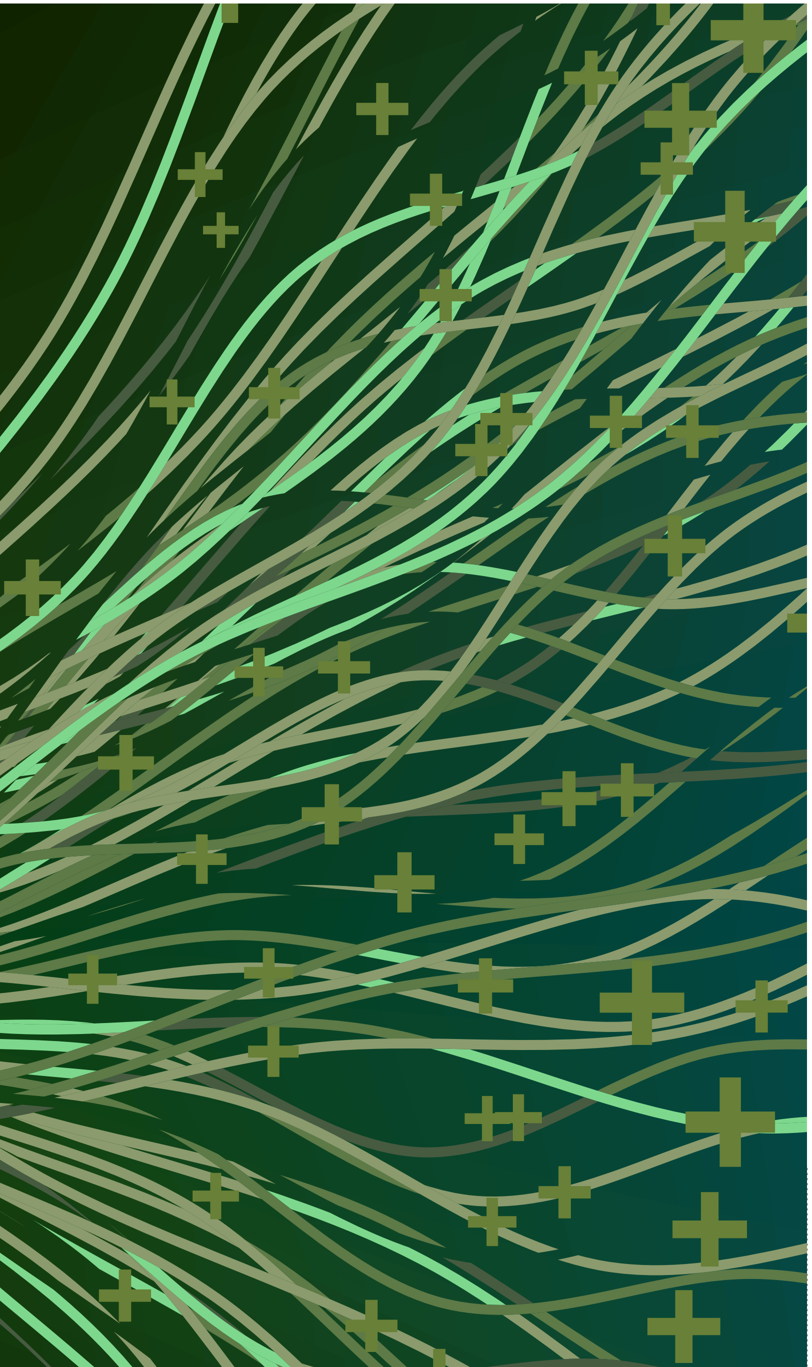


E-Guide

CONQUERING THREATS WITH USER BEHAVIOR ANALYTICS

TechTarget | SearchSecurity

Home

User behavioral analytics tools can thwart security attacks

User behavior analytics: Conquering the human vulnerability factor

THIS eGUIDE INTRODUCES user behavioral analytics tools that can help InfoSec pros determine what features they should consider before making a purchase. Read on to review both deployment strategies and reasonable performance expectations.

