# Critical Capabilities for Security Information and Event Management

Published 24 February 2020 - ID G00381141 - 52 min read

By Analysts Gorka Sadowski, Kelly Kavanagh, Toby Bussa

Security information and event management solutions keep evolving to address demands across a range of buyers and requirements. Security and risk management leaders responsible for security operations should use this research to evaluate and select the most appropriate solutions.

## Overview

### Key Findings

- SIEM solution capabilities and support, specifically for consumption models, architecture, analytics, user monitoring and operations, are increasingly varying across vendors.
- SIEM vendors are trying to solve, with varying degrees of success, the inherent complexities in deploying and operating SIEM tools. However, most SIEM solutions are still too complex for buyers with limited resources and expertise.
- Big data technologies as core components of SIEM solutions are starting to become table stakes — for example, Hadoop or Elasticsearch, which are now leveraged by most SIEM solutions.
- SIEM vendors have embraced security orchestration, automation and response (SOAR) via native capabilities, OEM and partnerships, or deeper integrations with leading SOAR vendors.
- Although most SIEM buyers continue to purchase on-premises software or appliance SIEM solutions, SaaS SIEM is gaining traction, and more SIEM tools are offered as SaaS SIEM only.

### Recommendations

IT security and risk management leaders responsible for security monitoring and operations:

- Focus your evaluation on the critical capabilities that align to their use cases (e.g., forensics, advanced threat detection and response), requirements, and current and future IT environments (e.g., on-premises versus cloud-based services).
- Improve response by leveraging new SOAR-type functionality that the SIEMs are providing natively before purchasing a dedicated SOAR.

- Give preference to SIEM solutions that can be consumed as a service to minimize overhead and management if you don't have complex, on-premises SIEM architecture requirements and are, or plan to be, a heavy user of cloud-based services.

## Strategic Planning Assumptions

By 2022, 50% of all SIEM tools will be cloud-native and delivered as a service from the vendor, up from 20% today.

By 2022, 75% of all SIEM vendors in the Gartner Magic Quadrant will offer advanced analytics features, as well as orchestration and automation features, up from 30% today.

## What You Need to Know

This document was revised on 2 March 2020. The document you are viewing is the corrected version. For more information, see the Corrections page on gartner.com.

Security and risk management leaders evaluating SIEM solutions *must* start by clearly understanding and describing their scope as well as their use cases, and then defining specific requirements from these inputs in conjunction with applicable stakeholders. These stakeholders should typically go beyond security and IT, and include such teams as audit, lines of business, legal and human resources. Additional factors to consider when evaluating SIEM solutions include:

- The scale and complexity of the deployment — for example, the types and locations of data sources in scope for distributed organizations or hybrid multicloud environments.
- Architectural considerations for deployment and consumption — for example, will the solution be deployed on-premises, in the cloud, via a hybrid approach or consumed as software as a service (SaaS)?
- Operational roles, such as use of internal resources versus service providers, and managed SIEM services
- Applicable compliance regimes and mandates, such as data retention and reporting requirements

Gartner recommends that organizations initiate any SIEM project with a clear understanding of their use cases (see "How to Build Use Cases for Your SIEM") to achieve long-term value from deploying a SIEM solution.

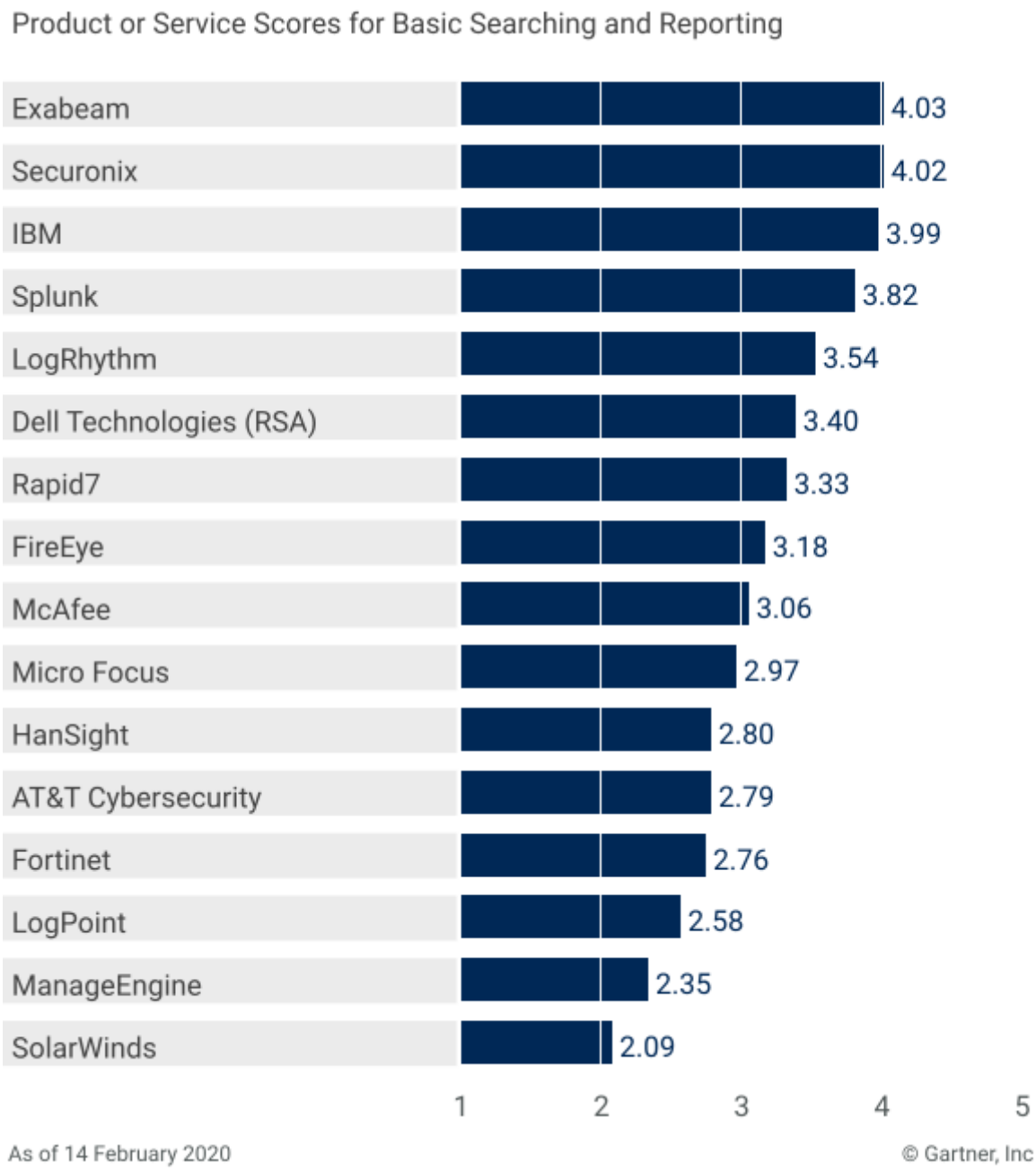
A phased acquisition and implementation approach, in which the most critical drivers and quick wins are implemented in the first phases and more-complex use cases occur in later phases, is also recommended. This will also allow the organization to rightsize its SIEM resources, both from a licensing and an operational costs perspective. This also requires being particularly careful with the selection and implementation of the foundational pieces.

Developing a multiyear, yet fluid, project roadmap for the SIEM solution's operation and expansion, with input from applicable stakeholders, aligned to the overall business direction as well as information security strategies, will ensure that any solution purchased remains fit for purpose. (For more information on SIEM deployments, see "How to Architect and Deploy a SIEM Solution"). Such a roadmap needs to be revisited regularly, typically after an audit or a significant incident, or as new laws and regulations are adopted. Finally, organizations need to evaluate the SIEM solution vendors' deployment and ongoing support capabilities, taking into account the resources and expertise available internally to the organization, and through the SIEM vendors and third-party service providers.

