# CylancePROTECT® +AppControl

## A Better AppControl Solution

CylancePROTECT+AppControl permits only good applications to be whitelisted. It reduces management overhead and has far less impact on productivity than traditional application control solutions. CylancePROTECT+AppContol's predictive model is the perfect solution for providing an exceedingly high degree of security for fixed-function devices such as data center servers, point of sale systems, industrial control systems, ATMs, and kiosks.

CylancePROTECT+AppControl is the industry's first application control product to use a predictive mathematical model to only permit good applications to be whitelisted during installation or update. But unlike simple whitelisting solutions, CylancePROTECT+AppControl enables administators to achieve a high degree of security WITHOUT the hassle of continuous management overhead, productivity impact on users, and the mistakes that can be made when pressed to quickly make decisions about the safety of applications.

## What is AppControl?

Legacy antivirus products use a blacklisting approach that allows all applications to run unless they are known to be malicious or exhibit known bad behaviors. Application control reverses this paradigm, only allowing execution of code that is on a whitelist of known good applications. Application control is widely acknowledged as a highly effective way to protect low-change environments.[1]

Despite having a more secure model, many whitelisting solutions have not achieved widespread adoption because they require strict change control policies around applications. This causes friction with users due to a negative impact on productivity. Application control solutions support numerous 'trusted sources of change' in a bid to reduce the pain of installing/upgrading newer applications.

Unfortunately, this whitelisting model puts stress on administrators. Admins are not malware analysts, so burdening them with making decisions about what applications should run can greatly increase their workload. With a default closed policy, work can be blocked until an admin makes a decision on a suspect application, slowing efficiency. Administrators are prone to make mistakes when under time pressure.

## CylancePROTECT

CylancePROTECT uses a predictive mathematical model to identify malware, instead of relying on signatures to determine if an application is malicious. Unlike most traditional malware prevention tools, such as antivirus software, CylancePROTECT can detect malicious programs even when they have never been seen before or belong to a whole new family of malware. Granular policies to quarantine unsafe applications before they run can be configured in the CylancePROTECT console.

CylancePROTECT supports a workflow very similar to that of legacy antivirus products, but provides the ability to classify even previously unknown or unseen samples, improving security without the cumbersome operational overhead of application control solutions.

[1]Gartner G00270462 – "*Market Guide for Application Control Solutions*," 10/13/2014 by Peter Firstbrook

## About Cylance

Cylance® is the first company to apply artificial intelligence, algorithmic science and machine learning to cybersecurity and improve the way companies, governments and end-users proactively solve the world's most difficult security problems. Using a breakthrough predictive analysis process, Cylance quickly and accurately identifies what is safe and what is a threat, not just what is in a blacklist or whitelist.

By coupling sophisticated machine learning and artificial intelligence with a unique understanding of an attacker's mentality, Cylance provides the technology and services to be truly predictive and preventive against advanced threats.

## CylancePROTECT+AppControl

Because of its predictive model, CylancePROTECT is the best solution for dynamic environments where users are frequently installing/updating applications. But, what about a solution for fixed-function devices with a low change factor such as data center servers, point of sale systems, industrial control systems, ATMs, and kiosks? For those environments, the best solution is CylancePROTECT+AppControl.

With CylancePROTECT+AppControl, administrators of these fixed-function devices can achieve an exceedingly high degree of security based on a default-deny policy, without the hassle of continuous management overhead. Once a device is placed in application-control mode, all changes are preempted and logged in an audit trail. This ensures the integrity of the system.

CylancePROTECT registers with the Microsoft Windows® OS as an anti-malware/anti-spyware solution and is compliant with all the requirements of PCI-DSS Section 5. Also, the agent footprint is the same for both CylancePROTECT and AppControl, eliminating the need to have both antivirus and application control on resource-constrained systems.

With CylancePROTECT, customers can manage devices such as industrial control systems, which can never have a duplex connection back to a central console. Administrators can export signed policies from the console, which can be distributed to systems without a central console connection. To prevent exploitation of vulnerabilities in applications, CylancePROTECT+AppControl policies are always configured to use built-in anti-exploit technology to terminate exploit attempts.

## Key Benefits

**SINGLE AGENT/SINGLE CONSOLE**

CylancePROTECT enables admins to manage dynamic endpoints (laptops, desktops) and fixed-function devices (point of sale systems, ICS, ATMs) from the same console with different policy options. Since both approaches leverage the same underlying technology, it's easy to reap the benefits on all of your devices.

**CERTIFIED ANTIVIRUS**

Cylance® is a member of the Microsoft Virus Initiative and CylancePROTECT registers with the Microsoft Windows® operating system as an anti-malware solution.

**PCI-DSS SECTION 5 COMPLIANT**

Legacy application control systems require a separate product or component to maintain PCI compliance. CylancePROTECT+AppControl can be used to lock down fixed-function devices and comply with PCI-DSS Section 5.

**FULL SUPPORT FOR AIR-GAPPED NETWORKS**

CylancePROTECT supports disconnected/air-gapped networks and is the best solution for sensitive systems like ICS, which cannot be directly connected to outside networks such as the Internet.

+1-844-CYLANCE
sales@cylance.com
www.cylance.com
18201 Von Karman Avenue, Suite 700, Irvine, CA 92612