Fortscale User Behavior Analytics

Insider threats, including attacks leveraging shared or stolen credentials, are responsible for the vast majority of costly data breaches. Even the most sophisticated enterprise security operations in the Fortune 2000 still struggle to find effective solutions.

Fortscale addresses this gap by detecting the unauthorized logins and activities of hackers and employees that conventional authentication systems miss. Fortscale ascertains when stolen but valid credentials are used to log in, and when legitimate users access resources that they shouldn’t.

Fortscale provides Fortune 2000 enterprises with an industry-leading user behavior analytics (UBA) platform for insider threats. The system collects authentication and access data from SIEM products and other critical applications within the enterprise, and applies an entity-level behavioral model that accurately identifies malicious activity and compromised accounts.

Fortscale is specifically optimized for analyzing user behavior associated with authentication and access of resources. And because Fortscale doesn’t use rules or static thresholds, it doesn’t produce the high number of false positives that other systems do. Fortscale learns the normal behavioral patterns of legitimate users, and constantly compares those patterns to behaviors obtained from a variety of logs and critical applications in order to detect abuse of user credentials.

Older UBA solutions rely on static rules and thresholds that make it very difficult, if not impossible, to interface with anything but the most common system logs and SIEM products.
But because Fortscale is application-agnostic and doesn’t use static rules or values to establish normal behavior, it can easily ingest data from almost any application and quickly baseline user behavior. Integration efforts are minimal compared to competing solutions.

Featuring an unrivaled machine learning engine, superior analytics capabilities, and context-based alerting, Fortscale empowers security analysts to identify threats faster and respond more effectively.

**Fortscale’s System Architecture**

Fortscale’s solution benefits from a highly advanced Hadoop-based architecture. This allows it to scale to meet the needs of the largest enterprise and be application-agnostic – all while hosting the most advanced machine-learning-based UBA engine on the market.

The Fortscale platform comprises several proprietary data processing units. These units control data collection, enrichment processes, advanced analytics engines, and investigation capabilities.
Data Collection

Fortscale taps into an enterprise’s existing centralized log system and processes both historic and current data to create user behavior baselines across the environment. Then, behavioral modeling, enrichment, and scoring engines analyze and compile the accumulated data, generating meaningful anomaly indicators. These indicators, representing potential security threats, are used to spawn security alerts for security analysts.

Fortscale digests logs from virtually any data collection solution (e.g., big-data repositories, Hadoop, SIEM/Splunk). A collection module receives structured and unstructured data that can either be streamed or batch-loaded, according to customer needs. Data can be loaded into Fortscale using a built-in syslog connector or using a destination folder monitoring service. These adaptive collection methods make Fortscale highly adjustable to new formats of access and authentication logs.

Fortscale is built to scale horizontally using its Hadoop infrastructure. This enables scaling up and supporting large numbers of active users and more data sources over time.

A standard deployment of Fortscale includes log ingestion of Kerberos authentication, SSH, and VPN (Cisco ASA, Juniper, F5, and more). In accordance with customer demand, CRM and other proprietary sub-system (enterprise applications) logs can also be ingested, preferably via SIEM/Splunk.

Supported Log Management Repositories: All major SIEM and log management solutions are supported, including:

- McAfee Enterprise Security Manager (ESM)
- IBM Security QRadar
- RSA Security Analytics
- HP ArcSight
- Splunk
Supported Applications and Authentication/Access Logs: The following enterprise applications and logon/authentication systems are supported:

- Kerberos authentication events
- SSH
- VPN
- CRM

Other Supported Enterprise Applications: Fortscale is not limited to working with a specific set of applications. It can work with any system that can provide logged transactions that contain the following attributes:

- User account name
- Action performed (log in, log out, request for resource, etc.)
- User location and destination addresses
- When the action took place (timestamp)

Enrichment – Enhancing Collected Data

Fortscale enrichment modules fuse definitive data within the normalized stream of events to provide more context for each event. Through enrichment, extracted entities identified in the raw data stream are associated to other entities, such as User ID with Machine ID. Static enrichment inputs, representing specific custom user groups, can also be integrated into the enrichment engine. Enriched events enable Fortscale to conduct complex modeling and scoring that make for more accurate and fine-grained anomaly detection.