## Analysis

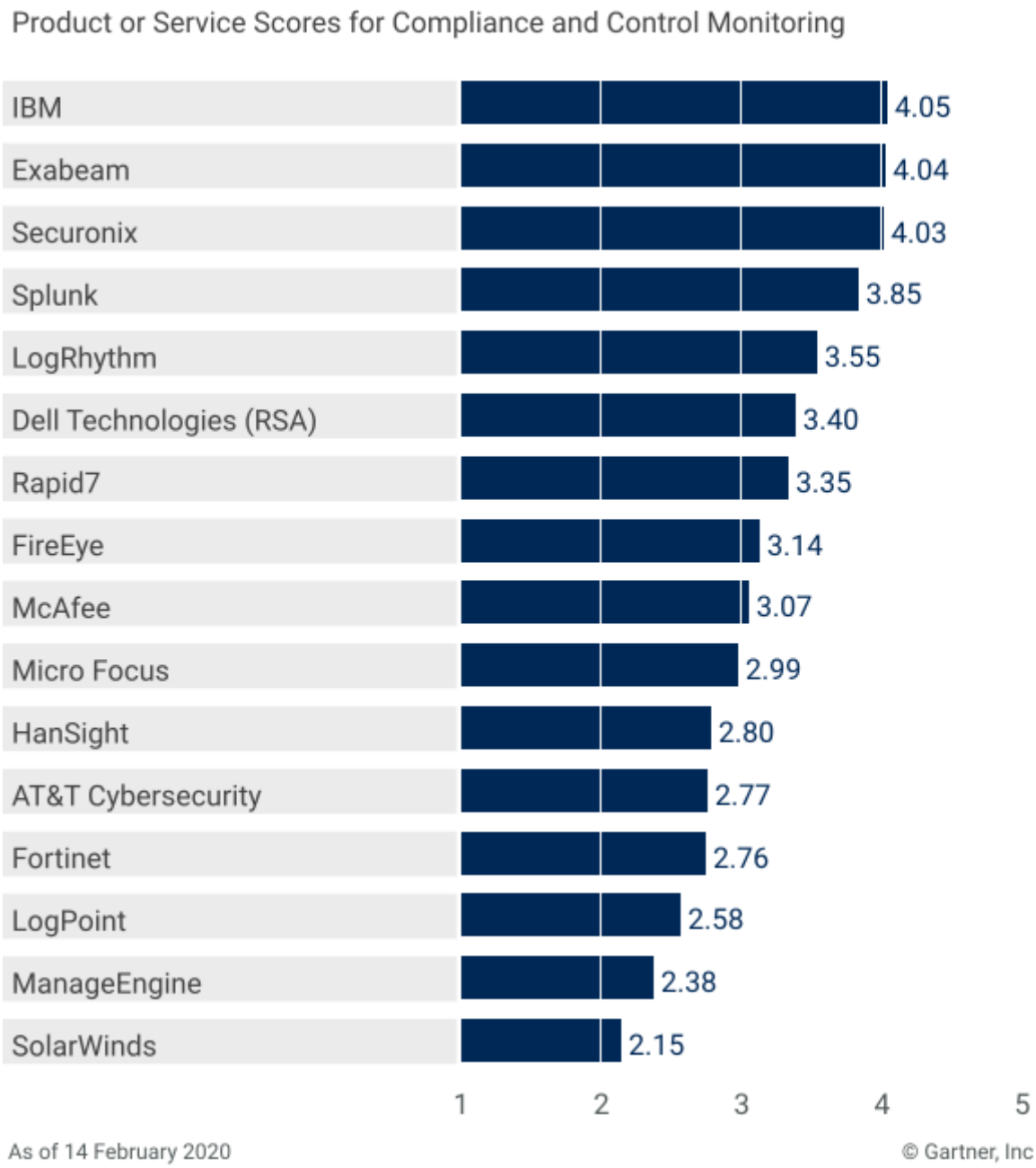
### Critical Capabilities Use-Case Graphics

**Figure 1. Vendors' Product Scores for Basic Searching and Reporting Use Case**



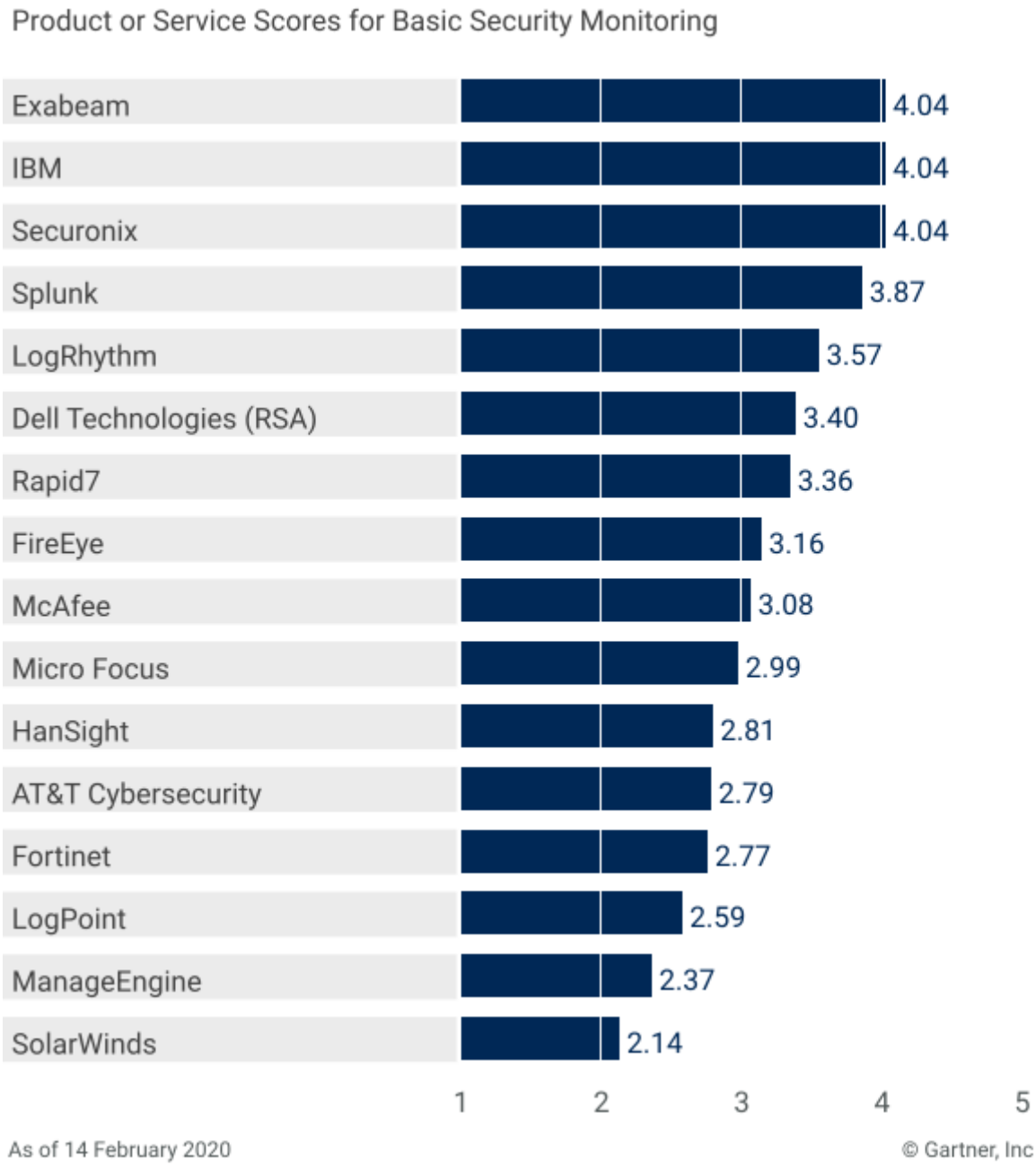

Source: Gartner (February 2020)

## Figure 2. Vendors' Product Scores for Compliance and Control Monitoring Use Case



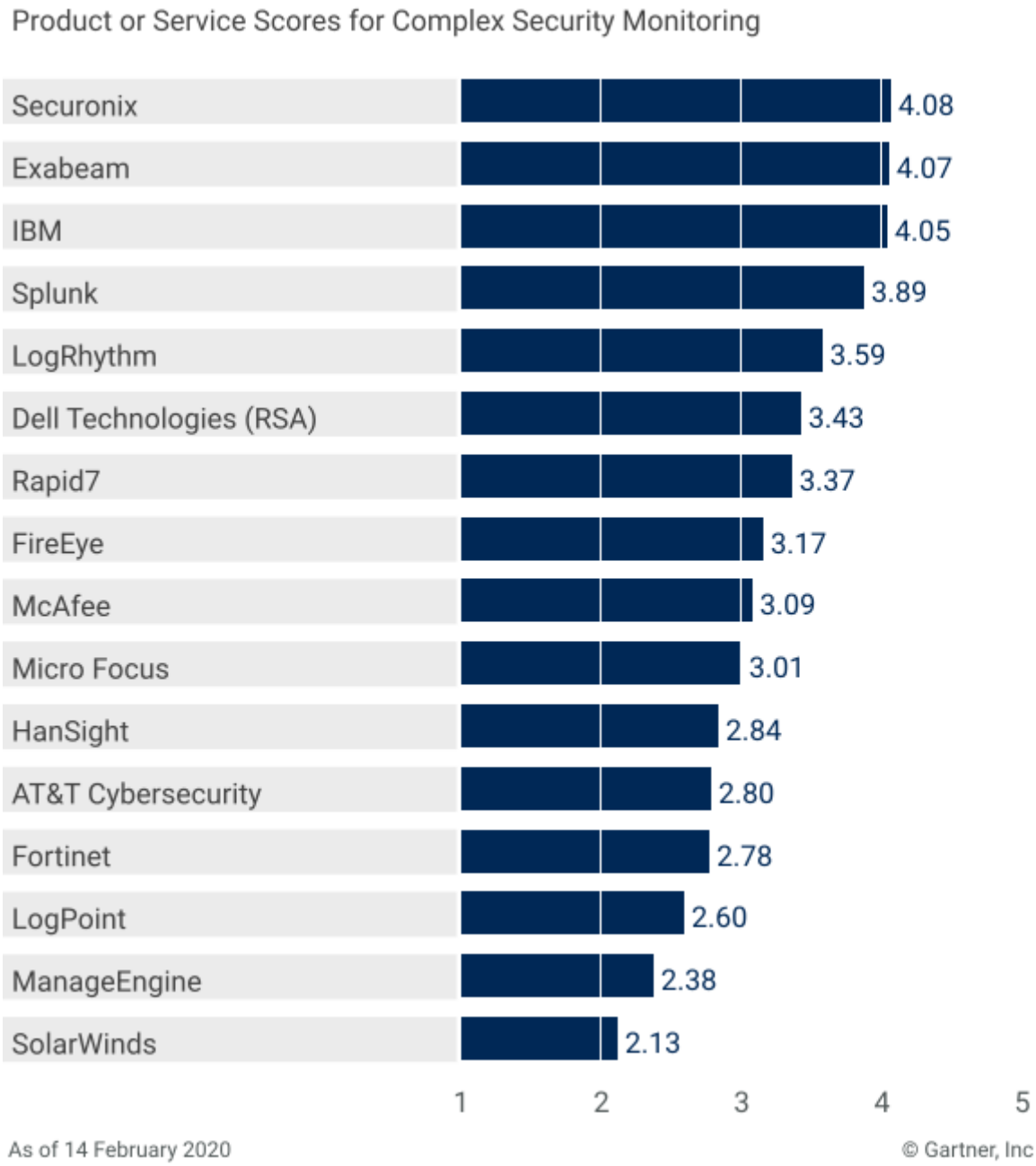

Source: Gartner (February 2020)

