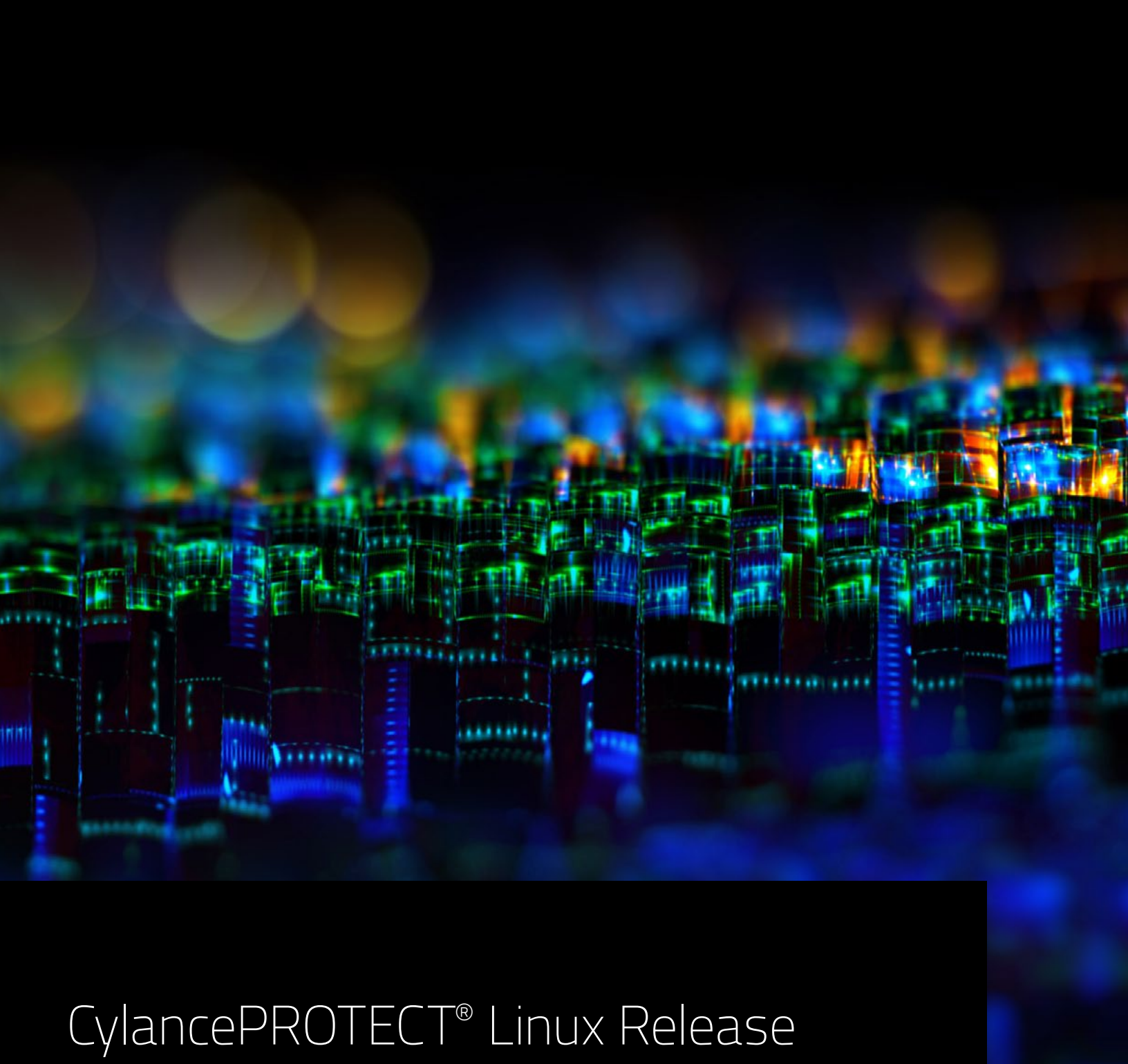


CylancePROTECT® Linux Release

Solution Brief

CYLANCE™



Executive Summary

Cylance® is revolutionizing cybersecurity with products and services that proactively prevent execution of advanced persistent threats and malware at the most vulnerable point: the endpoint. Cylance's award-winning product, CylancePROTECT, stops what others don't, without requiring a cloud connection or frequent updates, all while using a fraction of the system resources associated with antivirus and endpoint security software. CylancePROTECT is a radically different technological approach to cybersecurity that employs artificial intelligence to analyze the DNA of files before they execute. With the 1430 agent release, Cylance extends the reach of CylancePROTECT to the Linux server environment.