USER BEHAVIORAL ANALYTICS TOOLS CAN THWART SECURITY ATTACKS

Johna Till Johnson

As an information security professional, you've probably invested quite a bit of time and money trying to understand what's going on in your environment. You've deployed tools ranging from log management to security information and event management (SIEM) to security operational intelligence. And you're still struggling with the key question: How can I tell when something's happening in my environment that shouldn't?

Enter the new world of security user behavioral analytics (UBA). A host of emerging vendors, such as Bay Dynamics, ClickSecurity, GuruCul, Fortscale and Securonix, are deploying big data techniques to quickly baseline the performance of an environment and detect anomalies that indicate attacks. And existing vendors like Lancope, Solera and Splunk are extending their suites to deliver such capabilities, too.

This guide tackles reasonable expectations and deployment strategies for user behavioral analytics tools. You'll learn what you can expect when deploying such tools and how they integrate into your existing environment.

USER BEHAVIORAL ANALYTICS EXPLAINED

If you attended the recent RSA security conference, you probably heard the new buzz phrase user behavioral analytics. The use of analytics is at the forefront now in security architectures, as InfoSec professionals are increasingly encountering the needle-in-a-haystack problem: Security systems provide so much information that it's tough to uncover information that truly indicates a potential for real attack. Analytics tools help make sense of the vast amount of data that SIEM, IDS/IPS, system logs, and other tools gather.

UBA tools use a specialized type of security analytics that focuses on the behavior of systems and the people using them. UBA technology first evolved in the field of marketing, to help companies understand and predict consumer-buying patterns. But as it turns out, UBA can be extraordinarily useful in the security context too.

HOW USER BEHAVIORAL ANALYTICS WORKS

UBA tools perform two main functions. First, they determine a baseline of "normal" activities specific to the organization and its users. Second, UBA tools quickly discern deviations from that norm that require further exploration. That is, they spotlight cases in which abnormal behavior is underway. That behavior may or may not signal a problem: InfoSec pros must investigate it and make that determination.

The big distinction between UBA and other forms of security analytics is that UBA tools focus on users (rather than events or alerts). In other words, UBA answers the question, "Is this user behaving anomalously?" rather than "Is this an anomalous event?"

The distinction is subtle, but important. An event may be benign in one context and prove nefarious in another. For example, an accountant accessing a tax system at midnight on April 14 may be behaving in a perfectly reasonable manner but not when he accesses that system on, say, August 14.

USER BEHAVIORAL ANALYTICS FEATURES

Although many companies are beginning to claim UBA capabilities for their products, there are a small but growing number of pure-play UBA providers.

Home

User behavioral analytics tools can thwart security attacks

User behavior analytics: Conquering the human vulnerability factor

These vendors' products all function roughly the same way: There's a core engine, running proprietary analytics algorithms, that takes in data feeds from existing sources and analyzes the data. The tools then display their findings in a user dashboard. The goal is to provide InfoSec pros with actionable information.

At present, these tools don't take defensive action themselves but merely provide security operators with the insight to determine whether action is needed. However, it's reasonable to anticipate the availability of tools integrated with firewalls and other defensive systems to enable automated response within the next 6 to 24 months.

The analytics algorithms are the "special sauce" that powers these tools. When assessing UBA products, InfoSec professionals should be sure to ask for the details of how these algorithms work. Other important differentiators between UBA products include the following:

- Data sources, which refers to the types of data the tool integrates with, including the supported formats (CSV, Excel, others) and types of log files (from routers, firewalls, VPNs, file systems, others). Ask about whether it comes preconfigured to integrate with other tools and its integration mechanisms.