## Figure 3. Vendors' Product Scores for Basic Security Monitoring Use Case



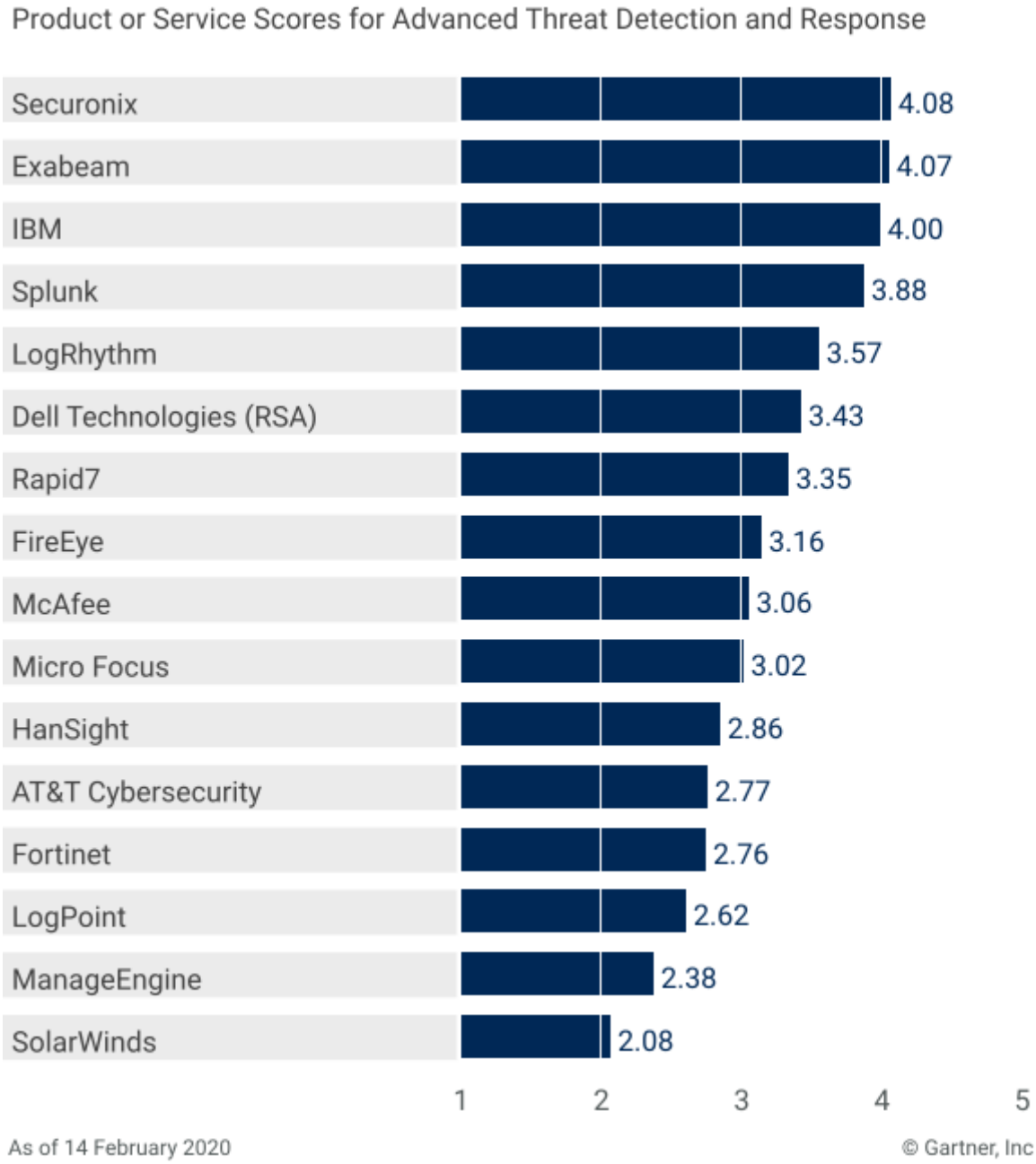

Source: Gartner (February 2020)

**Figure 4. Vendors' Product Scores for Complex Security Monitoring Use Case**




Source: Gartner (February 2020)

**Figure 5. Vendors' Product Scores for Advanced Threat Detection and Response Use Case**




Source: Gartner (February 2020)

## Vendors

### AT&T Cybersecurity

AT&T Cybersecurity, part of the AT&T Business portfolio, is headquartered in Dallas. AT&T Cybersecurity's SIEM solution is called Unified Security Management (USM) Anywhere, and is delivered as a SaaS SIEM from the Amazon Web Services (AWS) cloud. The solution includes several built-in capabilities, including asset discovery; vulnerability assessment; intrusion detection system (IDS) for network and cloud; and an endpoint detection and response (EDR) agent. The solution has an app framework that enables integrations with third-party security products for detection, automation and response. USM Anywhere also includes basic user and entity behavior analytics (UEBA) functions. Additional offerings include AT&T Alien Labs, which provides a threat intelligence subscription as part of the core SIEM product via the Open Threat Exchange (OTX) threat intelligence sharing capability. An on-premises software deployment, USM

Appliance, is still available and supported. Prospective customers should know that there is no feature parity between to two offerings.

USM Anywhere runs in AWS, and customers deploy data collection sensors as VMware or HyperV images, or templates for 13 supported AWS regions, Microsoft Azure or Google Cloud Platform. Integrations with SaaS solutions are provided via AlienApps. Country-specific data storage is available for the U.S., Ireland, Germany, Japan, Australia, the U.K., Canada, India and Brazil. The solution includes an optional EDR agent for Windows, Linux and Mac. Weekly updates to data collectors are managed by the vendor. EDR agents can autoupdate or be managed by customers.

Detections and alerting in the USM Anywhere platform are largely dependent on the real-time detection rules and analytics methods created and maintained by the vendor based on internally sourced threat research. All rules, response templates, algorithms and associated threat research are included in the solution. Alarms can be viewed in the context of a kill chain or the ATT&CK framework.

USM Anywhere pricing is generally based on data volume (GB per month).

### Dell Technologies (RSA)

RSA is a business within Dell Technologies, which is headquartered in Round Rock, Texas. RSA's NetWitness Platform (RSA NWP) is composed of a variety of components (versions introduced in April 2019 and reviewed for this research):

- RSA NetWitness Logs (version 11.3)
- RSA NetWitness Endpoint (version 11.3)
- RSA NetWitness Network (version 11.3)
- RSA NetWitness UEBA (version 11.3), with competencies derived from the acquisition of Fortscale in 2018
- RSA NetWitness Orchestrator (version 4.5 introduced in July 2019), an OEM of Demisto's SOAR solution

RSA NWP can be deployed in a variety of formats, ranging from software to physical and virtual deployments — on-premises and in public cloud services, such as AWS and Azure. It is flexible in how and where those components are installed to support simple deployments through complex, n-tier deployments across on-premises and cloud — infrastructure as a service (IaaS) — environments, as well as geographically distributed environments.

Various on-premises log and data sources, as well as contextual sources, are supported, in addition to common SaaS vendors (Office 365, Salesforce) and cloud service providers (CSPs; such as AWS, Azure and Google Cloud).

Decoders are used to collect logs and data, as well as perform analytics. Concentrators aggregate and index metadata. Smaller environments can use hybrid decoders/concentrators for collection and indexing. Event Stream Analysis is responsible for real-time analysis, correlation and notification. Archivers provide long-term data retention. All of these components are licensed together as part of a single SIEM SKU in the metered pricing model. RSA NWP Endpoint Insights is a free Windows and Linux endpoint agent to capture and forward endpoint logs, whereas the for-pay RSA NWP Endpoint agent has more EDR capabilities. RSA NetWitness Server is the single user interface (UI) into the solution. RSA NetWitness Platform Live is a cloud-based content distribution service. RSA also offers the for-pay NetWitness UEBA for advanced analytics, and NetWitness Orchestrator for SOAR capabilities.

RSA NWP pricing is generally based on data volume (GB per day).

### Exabeam

Exabeam is headquartered in San Mateo, California. Its SIEM, branded as Security Management Platform (SMP), is composed of seven products (version 2019.2 was introduced in February 2019 and reviewed for this research):

- Data Lake (version i31) for CLM-type functionality
- Advanced Analytics (version i48), a user-focused UEBA
- Threat Hunter (version i48), for forensics, investigations and searches
- Entity Analytics (version i48), an entity-focused UEBA
- Incident Responder (version i48), a workflow-automation-focused SOAR
- Case Manager (version i48), an incident response/case management platform
- Cloud Connectors (SkyFormation v2.4) from the SkyFormation acquisition for cloud coverage

Exabeam takes a module approach to its platform, where different solutions can be purchased individually and run in various combinations. Buyers seeking a SIEM solution will need to purchase Data Lake, Advanced Analytics and/or Entity Analytics (depending on the use cases), and Incident Responder. The platform leverages several big data technologies like Elasticsearch, HDFS, MongoDB, Kafka and Spark.

