User and entity behavior analytics (UEBA)

User and entity behavior analytics (UEBA) is a valuable tool for detecting signs of malicious activity within your network.

UEBA monitors the activities of users and entities (such as hardware devices and networks) and compares present activity to "normal" or "baseline" behavior. Using advanced statistical analysis and, in some cases, machine learning algorithms, the aim is either to detect anomalous activity, which could be an indication of an intrusion or malicious "insider" actions, or to spot known malicious behavior patterns. As such, UEBA provides a layer of internal defense after preventive technologies have failed.

UEBA capabilities are increasingly being integrated into other security solutions, particularly security information and event management (SIEM) systems, i ntrusion detection and prevention systems (IDPS), and identity and access management (IAM) systems.

In late 2017, a Crowd Research Partners survey found that 38% of companies were using some sort of UEBA security solution, but the figure today is likely higher, as the market for UEBA technology is growing strongly. Despite 40% growth rates, Gartner expects UEBA technology to eventually be absorbed by other security solutions.

UBA vs UEBA

When looking at UEBA solutions, you may also come across the term UBA: user behavior analytics. So what is the difference between UBA and UEBA?

- **UBA:** When behavior analytics was first introduced, it was in the context of protecting data against theft by malicious actors, and the prevention of fraud perpetrated by malicious users who had access to and misused data. The focus was on analyzing how users interacted with data, hence the name user behavior analytics.
- **UEBA:** This term was first used by Gartner, because the use of behavior analytics very quickly went beyond monitoring users' behavior for data theft and fraud detection purposes. The term UEBA "recognizes the fact that other entities besides users are often profiled in order to more accurately pinpoint threats, in part by correlating the behavior of these other entities with user behavior," Gartner said.

What can UEBA do?

UEBA can protect your organization in a number of ways, including:

- **Spotting malicious insider threats**: UEBA can be used to spot anomalous or known malicious activity carried out by employees (and other authorized users such as contractors). It can also spot threats caused by genuine mistakes made by innocent employees.
- **Identifying advanced persistent threats (APTs) and targeted attacks**: These are notoriously difficult to detect because they usually involve exploiting previously unknown vulnerabilities and entail complex behavior that has not previously been identified as malicious. However, since they usually involve user or entity behaviors that deviate from normal baseline activity, UEBA can be used to flag them for more investigation.
- **Finding misuse of privileged accounts**: UEBA can monitor privileged accounts (which are prime targets for malicious actors because of their powers) to spot if they are being used in unexpected or unusual ways. This could include use by a non-privileged user, or spotting the collection and exfiltration or modification of large amounts of data or high-value data (such as credit card information).
- **Monitoring applications (including cloud-based applications)**: UEBA can help security staff see if any applications start behaving unusually, which could be an indicator that they have been compromised.

How UEBA works

At the most basic level, a UEBA system does two things:

1. **Data collection**: a UEBA system collects user and entity data from a number of different sources. These can include web proxy data, directory data, access logs, structured data access, network data, and even HR information, email and chat content, and building access card data.
2. **Data analysis**: the system then analyses the data using various techniques to learn normal behavior, spot unusual behavior, and recognize bad or malicious behavior.

The simplest way to analyze the data is to use simple patterns and rules to spot anomalous behavior. More sophisticated systems use statistical analysis, and the most powerful analysis techniques involve machine learning (ML). This can be applied in a number of ways:

- **Supervised ML**: this type of ML involves training the system by supplying it with sets of good or normal behaviors and sets of malicious behaviors. This enables the system to "learn" to recognize each type of behavior, and identify and flag bad behavior when it encounters it.
- **Unsupervised ML**: this type of ML is more general because the system builds up a view of what normal activity looks like by itself, and then alerts administrators if it spots abnormal behavior. It is then the job of the administrators or security analysts to decide if the abnormal behavior is actually malicious, perhaps as the result of a targeted attack, or simply unusual but legitimate.
- **Hybrid or semi-supervised ML**: here the system uses unsupervised ML to generate alerts of anomalous behavior, but the outcome of human analysis of the alerts is then fed back into the system to allow the system to learn over time.