Use Cases for CylancePROTECT Linux

With this entry into the Linux computing environment, Cylance has extended the reach of artificial intelligence based anti-malware technology to cover a broader set of threats in both data centers and industrial environments. Examples of this extended footprint include servers, point of sale (POS)/ automated teller machine (ATM) terminals and Linux-based fixed-function devices. Use cases for each of these are described below.

Use Case: Linux Servers

In enterprise data centers utilizing X86-based servers, Linux is a widely-utilized operating system for both bare-metal machines and virtual machines within hypervisors. This growth is being further accelerated by the movement within data centers to containers. While endpoints are often the initial target of malware attacks, the primary target is the data on the servers, whether in financial services, e-commerce, or other enterprise applications. There is a mindset within the IT community that if the operating system isn't Windows, malware is not a meaningful threat. A January 2017 article by Alex Campbell in PCWorld dispels this notion, and highlights the risks that malware poses for Linux-based systems. Web servers running Linux are a particular target, given their direct presence on the Internet; Mumblehard is one example of a malware package that has been used to target Linux-based web servers. Ransomware such as KillDisk has been used to attack Linux-based servers and systems. Rootkits are also a significant concern, as their installation can provide full access to a Linux server, and all of the storage to which the server has access. The new CylancePROTECT Linux agent enables IT staff to deploy a defense-in-depth strategy to stop malware attacks across the enterprise, and not just at the endpoint.

Use Case: POS/ATM Terminals

Like many embedded systems, POS and ATM terminals generally utilize the Linux operating system. The attractiveness of these devices as malware targets would seem obvious; yet these systems (particularly POS terminals) have often not had robust protection against cyberattacks. Because of this, POS and ATM terminals have been used as conduits for attacks against both retail and financial services companies, resulting in the compromise of identity data for millions of consumers and significant liability events for the organizations. An article in CSO Online from December 2016 described how POS malware attacks are becoming more aggressive. The actual theft of customer data is usually the final act of an attack that has been built up over years, and often starts with infiltration of the POS system by malware. New attacks are also targeting POS terminals at smaller retailers, who often do not have the SEIM tools utilized by large enterprises. Similar attacks are occurring against ATM machines (known as jackpotting) in a variety of geographies; a malware package known as Ploutus-D is just the latest example of these malware-based attacks on ATMs. The best strategy to stop these attacks is to understand the likely vulnerabilities of POS and ATM systems, and ensure that malware doesn't use these vulnerabilities to

penetrate these systems. By integrating a deep understanding of attackers and attack vectors with the most sophisticated artificial intelligence and machine learning, CylancePROTECT neutralizes virtually all malicious files before they can execute, significantly reducing the threat of malware attacks to POS and ATM terminals.

Use Case: Fixed-Function Devices

PC-based fixed-function devices are growing exponentially, with use cases as diverse as industrial automation systems, Internet of things (IoT) devices, medical equipment, facility management systems, and vending machines. These devices, which are often mission-critical assets in industries such as healthcare, manufacturing, utilities and gaming, overwhelmingly run the Linux operating system. Fixed-function devices have historically been easy targets for cybercriminals to attack and penetrate, as they may not receive updated patches on a regular basis, and their default credentials are often not modified after these devices are installed. These vulnerabilities have been demonstrated recently in the October 2016 DDoS attack which utilized Merai botnets executing on unprotected IoT devices. Preventing malware from being installed on these devices would have mitigated this attack. CylancePROTECT's new Linux agent provides the ability to protect fixed-function devices against the installation of malware, ransomware, and other cyberattack vectors.

About Cylance

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

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

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



©2017 Cylance Inc. Cylance® and CylancePROTECT® and all associated logos and designs are trademarks or registered trademarks of Cylance Inc. All other registered trademarks or trademarks are property of their respective owners.

20170606-1254