SECURONIX™

SOLUTION BRIEF

Securonix Application Security

Business-critical applications live in the cloud and increasingly utilize open source components. While this opens huge integration possibilities, it also increases your exposure to security vulnerabilities. Attackers are taking advantage of this. According to the 2018 State Of Application Security Report by Forrester, software vulnerabilities and web application attacks (such as SQL injection and cross-site scripting) were the top two external attack vectors in 2018.[1] At the same time, insider threats are on the rise too. According to the Cybersecurity Insiders' 2019 Insider Threat Report, 70% of cybersecurity experts surveyed said insider attacks have increased over the past year. [2]

Most organizations rely primarily on access controls and network security solutions that are ineffective against an insider threat or an external targeted attack. Organizations need real-time, continuous monitoring to provide them with visibility into application-targeted threats before it is too late.

The Securonix platform addresses this need by monitoring critical applications and systems at the transaction, data set, and sensitive user record level. Securonix continuously builds a risk profile for all applications and systems while identifying all high-risk users, access, and activities associated with sensitive data and transactions. Results are scored and presented in application risk scorecards.

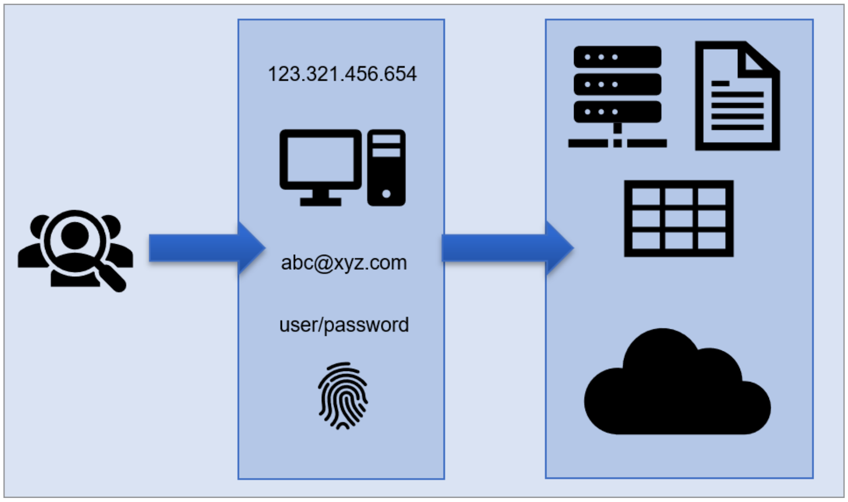


Figure 1: Securonix application security focuses on application usage, looking at users, activities, and access instead of application states. Application state monitoring can sometimes be deceiving, as insider attack attempts can often be interpreted as legitimate application requests.

[1] https://www.forrester.com/report/The+State+Of+Application+Security+2018/-/E-RES141676
[2] https://www.securonix.com/resources/2019-insider-threat-survey-report/

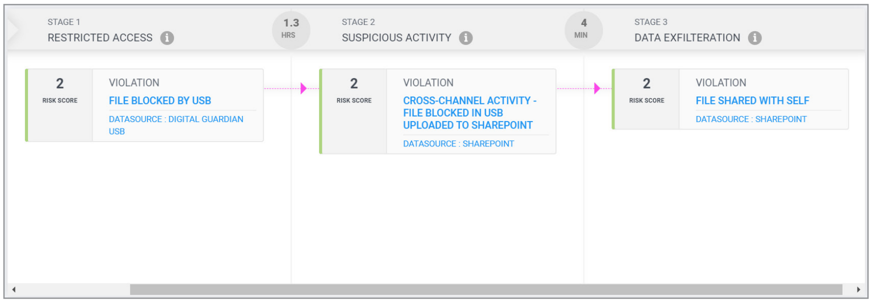
Solution Benefits

- Continuous control and compliance monitoring.
- Automated, rapid detection of high-risk activity through behavior analytics.
- Detection and logging of access and activity that may indicate possible threats.
- Continuous detection and monitoring of critical information for DLP.
- Enrichment of data with identity, behavior, and business context for security and compliance management.
- Proactive detection and management of fraud, misuse, snooping, and other illicit activity.
- Custom packaged apps for specific use cases such as healthcare and fraud detection.
- Hundreds of built in integrations.
- MITRE ATT&CK compliance, with the threat chains methodology that is in line with MITRE's own staged threat framework.
- Support for multiple cloud provider environments.

The Securonix platform recognizes the reality that application security is dependent on the users that use them. The platform links all security events to a single identity (linked across IP addresses, usernames, devices, biometric data, hostnames and application identities), securing all applications accessed by an entity instead of securing individual applications from all users.

Key Solution Features

- Real-time visibility with continuous monitoring and AI-driven analytics.
- Real-time event monitoring and complete visibility with the Securonix platform. Review threats, identify all relevant data with event enrichment, and take action with built-in SOAR capabilities.
- Multi-stage threat chain methodology looks beyond alerts, linking events across applications, users, host machines, devices, and IP addresses with intelligent analytics to identify viable, clear threats. All threats are scored with a policy-based risk scoring capability.



STAGE 1
RESTRICTED ACCESS

2 RISK SCORE
VIOLATION
FILE BLOCKED BY USB
DATASOURCE : DIGITAL GUARDIAN USB

1.3 HRS

STAGE 2
SUSPICIOUS ACTIVITY

2 RISK SCORE
VIOLATION
CROSS-CHANNEL ACTIVITY - FILE BLOCKED IN USB UPLOADED TO SHAREPOINT
DATASOURCE : SHAREPOINT

4 MIN

STAGE 3
DATA EXFILTERATION

2 RISK SCORE
VIOLATION
FILE SHARED WITH SELF
DATASOURCE : SHAREPOINT

Figure 2: Multi-stage threat chaining with alerts plotted along a structured attack lifecycle.

Example Security Use Cases

- Using behavioral analytics Securonix can detect a sudden spike in objects accessed by a user or when a user is accessing objects that are not normally accessed by others in the same peer group. These anomalies can potentially point to malicious users or users with compromised credentials.
- Monitor data exfiltration attempts and detect attempts at downloading or inappropriately sharing large amount of data.
- Monitor suspicious object sharing events. Discover instances where a user shares objects with a high-risk security label with somebody who doesn't need access to the object. Or, find instances when a high-risk object has been added to a low-risk project and was shared.
- Monitor suspicious copy and rename events. Discover instances where a user has renamed high-risk files to make them sound more innocuous or generic to bypass controls.
- Monitor for anomalous permissions, such as an employee who has access to an excessive number of files.

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