Exabeam SMP is available as an on-premises deployment or as a SaaS-based solution (Exabeam SaaS Cloud). SMP is offered as physical or virtual appliances. Docker container versions are also available. The solution can be deployed in IaaS, like AWS, Azure and Google Cloud, and hybrid options — through a combination of appliances and software installations — are supported. Exabeam also has partners to deliver managed SIEM on a per-customer basis. Multitenancy is supported via a combination of logical data segmentation and role-based access control (RBAC) controls. Content and integrations can be downloaded by customers and from the Exabeam community portal.

Exabeam SMP pricing is generally based on the number of employees in the organization.

### FireEye

FireEye is headquartered in Milpitas, California. FireEye's SIEM capabilities are delivered by its Helix platform, which integrates with other FireEye security solutions for email, network and endpoint that are sold separately. FireEye Threat Intelligence, supporting detections and threat hunting, and FireEye Security Orchestrator, for workflow automation, are also integrated into the Helix platform. The solution includes (at no added cost) virtual sensors to collect network metadata for monitoring. FireEye also offers services branded Expertise On Demand to provide support for tuning detection rules, investigating alerts and responding to incidents.

FireEye Helix is offered as a SaaS solution, deployed in multiple regions in AWS and managed by FireEye. Data collection is handled via one or more Communications Broker agents running on customer premises or in customer cloud environments. Helix orchestration capabilities are typically deployed on-premises to support integration with vulnerability scanning solutions. Several integrated FireEye security solutions also run in the cloud, but can be optionally operated on-premises, on physical or virtual systems. These solutions also include Communications Broker connectivity to Helix.

FireEye creates and maintains detection rules and analytics algorithms based on internally sourced threat research from Mandiant incident response engagement findings and threat intelligence services. Alerts are created by a combination of real-time rule matching and the postprocessing application of threat intelligence and indicators of compromise against events ingested by the platform. All rules, algorithms and associated threat research is included in the solution, and users can add rules to support additional use cases.

FireEye Helix pricing is generally based on data velocity (events per second [EPS]).

### Fortinet

Fortinet is headquartered in Sunnyvale, California. The Fortinet SIEM solution (version 5.2.1 introduced in June 2019 and reviewed for this research) is composed of the following components:

- Fortinet FortiSIEM
- FortiSIEM Advanced Agent (a for-pay, server-focused endpoint agent for Windows and Linux with some file integrity monitoring [FIM] and EDR capabilities)
- FortiGuard IOC (a for-pay threat intelligence subscription feed)
- FortiInsight (a for-pay pure-play UEBA tool derived from the ZoneFox acquisition)

Fortinet FortiSIEM is part of Fortinet's Security Fabric, which allows enhanced collaboration and integration between several of the vendor's portfolio solutions (e.g., Fortinet FortiSandbox) for additional, multitool use cases.

All FortiSIEM nodes can be deployed as virtual machines, and each component can be deployed on-premises or in a public/private cloud as long as the hypervisor is supported. For small installations, FortiSIEM can be deployed as a single virtual appliance with a local disk or as a hardware appliance (sold by Fortinet). As complexity and performance requirements grow, customers can scale vertically with bigger appliances, and/or can scale horizontally by adding Worker and Collector appliances (virtual or hardware).

FortiSIEM can manage most common on-premises data sources and cloud sources (although Google Cloud Platform, for example, is not supported), and can also ingest network flow data from firewalls and other network devices in the form of NetFlow version 5, version 9, IPFIX, sFlow, JFlow, and Cisco AVC, VPC Flow and Syslog.

FortiSIEM's distributed architecture consists of three kinds of nodes: Supervisor, Worker and Collector. An additional Report Server node is needed when integrating third-party business intelligence software with FortiSIEM. The Collector node discovers devices in remote locations, gathers events from these devices, parses and then preprocesses the events with enrichment, compresses them, and forwards them to the Supervisor or Worker nodes. Workers process and store events, and perform partial queries sent to the Supervisor. The Supervisor node processes the partial query/rule results from the Worker nodes to produce the final result. FortiSIEM clients can select between a proprietary FortiSIEM NoSQL event database or Elasticsearch for event storage, while the Supervisor node provides a single system database image to the user by unifying the Discovery and Event databases.

FortiSIEM pricing is generally based on the number of assets in scope (number of IP addresses).

### HanSight

HanSight is headquartered in Beijing, China. HanSight Enterprise SIEM (version 5.1 introduced in May 2019 and reviewed for this research) is the core product that is part of an ecosystem of solutions that includes HanSight UBA, HanSight NTA, and HanSight TIP (all also at version 5.1). Other solutions available within the HanSight ecosystem include vulnerability management, asset discovery and data loss prevention (DLP). HanSight does not have its own EDR and cloud workload protection platform (CWPP) tools, and instead has partnerships with several Chinese security technology vendors (e.g., 360 Total Security, Magic Shield and Qingteng).

HanSight Enterprise SIEM is available as software, as a hardware appliance (aimed at midsize enterprises) or as a per-customer hosted environment. There are five components that can be deployed in various configurations (all in one, individually, combinations) — Data Collector Clients, NTA, Central Management, Threat/Detection and Incident Management and Elasticsearch. Real-time analytics are performed by the Security Analytics Engine, while batch processing is handled through HanSight Query Language (HQL) search and the UEBA module called HanSight UBA. HQL can implement machine learning algorithms, and the HanSight Notebook allows more-advanced users to create their own machine learning in Python or Java.

HanSight Enterprise SIEM pricing is generally based on data volume (EPS).

### IBM

IBM Security is headquartered in Cambridge, Massachusetts. The QRadar Security Intelligence Platform (SIP; version 7..3.2 introduced in May 2019 and reviewed for this research) consists of QRadar SIEM and other separately priced components:

- IBM QRadar Vulnerability Manager provides vulnerability assessment.
- Network monitoring support in SIP includes IBM QRadar Network Insights for network flows, and the IBM QRadar Network Packet Capture appliance.
- QRadar Risk Manager monitors device configurations.
- IBM QRadar Incident Forensics provides investigation support.
- IBM QRadar Advisor with Watson provides automated research for threats and actors.
- IBM QRadar User Behavior Analytics (UBA) is a free add-on module for user-monitoring use cases.
- IBM Resilient SOAR, a solution that has supported bidirectional integration between Resilient and the QRadar SIEM solution.

In addition to these IBM QRadar components, IBM offers the Security App Exchange, with integrations developed by IBM and third parties.

QRadar uses a proprietary data store for environmental and event data. Alerts (offenses) are created by a combination of real-time correlation and baselining (vendor-provided and user-created or modified rules) and machine learning analytics to detect anomalous behaviors.

Deployment options include on-premises software, hardware and virtual appliance options (for most components), or deployed as SaaS by IBM via the QRadar on Cloud offering. Smaller deployments can be addressed in an all-in-one appliance, and larger deployments can scale horizontally with additional appliances.

IBM QRadar pricing is generally based on data velocity (EPS).

### LogPoint

LogPoint is headquartered in Copenhagen, Denmark. LogPoint SIEM solution is composed of the following modules (generally introduced in June 2019 and reviewed for this research):

- LogPoint Core SIEM (version 6.6.1)
- LogPoint UEBA (version 2.1.0)
- LogPoint Director Console (version 1.5.0)
- LogPoint Director Fabric (version 1.5.0)

- LogPoint Applied Analytics (version 2.0)

LogPoint can be deployed as an all-in-one virtual or hardware appliance running a hardened version of Ubuntu Linux 16.04 combining the Collector, Backend and Search head. Scalability is achieved via the use of larger appliances and/or additional Collector/Backend modules deployed in key locations. These collection instances parse, normalize, enrich, filter, route, compress and buffer event data. Larger and more complex deployment (e.g., federated model) will introduce LogPoint Director to manage the various components. LogPoint, through the use of NIFI, supports connections to query remote data lakes, including Hadoop and Elastic data stores. LogPoint utilizes Apache Lucene and NoSQL flat-file storage split into several components, raw log data, key/value pair data and enriched data (if available).

The analysis tier in LogPoint is delivered in a hybrid model. Inside LogPoint SIEM, the analysis node of LogPoint, is a component that consumes data from many LogPoint Backends. The Backends stream data in real time toward the analytics node, where data is processed for real-time correlations and alerting. Whenever an analyst requires forensics data or conducts a long-term analysis, queries are executed against the data stores.

The for-pay LogPoint UEBA is delivered through a cloud service that relays insights back to LogPoint SIEM.

LogPoint SIEM pricing is generally based on the number of assets in the organization.

### LogRhythm

LogRhythm, headquartered in Boulder, Colorado, brands its SIEM solution as LogRhythm NextGen SIEM Platform (version 7.4 introduced in October 2018 and reviewed for this research). The core SIEM component is the XDR Stack and includes the DetectX, AnalytiX and RespondX components.

Additional modules for user and network monitoring include:

- UserXDR (for UEBA capabilities)
- NetworkXDR (for NTA capabilities)
- LogRhythm System Monitor (aka SysMon version 7.4), a host agent for data collection and EDR capabilities available in Lite and Pro versions
- Network Monitor (aka NetMon version 3.9 and NetMon Freemium), the means to collect network data to support NetworkXDR

The platform leverages a mix of Windows and Linux OS, as well as Microsoft SQL and Elasticsearch for data management.

The LogRhythm platform supports large and smaller organizations with two versions — LogRhythm Enterprise and LogRhythm XM (an all-in-one appliance). These can be deployed either on-premises as software, a physical appliance or virtual appliance. IaaS deployments are

supported as well, and hybrid models of IaaS and on-premises, and mixing and matching of virtual, physical and software installs, are also supported. LogRhythm's SaaS SIEM offering is called LogRhythm Cloud. LogRhythm UserXDR is only available as a SaaS offering. Multitenancy is natively supported in the solution. Content is made available to customers via the LogRhythm Knowledge Base and is updated on a weekly basis.

