O365 Security Checklist:

As you prepare for your O365 implementation, this checklist will serve as a guide to assist you through the multiple dimensions of an O365 migration and the selection of your solution for securing it.

Contextual Visibility

- ☑ **Continuously scan** Office 365 content, emails, and transactions to remediate and prevent the proliferation of ransomware, advanced persistent threats (APTs), and other malware.
- ☑ **Strive to achieve a single console** for visibility and policy controls, including access governance, data security, threat protection, account hijacking, and compliance reporting across SaaS apps and Infrastructure services. These services might include file sharing, data storage, email, messaging, collaboration, and other business enablement services.
- ☑ **Activate advanced threat analytics**, inclusive of indicators of compromise (IoC), for efficient discovery and remediation.

Alerts

- ☑ **Create passive mode alerting** to test existing policies to reduce triggering false positives that could introduce friction to employees
- ☑ **Categorize alerts** based on severity (low, moderate, high) in an effort to begin to see where automation opportunities may exist.
- ☑ **Report and communicate** anomalies across all applications, data sources, and clouds to internal teams and executive champions.

Policies

- ☑ **Create access controls and authentication methods** that protect the front doors into businesses systems, inclusive of polices that trigger additional means of authentication based on behavior.
- ☑ **Enforce usage controls** and authorization policies based on location, device type, user group, and user behavioral risk level. Ideally, create a single policy that encompasses email, file sharing, collaboration, Office 365, and other cloud apps.
- ☑ **Reduce operational complexity** in a multi-cloud world with consistent policy controls and directory integration.

Protection

- ☑ **Embrace data loss prevention** (DLP) in the cloud that automatically classifies and tracks structured, unstructured, and interactive content in OneDrive, Email, SharePoint Sites, Teams and Groups, and Yammer.
- ☑ **Implement one solution** to protect across all cloud services while triggering encryption of sensitive data.
- ☑ **Test** for detection efficacy and false positive rates.

Detection

- ☑ **Continuously analyze** external and internal email content, activity in apps, transactions with apps, content-in-motion and content-at-rest in Office 365 to detect, block, or quarantine threats.
- ☑ **Utilize machine learning,** email threat isolation, impersonation controls, link protection, cloud sandboxing, user behavior analytics, and threat analytics.
- ☑ **Be prepared** for sophisticated attacks that cannot be stopped or detected with single point security tools.

Automation

- ☑ **Create security and access controls** over data-in-motion and data-at-rest end-to-end from the user to the cloud for your Office 365 and other SaaS and IaaS accounts.
- ☑ **Automatically identify** high risk user accounts, compromised accounts, and insider threats with data science-driven user behavior analytics and adaptive authentication that forces policies based on user behavior.
- ☑ **Leverage artificial intelligence** (AI) built into the cloud that provides visibility into external and internal vulnerabilities and helps to remediate issues without manual intervention.

Created exclusively for Symantec by The Enterprise Stratgey Group, Inc. 2018

Symantec