SECURONIX™

SOLUTION BRIEF

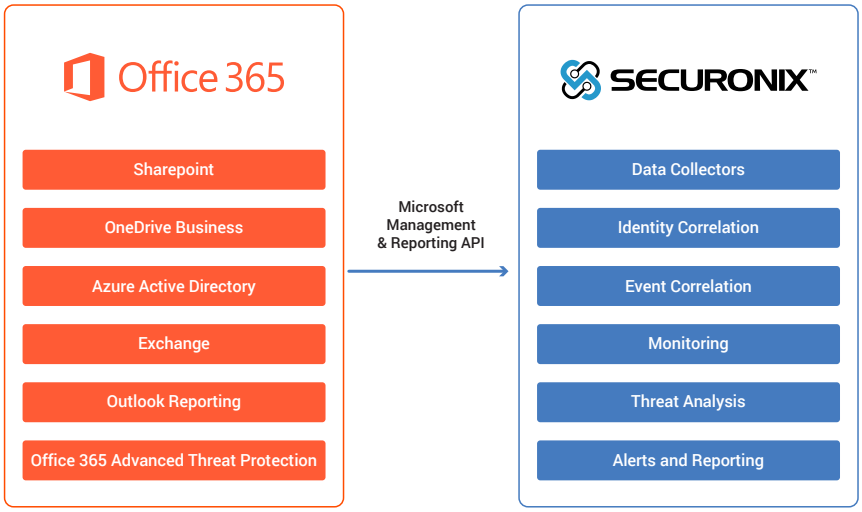
Securonix Security Monitoring for Microsoft Office 365

Enterprise adoption of Office 365 is growing steadily. However, moving to the cloud with Office 365 brings its own security challenges – and, as with any cloud native application, takes control away from IT management. A robust security solution, built for the cloud-native enterprise, is required.

Securing Against Data Exfiltration and Advanced Threats

Common security concerns with cloud data sharing applications include how to identify sensitive data movement in the cloud, access control, unauthorized activities, privilege misuse or compromise, unauthorized sharing, and data exfiltration. These concerns are increased with high usage applications. Office 365 has a large number of applications in use, several of which support functions that make phishing attacks (Exchange), data exfiltration (SharePoint), and unauthorized access (Azure AD) very real threats.

Securonix supports multi-application integration with Office 365 for constant threat monitoring. In addition to standard benefits, such as analysis of user entitlements and events to look for malicious activity, the platform also supports multiple built-in Office 365 specific use cases. It correlates Office 365 cloud-based data with data from on-premises sources (such as Active Directory) to add entity context information and analyze the end-to-end activities of users and detect actionable threat patterns.

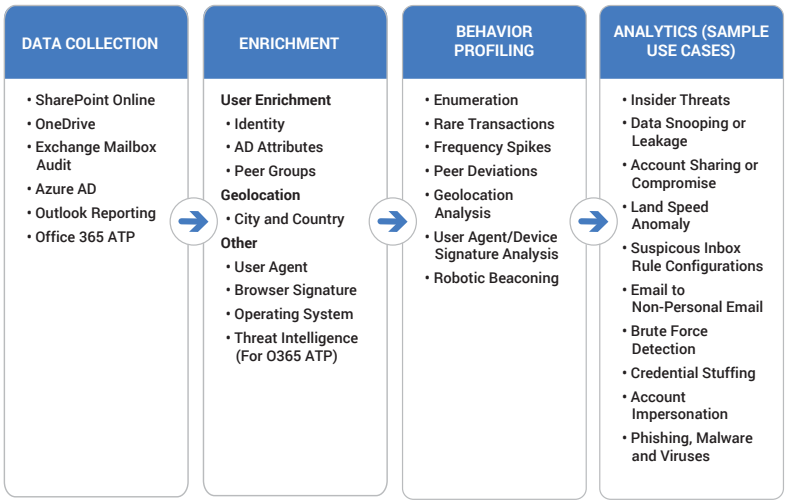


Solution Benefits

- API integrations with multiple Office 365 components.
- Out-of-the-box content for monitoring advanced Office 365 threats.
- Enrichment of data with additional context from on-premises data sources and other applications for threat modeling.
- MITRE ATT&CK compliance with threat chains methodology that is in line with MITRE's own staged threat framework.

Custom Built for Office 365 Security

Securonix aggregates information from multiple Office 365 sources, enriches it, and performs behavior profiling and analysis in order to identify real threats.

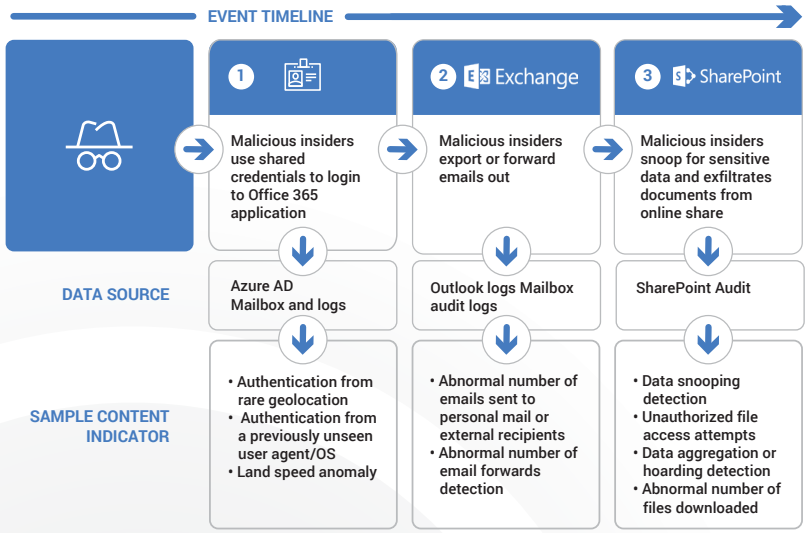


Securonix Case Study: Protecting Sensitive Data

A large telecommunications organization discovered that insiders (contractors) with internal account credentials for Office 365 access, were sharing these credentials prior to their contract termination and misusing their access privileges to exfiltrate sensitive data and project documents.

Securonix detected the threat as it emerged, giving security analysts enough time to mitigate the threat by disabling access for the compromised accounts and initiating actions to remediate the loss of information (such as recalling emails sent out by the malicious insiders).

Here's how the threat event evolved over time:



Securing Office 365 with Securonix

With comprehensive information gathering, tailored threat content, as well as strong behavior and event analytics, Securonix allows you to see threats that would never be detected by simple alert logging.

Key Use Cases

- Detect suspicious file sharing, permission changes, and downloads.
- Detect account compromise.
- Identify phishing attempts.
- Identify suspicious email patterns.
- Spot unauthorized Exchange permission changes.
- Detect credential sharing.
- Identify privileged account misuse.
- Locate insider threats.
- Identify suspicious login events.
- Detect password attacks.
- Track malware, phishing, and virus attacks.

About Securonix

The Securonix platform delivers positive security outcomes with zero infrastructure to manage. It provides analytics-driven next-generation SIEM, UEBA, and security data lake capabilities as a pure cloud solution, without needing to compromise. For more information visit www.securonix.com.

SECURONIX™

LEARN MORE
www.securonix.com

LET'S TALK
+1 (310) 641-1000