LogRhythm's core SIEM product pricing is generally based on velocity (messages per second [MPS]).

### ManageEngine

ManageEngine has headquarters in India (Chennai), as well as in the U.S. (Austin, Texas). ManageEngine's core SIEM product is Log360, and there are several modules, individually licensed, that address security and IT operations use cases. These include (versions as of July 2019 and reviewed for this research):

- ManageEngine ADAudit Plus (version 6.0; Active Directory change auditing and reporting)
- ManageEngine EventLog Analyzer (version 12.0.5; central log management)
- ManageEngine Cloud Security Plus (version 4.0; CLM and SIEM for AWS and Azure)
- ManageEngine Log360 UEBA (version 4.0; user and entity behavior analysis)
- ManageEngine DataSecurity Plus (version 5.0; data discovery and file server auditing)
- ManageEngine O365 Manager Plus (version 4.3; Office 365 security and compliance)
- ManageEngine Exchange Reporter Plus (version 5.4; Exchange Server change audits and reporting)

Event data is ingested via agent-based and agentless methods, including log import. Alerts are created via real-time correlation rules packed with the solution or developed by users. The UEBA add-on module detects anomalous activities.

ManageEngine Log360 software can be deployed on-premises on physical or virtual systems. The ManageEngine Log360 Cloud solution stores the data collected by the log management module, EventLog Analyzer; however, it is not a SaaS-based SIEM tool. Typical small deployments would make use of the EventLog Analyzer and ADAudit Plus components.

Log360 pricing is generally based on the number of assets in scope (number of IP addresses).

### McAfee

McAfee is headquartered in Santa Clara, California. McAfee Enterprise Security Manager (ESM) version 11.2.1 (reviewed for this research) was introduced in July 2019 and is composed of the following modules:

- McAfee Event Receiver (ERC), for collection and correlation of data

- McAfee Enterprise Log Search (ELS), for Elastic-based log search
- McAfee Enterprise Log Manager (ELM), for long-term log storage and management
- McAfee Advanced Correlation Engine (ACE), for dedicated correlation including risk and ruleless (behavior-based) correlation, as well as statistical and baseline anomaly detection

Some McAfee ESM modules can be deployed as physical or virtual appliances. Appliances are available in both hardware and virtual (on-premises or cloud) form for ESM, ERC, ELS, ESM, ACE and ADM. Virtual machines can be deployed in AWS, Azure and Oracle cloud environments. They can also be deployed in on-premises virtualized environments running ESX, KVM, Hyper-V and Xen.

The McAfee ERC allows agentless collection of 500-plus data sources. The ERC performs a number of functions, including raw log collection, log parsing and data enrichment. The ERC uses Kafka to publish data to which other components within the environment can subscribe to obtain raw and parsed data. The ERC performs real-time alerting simple analytics. McAfee SIEM Collector is an optional agent, deployable via SCCP, SCCM or McAfee ePO, capable of collecting various logs (e.g., traditional Windows Event logs, flat file logs like DNS or DHCP, or customer defined application logs). The SIEM Collector supports servers acting as a Windows Event Forwarding host. The SIEM Collector can provide a native SQL connector to Microsoft SQL and Oracle RDBMS systems to allow customized queries against database views and tables.

McAfee ESM pricing is generally based on data velocity (EPS).

### Micro Focus

Micro Focus, headquartered in Newbury, U.K., offers the ArcSight platform as its SIEM solution. Micro Focus ArcSight's architecture is now based on big data technologies (e.g., Kafka bus for improved data transfers and horizontal scaling of data ingestion) and is composed of the following components (versions are those reviewed for this research):

- ArcSight Enterprise Security Manager (ESM; version 7.0 introduced in May 2019), providing core SIEM functions of real-time analytics and monitoring and incident management
- ArcSight Logger (version 6.7.1 introduced in May 2019), providing event and data processing and storage
- ArcSight Transformation Hub (version 3.0 introduced in July 2019) as part of the Security Open Data Platform (SODP) for data management and routing
- Interset UEBA (version 5.8 as of the July 2019 cutoff date for this research) for user and entity monitoring
- ArcSight Investigate (version 2.3 introduced in July 2018) for data searching and visualizations to support incident investigation and threat hunting use cases

- ArcSight Management Center (ArcMC; version 2.92 introduced in July 2019) is the stand-alone utility used to manage ArcSight components
- SmartConnector (version 7.13 introduced in July 2019), Micro Focus' content for data parsing and normalization

In addition, there are premium add-ons that cover additional content, and Micro Focus has other products in its portfolio that complement ArcSight. Content and third-party technology integrations are managed through the ArcSight Marketplace.

ArcSight components are provided as stand-alone appliances or software that can be installed on the customer's own infrastructure (physical and virtual) or installed in IaaS. SaaS is not available, but hosted offerings can be provided by third parties. Multitenant functionality is native to ArcSight ESM for managed security service providers (MSSPs), managed service providers (MSPs) and organizations that need to monitor multiple organizations in a single solution.

ArcSight pricing is generally based on data velocity (EPS).

### Rapid7

Rapid7 is headquartered in Boston, Massachusetts. Its SaaS SIEM offering is InsightIDR, and the underlying AWS-based Insight platform includes these other modules:

- InsightVM (vulnerability assessment)
- InsightAppSec (application security)
- InsightConnect (SOAR)
- InsightOps (log management for IT operations).

Rapid7 offers Insight Agent as its preferred endpoint agent to enable telemetry gathering and basic bidirectional response integration capabilities with Rapid7 InsightIDR, Rapid7 InsightVM and Rapid7 InsightOps. InsightIDR also offers integration with InsightVM, which enables customers to deploy one agent across the environment to instrument and collect vulnerability assessment data while performing detection and response functions. Insight Collectors provide event ingestion, and an unlimited number of Collectors or Agents are available without additional licenses. Rapid7 also offers a managed service built around the Insight platform, including managed detection and response and vulnerability management.

Data is ingested via Collectors (syslog, plus directories, AWS CloudTrail, Azure Event Hubs, etc.) and Agents (which are optional for event collection, but required for response actions and vulnerability management). Alerts are created by vendor-provided and customer-developed rules, and with statistical and machine learning analytics based on open-source, proprietary and AWS technologies. Basic response capabilities using Agents are available from InsightIDR, with more complete integrations available for InsightConnect.

InsightIDR pricing is generally based on the number of assets in scope (number of IP addresses).

### Securonix

Securonix is headquartered in Addison, Texas. The Securonix SNYPR SIEM platform consists of the following components (version 6.2 was introduced in October 2018 and the CU4 was introduced in May 2019; both were reviewed for this research):

- Securonix SIEM (v.6.2, CU4)
- Securonix Security Data Lake (v.6.2, CU4)
- Securonix UEBA (v.6.2, CU4)
- Securonix SOAR (v.2.0)
- Securonix NTA (v.2.0)
- Securonix Threat Intelligence (v.2.0)
- Securonix Apps (v.6.2, CU4): Insider Threat, Cyber Threat, Cloud Security Analytics, Identity and Access Analytics, Fraud Analytics, Trade Surveillance, Patient Data Analytics, Application Analytics

Securonix SNYPR is available primarily as cloud-delivered SaaS service, although MSSPs and key customers are known to run SNYPR either on-premises or in their own clouds.

Securonix is capable of managing hybrid multicloud environments, with support for most cloud IaaS and PaaS as well as many SaaS applications, on-premises logs and other contextual data, as well as network traffic and flows.

Securonix SIEM architecture is composed of three tiers — ingestion, compute/storage, and master console tiers. The ingestion and data acquisition tier is composed of remote ingesters (aka RIN), which are deployed on-premises in the customer data center or in the cloud, depending on the source of the log events. The data is compressed, encrypted and forwarded by the RINs to the compute/storage tier, where it gets processed — parsed, normalized, enriched, indexed, stored (for compliance) and analyzed for potential threats. The master console tier provides UI and administration services.

Securonix SNYPR is based on the Hadoop stack, and all data is stored and managed in typical big data components. Kafka, Solr, HDFS, HBase and Spark. Analytics are done via a Lambda architecture with streaming and batch-processing services. Analytics applications such as event correlation utilize Spark streaming services to analyze the data in real time, whereas applications requiring lookup of historical data (e.g., risk scoring) utilize the batch-processing layer. Batch processing is also utilized for alerting on historical data, training machine learning algorithms and running hunting queries on historical data.

Securonix SIEM pricing is generally based on the number of employees in the organization.

### SolarWinds

SolarWinds is headquartered in Austin, Texas. SolarWinds' SIEM solution is Security Event Manager (SEM; version 6.7 introduced in May 2019 and reviewed for this research). SEM includes core SIEM features that provide data management, real-time correlation and log searching to support threat and compliance monitoring, investigations and response.

SEM's architecture is straightforward, with only two components: a virtual appliance for all SEM features and functions, and a multifunction endpoint agent that provides log collection and forwarding, FIM, EDR (including active response functionality), and lightweight DLP capabilities.

Scalability can be achieved either by increasing resources to a virtual appliance or by splitting the SEM database and appliances across multiple virtual machines. Multitenancy is not native, but through the use of a master console, multiple SEMs can be viewed in a single pane.

SEM is complemented with other products in the SolarWinds portfolio for ticketing and case management, user monitoring, and network and application monitoring, through for-pay solutions such as Access Rights Manager, Identity Monitor, Service Desk, Server & Application Monitor and Papertrail, among others.

SolarWinds pricing is generally based on the number of assets in scope (number of IP addresses).

