securonix

Microsoft 365

SOLUTION BRIEF

Microsoft 365 Security Monitoring

Identify patterns and pinpoint potential threats in your Microsoft 365 environment

Remove Cloud Security Blind Spots

Microsoft 365 is widely used by many organizations to help drive collaboration and productivity. While Microsoft 365 enables businesses to be more efficient, it is also a high-value target for cybercriminals. The security controls organizations have in place for on-premises protection are not effective at protecting cloud applications.

Our Approach

Securonix analyzes possible security events to look for malicious activity. Through integrations with Microsoft 365, SharePoint Online, Exchange Online, and Azure AD, Securonix leverages Microsoft's security infrastructure to collect all threat information into a single source of truth for detection and response.

Solution Benefits

Detect and respond to applications and email-borne threats.

Gain 360 Visibility

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

Detect Threats Faster

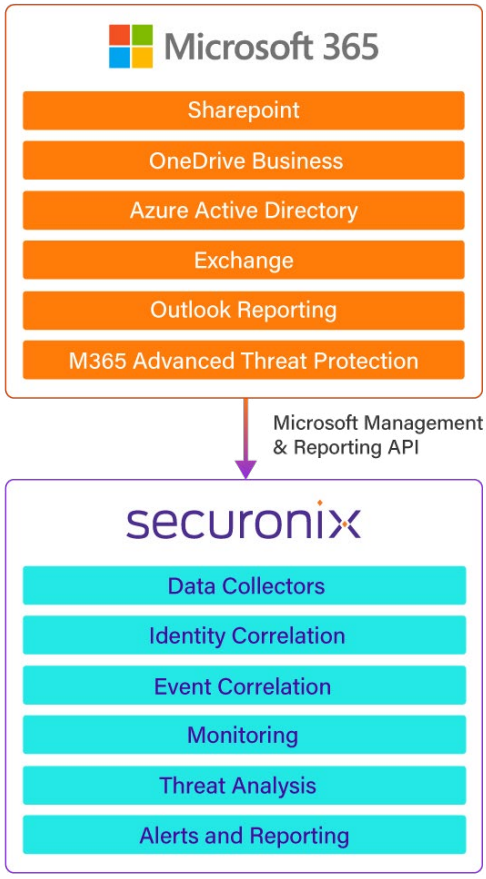
Decrease your mean-time-to-detect with context-enriched data insights and advanced threat chain analytics.

Unlock Data Insights

Visualize security events and changes in your Microsoft 365 environment with out-of-the-box and custom dashboards and reports.

How it Works

Securonix supports multi-application integration with Microsoft 365 for constant threat monitoring. In addition to standard benefits, such as analysis of user entitlements and events to find malicious activity, the Securonix also supports multiple built-in Microsoft 365 specific use cases. It correlates Microsoft 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.



Detect Faster with Microsoft 365-specific Threat Models

Microsoft 365 applications support functions that make phishing attacks through Exchange, data exfiltration from SharePoint, and unauthorized access to Azure AD attractive targets. A direct API integration with Microsoft 365, Azure AD, and other cloud sources provides you with the relevant event logs needed to uncover unknown threats. Securonix correlates events with contextual information from other on-premises data feeds, such as Active Directory watchlists to detect low and slow threats across your entire environment.

Key Use Cases

Securonix provides pre-built cloud security monitoring content to detect anomalous security events including:

- Account compromise
- Phishing attempts
- Suspicious email patterns
- Unauthorized exchange permission changes
- Credential sharing
- Privileged account misuse
- Insider threats
- Suspicious login events
- Password attacks
- Advanced threats
- Suspicious file sharing

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 365

Microsoft 365 encompasses subscription plans that allow use of the Microsoft Office software suite over the life of the subscription, as well as cloud-based software-as-a-service products for business environments, such as hosted Exchange Server, Skype for Business Server, and SharePoint, among others. All Microsoft 365 plans include automatic updates to their respective software at no additional charge, as opposed to conventional licenses for these programs—where new versions require purchase of a new license. For more information visit www.microsoft.com/microsoft-365