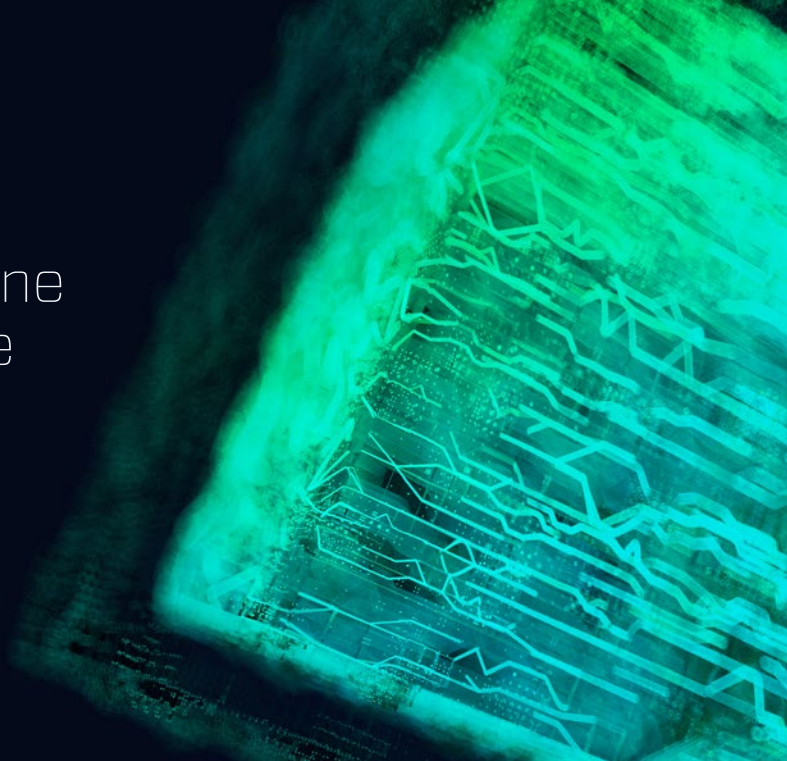
Device Control is available as part of CylancePROTECT and provides administrators the ability to control the usage of USB mass storage devices in their environment. Administrators can enable Device Control per the existing Device Policy and can choose to allow or block access to USB mass storage devices.

Device Control policy will only apply to those USB devices classified as mass storage. USB peripherals are not affected. For example, if an administrator creates a policy to block USB mass storage devices, an end-user can still use a USB mouse, but not a USB thumb drive.

As part of Device Control policy, administrators also can define exceptions to the policy. This is done by using the Vendor ID, Product ID, and Serial Number to specify the exception.

Application Control for Fixed-Function Devices

CylancePROTECT Application Control gives organizations the ability to ensure fixed-function devices are in a pristine state continuously, eliminating the drift that may occur over time when devices are left unmanaged.



Securing an organization's endpoints and servers from compromise is the number one priority of BlackBerry Cylance security solutions.

Augmenting the AI-driven malware prevention capabilities of CylancePROTECT, Application Control is the easiest way to ensure fixed-function devices:

- Remain compromise free continuously
- Are available for their specific function 24x7
- Are no longer susceptible to disruptions from a successful attack

Unauthorized applications on fixed-function devices, such as an ATM or kiosk, significantly increase the risk of a breach or compromise. To combat the risk associated with an attacker gaining access to these devices and installing a malicious app, organizations need an easy way to ensure the device is only used for its intended purpose.

The Application Control capability included with CylancePROTECT provides a streamlined approach to application usage enforcement and policy management.

Management Console Reporting

Securing an organization's endpoints and servers from compromise is the number one priority of BlackBerry Cylance security solutions. Using patented AI and purpose-built security features, BlackBerry Cylance products deliver continuous prevention, ensuring sensitive data remains secure.

With BlackBerry Cylance's management console reporting capabilities, users can easily get real-time interactive statistics, increasing their situational awareness and gaining insight into their potential attack surface.

