UserInsight

Monitor User Activity Across On-Premise, Cloud, and Mobile Environments

Security analysts have vast amounts of log data but few tools that provide insight into the actions users take across on-premise, cloud, and mobile environments. This masks a large number of threats including data being exfiltrated to cloud services or mobile devices and attempted access from unknown attackers.

Now in limited release, Rapid7 UserInsight helps you:

> **Gain visibility** into user behavior, including cloud services and mobile devices.

> **Improve incident response** by rapidly identifying which user took a particular action.

> **Determine** when users' credentials may have been compromised.

Comprehensive User Visibility

Only Rapid7 UserInsight provides visibility into user activity across on-premise, cloud and mobile environments. Traditional monitoring tools have focused on monitoring traffic between assets within the firewall but this paradigm is failing as more activity occurs outside the perimeter in cloud services or on user-supplied devices. In addition to tracking activity on traditional sources such as the firewall and web proxy, UserInsight deeply integrates with ActiveSync to monitor mobile devices and key cloud services such as SalesForce and Box. This means that you get visibility when users are accessing corporate resources even if they're not on a corporate network or are using their own devices.
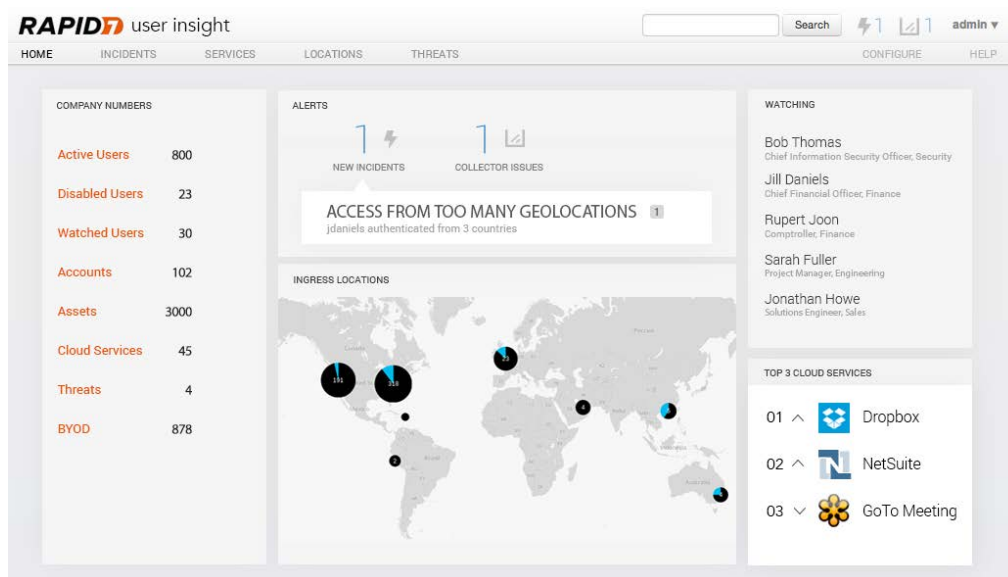
Key Benefits

> **Unify User Activity:** Security analysts get a full picture of a user's accounts, network activity, cloud services, mobile devices and network activity in one place, unifying information normally scattered across systems.

> **Map Access Activity:** Geolocate users and detect potentially malicious activity with visibility into where users access the network. UserInsight locates users based on where they access network resources, use monitored cloud services, or access mail on a mobile device.

> **Identify Cloud Services:** With one click, security analysts can see which cloud services are in use. This allows them to maintain control and create secure solutions to address business needs.

> **Validate Cloud Service Policies:** Easily identify when information may be shared outside of corporate policy by monitoring use of sanctioned and unsanctioned cloud services.

> **Reduce Investigation Time**: Security analysts can conduct more thorough investigations in less time by easily linking users and actions.

> **Alert on Suspicious Activity:** UserInsight alerts security analysts to potential indications of compromise by correlating activity across multiple systems.