Home

User behavioral analytics tools can thwart security attacks

User behavior analytics: Conquering the human vulnerability factor

- Partnerships, which provide a measure of the tool's plug-and-play ability with existing infrastructure.
- Timeframe and degree of automation of baseline establishment, which relates to whether the tool establishes the baseline in an entirely automated and dynamic fashion, or requires the user to tune and tweak it. Note that some tools make determinations based on just a few days of historical record; others can review weeks to months. Longer records tend to provide for more accurate baselines, because they can take into consideration seasonal variations such as the end-of-quarter close, tax season and Christmas sales.
- Time to results (TTR) refers to how quickly after initial integration the solution begins to produce actionable results. Note that this is not an obvious metric: A clear definition of "results" is required; a good one is "delivering previously unknown insights" following the initial configuration and establishment of a baseline.
- Dashboard flexibility concerns whether or not the UBA tool was designed with the assumption that the dashboard operator will be an InfoSec professional. Other UBA tools can be customized to provide business-level reporting.

- Delivery mechanism refers to how the tool is delivered. That is, providers typically offer an on-premises version of the product (either software-only or an appliance). Most vendors also offer, or are planning to offer, a cloud-based version as well. One major challenge with cloud products is that UBA tools require close integration with many data sources that companies consider proprietary or sensitive (e.g., HR feeds) and don't wish to expose this data to the cloud. However, in the next 3 to 5 years, even this sensitive data will increasingly move to the cloud, and so cloud-based delivery of UBA tools is likely to become more palatable to enterprises.

THE BOTTOM LINE

Gathering data isn't enough: You need to invest in tools that make sense of that data and that can find those critical indicators of a potential security breach—"needles in a haystack." UBA tools can effectively provide early indications of questionable behavior by users, systems and devices, and give InfoSec professionals valuable direction in determining whether there is a security problem that requires attention.

USER BEHAVIOR ANALYTICS: CONQUERING THE HUMAN VULNERABILITY FACTOR

Kathleen Richards

The one-two punch of Edward Snowden caused security officers to spend more time monitoring “credentialed users” as the threat of additional privacy regulations and compliance loomed following the exposure of NSA’s widespread surveillance.

But in an ironic twist, the insider threat is one of the use cases drivingnew approaches to user behavior analytics (UBA), which enables on-premises security analysts to track individual data and activities with less heavy lifting than earlier technologies. What’s the difference between security analytics and these tools? These identity-based technologies focus on individuals first, monitoring their interactions and building baseline profiles to compare with historical behaviors and that of their peer groups. Most of these platforms are designed to track every user, not just those deemed high risk.

Whether it’s theft of sensitive data and intellectual property or accidental data loss caused by well-intentioned employees who have been socially

