SECURONIX™

SOLUTION BRIEF

Securonix Security Monitoring for Microsoft Azure

With a strong service set, backed by Microsoft's own technology and products, Microsoft Azure is a top choice for enterprises to deploy on – as well as for attackers to exploit. As with any major public cloud, the number of touchpoints you need to monitor is massive. Prioritizing and identifying the right touchpoints is critical to secure your Azure deployment.

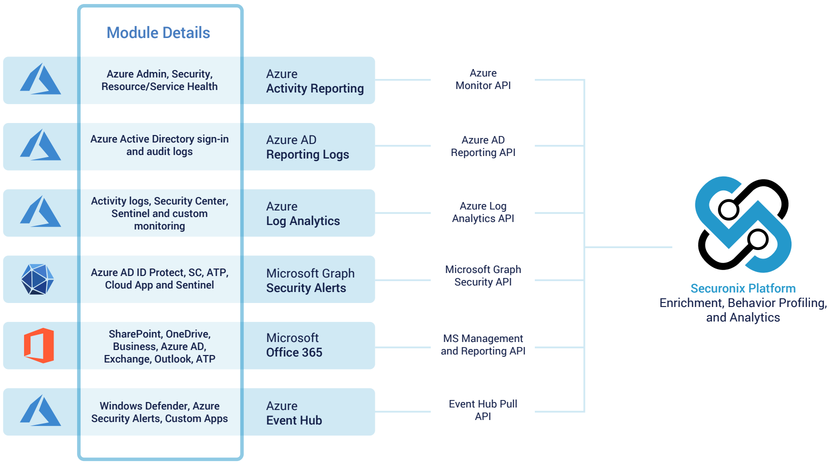
Securing Your Cloud Infrastructure

Azure handles many things – from identity (with Azure Active Directory) and email (Exchange), to cloud resource provisioning and a full featured platform as a service (PaaS). In order to implement a secure cloud environment, though, several use cases must be handled effectively:

- Identify sensitive data movement and suspicious login activity on the cloud
- Access control
- Monitoring unauthorized and/or unexpected activities
- Detect privilege misuse or compromise
- Detect unauthorized sharing and data exfiltration

The breadth of Azure's offerings increases the number of touchpoints that could allow attackers access to your enterprise. Securonix provides multi-point, multi-level integrated security for Microsoft Azure. It monitors to critical touchpoints needed to ensure a complete, comprehensively secure cloud environment for your enterprise.

By connecting to multiple sources logs, Securonix ensures constant threat monitoring of Azure. In addition to standard benefits, such as analyzing user entitlements and events to look for malicious activity, the platform also supports multiple built-in Microsoft Azure specific use cases. It also correlates 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. Securonix threat modeling then automatically stitches together anomalies over a period to detect and prioritize high risk threats. Through integrations with Azure Sentinel, Security Center, and Windows Defender, Securonix is able to leverage Microsoft security infrastructure and collate all threat information into a single source of truth.

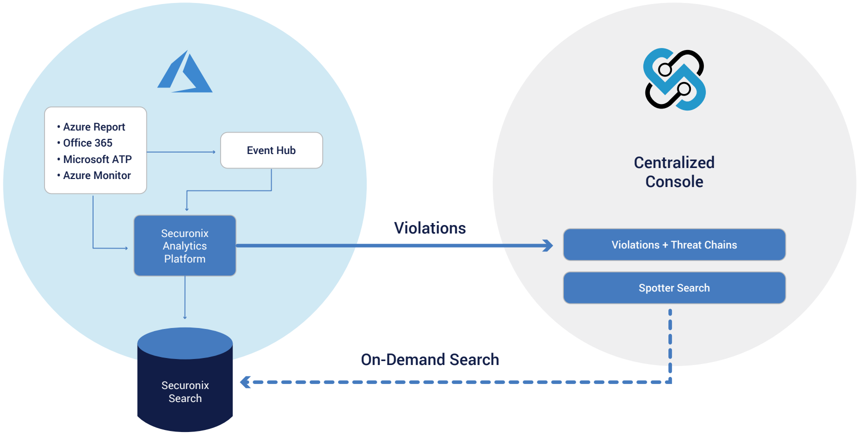

Module Details
Azure Admin, Security, Resource/Service Health
Azure Activity Reporting
Azure Monitor API
Azure Active Directory sign-in and audit logs
Azure AD Reporting Logs
Azure AD Reporting API
Activity logs, Security Center, Sentinel and custom monitoring
Azure Log Analytics
Azure Log Analytics API
Azure AD ID Protect, SC, ATP, Cloud App and Sentinel
Microsoft Graph Security Alerts
Microsoft Graph Security API
SharePoint, OneDrive, Business, Azure AD, Exchange, Outlook, ATP
Microsoft Office 365
MS Management and Reporting API
Windows Defender, Azure Security Alerts, Custom Apps
Azure Event Hub
Event Hub Pull API
Securonix Platform
Enrichment, Behavior Profiling, and Analytics

Solution Benefits

- Direct API integrations with Azure Active Directory, logging engines, and security.
- Out-of-the-box content for monitoring advanced Azure and Office 365 threats.
- Multi-tier monitoring coverage, utilizing multiple reporting APIs for comprehensive security.
- 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.

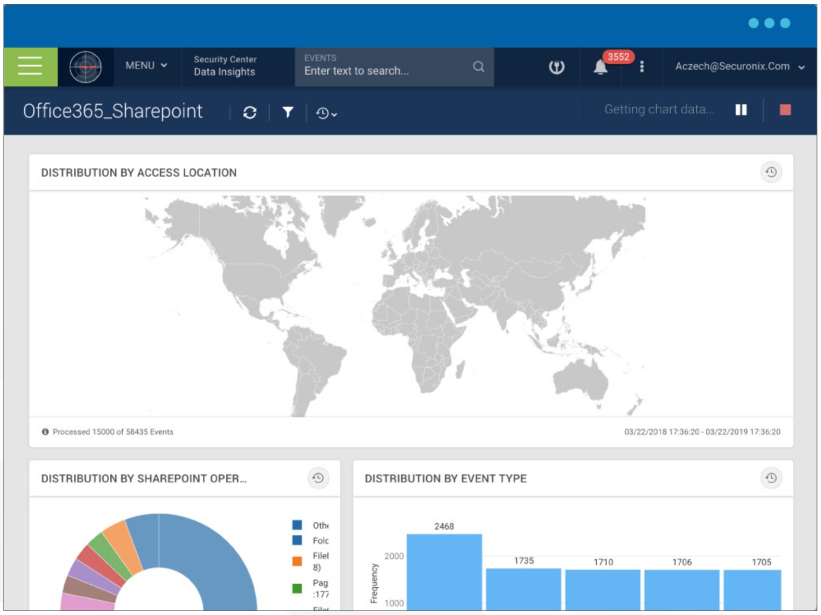
Purpose Built for Microsoft Azure Security

Securonix is a cloud native SIEM solution that deploys as a service. This allows anywhere, anytime configuration and management. The Securonix platform aggregates information from multiple Azure sources, enriches it, and performs behavior profiling and analysis in order to identify real threats. Securonix Spotter search also allows for the fast, on-demand retrieval of alerts.



Focus on Visibility and Information Access

Besides tracking threats, a key benefit of the Securonix platform is the detailed visibility into every aspect of enterprise security. The dashboard provides a bird's eye view of current environment status, while an easy to access event search widget allows quick event access from the first page.



Key Use Cases

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