Office 365

CYBER OBSERVER

Solution Brief

Cyber Observer and Office 365 Integration

Unified cybersecurity management and awareness

Challenge

Today's challenging cybersecurity landscape offers an over-abundance of cybersecurity tools. As the number of breaches proliferates, so have the solutions and technologies designed to stop them. The state of cybersecurity is not getting easier to manage, despite enterprises and organizations worldwide spending more money than ever on new technologies and solutions.

Designed for CISOs and senior InfoSec managers (such as CIOs, C-level managers, risk officers, SOC managers and IT Infrastructure personnel), Cyber Observer empowers leadership with a **unified dashboard** of their entire cybersecurity ecosystem. Cyber Observer can be fully deployed within an enterprise in a few hours, enabling easy **identification** of **weaknesses**, **reduction of mean-time-to-detect (MTTD)**, **prevention of breaches**, and advancement of your organization's **cybersecurity posture** and **maturity**.

Solution

Cyber Observer's partnership with Office 365 enables CISOs to better manage their cybersecurity ecosystem. They receive alerts from Cyber Observer on the key aspects and issues in Office 365 such as **configuration**, **incident** and **investigation management**, **password policies**, **user** and **role administration** and more. This joint effort helps enterprises manage their cybersecurity environment and **continuously monitor their cybersecurity ecosystem posture**.

KEY FEATURES

- Identifies cybersecurity tools that are misconfigured, malfunctioning, or missing
- Finds security gaps and provides recommendations for fixing
- Builds an ongoing security program to ensure alignment with new threats
- Uses continuous analytics to send alerts when there are deviations from normal behavior
- Automatic reporting

Office 365

CYBER OBSERVER

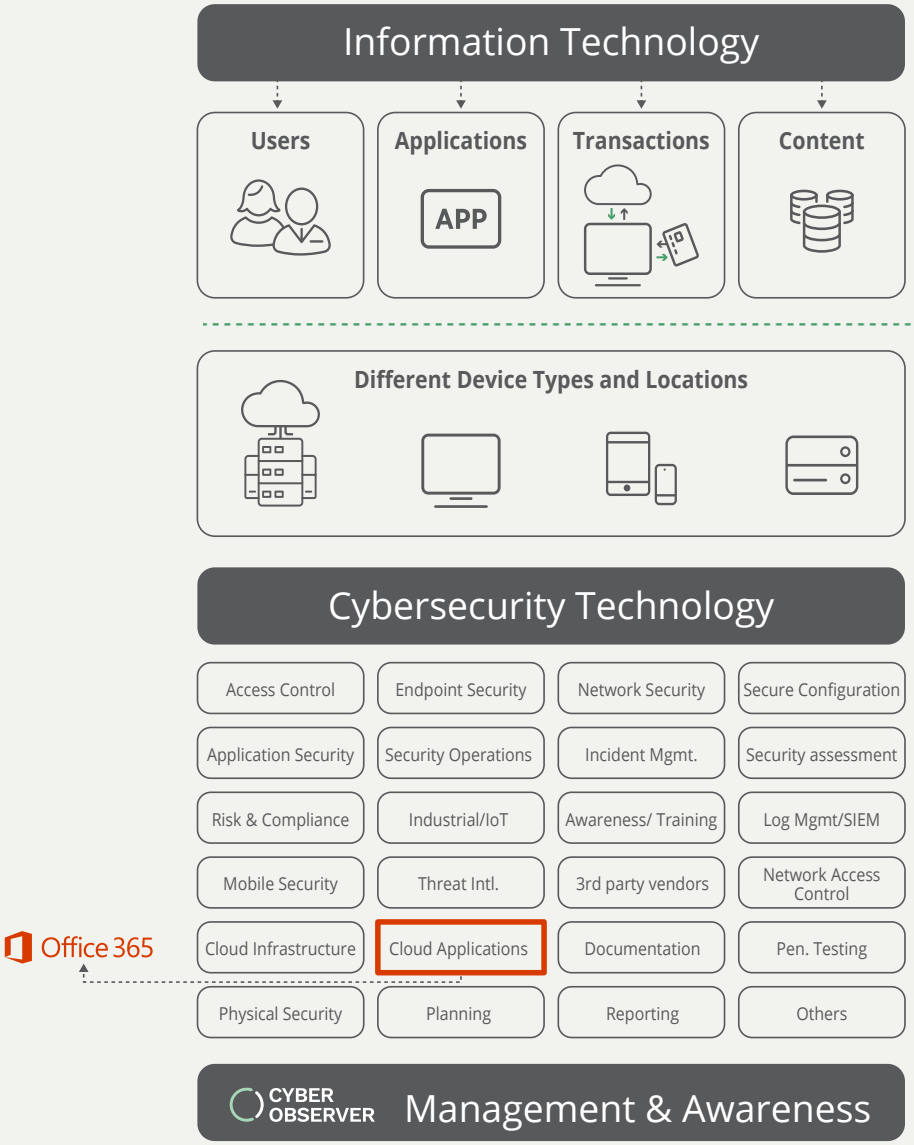
The integration between Cyber Observer and Office 365 offers CxOs powerful and effective **resilience visibility** along with **compliance validation** and **controls**, to secure and monitor Office 365 in an unprecedented manner.

