SOLUTION BRIEF

FortiInsight User and Entity Behavior Analytics

Executive Summary

Identifying and responding to emerging threats from negligent and malicious insider sources remains a complex challenge for organizations. This is not a problem that can be ignored. Integrated into the Fortinet Security Fabric, FortiInsight user and entity behavior analytics (UEBA) minimizes insider threats using forensic machine learning. FortiInsight allows organizations to profile users, endpoints, applications, peer groups, files, and data movement for superior protection against internal threats.

Risk exposure from users within an organization—whether the behavior is intentional or inadvertent—can be a serious blind spot in terms of cybersecurity. But current regulations—such as the EU's General Data Protection Regulation (GDPR), the Health Insurance Portability and Accountability Act (HIPAA), the Markets in Financial Instruments Directive (MiFID), and International Organization for Standardization (ISO) regulations—can impose large penalties against companies that cannot document their ability to respond to actions that lead to security events or data breaches.

The **Fortinet Security Fabric** includes unique data security and threat detection capabilities that provide advanced threat hunting. Powered by endpoint monitoring and behavior analytics capabilities, this enables organizations to detect, respond to, and manage risky user behaviors that put business-critical data at risk.

FortiInsight Enhances Protection Against:

- Policy violations
- Unauthorized access of assets
- Data exfiltration and IP theft
- Compromised accounts
- Insider fraud

Protecting Data From Internal Threats

FortiInsight detects known and unknown threats, ranging from user error, to policy violation, to malicious insider activity, to compromised accounts or account takeover by malicious outsiders.

FortiInsight combines powerful and flexible machine learning with detailed forensics around user actions. This provides 360-degree visibility of activities around an organization's data (the who, what, where, and when) by monitoring user behavior and data movement—both on and off the network.

FortiInsight examines user behavior around data flow to spot unusual activity (such as users accessing files they do not normally seek out) or changes in work patterns, compromised accounts, or unusual peer-group actions. When anomalous behaviors are identified, real-time alerts are sent to relevant stakeholders for immediate investigation.

Key benefits in FortiInsight include:

- **Providing real-time insights around data flow and user behavior** without impacting system resources
- **Enabling rapid incident responses** through real-time processing and analysis of user behavior
- **Providing critical, centralized intelligence** via compliance reporting and investigation tracking
- **Eliminating false positives** via a rule-based engine that can spot potentially dangerous user behavior with high accuracy
- **Delivering comprehensive protection and deep forensic capabilities** by learning normal activities at the user, system, and network layers