Finally, integral statistical models are used to enrich the collected stream of log data. For example, Fortscale combines data from Cisco’s Identity Service Engine (ISE) with DHCP and Windows authentication events, enriching the data and enabling IP-address resolution for a wide range of secondary applications (locations, hostnames, etc.). Likewise, user and machine lists are imported from Microsoft Active Directory and similar user repositories to permit user-to-machine correlations. These correlations are an important key to creating baseline behaviors in later phases.
Enrichment Sources

- Cisco ISE
- Windows Logon Events
- Windows Active Directory
- DHCP
- DNS

Fortscale Analytics Engine

Fortscale has developed a highly advanced and unique anomaly detection engine that uses autonomous machine learning to provide optimized detection of abnormal user behaviors. Fortscale synthesizes the total rarity and risk of an event into a distinctive normalized score.

This score is based on three layers:

1. **Parameter-level modeling** - Fortscale’s algorithms model behaviors across a broad set of different parameters (IP addresses, transaction entities, locations, timestamps, etc.). Fortscale establishes baseline behaviors based on these parameters combined with historic data. For example, each user’s commonly used machines will be considered baseline and any deviation from this behavior, in the form of
anomalous machine access, might be considered a risk-scored event. If a behavior is highly anomalous for this user (e.g., this user never accesses any machines except his personal workstation), the risk score will be high. If this behavior is not anomalous (e.g., this user accesses many machines that are not his own workstation), the risk score will be low.

2. **Group-level modeling** - Using data-clustering techniques, Fortscale factors in the environmental rarity of a user’s activity relative to overall organizational activity. Fortscale then models baseline behaviors by observing machine usage patterns to determine if access to a particular machine was anomalous. For example, when a corporate resource usually used in the morning is accessed late at night, this might be considered an anomalous activity.

3. **Statistical modeling** - Statistical models help quantify deviations of events from an expected norm. Fortscale's overall risk score for a given user, entity, or event reflects the weight of deviations across multiple dimensions, synthesizing these into a unified final score reflecting threat level.

Fortscale's analytics algorithms were built to provide user behavior analytics for all network environments. All algorithms are designed to be application-agnostic, enabling quick adaptation and generic learning capabilities. Additional tweaks to scoring models can be made according to customer demands.

Finally, integral statistical models are used to enrich the collected stream of log data. For example, Fortscale combines data from Cisco’s Identity Service Engine (ISE) with DHCP and Windows authentication events, enriching the data and enabling IP-address resolution for a wide range of secondary applications (locations, hostnames, etc.). Likewise, user and machine lists are imported from Microsoft Active Directory and similar user repositories to permit user-to-machine correlations. These correlations are an important key to creating baseline behaviors in later phases.
Fortscale SMART Alert Generation

Fortscale contains a unique, consolidated alert-generation engine. This new aggregation and correlation mechanism transforms traditional event-risk scores into indicators of compromise. Indicators, both single and bundled, are compiled to form Fortscale Significant Multidimensional Anomaly Reduction Technology (SMART) Alerts. Unifying multiple anomalies and their supporting information into a single alert eases investigation, reduces incident response time, and simplifies response.

A SMART Alert is a consolidation of indicators, complete with the supportive information that merits further examination. An additional layer of machine learning that discovers anomalies among anomalies enables quick adaptive behavioral analytics in dynamic and frequently changing environments. Sorted by severity to reflect the security importance, SMART Alerts can be managed by the analyst, for further investigation and feedback.

- SMART Alert generation is based on a combination of statistical and machine learning algorithms that provide granular user behavior analytics, reducing false-positive ratios and identifying threats that can’t be found by other security solutions.

- SMART Alerts are based on identifying unique relationships between anomaly types. Thanks to SMART Alerts, Fortscale often identifies stealthy anomalies that wouldn’t have been detected otherwise.