Garter notes that building up a picture of baseline or normal behavior can be much harder than many organizations imagine for a number of reasons. These include:

- the behavior of privileged users, IT developers and others can be highly irregular depending on their job functions;
- a given user or peer group can be "bad" from the start of profiling so that ongoing bad behavior will not be noted as anomalous to the baseline.

UEBA in action

Here's one way UEBA can work. Imagine that a company has a developer named Bob on staff. Every morning, Bob logs in to the network around 8 a.m., sometimes from home and sometimes from the office. He first checks his email and the company collaboration platform. Then he spends most of his time each day writing code in his IDE, working within the company's cloud-based dev and test environments, and visiting development-related websites. He has access to many different corporate databases that are integral to the applications he is creating. He frequently works through lunch, but he always takes a one-hour lunch break at noon on Thursdays. And he usually logs off for the day around 6 or 7 p.m.

Then one day after Bob logs out at noon on a Thursday, he logs back in from home. And instead of checking his email or opening up his IDE, he goes straight to the database full of customer information and begins looking up specific names. He doesn't appear to copy or transfer any information digitally, but he does look up about twenty-five individuals, all of whom happen to be executives at Fortune 500 companies.

This type of activity is obviously a little suspicious. Maybe Bob just skipped his usual lunch date and is feeling a little nosy and needs some disciplinary action. Or maybe his password has been compromised and hackers are looking for data they can use to mount a spear-phishing attack against the company's customers. Or maybe an advanced persistent threat has paid Bob a lot of money to get them some information from the company database.

This type of behavior might go undetected by other security solutions, but UEBA solutions could spot it and flag it in real time or near-real time, allowing security personnel to investigate and respond very quickly.

Do you need UEBA?

Standalone UEBA systems are targeted at very large global organizations, and even in this group they are far from ubiquitous. The reason for this is that UEBA solutions are expensive to acquire, implement, maintain, and use, according to Gartner. Those companies that do own or are considering implementing UEBA systems generally have a compelling reason to do so, such as augmenting an existing SIEM solution or as part of a comprehensive insider threat protection program.

Outside of this group, the most likely reason that any organization will acquire UEBA technology is when it is added to an existing security tool such as a SIEM system as part of a product update.

How to implement UEBA

implementing a UEBA security solution is a major undertaking that is not for the faint of heart. Gartner's Market Guide for User and Entity Behavior Analytics points out that standalone UEBA tools are generally deployed on-premises or offered as a cloud-based service (with some requiring both).

Standalone UEBA vendors often require organizations to install appliances or deploy software for the core components of the solution, in addition to appliances (virtual or physical) for monitoring network traffic and endpoint agents.

Some have specific requirements around data platforms, such as requiring that data be sent to a standalone data lake managed by the vendor.

Alerts generated by standalone UEBA systems are generally presented in a proprietary UEBA console. These may warn of known malicious behavior, but more commonly they will flag suspicious behavior that warrants investigation.

Gartner recommends that when implementing a UEBA tool, start "small," with a narrow set of well-defined use cases and a limited set of data.

In any case, most companies that implement a UEBA solution find that it takes at least three to six months to get the system up and running and tuned (so that different log sources are given the correct weighting in the overall analysis) to deliver UEBA benefits.

UEBA market size

The market for standalone UEBA security solutions is experiencing explosive growth, with Gartner predicting that it will grow at a compound annual growth rate of 48% per year to reach in excess of $350 million by 2020. In addition to this, many companies will gain access to UEBA through other security systems.

The future of UEBA

The number of standalone UEBA vendors has decreased over the last year or so due to acquisition by bigger companies: Niara was acquired by HPE-owned Aruba, Balabit was bought by One Identity, E8 Security was acquired by VMware, and Fortscale was bought by RSA, to name a few examples.