### Splunk

Splunk, headquartered in San Francisco, provides SIEM solutions via a combination of:

- Splunk Enterprise for core log management capabilities, delivered either on-premises (Splunk Enterprise version 7.3 introduced in May 2019) or as SaaS SIEM via Splunk CloudSplunk Enterprise Security (ES version 5.3.1 introduced in July 2019), also available on-premises or in the cloud as a service
- Additional (on-premises-only and for-pay) premium apps include Splunk User Behavior Analytics (UBA) and Splunk Phantom, as well as Splunk Security Essentials for Ransomware and Splunk App for PCI Compliance for more specific use cases

Splunk ES provides core SIEM features and functionality on top of the Splunk core. Splunk UBA complements Splunk ES's rule, correlation and basic statistical analytics through the addition of machine learning capabilities focused on user and entity anomaly monitoring. SOAR capabilities in Phantom are an enhancement over the adaptive response framework incident management and automation natively provided in Splunk ES.

Splunk is primarily delivered as software, or via SaaS as Splunk Cloud. Splunk can be installed on customer hardware, in virtual environments or in IaaS. Splunk's architecture contains only Universal Forwarders, Search Heads and Indexers. Universal Forwarders are agents that provide log collection and forwarding. Indexers and Search Heads are the two main components to collect, analyze and visualize data and outputs. The architecture is scalable both horizontally and vertically using these components. Splunk Stream provides a means for collecting network data

off the wire. Buyers looking for an appliance-based approach can find offerings from various third parties.

Splunk Enterprise and Splunk Cloud pricing is generally based on data volume (GB per day).

## Context

The SIEM market is evolving to address wide demands across a range of buyers.

SIEM tools' role as the central threat detection technology in enterprises is confirmed, while they are increasingly natively addressing the response phase after the detection. Gartner continues to see security operations centers (SOCs) built around a SIEM solution to deliver threat detection and response services.

At the same time, SIEM continues penetrating the small and midsize business segment, which does not have, nor does it plan to have, the required expertise to manage a SIEM and pursue advanced use cases. SIEM vendors are addressing this need with:

- Easier consumption models, such as SaaS SIEM along with predictable pricing models
- Stronger packaging of the content, availability of an app store and overall better user experience around the inherent complexity of these tools
- Use of advanced analytics to supplement the lack of this skill set in organizations
- Use of automation features to augment the availability of organizations

SIEM solutions are modernizing across the log management, analytics and operations tiers to deal with evolving buyer requirements, which requires enhancing features and adding new functionality. As an example, the ability to ingest and analyze data from cloud environments is now expected from clients looking for a SIEM tool. As described in "Technology Insight for the Modern SIEM," standard architectures have emerged for SIEM tools to address complexities in data management, analytics and operations, via a well-architected three-layer approach. This is done to address the following issues:

- As security teams deal with the challenges of increasing volumes of data from a variety of new sources with growing velocities, SIEM technology vendors are adopting big data technologies, such as Hadoop, NoSQL, Elasticsearch and Kafka to replace legacy data management capabilities oriented around proprietary methods and relational databases.
- To cope with an evermore hostile threat environment, both external attackers and insider threats, SIEM vendors are adding more sophisticated analytics methods, such as machine learning, to complement existing analytics capabilities, in addition to custom content focused on specific types of threats, such as ransomware or threat profiles modeled after their tactics, techniques and procedures. UEBA technologies (see "Market Guide for User and Entity Behavior Analytics") have been quickly embraced by existing SIEM vendors (either via self-developed technology or acquisition, or through white labeling), in addition to UEBA vendors that have

pivoted to the SIEM technology market. Machine-readable threat intelligence is increasingly made available, both with the core SIEM solution and as a premium feature. However, the quality of out-of-the-box threat intelligence and support for third-party feeds varies among vendors.

- At the operational tier, SIEM solution buyer requirements are driving demand for more sophisticated case and incident management features, as well as ways to measure, track, report on and improve the mean time to detect (MTTD) and mean time to respond (MTTR) to threats. The automation of specific activities done manually by SIEM tool users in both investigating events and alerts, as well as in initiating response actions, strongly aligns to the SOAR tool market and its use cases. As a result, SOAR features (see "Innovation Insight for Security Orchestration, Automation and Response") are starting to be added to SIEM solutions in a trajectory similar to the adoption of UEBA — via acquisitions, white-label partnerships, third-party integrations and native development.

Some SIEM buyers opt for and prefer vendors providing a full portfolio of security solutions that have (pre)integrated their offering within a platform approach, offering a range of threat management — as well as broader security operations — capabilities that complement the vendor's core SIEM solution. These threat management solutions typically include multifunction endpoint agents, or sensors, that can provide log collection and forwarding, FIM, EDR, and even DLP functions. Network monitoring technologies provide similar capabilities, such as data collection and forwarding of network flow and metadata, partial and full packet capture, and threat detection (via signatures and network traffic analytics). For buyers who are underinvested in these complementary threat detection solutions, the integration and ease of use with the core SIEM solution are beneficial; however, for those buyers who have already invested in third-party solutions, this approach can be less beneficial and reduces flexibility.

As integration with a vendor's existing technology portfolio, as well as with third-party technologies, increases in importance, in addition to buyer demands for easier management and use of SIEM tools, SIEM vendors are adding or improving centralized management capabilities. These capabilities may follow the app store or marketplace model, or be provided via a support website, where precanned integrations, packaged content and other SIEM solution updates can be accessed.

Context is key for effective threat detection and response. SIEM solutions are becoming more sophisticated in their ability to consume, but also generate, contextual information. The enrichment of log event data upon ingestion at the data tier is becoming more common. The adoption of APIs for data collection, as well as accessing contextual data held in federated repositories (e.g., CMDBs, IAM tools, vulnerability assessment tools), is expanding and continues to grow across vendors. These integrations are also proving important to support the adoption and expansion of orchestration and automation features.

SIEM technologies consumed in a SaaS model (see "Selecting and Deploying SaaS SIEM for Security Monitoring" and "10 Questions to Answer Before Adopting SaaS SIEM") are gaining in

popularity. In fact, some tools, such as those from AT&T Cybersecurity, FireEye, Rapid7 and Securonix, are now offered only as a service (exceptions are possible for key accounts), while almost all vendors offer SaaS SIEM, either natively or via their ecosystem of partners and service providers.

Additionally, log management-as-a-service vendors are beginning to compete in the SIEM space by adding core SIEM capabilities. (For more information on central log management, see "Use Central Log Management for Security Event Monitoring Use Cases"). The trend toward leveraging cloud services to locate the SIEM solution closer to the data source, as well as enable advanced analytics such as UEBA, is a clear catalyst for the current and short-term/midterm SaaS SIEM adoption.

## Product/Service Class Definition

SIEM technologies provide core security information management (SIM) and security event management functions, along with a variety of advanced features and complementary solutions and capabilities. This supports near-real-time security event monitoring, threat detection (both real-time and via historical analysis), incident investigation and response, and compliance requirements. Core functions include:

- The collection of security event information from a wide variety of sources in a central repository where it can be processed and stored in various forms (e.g., raw version, enriched, normalized)
- Real-time and historical analysis, and alerting of potential threats
- Reporting and dashboards
- Searching across historical data for forensics and threat hunting
- Workflow and case management
- Integrations and automation for extending the value proposition and achieving more functionality

SIEM technology is typically deployed to:

- Monitor, correlate and analyze activity across multiple systems and applications
- Discover external and internal threats
- Monitor the activities of users and specific types of users, such as those with privileged access (both internal and third parties), and users with access to critical data assets such as intellectual property, and executives
- Monitor server and database resource access, and offer some data exfiltration monitoring capabilities

- Provide compliance reporting
- Provide analytics and workflow to support incident response, and increasingly the ability to orchestrate and automate actions and workflows, powering SOC types of use cases

SIEM technology aggregates and analyzes the event data produced by networks, devices, systems and applications. The primary data source has been time-series-based log data; however, SIEM technology is evolving to process (e.g., for real-time monitoring) and leverage (e.g., for incident investigation and response) other forms of data to obtain context about users, IT assets, data, applications, threats and vulnerabilities (e.g., Active Directory [AD], configuration management database [CMDB], vulnerability management data, HR information and threat intelligence).

## Critical Capabilities Definition

Here, we evaluate nine capabilities across SIEM technologies. Security and risk management leaders should use this research to understand the differing capabilities across the SIEM technology landscape aligned to their specific use cases.

### Architecture/Deployment/Scalability

This capability encompasses the architecture of the solution and its modules, its deployment alternatives, as well as horizontal and vertical scalability.

SIEM solution architectures must support a variety of buyer environments, ranging from smaller enterprises that may only need a single appliance solution to global enterprises and MSSPs with complex environments that require distributed, n-tier architectures, and even enterprises looking for a cloud-delivered, SaaS SIEM. SIEM tool buyers must evaluate the complexity of deployments, such as an all-in-one box approach versus individual or combined modules to support large-scale deployments, or their ability to send potentially massive amounts of logs through their gateway for SaaS SIEMs. They also need to assess how to deploy those components — for example, using physical or virtual appliances or software, provided as a service, or a combination thereof. To deal with the increase in the volume, velocity and variety (and retention) of data across organizations of all sizes, SIEM solutions are adopting and leveraging big data technologies. Buyers in organizations with “cloud first” policies are looking to SIEM solutions that are delivered as a service or that can be installed in IaaS or hybrid deployments. Support for integrating with an array of security and nonsecurity technologies is also increasingly important, with the growing adoption of APIs in security and other IT technologies.

### Cloud Readiness

This capability focuses on emerging or more established use cases centered on cloud, as well as the use of cloud as a deployment alternative for the SIEM solution.