Post-Execution Protection

Augmenting CylancePROTECT prevention, CylanceOPTICS™ is an endpoint detection and response (EDR) component that enables easy root cause analysis, threat hunting, and automated threat detection and response. Unlike other EDR products that require organizations to make a significant investment in on-premises infrastructure and/or stream data to the cloud continuously, and employ highly-skilled security resources, CylanceOPTICS is designed to automate the threat detection and response tasks using existing resources.

With CylanceOPTICS, security analysts can dissect any CylancePROTECT-prevented attack to determine the root cause to improve their overall security framework. CylanceOPTICS also provides enterprise-wide threat hunting capabilities powered by InstaQuery (IQ), enabling on-demand threat hunting with instant access to the results. Analysts can then quickly determine if an endpoint is at risk, minimizing dwell time and reducing the attack surface. Further, analysts can use the automated threat detection and response capabilities to create custom rules, or use the rules provided by BlackBerry Cylance, to automatically detect suspicious behaviors and take specific response actions without human intervention. Finally, CylanceOPTICS delivers AI-driven incident prevention, a force multiplier for any security team. Powered by machine learning threat detection modules developed to run on the endpoint, CylanceOPTICS continuously analyzes changes occurring on each endpoint. This analysis can uncover threats that would be difficult, if not impossible, for a human analyst to uncover in a reasonable amount of time. When a potential threat

is identified, CylanceOPTICS can take decisive actions, in real time, to stop the attack and avoid the cost, risk, and long-term impacts that come with a widespread security incident.

Perform Targeted Threat Hunting

Some malicious activities are easy to identify, while others are anything but cut and dry. When a computer begins to behave irregularly, or it is determined that an endpoint may be at risk of compromise, it is critical that an organization's security toolkit gives it the visibility required to make definitive judgments. BlackBerry Cylance provides immediate access to the forensically-relevant data stored on any endpoint. Within moments of a suspicious activity being identified, searches can be targeted to the exact threat being investigated.

Use Indicators of Compromise To Find Threats

Threat hunting can be described as the act of forming a hypothesis and then running a series of searches/investigations, using indicators of compromise or other terms, to either prove or disprove that hypothesis. Having access to the right data is at the essential core of performing this skill effectively. Targeted threat hunting with refined results is capable with BlackBerry Cylance, delivering access to both current and historical endpoint data. Unlike other tools that store every piece of data from an endpoint, BlackBerry Cylance stores only the forensically-relevant data, meaning security teams won't have to spend time sifting through mountains of irrelevant information to find threats.

Dynamic Threat Detection

There are several ways to identify potential threats and compromises. First, security analysts can perform searches across endpoints to identify suspicious artifacts, and through manual investigation, determine that a threat exists. While there is tremendous value in this process, it simply does not scale across an enterprise. To root out threats hidden on endpoints, an automated approach to threat detection must be used. BlackBerry Cylance includes a rule-based engine deployed on every endpoint, called the Context Analysis Engine (CAE), to identify potential threats automatically. The CAE is a high-performance analysis and correlation engine that monitors events as they occur on an endpoint in near real time to identify malicious or suspicious activities. This 24x7 monitoring occurs with no need for a cloud connection. The CAE includes a set of curated rules provided by BlackBerry Cylance as well as the ability to create customized rules.

While detection rule engines are necessary, it is difficult to model all potential attack behaviors. To that end, BlackBerry Cylance includes AI-based incident prevention.

Powered by machine learning threat detection modules for the endpoint, CylanceOPTICS continuously analyzes changes occurring on each endpoint to uncover threats that would be difficult, if not impossible, for a human analyst to uncover in a reasonable amount of time.

When a potential threat is identified, CylanceOPTICS can take decisive actions, in real time, to stop the attack and avoid the cost, risk, and long-term impacts that come with a widespread security incident. The combination of these threat detection capabilities provides broad protection against attacks.

MITRE ATT&CK Framework Rules Packages

The BlackBerry Cylance CAE, the driving force behind threat detection and response, comes with a pre-configured set of rules mapped to the MITRE ATT&CK Framework, improving threat detection capabilities.

Endpoint Only Response Actions

Even with security controls in place, no business can guarantee that every single attack can be stopped. This means organizations must be prepared to respond when an attack is detected. With BlackBerry Cylance, enterprises get fully-integrated automated incident response capabilities. If an attack is detected, a response can be initiated automatically, with no human intervention and with no cloud connection required. All detection and response mechanisms are self-contained on the endpoint and therefore can act immediately.