- SMART Alerts improve over time; as more log data experience empowers the existing models, more accurate anomaly detection results are delivered.

Rapid Response Toolbox

Fortscale has several advanced capabilities that help security personnel rapidly see the full context of user actions and make efficient, appropriate decisions. These features include an alert-based dashboard with single-screen investigation, Fortscale SMART Alerts, numerous reporting functions, and more.
Investigation

Alert investigation and resolution features have been designed to make sure analysts have immediate access to relevant supporting information, in context, together with comprehensive graphs and quick-view filters. These capabilities allow analysts to make rapid and accurate decisions.

When performing deep incident forensics, analysts can research historic data. Built-in analytics packages encourage analysts to generate hypotheses and use Fortscale risk scores to validate or disprove an incident storyline.

An interactive analyst feedback interface helps ensure the alert-management process is optimized for maximal analyst effectiveness. It also enables analysts to determine and record resolution status, indicating if an alert was accepted, rejected, or left unresolved.

Fortscale’s investigation visualization framework enables large-scale visual data inquiries. Visualizations include scatterplots, bar charts, world maps, and more, with fully featured zoom, filtering, and exportation capabilities. Analysts can also export graphs and reports into CSV, PNG, JPEG, PDF, and SVG visual formats.
Reports

Fortscale provides sophisticated built-in analytics packages that enable instant visibility into suspicious user behaviors across the network. These reports give additional insights into historic anomalous behaviors across all data sources, and are always supported by contextual data.

Fortscale reports cover five categories of at-risk user accounts:

1. High-Privilege Users – Instant visibility into anomalous behaviors seen at administrator, executive, and service accounts.
2. Suspicious Users – A quick view of highest-scored events for every available data source.
3. External Accesses – Insights into unusual incidents based on geography and data usage patterns.
4. Device Accesses – A quick view of the highest scored events per end-point devices and sensitive resources in the network.
5. Stale Accounts – Behavior-based anomaly detections of stale user accounts (disabled users, inactive users, etc.).

Additional reports can be designed according to specific customer demands.
Enterprise Operational Workflow

Fortscale easily integrates into your everyday workflow. Scored events can be forwarded or exported for further consideration to other tools (like your SIEM system) as part of your enterprise’s existing standard operating procedures.

This enables security teams to prioritize their work and rapidly respond to threats with minimal disruption to their routines. Using Fortscale’s forwarding feature, intelligence regarding any given security incident can be seen within your existing SIEM system – maximizing your effectiveness and reducing staffing requirements.

Fortscale also enables selective data export via the following formats: CSV, PNG, JPEG, PDF, and SVG. This can dramatically improve research assignments and incident documentation.

Deployment

Fortscale is software-based. The solution is a self-contained installation on a RedHat server, but can also be deployed directly to a Virtual Machine. The system provides fully independent data storage and querying solutions using MongoDB as an online pathway and Hadoop as an offline pathway.

Product deployment is simple and quick. The machine learning engine is initially trained-up by ingesting and analyzing historical data – typically one to three months’ worth of logs. This establishes a baseline of normal user behavior and prepares the system for full operation.

When you’re ready to deploy, Fortscale will recommend specific hardware spec for your Fortscale instance, and our professional services team will work with you to install the software itself, as well as any adjacent systems you might need (such as Cloudera Hadoop).

Fortscale’s professional services team will also provide on-site training and ongoing support.
Summary

Fortscale helps security professionals stay focused and stay sane by automating some of the toughest parts of insider threat detection and investigation. Fortscale customers benefit from its user-centric approach to securing enterprise networks. SMART Alerts, single-screen investigation, responsive analyst feedback, and other features provide a tremendously effective set of tools for incident detection and response.

These capabilities, coupled with the capacity to integrate with virtually any system – including custom enterprise applications – make Fortscale a powerful weapon against insider threats.

For more information or to schedule a demo, please visit www.fortscale.com.