As organizations are looking to benefit from the cloud, some adopt a cloud-first approach that prioritizes the use of cloud services, while most organizations have a hybrid environment with a combination of on-premises assets (e.g., firewalls, routers, servers), and cloud workloads in the form of SaaS solutions (e.g., Office 365) or IaaS/PaaS (e.g., AWS, Azure or Google Cloud

Platform). This trend has been sustained over the past few years, to the point where a SIEM tool's ability to operate in cloud and hybrid environments is now key for most, if not all, organizations.

This critical capability will take into account: (1) the tool's ability to be delivered as a cloud service (and in this case, whether the solution is an on-premises image merely hosted by the vendor, or whether the solution is a genuine cloud-native SaaS service); and (2) the scope of cloud providers and services that the SIEM tool can natively offer use cases for (and in this case, whether the SIEM tool can interact with them in a bidirectional way).

### Operations and Support

SIEM solutions are recognized as complex technologies that can be difficult to deploy, and require ongoing maintenance and support to stay fit for purpose.

Combined with a shortage of available SIEM engineering expertise, the ability to deploy and sustain the administration of SIEM tools becomes increasingly challenging. An integrated management console and user experience that enables efficient management of the SIEM solution is important. From this management console, log and data source management, administration of analytics content (e.g., correlation rules, whitelist matching and machine learning algorithms), reporting, and user administration through role-based access control are provided. Likewise, the SIEM tool should provide an easy way to define and manage automated responses via playbooks and workflow integration.

Vendor support is most visible in maintenance contracts purchased by SIEM tool buyers. This includes product support (e.g., patches, hotfixes, version upgrades and content updates), as well as human support to assist SIEM solution owners. Support is typically provided via remote means, but can vary across options such as email, phone and even access to Slack channels. Support may also be provided in tiers to help buyers who may not need, or can't afford, expensive support plans. Finally, support for implementation is a crucial element for new SIEM implementations and upgrades, and may be provided directly by the vendor or through designated third parties.

### Data Management Capabilities

This capability captures the SIEM tool's ability to properly and easily manage data, from standard logs from security devices, to NetFlow, packet captures, vulnerability scanning data and external context data.

External context data includes machine-readable threat intelligence (MRTI) or user and asset context, such as AD or CMDB.

The ability to support data acquisition of IaaS and SaaS and IoT/OT devices is increasingly important as well, and clients expect this feature to be provided natively by the tools, as outlined in the Cloud Readiness capability.

A SIEM tool needs access to the right data, and these data points can range widely from on-premises sources to cloud compute sources, and encompass security data sources as well as nonsecurity ones, such as IT, organizational and HR data. These data points can be structured or

unstructured, and collected via syslog, push or pull, or invoking API calls. In addition to getting the data via connectors, the SIEM needs corresponding parsers in order to make those data points insightful. Once collected, the data can be stored in raw form or normalized, enriched or contextualized form, or a combination thereof. Tools can also offer compression capabilities to minimize storage requirements, often at the expense of performance. Tools that offer an organization the ability to convince a court that the evidence is sound need to look at the full life cycle of data management, from secure transport of the data sources with nonrepudiation to secure storage with guaranteed integrity of each event and event sequence. Capabilities to provide fine-grained access control (usually RBAC) to logs, along with obfuscation and anonymization features and flexibility to provide multiple retention policies, will also be taken into account.

### Analytics Capabilities

This capability describes the tool's ability to offer the right analytics to get the most accurate insights for multiple use cases.

Once the data is collected, it needs to be analyzed in as real time as possible to detect threats as quickly as possible. To achieve a good level of accuracy, several analytics methods can run in parallel, ranging from simple pattern matching to more complex supervised and/or unsupervised machine learning. Some analytics are open, and clients can understand and modify the analytics, whereas some others are not, and behave more like a black box. Some SIEM tool's analytics are both powerful and flexible enough to extend beyond threat detection and into adjacent use cases (such as some fraud use cases), and can offer a bench to evolve existing machine learning models or create new ones. Likewise, some SIEM tools map the analytics to known approaches such as Lockheed Martin's Cyber KillChain, or MITRE ATT&CK frameworks to better understand what is happening in the organization.

While the analytics dynamically compute risk scores for users and/or entities based on actions or events taking place, the tool needs to help organizations prioritize their threat landscape by offering an intuitive UI.

### Response and Incident Management

An organization's ability to quickly open cases at any moment (such as directly from the real-time monitoring UI or during a threat hunt) with full context around the case will accelerate case resolution and improve the overall security posture.

For larger organizations dealing with a deluge of alerts, the tool can apply analytics to help triage cases to the right analysts by mapping skill sets to the focus of the case based on each analyst's load (e.g., endpoint-centric cases assigned to available endpoint experts). For complex cases, the tool can likewise help the collaboration of multiple analysts by providing simple Slack-like features or advanced RBAC, where analysts with different clearance levels can still collaborate on cases.

Incidents or cases should have the ability to change the status (preconfigured and custom), support notes and annotations, and assign to other users. Integrations with enterprise IT help

desk and IT service management (ITSM) systems, enabling interaction with business units outside of security (such as IT operations) are commonly required by buyers.

All steps performed during a case need to be logged and kept securely, as an organization should always be ready to go to court and demonstrate court-ready evidence. Attributes such as nonrepudiation, integrity of each event and integrity of the event sequence are important for incident and case management.

Interfaces that offer the ability to drill down on an alert and/or integrate with forensics and threat hunting capabilities allow rapid and contextual reactions to monitoring (e.g., open a case or launch an investigation).

### Content Packaging and Management

Content for SIEM includes collectors and parsers for data sources, complete use cases, compliance packages, rules and models for analytics, and response and playbook capabilities.

All this content must be organized, packaged and managed easily to minimize operational costs of accessing, modifying and deploying content.

This content is required for the SIEM tool to function properly, and leveraging extensive and well organized content provided natively by the vendor, integrators, consultants or the community offers significant value to all organizations, especially the smaller ones, or the larger ones initiating their SIEM journey.

SIEM vendors tend to build ecosystems of technology alliances with complementary security and nonsecurity vendors to offer a rich and robust set of connectors, parsers and additional content such as analytics and/or response capabilities. In this case, ecosystem density is key for larger environments that implement nonstandard technologies or applications. Leveraging vendor-provided native content is particularly important for the response and playbook features, as these connections are bidirectional and integrations need to be done on both sides.

In addition to raw content, the tool should offer a management framework for accessing, updating and managing this content, and enabling its functionality. Particularly important for first-time SIEM buyers and those with limited resources, predefined functions and ease of deployment and support are valued over advanced functionality and extensive customization. The use of an app-store-type feature to provide a centralized location for locating and installing new content, integrations and other features is beneficial for all organizations and use cases.

### Forensics and Threat Hunting

Investigation capabilities encompass the ability to use a SIEM tool to search for particular evidence to investigate an incident, be used as a forensics tool or to support threat hunting.

Search features and functionality are fundamental in a SIEM tool, and need to accommodate a wide range of organizational maturity. While some may prefer to search using a descriptive taxonomy and drop-down menus, others may prefer free-flowing search queries with either regular expression (regex) or boolean, or simple vendor-specific language. Response times can vary

widely across SIEM tools, and preference should be given to quick response time for wide searches across large datasets, and for a user-intuitive visualization that will help analysts uncover interesting events or patterns. The ability to pivot from result to result, using simple clicks rather than copying and pasting into another console, is important, as is the ability to open a case at any point in a hunt. Finally, SIEM tools capable of searching across several data stores in large and mature organizations should be privileged.

### User Experience and User Interface

Because of their flexibility and sheer complexity, SIEM tools are complex to operate and manage. Thus, it's important for the tool to offer a user experience that is appropriate for both the size and maturity of the client organization, as well as the use case to implement.

Some SIEM tools assume that the client will have a high maturity level, and will offer workflows and operational models that are very efficient but require deeper expertise, while others clearly cater to less mature organizations and offer more guidance to the user, usually at the cost of efficiency.

The user experience encompasses the UI and the presentation layer of these tools, including dashboards, reports, alerts, how configurable these are and how well suited they are for the audience that the tools cater to.

Setup and ongoing management of the tool also vary widely, based on the client environment and the size of the deployment. Some tools aim to be used in SOCs with dozens or hundreds of security analysts, implying requirements to facilitate the description of the SOC team to help triage cases. Other tools typically operate in environments with no dedicated SIEM expertise, and forcing clients to describe their SOC expertise would not make sense.

Tools that offer a user experience that can scale with growing environments should be privileged.

## Use Cases

### Basic Searching and Reporting

This use case focuses on the simplest use case for SIEM, searching and reporting on the pool of logs.

These searches are often used for basic queries such as "Who logged in this weekend to our VPN concentrator?" and sometimes then run as periodic reports. Often the users are less mature organizations that do not have the skill set, availability or appetite to embark on more complex real-time monitoring use cases. However, these organizations also understand the benefit of using SIEM tools for searching and reporting across the enterprise, and want a path to more sophisticated real-time monitoring use cases.

A tool's ability to rapidly allow nonexpert users to get an answer to their question, benefit from relevant visualizations, and intuitively pivot to more searches or to the creation of reports will be key to this use case.

### Compliance and Control Monitoring

This use case is aimed at demonstrating compliance with specific mandates like PCI DSS, HIPAA or SOX, or best practices or control policies like ISO 27001 or CIS Controls.