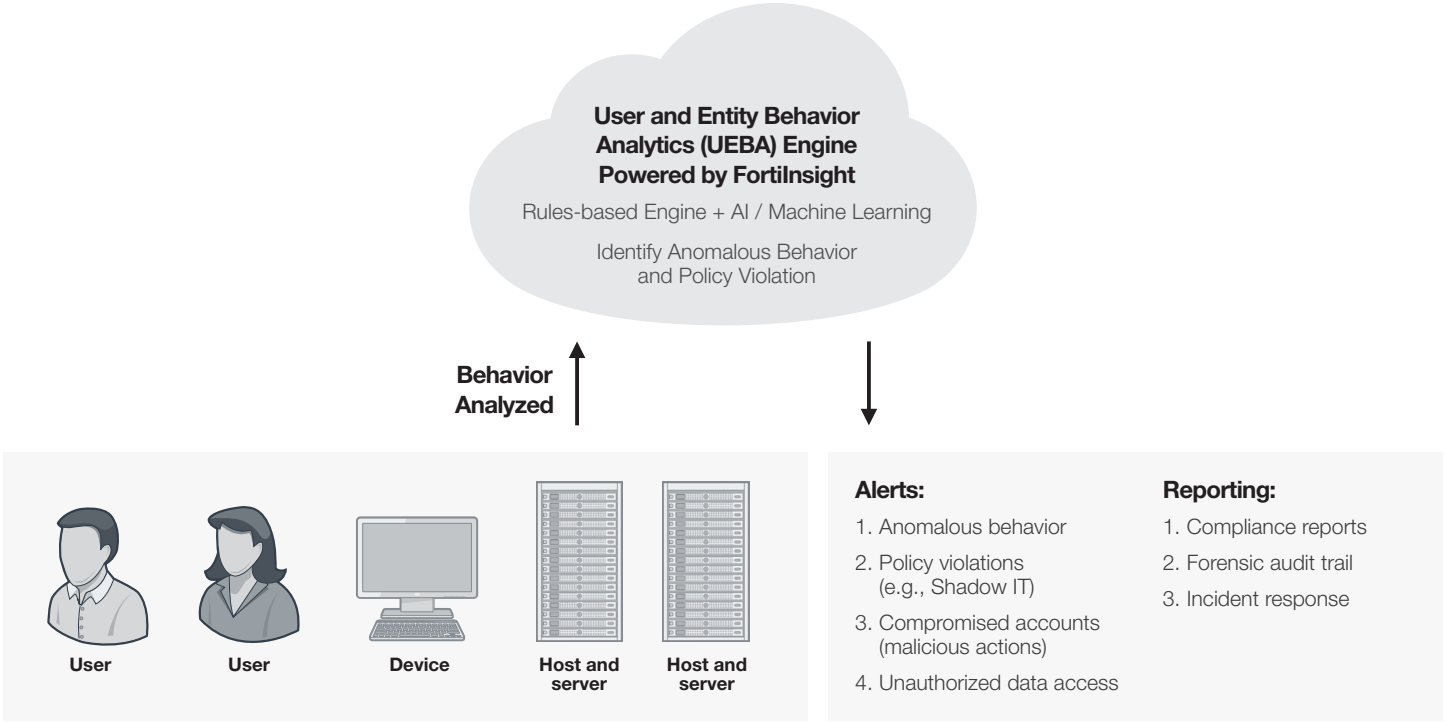

FIGURE 1: FortiInsight combines endpoint monitoring with behavioral analytics and is integrated into the Fortinet Security Fabric.

FortiInsight Solution Features

Integrated into the Security Fabric, FortiInsight incorporates real-time, actionable insights into anomalous user behavior around business-critical data. This enables comprehensive profiles of users, applications, peer groups, files, endpoints, and networks. Core capabilities include:

- **Endpoint and database connectors.** Gain complete visibility of data flow (both on- and off-network) via a lightweight stream of user and endpoint behaviors, across platforms and form factors. Track user access, data queries, and database changes in real time from Microsoft SQL Server databases.
- **Federated security.** Assign multiple usernames and passwords to different team members for alerts and incident response tasks.
- **Compliance reporting.** Dedicated reporting capabilities help maintain regulatory compliance such as GDPR and HIPAA.
- **Visualization and dashboards.** Zero-touch implementation of charts, graphs, and dashboards for custom visibility into user behaviors. FortiInsight pushes data to a centralized console. It provides key data around the user, processes, endpoint, type of resource (e.g., file, database, application), and behavior. There are no logs to collect and parse, and no delay before analysis.
- **Detailed forensics trail.** A complete record of all user and endpoint activities supporting rapid responses to potential or actual breaches; essential for effective incident response, casebuilding, and compliance obligations (e.g., the GDPR's 72-hour disclosure rule).

Protecting Networks—Inside and Out

Integrated into the Security Fabric, FortiInsight protects organizations from insider threats by continuously monitoring users and endpoints with automated detection and response capabilities. It automatically identifies noncompliant, suspicious, or anomalous behaviors (on- or off-network) and then rapidly sends alerts. By leveraging machine learning and advanced analytics, Fortinet's proactive approach to threat detection delivers additional protection and visibility across the entire enterprise network.

FORTINET

www.fortinet.com

March 1, 2019 8:52 AM

315542-A-0-EN

Macintosh HD:Users:mbunnell:Documents:Egnyte:Shared:CREATIVE SERVICES:Team:Michael-Bunnell:Solution-Brief:SB-fortiInsight-UEBA:sb-fortiinsight-ueba