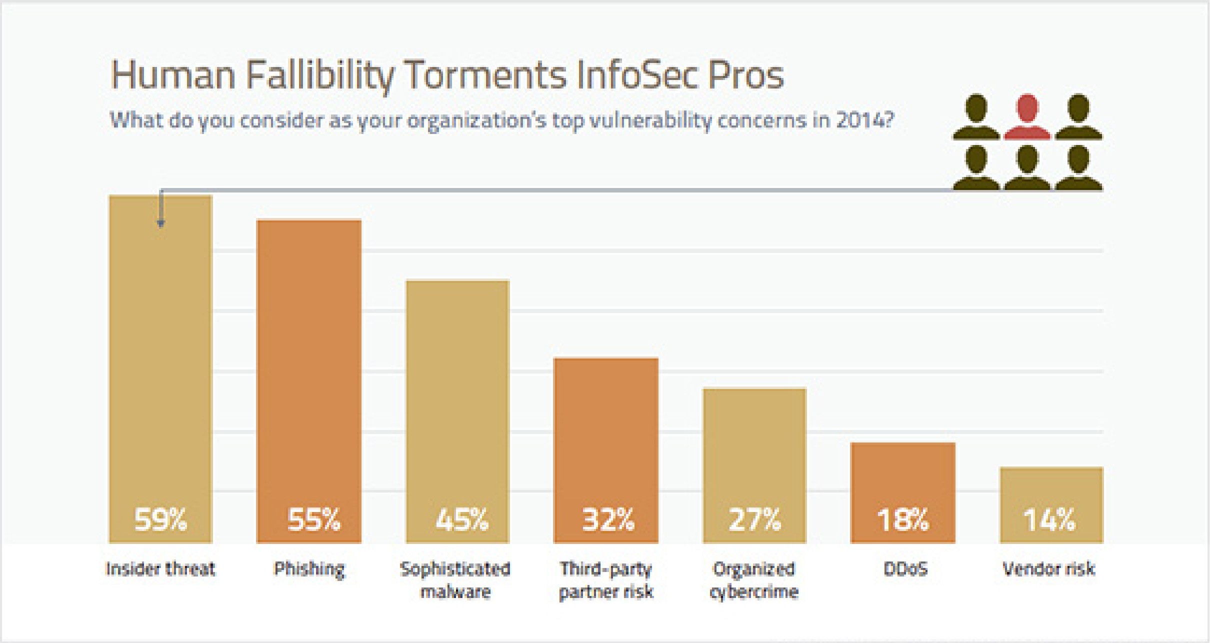
Home

User behavioral analytics tools can thwart security attacks

User behavior analytics: Conquering the human vulnerability factor

engineered, monitoring risky user behavior remains a top concern for senior security professionals.

According to a 2014 Wisegate member survey, insider threats topped the list of organization's vulnerability concerns at 59%, followed by phishing at 55%. Third-party partner risk ranked fourth, at 32% (after malware, at 45%). The senior IT and security professionals who were surveyed also reported concern about finding the staff to fight these threats.