Cyber Observer deploys to the corporate network automatically, in a matter of a few hours, predefined with security domains and CSC measurements to deliver three unique cybersecurity ecosystem views:

- First, it provides organizations with the best indicators of the cybersecurity tools that may be **misconfigured**, **malfunctioning**, or **missing** and should be added to provide complete cybersecurity protection.
- It then **reveals the security gaps** that exist in each security domain and **delivers continuous proactive recommendations to close these gaps**.
- Finally, Cyber Observer's machine learning analytics engine continuously calculates online measurements that represent normal behavior, and then **alerts when a deviation from normal behavior is detected**.

Fast and Secure Deployment

The Cyber Observer connector for Office 365 receives security and configuration data from Office365 via a secure REST API and PowerShell.



Office 365

CYBER OBSERVER

Key Features & Benefits of This Integration

- **Cyber Hygiene Analysis and Reporting:**
  Alerts and reporting regarding Office 365 current configuration implementation status based on Microsoft best-practices and security standards best-practices, including insecure policies configurations, security configuration issues, various functioning issues and more.
- **Continuous Monitoring and Alerts:**
  Cyber Observer provides the CISO and other relevant managers in the organization, as well as the Office 365 technical owners with continuous monitoring and alert regarding high severity events and occurrences, including malicious content found in emails, phishing attacks, spam, spoofed emails and more.
- **Continuous Incident Response:**
  Mitigation recommendation and steps to improve, for securing and monitoring Office 365 implementation, effectiveness, maturity and resilience from a management perspective in an unprecedented manner.
- **Customizable Views and Reports**
  Cyber Observer is highly customizable – all views and reports could be modified to the organization's needs and structure. The integration between Cyber Observer and Office 365 offers CxOs powerful effectiveness and resilience visibility, as well as compliance validation and controls.

Key Use Cases

1 Immediate alerts and detailed information regarding high severity events and occurrences

- Impersonation senders
- ATP File Types Report Malicious URLs
- ATP File Types Report Malicious Executables attachments
- Phishing Emails
- Spoofed Emails
- Quarantined Emails released

2 Detailed information regarding mis-configured and insecure policies

- ATP Anti-phishing policies
- ATP safe attachments policies
- Anti-spam policies
- Action to take for incoming High confidence spam is not
- to Quarantine message
- Action state is off for malware in attachments

3 Detailed information regarding insecure, misconfigured features

- ATP Anti-phishing policies off
- Spam Zero-hour auto purge is off
- Phish Zero-hour auto purge is off
- Domains Dkim is disabled
- Malware Zero-hour Auto
- Purge is off

About Microsoft

Microsoft Corp. (Nasdaq: MSFT), Microsoft is a worldwide leader in providing IT products and solutions to both the public and private sectors - leading the industry in key security initiatives such as Trustworthy Computing, the Security Development Lifecycle, botnet takedowns, and the Windows Defender Security Intelligence group. The Microsoft Services Detection and Response Team is comprised of senior IT and IT Security leaders and experts with extensive experience in both the private sector and government. The Cybersecurity Operations Service employs a highly-skilled, diverse group of resources to defend the world’s largest enterprise organizations in the fight against cybercrime.

About Cyber Observer

Cyber Observer is the premier critical controls monitoring (CCM) solution that simplifies the way cybersecurity tools are monitored and managed. Cyber Observer integrates hundreds of popular cybersecurity tools into a single intuitive interface that enables security and risk management executives to continuously monitor their security tools and improve their cybersecurity posture in alignment with cybersecurity, business, and regulatory frameworks.
Learn more at **cyber-observer.com**.