CYLANCE™

BUSINESS BRIEF

NIST 800-53 RECOMMENDS NONSIGNATURE-BASED APPROACHES FOR MALWARE DETECTION

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.

WHAT IT IS

Government and critical infrastructure networks are under a constant state of attack, and the attackers' goal is accessing the endpoint to gain a foothold into the agency system. At the same time, cybercriminals continue to innovate and launch successful attacks, such as WannaCry, which locked up more than 230,000 computers across the globe in early 2017. In light of the recent global attacks and their headline-catching victims, it is clear that traditional, signature-based antivirus detection is failing to protect the endpoint.

Cybersecurity is a top priority for federal and local government agencies across the United States. As a result, the National Institute for Standards and Technology Special Publication 800-53 (NIST SP 800-53) is consistently reviewed to ensure it reflects current best practices for adopting and managing cybersecurity and risk management framework.

In its fifth revision, NIST SP 800-53 introduced enhancements to better protect the endpoint and agency systems against advanced persistent threats and other zero-day attack techniques. One control is System and Information Security 3 (SI 3), which recommends that agencies adopt nonsignature-based approaches to protect from malicious code.

> **NIST SP 800-53 SI 3**
> **Malicious Code Protection**
>
> Implement [Selection (one or more): signature based; nonsignature-based] malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code.
>
> Nonsignature-based detection mechanisms include, for example, artificial intelligence techniques…to detect, analyze, and describe the characteristics or behavior of malicious code and to provide safeguards against such code for which signatures do not yet exist or for which existing signatures may not be effective.

CylancePROTECT® Benefits

- Protects your federal and local government agency endpoints with artificial intelligence that evolves daily and prevents cyberattacks from ever being successful
- Stops over 99% of advanced threats without impacting system performance or requiring signature updates
- Simplifies deployment and management with our FedRAMP-certified, cloud-based management console

WHY THIS MATTERS

Signatures and heuristics use pattern matching to detect malicious files. This reactive approach means the malware must first be seen for traditional antivirus vendors to create the signature. The result is a static detection method that provides low threat coverage against unknown and zero-day attacks.

Conversely, nonsignature-based malware prevention and detection, such as artificial intelligence, provides agency endpoints with greater protection by applying techniques that deliver analysis of malicious code pre-execution on the endpoint. This method delivers the strongest efficacy against new and emerging threats with the least amount of performance impact.

Nonsignature-based methods that apply artificial intelligence, algorithmic science, and machine learning to cybersecurity proactively detect the vast majority of cyberattacks, including zero-day and unknown threats, before they execute and cause damage. NIST SP 800-53 SI 3 recognizes the value of this technique as a key part of an agency's cybersecurity arsenal.

RECOMMENDED ACTIONS

Cylance helps government agencies meet the control recommendations for NIST SP 800-53 SI 3 with the most accurate, efficient, and effective signatureless solution for protecting your agency endpoints.

CylancePROTECT redefines what endpoint security can and should do by applying artificial intelligence to detect and prevent zero-day attacks on your endpoints before they execute and cause damage. Our solution applies a mathematical approach to malware identification using patented, machine learning techniques instead of reactive signatures and sandboxes. This renders new malware and unknown, future threats useless.

At the core of Cylance's unprecedented threat prevention capability is a revolutionary machine learning research platform that harnesses the power of algorithmic science and artificial intelligence. It analyzes and classifies millions of characteristics per file, breaking them down to an atomic level to discern whether an object is good or bad in real time.

Learn more about how Cylance can help your agency meet NIST SP 800-53 requirements for control SI 3.

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

CYLANCE™