

insightUBA

Find the attacks you're missing

Rapid7 InsightUBA (formerly UserInsight) allows you to detect and investigate security incidents faster. It identifies intruders that use stealthy attack methods, such as stolen credentials and lateral movement. InsightUBA and InsightIDR are the only solutions that provide visibility into attacker behavior across your entire ecosystem, from the endpoint to the cloud.

Detect Stealthy Attacks

While defenders focus on advanced malware, attackers are using compromised credentials to impersonate regular users and laterally move across the network. 90% of organizations are worried about attacks using compromised credentials, but only 40% can detect these attacks today.* On top of that, security professionals are buried under hundreds of false-positive alerts, often generated by siloed point solutions. Instead of focusing on the perimeter, you need detection in depth, covering end-points, cloud services, and mobile devices.

With InsightUBA, you'll confidently detect security incidents before attackers cause damage. You'll be able to focus on what matters because you won't be distracted by false-positive alerts. InsightUBA correlates user behavior across your entire ecosystem so intruders have nowhere to hide. Best of all: By leveraging our knowledge of attacker behavior through our pre-packaged analytics, you'll no longer have to write, test, and maintain rules to detect attacks.

With InsightUBA you can:

- Detect stealthy intruder movement
- Eliminate alert fatigue
- Get endpoint visibility without "yet another agent"
- Set traps for intruders
- Put your threat intelligence to work
- Move at the speed of the attacker



33% of all reported incidents take more than a month and up to a year to discover.

-Verizon Data Breach Investigations Report 2014/15



62% of organizations receive more daily alerts than they can investigate from their SIEM alone.*

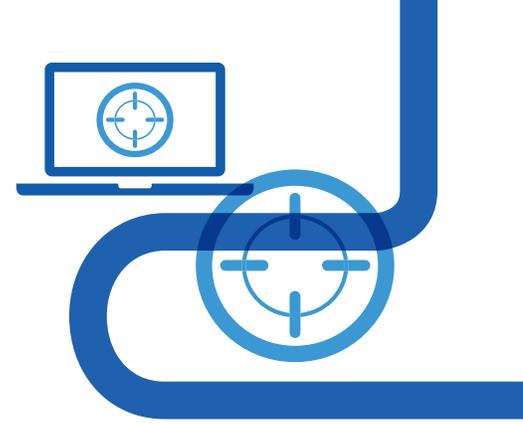


While 79% of companies allow the use of approved cloud services, only 33% have security visibility into those services.*

* Data from the Rapid7 2015 Incident Detection and Response Survey

"[InsightUBA has] cut our incident investigation and reaction time down by a factor of 20. [InsightUBA] allows us to quickly and easily assess where a user has been, what they've been doing, and what applications they've been running."

*Cameron Chavers, Manager, IT Risk Management,
Acosta Sales & Marketing*



Investigate Incidents Faster

Time is ticking when you have an attacker on your network, but incident analysis and investigation face some tough challenges. Investigating incidents requires specialized expertise that few team members possess, and it's hard to hire qualified staff. What's worse, incident investigation tools are not optimized to provide answers quickly, wasting valuable time. These challenges become harder as intruders mask as regular users, and it can take hours to understand even just a day of user activities.

With InsightUBA, your team will claim back your network as your home turf in the battle against intruders. You'll be able to pull together the entire team at a time of crisis to participate in investigations, without requiring highly specialized knowledge. By seeing all user activity at the click of a button, you'll quickly unmask intruders hiding behind user identities.

With InsightUBA you can:

- Investigate faster
- See user context for all activities
- Enable all team members to investigate an incident
- Keep years of data immediately available for analysis
- Pin your findings on a timeline
- Investigate phishing attempts

Expose Risky Behavior from Endpoint to Cloud

Users and even IT staff are not trained security professionals, so their decisions often run counter to security best practice. Users sharing passwords, the IT helpdesk setting passwords to never expire, or users uploading data to unauthorized cloud storage solutions put the company at risk. Unfortunately, most security teams have no visibility to influence this behavior.

With InsightUBA, you'll get visibility into risky configurations, such as users sharing account passwords, accounts that don't require regular password changes, and the use of cloud services. Exposing this risky behavior on your network enables you to influence behavior, remain compliant with regulations, and improve your overall security hygiene. This reduces the likelihood of an audit fail and impact of a data breach in your organization.

With InsightUBA you can:

- Discover user behavior across your entire ecosystem
- Bring analytics to your SIEM

- Add user context to monitoring solutions
- Identify risky user behavior
- Discover cloud usage and monitor strategic cloud services
- Watch application transaction authentications
- Get value in days, not months



Learn more about InsightUBA at
www.rapid7.com/products/insightuba