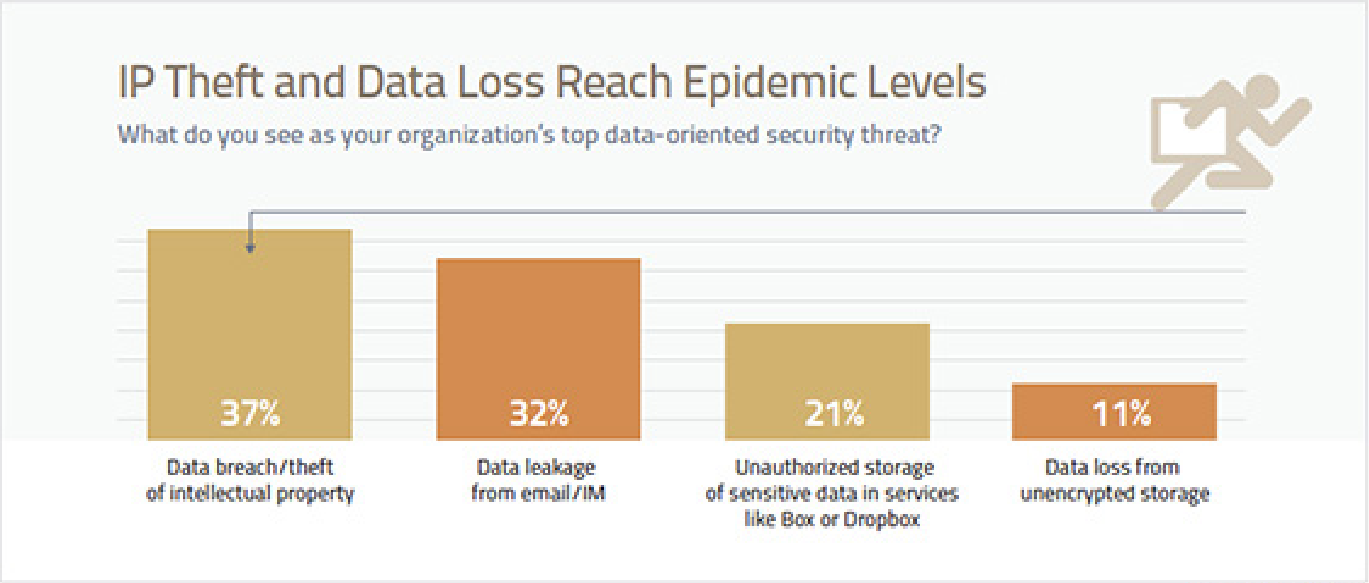
SOURCE: WISEGATE, APRIL 2014; RESPONDENTS COULD SELECT MULTIPLE CONCERNS

Home

User behavioral analytics tools can thwart security attacks

User behavior analytics: Conquering the human vulnerability factor

Insider threats range from current and former employees to contractors and business partners with authorized access to networks and critical data systems. They pose numerous security and fraud concerns for enterprises and their security officers, whether it's protecting the network against hijacked user credentials or ferreting out authorized users who take shortcuts for convenience like Dropbox or other shadow IT.



SOURCE: WISEGATE, APRIL 2014

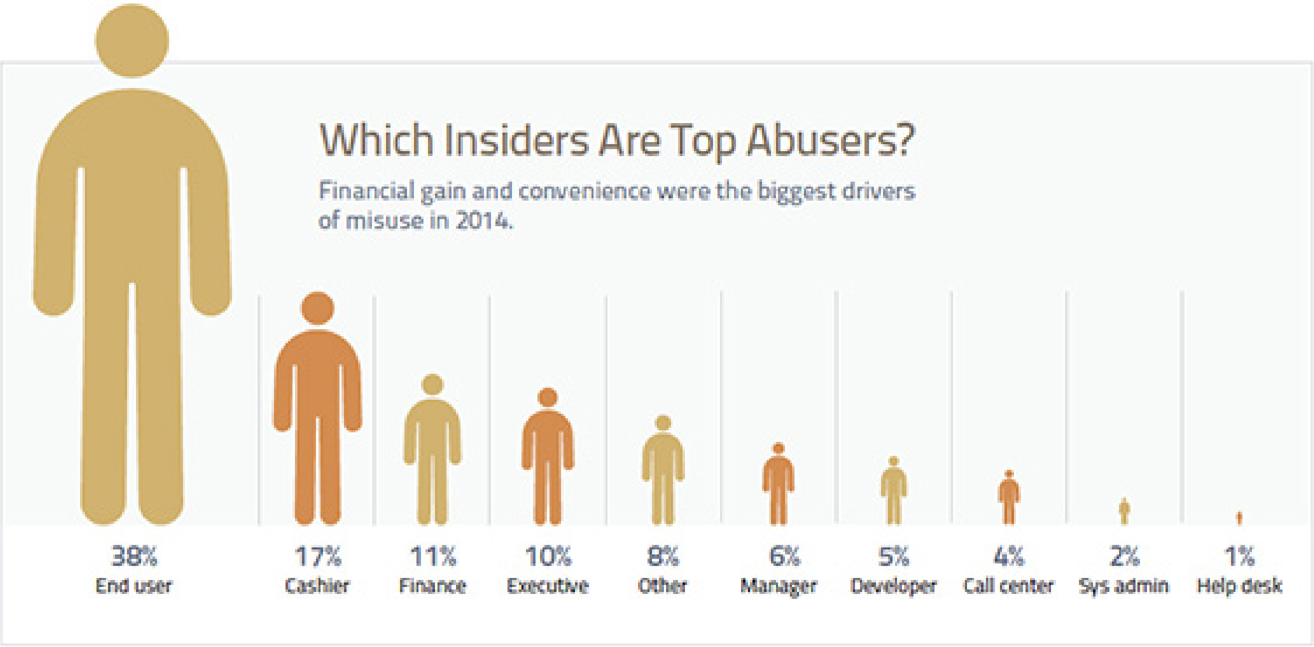
Some employees, such as Sergey Aleynikov, the former Goldman Sachs programmer, take IP with them when they leave the company. Undergoing his second trial for an alleged 2009 IP theft, Aleynikov is accused of copying source code for Goldman's high frequency trading platforms as he was exiting the company to join a startup, Teza Technologies. Part of his defense: He may have breached a confidentiality agreement but lifting code is not a crime.