Gartner expects this trend to accelerate, with the standalone UEBA market effectively ceasing to exist by 2021.

However, UEBA technology is not going to disappear in the near term. Instead, Gartner expects that core UEBA techniques and technologies will be embedded in 80% of threat detection and incident prioritization solutions. In the longer term, however, Gartner predicts that UEBA will be superseded by more encompassing security analytics technologies.

The most obvious destination for UEBA technology is in SIEM systems. Gartner predicts considerable convergence between the two, with all leading SIEM vendors already offering UEBA capabilities either by developing their own UEBA technology, integrating with other UEBA solutions, or partnering with a UEBA vendor. Some UEBA vendors such as Exabeam and Securonix have moved the other way, adding SIEM functionality to their feature sets.

Minimum features of UEBA products

What should a UEBA solution offer? This buying guide includes only standalone UEBA products. It is not comprehensive, but does include the majority of the best-known UEBA products currently on the market.

In order to be included in the buying guide, the UEBA solutions had to provide the following capabilities:

- Monitor and analyze the behavior of users and other entities
- Detect anomalous behavior that could indicate an insider attack or compromise of user credentials
- Use advanced analytics to detect multiple kinds of threats
- Offer the ability to correlate multiple anomalous activities that could be related to a single security incident
- Provide real time or near-real time performance

Top UEBA solutions

Solutions are arranged in alphabetical order, along with features we were able to obtain from vendor information. At the bottom of this article is a chart breaking down some of the features of these top UEBA products.

- Aruba
- Dtex
- Exabeam
- Forcepoint
- Fortinet
- Fortscale
- Gurucul
- Haystax Technology
- Interset
- LogRhythm
- Microsoft
- One Identity
- Palo Alto
- Preempt
- RSA
- Securonix
- Splunk
- Varonis
- Veriato
- VMware

Aruba Introspect

From Aruba (a Hewlett Packard Enterprise company), IntroSpect is an integrated UEBA and Network Traffic Analysis (NTA) solution that uses machine learning to detect, prioritize, investigate and respond to stealthy inside attacks that have evaded traditional perimeter-based security defenses.

Additional Features:

- Collects and analyzes everything from packets and flows to logs and alerts
- Detects gestating attacks from malicious, negligent or compromised users, IoT devices, and systems
- Machine learning models tuned for attack families such as ransomware
- Stops attacks by integrating with Aruba ClearPass NAC to automatically take policy-based enforcement actions (quarantine, port block, etc.)

Markets and use cases: Large organizations in healthcare, education, finance, legal, oil & gas, government, technology and retail

How Delivered: Appliance and software-only versions

Scalability: No limit

Throughput/Bandwidth restrictions: None, scales horizontally

Pricing: Based on number of entities monitored

READ USER REVIEWS

Dtex Enterprise

Launched in Australia in 2000, Dtex Systems now makes its home in San Jose. It has raised $15 million in funding from Norwest Venture Partners and Wing Venture Capital. Its UEBA platform is its primary product offering.

Additional features:

- Visualizations
- Dashboards
- Forensic audit trail
- Expert tuning
- Alert review

- Integration with third-party solutions available in Platinum edition

Markets and use cases: Corporate security operations teams

Delivery: On-premises software

Endpoints: Unlimited

Throughput/bandwidth limits: None; the Dtex collector sends around 1-2 MB per user to the server per day.

Pricing: The Dtex Signal product, which only provides visibility into user behavior, starts at $2 per user per month. The Enterprise and Platinum versions, which incorporate analytics, have quotes available on request.

READ USER REVIEWS

Exabeam Advanced Analytics

Now four years old, Exabeam offers a SIEM platform that integrates with its standalone products for log management, UEBA, incident response, querying and cloud integration. Headquartered in San Mateo, Calif., it has raised $65 million in funding, including a $30 million round that closed earlier this year. The company's lead investors include Lightspeed Venture Partners and Cisco Investments. According to the firm, Exabeam Advanced Analytics is "the world's most deployed behavioral analytics platform."