If further responses are required, the item in question can be quarantined and the endpoint can be locked down, disabling its ability to communicate with any other endpoints. Forensic data from the impacted endpoint can be collected to gain further context about the incident. Identifying a security concern is important, but having the ability to respond automatically is a necessity. With BlackBerry Cylance, organizations have that ability. True endpoint security does not come from prevention or detection. To combat today's attacks, organizations must have strong prevention and detection capabilities in place to keep pace with attackers. With BlackBerry Cylance, enterprises get the best of both worlds in one solution, maximizing the return on security stack investments, making analysts more efficient, and making the business more secure.

Playbook-Driven Response

Initiate a set of discrete response tasks automatically if the rule is triggered. Playbook-driven response capabilities assist organizations in eliminating dwell time by ensuring threat responses are fast and consistent across the environment regardless of the skill-level of on-duty security personnel.

Behavioral and Biometrics Analytics

CylancePERSONA™ is an AI-driven behavior and biometric analysis solution designed to identify suspicious users in real time to prevent compromises.

Augmenting the AI-driven threat and incident prevention capabilities of CylancePROTECT and CylanceOPTICS, CylancePERSONA adds the user dimension to the attack surface protection provided by BlackBerry Cylance.

With CylancePERSONA, enterprises can:

- Reduce attacks executed by users with legitimate credentials
- Ensure the user is legitimate – stop stolen credentials – the basis of 80% of data breaches
- Proactively block identified users without taxing the security personnel for action

Managed Detection and Response

CylanceGUARD™ is a 24x7 managed detection and response offering that provides actionable intelligence for customers to prevent threats quickly while minimizing alert fatigue without requiring additional resources. Using the same expertise and methods as the BlackBerry Cylance incident response team, analysts from BlackBerry Cylance or a strategic partner, hunt through customer environments to find and contain threats, prevent significant breaches, and allow organizations to mature their security program.

CylanceGUARD leverages the BlackBerry Cylance AI Platform™ with the pre-execution abilities of CylancePROTECT and the post-execution of monitoring and blocking associated with CylanceOPTICS.

Consulting Services

BlackBerry Cylance also provides world-class cybersecurity consulting services. BlackBerry Cylance's consultants help clients address cybersecurity concerns and challenges of all types, working with clients to construct a reliable and effective security posture while utilizing prevention-first methodologies.

BlackBerry Cylance's industry-leading experts provide the technical expertise needed to effectively analyze cybersecurity requirements and to design comprehensive solutions to meet client goals and objectives. The number-one priority of BlackBerry Cylance's consulting services is to secure clients as quickly as possible using advances in automation, including artificial intelligence and machine learning.

Next Steps

While Microsoft has made great strides in securing Windows over the years, there are still many gaps in security, the most prominent of which is the human factor, that must be addressed by organizations in order to prevent damaging and costly breaches. Loss of reputation, loss of user and customer trust, as well as steep fines for non-compliance with security regulations can greatly impact the organizations that do not enhance the security features provided by Windows in order to address threats such as zero-day malware, fileless attacks, and phishing. While people can be an organization's greatest asset, they also can be its greatest threat when it comes to cyber attacks.

To learn more about how your organization can benefit from BlackBerry Cylance's AI-based security products and its team of security experts, visit www.cylance.com or contact us today.

About BlackBerry Cylance

BlackBerry Cylance develops artificial intelligence to deliver prevention-first, predictive security products and smart, simple, secure solutions that change how organizations approach endpoint security. BlackBerry Cylance provides full-spectrum predictive threat prevention and visibility across the enterprise to combat the most notorious and advanced cybersecurity attacks, fortifying endpoints to promote security hygiene in the security operations center, throughout global networks, and even on employees' home networks. With AI-based malware prevention, threat hunting, automated detection and response, and expert security services, BlackBerry Cylance protects the endpoint without increasing staff workload or costs.



+1-844-CYLANCE
sales@cylance.com
www.cylance.com