While privilege abuse remained the "defining action of the internal actor breach" in 55% of reported incidents, as in past years, according to the 2015 Verizon Data Breach Investigations Report, organizations "saw more incidents involving the end user than ever before." Since 2011, "cashier" has topped the report's "Insider Misuse" list, but in 2014, end users ranked highest at 37.6%, followed by cashiers at 16.8% and finance at 11.2%. Executives ranked 10.4%. Financial gain and convenience were behind 40% of incidents, according to report. The insider abuse was usually discovered by forensic analysis of devices after users left the company.

Home

User behavioral analytics tools can thwart security attacks

User behavior analytics: Conquering the human vulnerability factor



N=125 SOURCE: VERIZON DATA BREACH INVESTIGATIONS REPORT 2015

TRACKING INDIVIDUALS

Enterprises have analyzed network, systems and traffic behavior for years. As security analytics continues to gain a foothold, some tools are building on centralized log management repositories by adding functionality aimed at pinpointing user behavior and anomalies in near real time and historical data. That's a substantial undertaking in terms of computational power and performance for companies with upwards of 100,000 employees and credentialed users.

“It has been tough to understand the user problem itself,” says Barry Shteiman, a security researcher who was appointed director of Exabeam Labs in April. (He formerly worked with the company’s founders at Imperva.) “Companies have followed two main paths: One was logging … ‘If I record everything that happens the incident is in there.’ The other side was ‘Let’s find patterns that we know of attacks and see if attackers fall into those traps.’ ”

The startup company is taking the data that is written by SIEM or other log management repositories and building a “brain on top of it” using machine learning and advanced mathematical algorithms to model behavior, according to Shteiman, who says: “Let’s build models that learn instead.”

Announced in June 2014, the Exabeam platform is already in production at several customers, including the Safeway supermarket chain. The on-premises software is designed for user monitoring and data exploration by security staff of all levels. Exabeam has patented its User Session Tracking technology, which offers a Facebook-like timeline to help security analysts.

While Exabeam’s approach is new, UBA systems have been around in various forms for at least a decade -- generally, customized vendor or user-driven modules that monitored structured data. Most UBA systems analyze historical data logs -- network, system and authentication logs that are collected and stored in SIEM systems and Splunk -- and patterns to develop individual behavioral profiles. The technology then generates a baseline for each employee in the enterprise. The user's behavior is monitored based on the individual's history and their peer group.

While SIEM offers some level of context-based activity monitoring, UBA platforms generally offer more advanced profiling and exception monitoring that is not tied into policy definitions and authorization rights in identity and access management (IAM) systems, according to Gartner, which covered UBA technology in an extensive report last August. Companies should review the user monitoring, profiling and anomaly detection functionality in their current SIEM systems before evaluating UBA platforms, say the report's authors.

"It is all based on what you do," according to Shteiman, who says Exabeam lets the data speak for itself. "There's no need to 'tune' what is being learned, like a lot of systems that are logic-based."

However, Gartner cautions that every UBA system requires some form of tuning, even those with canned analytics.

Home

User behavioral analytics tools can thwart security attacks

User behavior analytics: Conquering the human vulnerability factor

RISK SCORES AT THE USER LEVEL

Fortscale, with headquarters in San Francisco and R&D in Tel Aviv, Israel, is another startup in the UBA space that features advanced analytics that do not require customized rules or defined signatures. The company recently enhanced its on-premises UBA platform with application-level visibility. Security analysts are alerted to anomalous behavior of credentialed users who interact with enterprise software, including customized applications. These correlations are based on logins, resource-access patterns, content transfer (volume), time of activity, location and so on.

“Most modern attack models talk about attack chains,” says Guy Mordecai, Fortscale’s director of product management. “A lot of it focuses the attention on how attackers get their foothold. One thing those models don’t take into account is what if I already have user credentials. That’s when most of those attack chains are short-circuited.

