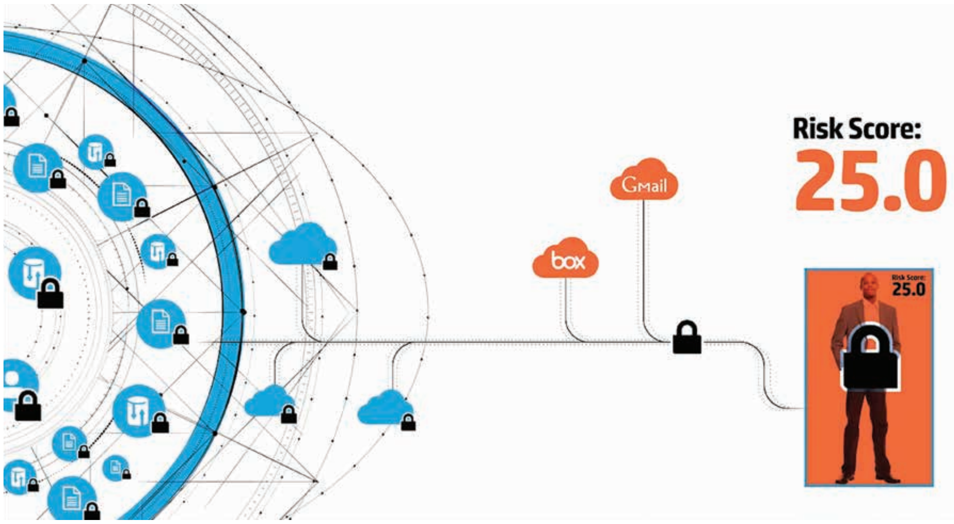
HPE Security ArcSight User Behavior Analytics



HPE Security ArcSight User Behavior Analytics (UBA) delivers insight into your highest risk users, aggregating activities and multiple indicators of compromise for users, peer groups and accounts. UBA detects unknown threats through data science techniques by creating baselines of normal user behavior and appropriate associations, identifying user and peer anomalies in real-time.

A users behavior and employment attributes are clear indicators for the motivation of a threat, enabling the security analyst to quickly determine whether a user is an insider threat or exhibiting account compromise. UBA can help organizations identify high risk data exfiltration, misuse of privileged and service accounts and detection of advanced, persistent threats.

UBA in conjunction with an installation of HPE Security ArcSight SIEM enables detection of advanced user based threats leveraging the same operational teams, data feeds and incident response processes already in place. This in turn drives investigation efficiency and operational savings.

Find the bad guys with advanced threat detection and reduce breach impact

By combining user identity management and access information with database, file, and all other user-centric activity, User Behavior Analytics can actively monitor the actions of privileged users for risky or unusual activity, lowering the risk and impact of cyber attacks by detecting unusual user behavior sooner. It includes advanced and targeted attack identification, identity correlation, insider threat identification and investigation, and privileged account misuse. This information is visualized in a useful way for the organization to find the bad guys faster.

Highlights

- Enhanced visibility of all user activity and processes.
- Streamlined investigations via comprehensive user activity reports.
- Boils down the most suspicious and abnormal activities, and transactions and access across users, accounts, systems, and applications to present risk-ranked threats.
- Detects the bad guys and insider threats, even if the bad guys are using legitimate credentials. Therefore, it can help detect breaches before significant damage occurs by finding the adversary faster.

Faster event resolution

Achieve faster event resolution with purpose-built security analytics and intelligence that mines, enriches, and transforms your SIEM information to produce actionable intelligence on known and unknown threats against the entire IT environment by providing detailed visibility into the user, mitigating threats before they occur.

Lowered monitoring and management costs

Achieve investigation efficiency by reducing noise, enabling organizations to have a unified look at the anomalous events, and prioritizing and scoring the critical alerts and users, thereby simplifying the alert management process and identity access management. Reduces time to investigate alerts and amount of staff required, as it is the only solution with user-behavior–based signatureless threat detection. User Behavior Analytics can detect bad actors and behavior, prioritize security alerts, reduce alert volume, and streamline alert investigations.

IP address to user mapping

Many logs for important systems like proxies do not record user behavior information but only IP addresses. Investigating user activity on those systems requires knowing which IP address the user had at a given time. User Behavior Analytics solves this problem by using identity correlation—a process that correlates data between addressing systems to attribute unauthenticated activity to individual users.

About Hewlett Packard Enterprise Security

Hewlett Packard Enterprise is a leading provider of enterprise security and compliance solutions for the modern enterprise that wants to mitigate risk in their hybrid environment and defend against advanced threats. Based on market-leading products from HPE Security ArcSight, HPE Security Fortify, and HPE Security—Data Security, the HPE Security Intelligence Platform uniquely delivers the advanced log and event correlation, application protection, and network defenses to protect today's hybrid IT infrastructure from sophisticated cyber threats.

Learn more at
hpe.com/software/userbehavioranalytics

f 🐦 in ✉

Sign up for updates

★ Rate this document

Hewlett Packard
Enterprise