Additional features:

- Integrates with other Exabeam products and most SIEM products
- Accepts data from hundreds of different sources
- Patented session data model
- Risk scoring
- Ransomware detection and prevention
- Session timelines
- Alert prioritization

Markets and use cases: Any large organization. Exabeam has a special advisory board and programs for federal government agencies.

Delivery: Physical appliance or cloud-ready virtual machine

Endpoints: Unlimited

Throughput/bandwidth limits: None; scales horizontally

Pricing: Quotes available on request

READ USER REVIEWS

Forcepoint Insider Threat

Forcepoint claims that its user behavior monitoring technology has been protecting governments and other organizations for more than 15 years. It was previously known as Websense, which was founded in 1994. It was renamed Forcepoint in 2016 after Raytheon bought the company for $1.9 billion and combined it with the Raytheon Cyber Products and Stonesoft organizations. Forcepoint currently claims more than twenty thousand customers.

Additional features:

- Distributed architecture
- Daily consolidated risk scores for individuals
- Risk prioritization
- Customizable policies
- Visualizations
- Video replay of users' screens
- Timelines
- Forensics
- Agent-based

Markets and use cases: Corporate security operations teams

Delivery: On-premises software

Endpoints: Unlimited

Throughput/bandwidth limits: None

Pricing: Quotes available on request

READ USER REVIEWS

Fortinet FortiInsight

Fortinet's UEBA technology protects organizations from insider threats by continuously monitoring users and endpoints with automated detection and response capabilities. Leveraging machine learning and advanced analytics, FortiInsight identifies non-compliant, suspicious, or anomalous behavior and rapidly alerts any compromised user accounts.

Fortinet acquired ZoneFox, which was covered in an earlier UEBA guide, and that technology is an integral part of FortiInsight. When integrated with FortiSIEM as part of the Fortinet Security Fabric, it provides visibility into data activity and reduces the risk of insider threats or to compliance issues with the likes of GDPR and HIPAA. It includes endpoint behavioral monitoring of devices even when they are off the corporate network and any resources accessed. A rule-based engine identifies policy violations, unauthorized data access, data exfiltration, whether data is being moved to the cloud or onto a local USB device, and compromised accounts.

Additional features:

- Data streamed securely from the endpoint to the Fortinet data store
- 5-factor data identification model
- Lightweight Agent Based Protection
- Windows OS support
- Native file system drivers
- Forensics
- Network monitoring
- Federated security

Key markets and use cases: Security operations teams, especially banks, manufacturers and game developers.

Delivery: Hosted solution

Endpoints: Scales well: In 15 days inside one organization, it recorded 130,000 events, 6.4 million user actions, and detected three cloud services used by 16 users, five tools associated with hacking and 14 high-risk users making use of removable storage.

Throughput/bandwidth limits: Consumes less than 0.5% of CPU, 20 MB of RAM memory and 5 KB/s of network traffic.

Pricing: Licensed based on number of endpoints protected, whether the endpoint is a server, desktop, laptop, database server or SharePoint server.

READ USER REVIEWS

Fortscale

Fortscale specializes in user behavior analytics, specifically at analytics designed to counter insider threats. It offers two products: Fortscale UEBA for SOC, which is designed for companies to deploy in their security operations centers, and Fortscale Presidio, a UEBA engine that other security vendors can embed in their products. Founded in 2012 in Tel Aviv, Israel, it has raised $39 million in funding, including a $7 million round that closed in February 2017. Key investors include Blumberg Capital, CME Ventures, Evolution Equity Partners, Intel Capital and Valor Capital Group

Additional features:

- Integration with DLP and other security solutions
- Multivariate risk scoring
- Smart alerts
- One-click investigation capabilities
- Alert forwarding
- Hadoop-based
- Darknet analysis
- Agentless

Markets and use cases: Security vendors, organizations of all sizes

Delivery: On-premises software (runs on Linux only) or embedded in other security solutions

Pricing: Quotes available on request

READ USER REVIEWS

Gurucul Risk Analytics (GRA)

Gurucul offers three different types of security analytics: UEBA, identity analytics and cloud security analytics. All are based on its Predictive Identity Based Behavior Anomaly Engine (PIBAE). Details about the company's financials are difficult to come by, but it was founded in 2009 by security veterans who had worked for identity management vendor Vaau, which was acquired by Sun Microsystems and then by Oracle. Its headquarters are in Los Angeles.

Additional features:

- Large library of machine learning algorithms
- Fuzzy logic-based link analysis
- Granular, self-tuning risk modeling
- Signature-less
- Modular architecture
- Transaction scoring
- Risk-ranked timelines
- Hybrid behavior analytics that incorporates UEBA and identity analytics

- Hadoop-based

Markets and use cases: Corporate security operations

Delivery: Appliance, virtual machine, cloud or bare metal

Pricing: Quotes available on request

READ USER REVIEWS

Haystax Technology Constellation Analytics Platform

Headquartered in McLean, Va., Haystax counts employees at many federal government agencies and financial institutions among its 50 million users. According to its website, it also "helped secure the last seven Super Bowls." Founded in 2012, it has raised just $4 million in funding, but it has already made three acquisitions: Digital Sandbox in April 2013, FlexPoint Technology in May 2013, and NetCentrics Corporation in August 2014.

Additional features:

- Integrated view of insider trustworthiness
- Bayesian analysis
- Low rate of false positives
- Collaborative visualization
- Threat alerting
- Asset cataloging
- Event monitoring
- Incident reporting
- Agentless

Markets and use cases: Federal government, financial industry, corporate IT security, public safety

Delivery: Software or cloud-based

Endpoints: Unlimited

Throughput/bandwidth limits: None

Pricing: Quotes available on request

READ USER REVIEWS

Interset

Based in Ottawa, Canada, Interset was previously known as FileTrek and offered cloud-based software for sharing and tracking enterprise content. Over time, the company developed big data analytics and security capabilities, and in 2014, it launched its Behavioral Analytics Platform. Today, the company is solely focused on security analytics and UEBA. It received $10 million in investment funding as Interset and $10 million when it was still known as FileTrek.

Additional features:

- Scalable to more than 250,000 users
- Used by multiple U.S. intelligence agencies
- Flexible, extensible analytics engine
- More than 200 machine learning models
- Integrates with most SIEM systems
- Hadoop-based
- Optional agent

Markets and use cases: Corporate security operations teams

Delivery: On-premises or cloud

Endpoints: Unlimited

Throughput/bandwidth limits: None (Bandwidth usage is very light)

Pricing: Available on request

READ USER REVIEWS

LogRhythm

LogRhythm UEBA detects known and unknown user-based threats via analytics, applying machine learning and scenario analytics to surface and prioritize critical events. This augments organizational security environments, functioning either as a standalone UEBA product or as an add-on to existing SIEM or log management solutions.

Additional features:

- Evidence-based starting points for investigation
- Scoring and prioritizing of risk associated with anomalous user behavior
- LogRhythm TrueIdentity builds comprehensive behavior profiles
- Automated user baselining and risk analysis
- Embedded security orchestration, automation, and response

Markets and use cases: Detection of insider threats, compromised accounts, privilege abuse and misuse, brute-force attacks, new privilege accounts, and unauthorized data access and exfiltration, especially in banking and finance, energy and utilities, healthcare, the federal sector, retail and hospitality.