“When we are talking about insider threats, it might be a contractor or an external attacker who is now trying to becoming an insider,” he adds. “Companies now need to know not just who logged in to the network, but what they did once they logged in.”

Home

User behavioral analytics tools can thwart security attacks

User behavior analytics: Conquering the human vulnerability factor

The company's self-contained Hadoop-cluster sits on top of SIEM or Splunk and uses machine-learning algorithms and contextual data (from IAM, accounts payable, human resources and travel systems, for example) to analyze logs and enrich them to build user profiles, monitor exceptions and create user risk scoring. Hadoop allows the technology to scale linearly and economically. It can also perform the batch operations quickly. The idea is to shorten incident response time and quickly pinpoint abnormal or suspicious behavior.

INSIDER ROGUE ACTIVITY A SURPRISE

Featured during an Innovation Sandbox presentation at the RSA conference in April, CEO and co-founder Idan Tendler said that the technology was finding stolen user credentials, but he was surprised that the majority of findings were users engaged in rogue activity (at their Fortune 1000 clients in industries such as finance, insurance retail and technology). "We find nosy admins; we find employees that were about to be terminated, to leave the company and started to dig into sensitive servers. Even if they failed we track them. We found employees -- call center representatives that dug into sensitive customer data at CRM applications -- and we helped the enterprise to stop that," he says.

"The benefits to the analysts are not only in pinpointing the bad users -- the bad employees inside the enterprise -- but also in making [their] workflow much faster, and much more accurate."

Fortscale is currently focused on visibility, but the company is interested in developing tools for policy and prevention, according to Tendler. Like other UBA technologies, the platform is designed for analyzing the data collected by SIEM or Splunk. If the data is not there, Fortscale "cannot do it today."

Like Exabeam, the Fortscale technology shipped in Q4 2014. The software is sold on a subscription basis in one-, two- or three-year contracts. Cost is primarily based on the number of accounts being monitored (priced per user), according to Mordecai. Typically, that's a six-figure investment, he says.

"Part of our challenge is to educate our users," says Mordecai. Some of the company's Fortune 1000 customers see UBA as a new discipline; even if they are highly skilled and have a lot of experience, they are not familiar with the user-centric approach. Fortscale has trained analysts as part of its team who work closely with customers so that they can drill down and efficiently use the software. The legal department is also involved at some clients, usually with regard to internal auditing and what kind of information must be mapped, he says.

In addition to Exabeam and Fortscale, some other vendors in the crowded UBA space include Bay Dynamics, Gurucul, IBM, Oracle, Secournix and even Splunk. HP introduced user behavior analytics to its ArcSight platform in April. But only a handful of vendors offer innovative approaches that detect advanced and insider threats.

Many companies are using UBA technologies “suboptimally” to investigate security or fraud events, according to Gartner. But analysts expect that to change over time with a greater focus on event detection and predictive analytics.

“We see 2015 as becoming the year of the user in cybersecurity,” says Mordecai.

FREE RESOURCES FOR TECHNOLOGY PROFESSIONALS

TechTarget publishes targeted technology media that address your need for information and resources for researching products, developing strategy and making cost-effective purchase decisions. Our network of technology-specific Web sites gives you access to industry experts, independent content and analysis and the Web's largest library of vendor-provided white papers, webcasts, podcasts, videos, virtual trade shows, research reports and more —drawing on the rich R&D resources of technology providers to address market trends, challenges and solutions. Our live events and virtual seminars give you access to vendor neutral, expert commentary and advice on the issues and challenges you face daily. Our social community IT Knowledge Exchange allows you to share real world information in real time with peers and experts.

WHAT MAKES TECHTARGET UNIQUE?

TechTarget is squarely focused on the enterprise IT space. Our team of editors and network of industry experts provide the richest, most relevant content to IT professionals and management. We leverage the immediacy of the Web, the networking and face-to-face opportunities of events and virtual events, and the ability to interact with peers—all to create compelling and actionable information for enterprise IT professionals across all industries and markets.