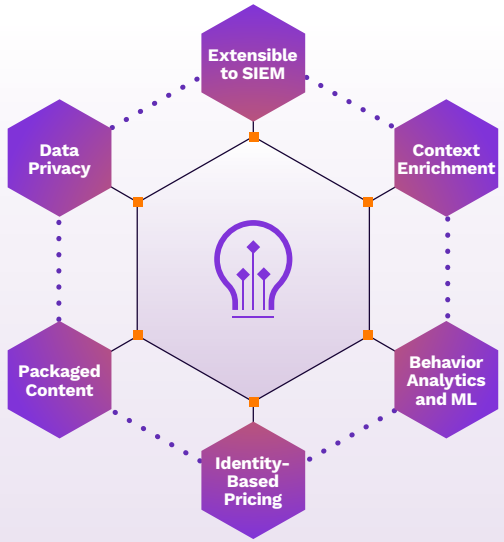
securonix DATASHEET

User and Entity Behavior Analytics

DETECT AND INVESTIGATE THREATS HIDDEN IN YOUR ENVIRONMENT



Detecting Unknown and Insider Threats

As cyberattacks become more complex, these threats are harder to detect. Traditional rule-based approaches are ineffective against advanced threats because rule-based solutions generate thousands of false alerts.

Securonix UEBA tracks anomalous user behavior, suspicious lateral movements, and insider threats within your organization – whether in the cloud, or on-premises. Your team will gain cloud monitoring with built-in APIs for all major cloud infrastructures as well as many security and business applications. Additionally, our UEBA solution reduces noise by leveraging machine learning capabilities and out-of-the-box use case content so your team can focus on the highest-risk alerts.

Stay Ahead of Insider and Advanced Threats

Insider threats are always a risk, whether malicious or negligent. Traditional security solutions aren't able to identify behavior changes, making it harder to detect advanced and insider threats. They react after the damage is done or are blind to the fact that an attack even took place.

Securonix UEBA helps you mitigate the risk of insider threats. Our UEBA solution takes a more proactive approach by monitoring user and entity behaviors. It applies machine learning and analytics to assign risk scores against users' behavioral patterns. High risks users are flagged for the security team, so analysts can add them to a watch list or investigate their behavior further. Securonix UEBA alerts you of behaviors such as data exfiltration, privilege account abuse and misuse, compromised users, and botnet infections.

Reduce False Positives and Noise with Behavioral Analytics

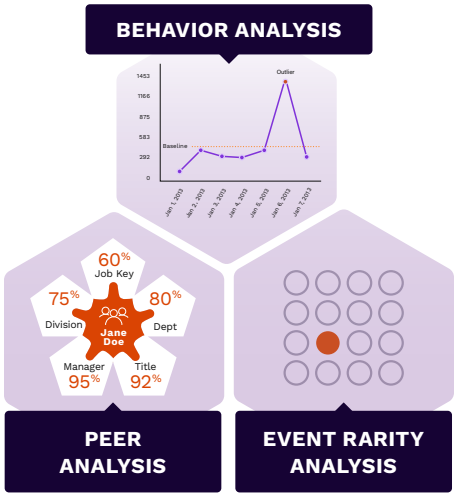
Many SIEM solutions generate a sea of false positive alarms that make it difficult to identify the actual threats in time to stop the damage. With Securonix UEBA, you find complex threats with minimal noise. Our solution helps correlate and identify threats that span across multiple events.

Detect Threats Faster

A single security alert without context or connection to related events isn't an efficient method to detect threats. Gain more efficiency and uncover threats faster using Securonix's threat chain models. Our threat chain models stitch together a series of events that are related. Instead of chasing multiple separate alarms, analysts receive one alarm with all the related events. Your teams can more rapidly identify complex threats using Securonix.

Use Advanced Analytics to Detect Sophisticated and Insider Threats

Understanding normal behavior versus abnormal behavior is critical to detecting insider threats. Securonix UEBA uses threat chains and advanced machine learning behavioral analytics to identify complex and insider threats.



THREAT CHAINS

Reduce the volume of alerts by stitching together related events to identify low and slow attacks. Threat chain models map to both MITRE ATT&CK and US-CERT frameworks.

BEHAVIOR ANALYTICS

Out-of-the-box analytics quickly finds complex threats with minimal noise. Our patented machine learning algorithms alert you to multi-level threats that deviate from established behavior baselines.

Maximize ROI on Your SIEM Investment

Upgrade without having to rip or replace your existing SIEM. Our solution's flexible technology stack allows you to easily upgrade your legacy solution by adding our UEBA analytics.

SIEM + UEBA

Securonix UEBA seamlessly integrates with any SIEM. We help you realize cost savings on your existing security investments without the need to replace your existing solution.

CLOUD-NATIVE

Our platform allows you to benefit from all the data in your IT environment with zero infrastructure to manage.

Realize Fast Time-to-Value

Securonix UEBA is a SaaS solution that can be deployed quickly, enabling faster time to value for detection and response. Our solution comes with out-of-box threat models, pre-built use cases, and built-in connectors that enable rapid deployment and helps your teams to identify sophisticated threats quickly.

PRE-BUILT USE CASES

Benefit from immediate, one-click access to content for insider threats, IP theft, fraud, and more.

BUILT-IN CONNECTORS

Built-in connectors allow you to investigate and respond to threats quickly, accurately, and efficiently within the Securonix UI. Over hundred built-in cloud connectors let you ingest data from a variety of sources across your hybrid infrastructure, giving you a complete picture of risk in your organization.

CLOUD CONNECTORS

Cloud Infrastructure

aws, Azure, CHEF, docker, GitHub, puppet

Cloud Data

box, Dropbox, SharePoint, hadoop, Office 365

Cloud Applications

Cerner, Epic, ORACLE, PeopleSoft, salesforce, SAP, workday.

Cloud Access Mgmt/CASB

FORGEROCK, netskope, okta, Ping Identity, RADIANT LOGIC, skyhigh

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