Delivery: Appliance, software, cloud

Number of Endpoints: Up to millions of endpoints

Throughput/bandwidth limits: Can analyze hundreds of thousands of evidence points per second and store petabytes of data

Pricing: Begins at $115/Identity per year

READ USER REVIEWS

Microsoft Advanced Threat Analytics

In November 2014, Microsoft announced its acquisition of Aorato, a security intelligence startup based in Israel. Before its acquisition, Aorato had received $11 million in equity funding. In 2015, Microsoft added Advanced Threat Analytics to its Enterprise Mobility Suite and also made it available as a standalone product. Somewhat confusingly, Microsoft considers Advanced Threat Analytics part of its Cloud Platform, but the product is available only for on-premises deployment.

Additional features:

- SIEM integration
- Attack timelines
- Mobility support
- Organizational security graph
- Email alerts
- Deep packet inspection
- Agentless

Markets and use cases: Small businesses

Delivery: On-premises software

Endpoints: Hundreds of thousands supported

Throughput/bandwidth limits: None

Pricing: Quotes available on request and negotiable under various licensing strategies. Estimated price for a standalone license is $80 per user, $61.50 per operating system per year.

READ USER REVIEWS

One Identity Safeguard for Privileged Analytics

One Identity delivers identity governance, access management, and privileged account management solutions. One Identity Safeguard for Privileged Analytics identifies high-risk privileged users, monitors questionable behaviors and uncovers threats using user behavior analytics technology. It provides full visibility into privileged account users and their activities. Organizations can identify risky users, keep a constant lookout for new internal and external threats, and detect unusual privileged behavior. If suspicious activity is discovered, Safeguard enables IT security managers to take immediate action and be well positioned to prevent potential data breaches.

Additional features:

- Detect threats in real time
- Pattern-free operation
- Screen content analysis
- Behavioral biometrics
- Reduce Alert Noise
- Automated Response

Markets and use cases: Organizations having their privileged accounts targeted such as financial services, healthcare, utilities and government

Delivery: Appliance

Endpoints: The focus is on safeguarding a small number of privileged accounts rather than all endpoints.

Throughput/bandwidth limits: Each node can support thousands of hosts.

Pricing: Sold by number of users or number of systems.

READ USER REVIEWS

Palo Alto Cortex XDR

Palo Alto Networks developed Cortex XDR as a detection, investigation and response app that natively integrates network, endpoint and cloud data. It uncovers threats using behavioral analytics, accelerates investigations with automation, and stops attacks before damage is done through tight integration with existing enforcement points.

Additional Features:

- Targeted attack detection
- Malware and fileless attack detection
- Insider threat detection
- Risky user behavior analysis
- Malware, ransomware, and exploit prevention
- Automated alert investigation with root cause analysis
- Supervised and unsupervised machine learning
- Custom rule-based detection of attack behaviors
- Incident response and recovery
- Post-incident impact analysis
- Threat hunting
- IoC and threat intelligence searches

Markets and use cases: Security operations teams

Delivery: Cloud

Endpoints: Can scale to support a virtually unlimited number of endpoints

Throughput/bandwidth limits: Virtually unlimited throughput and bandwidth

Pricing: Based on the amount of data stored for 30 days

READ USER REVIEWS

Preempt

Although founded in 2014, Preempt only emerged from stealth in the summer of 2016. It refers to its UEBA product as a "behavioral firewall," and it also offers an authentication solution and a free password health inspector. The company has raised $10 million in funding.

Additional features:

- Automated responses to alerts
- User risk scoring
- Multi-factor authentication capabilities
- Event triage and prioritization
- Incident response
- Forensic analysis
- Reduced alerts
- Integration with other security solutions

Markets and use cases: Corporate security operations teams

Delivery: On-premises software

Pricing: Quotes available on request

RSA NetWitness UEBA

RSA NetWitness UEBA is a purpose-built, big-data driven, user and entity behavior analytics solution integrated as a central part of the RSA NetWitness Platform. By leveraging unsupervised statistical anomaly detection and machine learning, it provides detection for unknown threats based on behavior, without the need for analyst tuning.

