securonix

Microsoft Azure

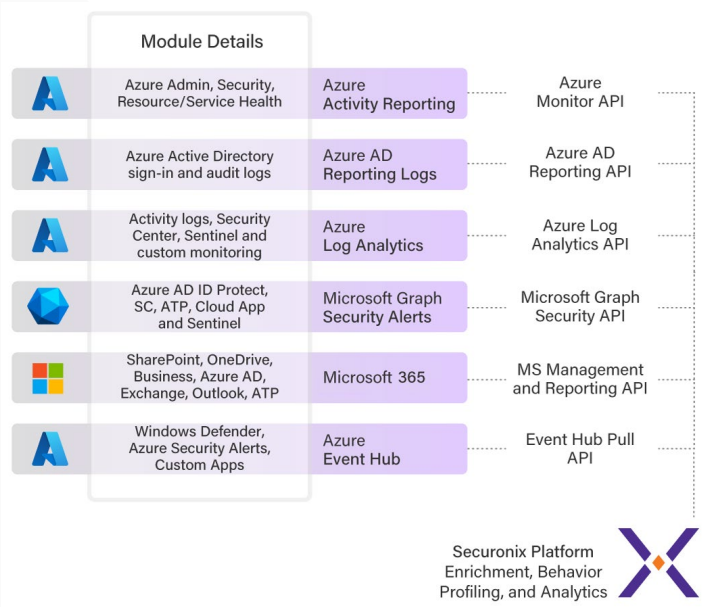
SOLUTION BRIEF

# Microsoft Azure Cloud Security Monitoring

Identify patterns and pinpoint potential threats in your Azure cloud environment

## Remove Cloud Security Blind Spots

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 alerts is critical to detect threats in your Azure environment.




## Our Approach

Securonix analyzes possible security events to look for malicious activity. Through integrations with Azure Sentinel, Security Center, and Windows Defender, Securonix leverages Microsoft's security infrastructure to collect all threat activities into a single source of truth for security teams to use for detection and response.

## Solution Benefits

Detect and respond to cloud threats in your Azure environment.

### Gain 360 Degree Visibility

Correlate cloud security events with on-premises network data. Now, your security team has a holistic security picture.

### Detect Threats Faster

Decrease your mean-time-to-detect with context-enriched data insights and advanced threat chain analytics.

### Unlock Data Insights

Visualize security events and changes in your Azure Cloud environment with out-of-the-box and custom dashboards and reports.

## How it Works

By collecting, enriching, and analyzing data across your environment, Securonix ensures your security team can monitor threats in Azure. Securonix analyzes user entitlements and events to look for malicious activity and supports multiple built-in Microsoft Azure-specific use cases. Our solution correlates cloud-based data with data from on-premises sources (such as Active Directory) to add entity context information and analyze user activity end-to-end.

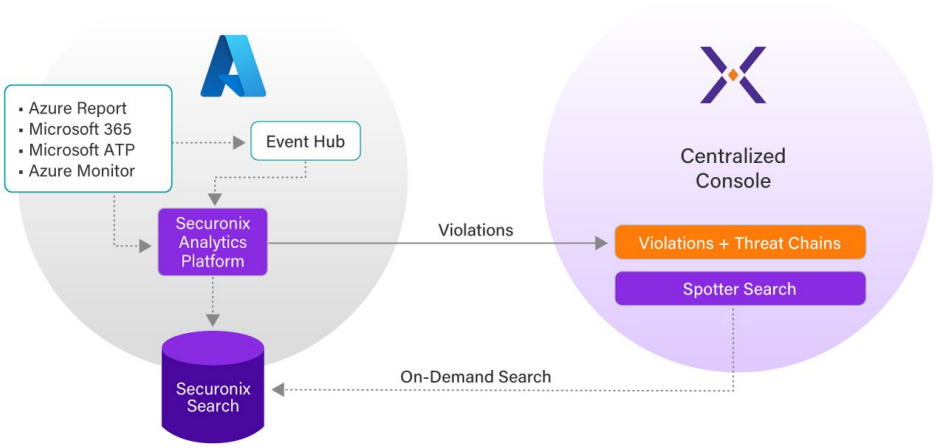
The Securonix Next-Gen SIEM then aggregates this data from multiple Azure sources, enriches it, and performs behavior profiling to help security teams understand real cybersecurity and insider threats.

## Key Use Cases

Common use cases include detecting:

- Suspicious instance and resource usage
- Account compromise or credential sharing
- Phishing attempts
- Suspicious email patterns
- Privileged account misuse
- Suspicious login events
- Advanced and insider threats

For more information about Securonix, schedule a demo at: www.securonix.com/request-a-demo




### About Securonix

Securonix is redefining SIEM for today's hybrid cloud, data-driven enterprise. Built on big data architecture, Securonix delivers SIEM, UEBA, XDR, SOAR, Security Data Lake, NDR and vertical-specific applications as a pure SaaS solution with unlimited scalability and no infrastructure cost. Securonix reduces noise and prioritizes high fidelity alerts with behavioral analytics technology that pioneered the UEBA category. For more information visit securonix.com

### About Microsoft Azure

Microsoft Azure, often referred to as Azure, is a cloud computing service operated by Microsoft for application management via Microsoft-managed data centers. For more information visit azure.microsoft.com