CylancePROTECT® for AWS EC2

Solution Brief

- Amazon Web Services (AWS) EC2 provide the ability to quickly scale application resources while eliminating capital expenditures and greatly reducing operating costs
- The AWS shared security model requires vendors to configure and/or provide security for their applications
- Events resulting from misconfiguration of security settings are expected to comprise 95% of security events by 2020[1]
- Cloud security services based on traditional antivirus (AV) technologies require significant configuration and signature updates, increasing the time to deploy application instances on the cloud
- CylancePROTECT for the Cloud does not require complex configuration activities to maintain its 99.1%[6] efficacy, resulting in faster application instance deployments with higher efficacy and less security management overhead than other cloud security offerings

The Cloud: Growing Fast, but So Are the Threats

The cloud computing industry is the fastest-growing segment within information technology. Cloud computing companies provide a complete range of offerings (PaaS, IaaS, SaaS, and cloud storage), typically managed by external customers utilizing APIs such as SOAP or REST. The cloud market worldwide will grow by 18.5% from 2016, reaching $260.2 billion[2]. AWS is the largest cloud computing provider with 34% of the cloud computing market over more than 90 services[3] and 2017 revenue of $17.46B[4].

As this market continues to grow, the threats to it from cyber criminals, attackers, and nation states has also grown, as indicated by the data below:

- Public clouds represent a huge attack surface area with access to the assets of a variety of organizations.
- Cloud security concerns still top the list of reasons that organizations are not adopting cloud services. In a recent study, 33% of organization said that security was the biggest barrier they faced[5].
- Mis-configuration of security settings is a far greater problem in the cloud than it is in private data center infrastructure. This is why Gartner predicts that by 2020, 95% of cloud security incidents will be the customer's fault[1]. This is a significant problem because most of the applications that organizations run on the cloud are existing in-house applications rather than applications specifically developed for the cloud.

The result is a market that is highly attractive to attackers.

Challenges of the Cloud Shared Security Model

Underlining the above statistics is the fact that the cloud environment is radically different than the environments in which most IT security staff have been trained and have experience. Unlike the hierarchical security model (defense in depth) utilized by most data centers, the cloud splits the responsibility for providing and configuring security capabilities. The cloud provider typically provides security capabilities such as user access control, encryption, and network access control. Cloud users are typically expected to provide protection for their application instances, as well as other capabilities such as performance monitoring and threat monitoring.

Further complicating the effective use of the shared security model are two cloud attributes that standard IT departments don't share:

- Visibility into the underlying software, hardware, network infrastructure, and storage on the cloud is limited, making identification of potential countermeasures to threats more difficult.
- Cloud computing allows every application instance to communicate with the Internet, meaning that each instance must be individually protected

Combined with the unfamiliarity of configuring the security services provided by cloud service providers, implementing effective security for cloud applications can be a significant challenge.

About Cylance®

Cylance uses artificial intelligence to deliver prevention-first, predictive security products and specialized security services that change how organizations approach endpoint security. Cylance's security solutions provide full spectrum predictive threat prevention and visibility across the enterprise, combatting threats such as malware, ransomware, fileless malware, malicious scripts, weaponized docs, and other attack vectors. With AI-based malware prevention, application and script control, memory protection, device policy enforcement, root cause analysis, threat hunting, automated threat detection and response, coupled with expert security services, Cylance can protect endpoints without increasing staff workload or costs.

Securing Application Instances on AWS EC2

Historically, endpoint security vendors have relied on virus definition signatures developed from a historical view of malware. While this once may have been a reasonable approach, it is one that is infeasible today. AV-TEST reported over 120 million new malware variants in 2017 alone. When combined with threats based on zero-day exploits, the approach of using malware signatures to combat cyber threats is obsolete and ineffective.

CylanceOPTICS™ products adapted for the cloud, takes a different approach. At the core of Cylance's unique cybersecurity capabilities is a revolutionary machine learning research platform that harnesses the power of algorithmic science and artificial intelligence. It utilizes a small agent that analyzes and classifies hundreds of thousands of file characteristics at the atomic level to discern whether a file is safe to run without a need for signatures or a connection to external systems. When combined with Cylance's other security technologies such as memory defense and script control, Cylance for the Cloud provides threat detection and protection with a demonstrated efficacy of 99.1%[6] for both Linux and Windows cloud applications.

Cylance doesn't employ this technology at the expense of simplicity, ease of use, or burden on application instance performance or on cloud security administrators. The agent at the heart of CylancePROTECT and CylanceOPTICS does not require complex configuration or signature file updates to maintain its efficacy. It also integrates with existing cloud management systems through its command line API or it can integrate directly with Cylance's own cloud console if desired. This simplifies the deployment of security infrastructure for cloud application instances, resulting in faster instantiation and teardown. The result is a lower operating expense for both the management and execution of applications in the cloud. No other cloud instance security product compares to the effectiveness, ease of management, and low impact of Cylance's solutions.

Conclusion

Moving IT to the cloud is extremely attractive for its ability to reduce costs and enable rapid scale-up and scale-down of those capabilities. Cylance has responded to this demand with lightweight, and easy-to-use cloud security products. Cylance does this by leveraging artificial intelligence to predict attacks, seeking first to prevent attacks, and by offering scalable threat detection and response for root cause analysis and threat hunting. Cylance's 99.1%[6] efficacy and ease of use are just a couple reasons why organizations worldwide utilize Cylance products to help secure their assets. Let Cylance help you achieve the same level of security for your AWS EC2 cloud application instances with Cylance for the Cloud.

[1] IDG Connect, The Most Common Causes for Data Breaches, February 2018

[2] Louis Columbus (Forbes), Cloud Computing Market Projected to Reach $411B by 2020, October 18, 2018

[3] Synergy Group, Cloud Growth Rate Increased Again in Q1 (2017), April 2018

[4] Jordan Novet (CNBC), Amazon cloud revenue jumps 45 percent in fourth quarter, February 1, 2018

[5] DeltaRisk, Cloud Security: 2017 Spotlight Report, 2018

[6] NSS Labs, Advanced Endpoint Protection (AEP) Test Report and Security Value Mapping, 2018

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

CYLANCE

20181210-1473