Additional Features:

- Leverages user, network and endpoint behavior profiling
- Detects abuse and misuse of privileged accounts, brute force attacks, account manipulation and other malicious activities
- Requires no customization, ongoing care, or rule authoring, creation or adjustment

Markets and use cases:

- Key markets include financial, retail, local and federal government, higher education and critical infrastructure

- Use cases include insider threat, brute force, account takeover, compromised account, privilege account abuse and misuse, elevated privileges, snooping user, data exfiltration, abnormal system access, lateral movement, malware activity and suspicious behaviors.

Delivery: Appliance and virtual formats

Endpoints: 100,000 users per server

Throughput/bandwidth limits: As above

Pricing: Based on the total number of employees that have corporate network access. For example, 1,000 to 2,500 users are licensed at $1.50 per user per month, with pricing dropping to a fifth of that for large deployments.

READ USER REVIEWS

Securonix Bolt

Securonix's most recent product, its SNYPR Security Analytics Platform, incorporates SIEM, UEBA and fraud detection capabilities. However, the company also offers a standalone UEBA solution called Bolt. The company was founded in 2008, and has offices in Addison, Texas; San Francisco; Jersey City, N.J.; Los Angeles; Atlanta, Georgia; Vienna, Va.; the UK and India. Securonix says one-third of the Fortune 500 companies use its products.

Additional features:

- More than 1,000 one-click deploy threat models
- 350 connectors
- Visualizations
- Investigation and response capabilities
- Fraud reporting
- Trade surveillance
- Patient data analytics
- Threat Model Exchange library
- Predictive and adaptive learning
- Integrates with SNYPR Security Analytics Platform
- Agentless

Markets and use cases: Corporate security operations teams, especially very large enterprises

Delivery: On-premises software or cloud-based

Pricing: Quotes available on request

READ USER REVIEWS

Splunk User Behavior Analytics

Although best known for its log monitoring and analytics solution, Splunk also offers a Hadoop-based UBA solution. Founded in 2003 to support the open source Splunk software, the company now claims more than 13,000 customers, including 85 of the Fortune 100. It is publicly traded under the NASDAQ symbol SPLK, and in 2016 it reported $950 million in revenue. Splunk employs more than 2,700 people and has its headquarters in San Francisco.

Additional features:

- Security dashboard
- Hadoop-based
- Multi-dimensional behavior baseline
- Integration with Splunk Enterprise and Splunk Enterprise Security
- Anomaly exploration
- Agentless

Markets and use cases: Corporate security operations teams

Delivery: On-premises software or as an AWS service

Endpoints:500,000 on a single node (additional scaling possible with additional nodes)

Throughput/bandwidth limits: None

Pricing: Quotes available on request

READ USER REVIEWS

Varonis DatAlert

Founded in 2005, Varonis offers a variety of data management, governance and security products, including its UBA offering called DatAlert. Its focus is primarily on securing companies against insider threats. In its startup days, Varonis raised $28.79 million from equity firms before going public in 2014. Its stock is now traded on the NASDAQ market under the symbol VRNS. In 2016, it reported $164.5 million in revenue. The company headquarters is in New York.

Additional features:

- Predictive threat models
- Security time machine
- Integration with other security solutions
- Web-based dashboards
- Alert scoring and prioritization
- Custom alert criteria
- Agents for some platforms, agentless for others

Markets and use cases: Corporate security operations teams

Delivery: On-premises software

Endpoints: Not applicable; UEBA occurs on servers rather than endpoints

Throughput/bandwidth limits: None

Pricing: Quotes available on request

READ USER REVIEWS

Veriato Recon

Headquartered in Palm Beach Gardens, Fla., Veriato specializes in employee monitoring solutions, including Recon, its UEBA product. Founded in 1998, the company was formerly known as Spectorsoft. It boasts more than 50,000 customers in more than 100 countries.

