CYLANCE

BUSINESS BRIEF

SECURELY MIGRATING TO MICROSOFT OFFICE365

Migrating to Microsoft Office 365 (O365) exposes an organization to specific security risks. Some of the risks are obvious, like O365 security protocols usurping those currently used by an organization. Others are less obvious, like vulnerabilities introduced when third-party apps connect to O365.

SECURITY IS A SHARED RESPONSIBILITY

Microsoft has invested considerable resources into making O365 a secure platform. However, security is a shared responsibility between vendor and customer. Microsoft assumes responsibility for securing their infrastructure and protecting data resting within their storage. They are not responsible for ensuring the security of applications or users accounts provisioned by customers. It is vital for organizations to maintain an effective cybersecurity posture rather than relying on the default security settings of cloud service providers.

CYLANCE® COMPLEMENTS EOP

Microsoft Exchange Online Protection (EOP) offers O365 users protection against malware, spam, and suspicious attachments. Like other signature-based protection software, EOP relies on data from previously identified threats to prevent breaches. This approach leaves EOP susceptible to mutated, customized, and zero-day payloads which have no existing signatures to reference.

Cylance uses artificial intelligence (AI) models trained on millions of safe and malicious file samples to identify malicious executables. This method allows Cylance AI to detect new and emerging threats in addition to securing systems against known malware. Understanding malware on a DNA level gives Cylance a predictive advantage, meaning Cylance's solution is able to identify malware that is identified well after the AI model has been trained and deployed. Independent testing from SE Labs has proven that CylancePROTECT® holds an average predictive advantage of 25 months over major malware families. This means the Cylance 2015 AI model was able to identify and prevent a threat which did not exist until 2017, over two years after the model had been trained and deployed.

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.

CylancePROTECT®

CylancePROTECT offers organizations migrating to O365 several additional benefits including:

- AI Driven Malware Prevention
- USB Device Usage Policy Enforcement
- Script Management
- Memory Exploitation Prevention
- Application Control for Fixed-Function Devices
- Zero-day Payload Prevention

CylanceOPTICS™

Cylance's endpoint detection and response (EDR) solution, CylanceOPTICS, deploys machine learning models which run locally on the endpoint. These models have been trained to identify malicious behaviors on the device and can take immediate response actions, without the use of static behavior rules. In addition to this capability, CylanceOPTICS provides:

- **Distributed Search and Collection –** Cylance's unique approach to data collection that optimizes data collection, search, and analysis
- **Consistent Cross-Platform Visibility –** With support for Microsoft Windows endpoint and server machines, as well as MacOS endpoints, organizations can maintain situational awareness across their entire environment with one solution
- **Root Cause Analysis –** Web-based, on-demand, root cause analysis of attacks blocked by CylancePROTECT as well as other interesting artifacts identified on endpoints
- **Enterprise-wide Threat Hunting –** Search endpoint data instantly for potential threats
- **Fast Incident Response –** Take incident response actions fast, quarantining, acquiring suspicious files, and/or isolating compromised endpoints from the network

MICROSOFT OFFICE 365 SECURITY CHECKLIST

Securing Office 365 does not have to be complicated. While every organization's needs differ, here are five things to keep in mind when considering O365 and security requirements:

- Who needs access to O365?
- What applications will connect to O365?
- What data will be in O365?
- Can I secure O365 with my existing security controls?
- Can I secure O365 with my existing security team?

Taking a pragmatic approach to these security decisions will ensure that organizations eliminate blind spots in their architecture that could give attackers a foothold in their Office 365 environment.

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

CYLANCE