> **Detect Mobile Device Risk:** With the vast majority of organizations permitting users to bring their own devices, security analysts need visibility into the number and types of devices connecting to the network.

> **Track Specific Threats:** Security analysts can monitor traffic to or from IP addresses and domains which they specify, enabling them to track potential threats and tie those threats to users.

Detect Compromised Credentials

According to the 2013 Verizon Data Breach Investigation Report, compromised credentials account for 76% of all network intrusions. Rapid7 UserInsight changes the game by monitoring the actions of users within the firewall and in the cloud to detect when their credentials may have been compromised. UserInsight is able to provide more accurate results by integrating external context and looking for patterns across the hundreds of thousands of users monitored.

Focused Incident Response

Determining which users were involved in a given incident causes significant lost time and ineffective incident response. Rapid7 UserInsight significantly increases the speed and accuracy of incident response through analysis of activity from key network components across on-premise, cloud and mobile environments. The unique focus on user activity enables security analysts to identify which user took a particular action and spot meaningful aberrations in that user's patterns of behavior.

Secure Cloud Deployment

Rapid7 UserInsight leverages secure cloud deployment to greatly simplify system maintenance compared to traditional monitoring tools. By leveraging cloud-scale data analysis, UserInsight automatically adjusts rules and thresholds, reducing false positives and enabling early detection of potentially dangerous anomalies.
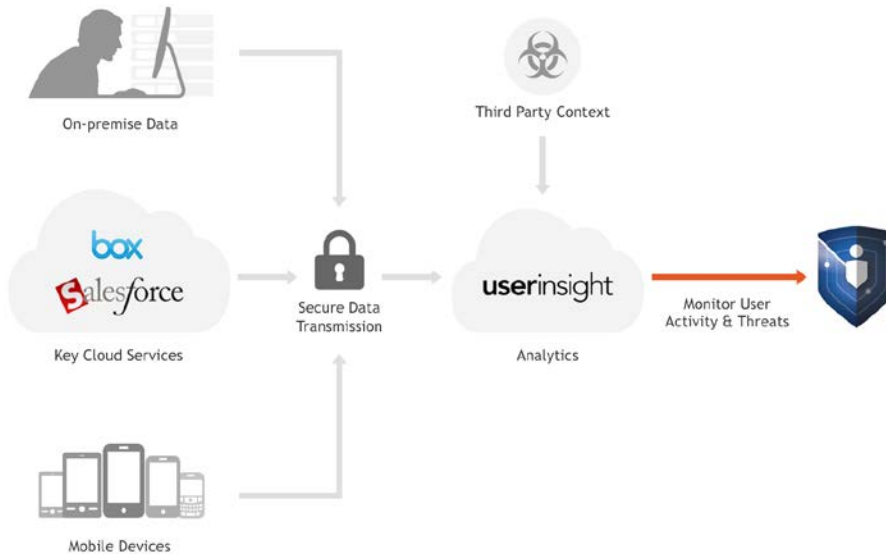
What Our Customers Say

"Monitoring user activity across on-premise, cloud and mobile environments helps to secure our environment today and into the future. We've been involved with UserInsight since the beginning and were able to use the beta version of the product to detect new things in our network."

– Robert Jones, Information Security Manager, City of Corpus Christi.

About Rapid7

Rapid7's solutions deliver visibility and insight that help you make informed security decisions, create credible action plans, and monitor progress. They simplify risk management by uniquely combining contextual threat analysis with fast, comprehensive data collection across your users, assets, services and networks, whether on premise, mobile or cloud-based. Rapid7's simple and innovative solutions are used by more than 2,500 enterprises and government agencies in more than 65 countries, while the Company's free products are downloaded more than one million times per year and enhanced by more than 200,000 members of its open source security community. Rapid7 has been recognized as one of the fastest growing security companies by *Inc. Magazine* and as a "Top Place to Work" by the Boston Globe. Its products are top rated by Gartner® and *SC Magazine*. For more information about Rapid7, please visit http://www.rapid7.com.