Additional features:

- Simple tuning
- Behavioral groups
- Alerting
- Integration with SIEM and other security solutions
- Psycholinguistic analysis
- Screen snapshots
- Keystroke recording
- Agent-based

Markets and use cases: Corporate security operations teams and HR departments

Delivery: On-premises software

Endpoints: 200,000 with a single instance

Throughput/bandwidth limits: None

Pricing: Quotes available on request

READ USER REVIEWS

VMware Workspace One

VMware Workspace ONE is an intelligence-driven digital workspace platform that securely delivers and manages any app on any device. By integrating access control, application management and multi-platform endpoint management, Workspace ONE connects siloed tools and teams to improve security of data, apps and devices. Additionally, it helps IT provide a seamless experience for employees who want instant access to all their apps – cloud, native, web and virtual – from anywhere on any device.

Additional features:

- Unified management for all endpoints
- Mobile device and app management
- Modern PC lifecycle management
- Device-aware access management
- Simple access to Win32 apps
- Engaging productivity apps

Markets and use cases:

- Unified Endpoint Management
- Simplified Access Management
- Modern Windows Management
- Intelligence and Predictive Security Across the Digital Workspace
- Virtual Desktops & Apps
- Especially popular with existing VMware users

Delivery: Cloud or on-premises

Endpoints: No limits

Throughput/bandwidth limits: None

Pricing: Starting at $3.78 per device and $6.52 per user

READ USER REVIEWS

UEBA product features comparison

Below is a chart comparing the 20 UEBA vendor solutions:

Top UEBA Vendors

UEBA Vendor	Use Cases	Special Features	Delivery
Aruba	High-risk and regulated industries	Integrated network traffic analysis	Appliance and software
Dtex	Security operations teams	Forensic audit trail	On-premises software
Exabeam	Large organizations, federal agencies	Ransomware detection and prevention	Physical appliance or cloud-ready virtual machine
Forcepoint	Security operations teams	Consolidated risk scores for individuals; video replays of users' screens	On-premises software
Fortinet	Banks, manufacturers and game developers	Monitors endpoints even when off network	Hosted solution
Fortscale	Organizations of all sizes; security vendors	Darknet analysis; DLP integration	On-premises software or embedded in other security solutions
Gurucul	Corporate security operations	Large library of machine learning algorithms; fuzzy logic-based link analysis	Appliance, virtual machine, cloud or bare metal
Haystax	Federal government, financial industry, corporate IT security, public safety	Integrated view of insider trustworthiness; low rate of false positives	Software or cloud-based
Interset	Security operations teams	Used by multiple U.S. intelligence agencies; more than 200 machine learning models	On-premises or cloud
LogRhythm	High-risk and highly regulated industries	Embedded orchestration, automation and response	Appliance, software and cloud
Microsoft	Small businesses	Mobility support; deep packet inspection	On-premises software
One Identity	Aimed at high-risk privileged accounts	Real-time threat detection, behavioral biometrics	Appliance
Palo Alto	Security operations teams seeking broad protections	The automated alert investigation, impact analysis, threat hunting	Cloud
Preempt	Security operations teams	User risk scoring; forensics; reduced alerts	On-premises software
RSA	Security operations teams seeking automation	Unsupervised anomaly detection and machine learning	Appliance and virtual formats
Securonix	Security operations teams, especially in very large enterprises	Fraud reporting; trade surveillance; patient data analytics	On-premises software or cloud-based
Splunk	Security operations teams	Multi-dimensional behavior baseline; anomaly exploration	On-premises software or AWS service
Varonis	Security operations teams	"Security Time Machine" analyzes past data; ransomware detection	On-premises software
Veriato	Security operations teams and HR departments	Psycholinguistic analysis; screen snapshots; keystroke recording	On-premises software
VMware	Security operations teams seeking broader app and device management	Integrates access control, application management and endpoint management	