Application Whitelisting:

A Better and Easier Way

CYLANCE™

Introduction

The Australian Signals Directorate has identified application whitelisting as the most effective strategy in its Strategies to Mitigate Targeted Cyber Intrusions. The intelligence agency, which operates as part of the Australian government, has reported that application whitelisting and the right combination of patches and administrative privilege restrictions can prevent at least 85% of targeted cyber intrusions.

BENEFITS OF APPLICATION WHITELISTING

Application whitelisting protects unauthorized or malicious code from executing; ensuring that only authorized applications will run. This proven cybersecurity approach can also prevent the installation or use of unauthorized applications by users.

In addition, an application whitelisting solution can help identify unauthorized attempts to execute malicious code on a system by a threat actor. By configuring an application whitelisting solution to generate failed execution event logs that cite the name of the blocked file, the date-time stamp, and the user name, system administrators can easily identify patterns that clearly indicate unauthorized use.

APPLICATION WHITELISTING + ANTIVIRUS SOFTWARE

While application whitelisting is definitely a strong weapon in the cybersecurity arsenal, it should be deployed in conjunction with the latest in antivirus and anti-malware technology.

Unfortunately, though, most traditional antivirus products use a blacklisting approach that allows all applications to run unless they are known to be malicious or exhibit known bad behaviors. This approach leaves Australian organizations vulnerable and out of compliance with identified best practices.

Application control can reverse this blacklisting paradigm, however, only allowing execution of code that is on a whitelist of known good applications. Sadly, 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.

Plus, 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-deny policy, work can be blocked until an admin makes a decision on a suspect application, slowing efficiency. To make matters worse, administrators are prone to make mistakes when under time pressure.

A SINGLE SOLUTION TO MANY CHALLENGES

Cylance® has solved these business challenges by developing CylancePROTECT®+AppControl, 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 traditional whitelisting solutions, CylancePROTECT+AppControl enables administrators 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.

CylancePROTECT+AppControl 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+AppControl can detect malicious programs even when they have never been seen before or belong to a whole new family of malware. Administrators can configure granular policies to quarantine or alert unsafe applications before they run.

Cylance's products support a workflow very similar to that of traditional antivirus, but provide the ability to classify even previously unknown or unseen samples, improving security without the cumbersome operational overhead of application control solutions.

ONE PRODUCT FOR DYNAMIC AND FIXED FUNCTION ENVIRONMENTS

CylancePROTECT+AppControl's predictive model is the best solution for dynamic environments where users are frequently installing and updating applications. But, administrators of fixed function devices with a low change factor such as data center servers, point of sale systems, industrial control systems, ATM's and kiosks also 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.

COMPLIANCE, CONSOLIDATION AND NO CONNECTION REQUIREMENT

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, CylancePROTECT+AppControl can eliminate the need to have both antivirus and application control on resource-constrained systems. CylancePROTECT+AppControl can exceed the capabilities of both your existing solutions in one product.

With CylancePROTECT+AppControl, 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.

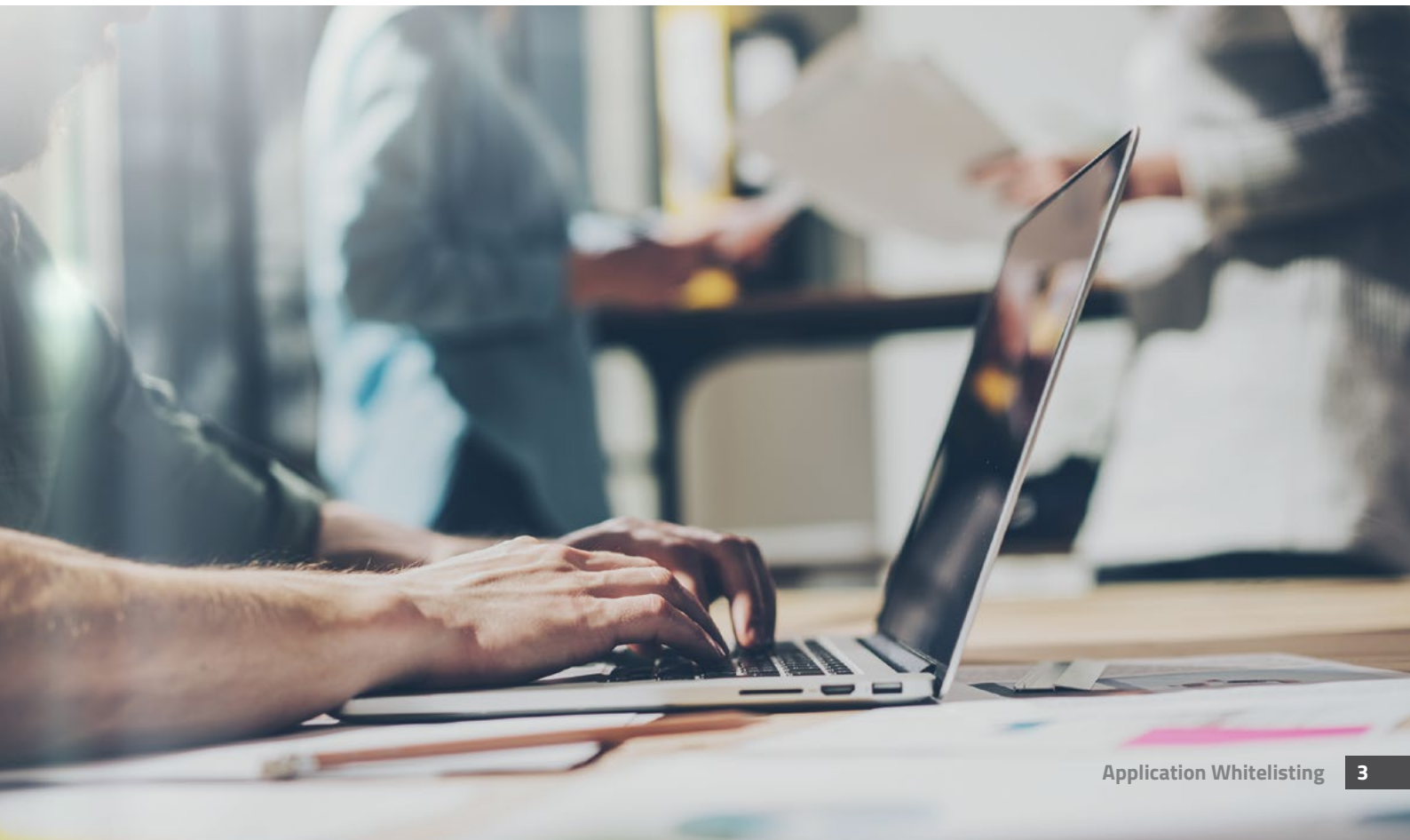
KEY BENEFITS

Single Agent/Single Console: CylancePROTECT+AppControl 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: Traditional 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.



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 a hacker's mentality, Cylance provides the technology and services to be truly predictive and preventive against advanced threats. For more information, visit cylance.com

+1 (877) 973-3336
apac@cylance.com
www.cylance.com
18201 Von Karman, Ste. 700, Irvine, CA 92612