These use cases tend to demonstrate that a particular event or series of events has indeed happened, or, on the contrary, never happened. Often in the form of checklists that can be hundreds or thousands of lines long that auditors need to validate, these compliance and control monitoring use cases are hard to manage manually. SIEM tools that offer stronger solutions for compliance and control monitoring use cases will facilitate the whole life cycle for this use case — from providing predefined content that caters to specific compliance and controls, to the way this content is organized in packages that are easy to customize based on unique needs, to how the vendor approaches the updates and new content for these packages, to how easily the reports can be generated and shared with auditors in an automatic way.

### Basic Security Monitoring

This use case supports basic broad-based threat detection use cases, as well as capabilities that help new and less mature SIEM buyers and users.

These include ease of deployment and operations, real-time monitoring, and analytics. It typically includes first-time SIEM solution buyers, and buyers focused on less sophisticated use cases. These buyers may be more likely to adopt “single box” solutions and as-a-service and hosted offerings. The focus is on solutions that are easier to implement and manage with packaged content (analytics, reports and responses) that solve discrete threat-monitoring use cases (e.g., ransomware) that do not focus on cloud or IoT/OT security.

### Complex Security Monitoring

This use case focuses on SIEM solutions with complex architectures (n-tier, hybrid), environments and user populations, as well as big data-type log and event challenges.

N-tier or hybrid architectures are required to support environments with challenges such as distributed geographies and multiple environments (on-premises, IaaS, SaaS) for data collection; high volumes, velocities and varieties of data collection; and multitenancy requirements. The scope for some use cases could include IoT/OT. Event monitoring, both real time and historic, leverages a variety of analytics in varying degrees of complexity. Best-of-breed security technologies may be employed, which requires integrations for both data collection and incident investigation and response activities.

### Advanced Threat Detection and Response

This use case focuses on the early discovery and analysis of advanced and targeted attacks, and the ability to rapidly respond to those attacks.

Advanced threat hunting activities enhanced by the tool are also included in this use case.

Organizations operating in high-risk verticals and environments face an ever-increasing hostile external threat landscape, where adversaries target specific organizations and attempt to

compromise them with persistence and an arsenal of tools and tactics in order to achieve their goals. SIEM solution buyers facing these advanced and persistent threat actors look to monitor, detect and respond to attacks across the range of the attack chain in near real time, and through advanced analytics and threat hunting across historic log events and data. These buyers usually seek complementary host and network threat detection and forensics tools, as well as other technologies like SOAR, which are directly integrated, or at least well integrated, with their SIEM solution, to facilitate the rapid investigation and response to detected threats.

In this case, there is a requirement to cross the boundaries between on-premises, cloud and IoT/OT scopes in order to offer a unified view of threats across the full threat landscape.

### Vendors Added and Dropped

#### Added

FireEye and HanSight were added to the SIEM Critical Capabilities research this year, based on their meeting the SIEM Magic Quadrant inclusion criteria.

#### Dropped

BlackStratus, Netsurion-EventTracker and Venustech were dropped this year because they did not meet the Magic Quadrant inclusion criteria for revenue or geographic presence.

## Inclusion Criteria

In this research, we've included software products for evaluation. The inclusion criteria are the same as for the SIEM Magic Quadrant:

- The product must provide SIM and security event management capabilities to end-user customers via software and/or appliance and/or SaaS.
- The SIEM features, functionality and add-on solutions must be generally available as of 31 July 2019.
- The product must support data capture and analysis from heterogeneous, third-party sources (that is, other than from the SIEM vendors' products/SaaS), including from market-leading network technologies, endpoints/servers, cloud (IaaS, SaaS) and business applications
- The vendor must have SIEM (product/SaaS license and maintenance, excluding managed services) revenue exceeding $32 million for the 12 months prior to 30 June 2019, or have 100 production customers as of the end of that same period. Production customers are defined as those who have licensed the SIEM and are monitoring production environments with the SIEM. Gartner requires that vendors provide a written confirmation of achievement of this requirement and others that stipulate revenue or customer thresholds. The confirmation must be from an appropriate finance executive within the organization.
- The vendor must receive 15% of SIEM product/SaaS revenue for 12 months prior to 30 June 2019 from outside the geographical region of the vendor's headquarters location, and must

have at least 10 production customers in each of at least two of the following geographies: North America, EMEA, the Asia/Pacific region or Latin America.

- The vendor must have sales and marketing operations (via print/email campaigns and/or local language translations for sales/marketing materials) targeting at least two of the following geographies as of 30 June 2019: North America, EMEA, the Asia/Pacific region or Latin America.

**Exclusion Criterion:**

- Capabilities that are available only through a managed service relationship — that is, SIEM functionality that is available to customers only when they sign up for a vendor's managed security or managed detection and response or managed SIEM or other managed service offering. By "managed services," we mean those in which the customer engages the vendor to establish, monitor, escalate and/or respond to alerts/incidents/cases.

**Table 1: Weighting for Critical Capabilities in Use Cases**

| Critical Capabilities | Basic Searching and Reporting | Compliance and Control Monitoring | Basic Security Monitoring | Comp Secu Monito |
|---|---|---|---|---|
| Architecture/Deployment/Scalability | 5% | 5% | 10% | 1 |
| Cloud Readiness | 5% | 5% | 5% | 5 |
| Operations and Support | 10% | 10% | 10% | 1 |
| Data Management Capabilities | 15% | 15% | 15% | 1 |
| Analytics Capabilities | 5% | 10% | 10% | 1 |
| Response and Incident Management | 5% | 5% | 10% | 1 |
| Content Packaging and Management | 5% | 25% | 15% | 1 |
| Forensics and Threat Hunting | 20% | 5% | 5% | 1 |

| Critical Capabilities | Basic Searching and Reporting | Compliance and Control Monitoring | Basic Security Monitoring | Comp Secu Monito |
|---|---|---|---|---|
| User Experience and User Interface | 30% | 20% | 20% | 1 |
| **Total** | **100%** | **100%** | **100%** | **1** |

Source: Gartner (February 2020)

This methodology requires analysts to identify the critical capabilities for a class of products/services. Each capability is then weighed in terms of its relative importance for specific product/service use cases.

## Critical Capabilities Rating

**Table 2: Product/Service Rating on Critical Capabilities**

| Critical Capabilities | AT&T Cybersecurity | Dell Technologies (RSA) | Exabeam | Fire |
|---|---|---|---|---|
| Architecture/Deployment/Scalability | 3.0 | 3.4 | 3.9 | |
| Cloud Readiness | 3.1 | 3.5 | 4.1 | |
| Operations and Support | 3.2 | 3.6 | 4.5 | |
| Data Management Capabilities | 2.9 | 3.4 | 4.0 | |
| Analytics Capabilities | 2.4 | 3.6 | 4.3 | |
| Response and Incident Management | 2.7 | 3.3 | 4.0 | |
| Content Packaging and Management | 2.7 | 3.3 | 3.9 | |
| Forensics and Threat Hunting | 2.8 | 3.4 | 4.0 | |

| Critical Capabilities | AT&T Cybersecurity | Dell Technologies (RSA) | Exabeam | Fire |
|---|---|---|---|---|
| User Experience and User Interface | 2.6 | 3.3 | 3.9 | |

Source: Gartner (February 2020)

Table 3 shows the product/service scores for each use case. The scores, which are generated by multiplying the use-case weightings by the product/service ratings, summarize how well the critical capabilities are met for each use case.

Table 3: Product Score in Use Cases

| Use Cases | AT&T Cybersecurity | Dell Technologies (RSA) | Exabeam | FireEye | Fortinet |
|---|---|---|---|---|---|
| Basic Searching and Reporting | 2.79 | 3.40 | 4.03 | 3.18 | 2.76 |
| Compliance and Control Monitoring | 2.77 | 3.40 | 4.04 | 3.14 | 2.76 |
| Basic Security Monitoring | 2.79 | 3.40 | 4.04 | 3.16 | 2.77 |
| Complex Security Monitoring | 2.80 | 3.43 | 4.07 | 3.17 | 2.78 |
| Advanced Threat Detection and Response | 2.77 | 3.43 | 4.07 | 3.16 | 2.76 |

Source: Gartner (February 2020)

To determine an overall score for each product/service in the use cases, multiply the ratings in Table 2 by the weightings shown in Table 1.

## Critical Capabilities Methodology

This methodology requires analysts to identify the critical capabilities for a class of products or services. Each capability is then weighted in terms of its relative importance for specific product or service use cases. Next, products/services are rated in terms of how well they achieve each of the critical capabilities. A score that summarizes how well they meet the critical capabilities for each use case is then calculated for each product/service.

"Critical capabilities" are attributes that differentiate products/services in a class in terms of their quality and performance. Gartner recommends that users consider the set of critical capabilities as some of the most important criteria for acquisition decisions.

In defining the product/service category for evaluation, the analyst first identifies the leading uses for the products/services in this market. What needs are end-users looking to fulfill, when considering products/services in this market? Use cases should match common client deployment scenarios. These distinct client scenarios define the Use Cases.

The analyst then identifies the critical capabilities. These capabilities are generalized groups of features commonly required by this class of products/services. Each capability is assigned a level of importance in fulfilling that particular need; some sets of features are more important than others, depending on the use case being evaluated.

Each vendor’s product or service is evaluated in terms of how well it delivers each capability, on a five-point scale. These ratings are displayed side-by-side for all vendors, allowing easy comparisons between the different sets of features.

Ratings and summary scores range from 1.0 to 5.0:

1 = Poor or Absent: most or all defined requirements for a capability are not achieved

2 = Fair: some requirements are not achieved

3 = Good: meets requirements

4 = Excellent: meets or exceeds some requirements

5 = Outstanding: significantly exceeds requirements

To determine an overall score for each product in the use cases, the product ratings are multiplied by the weightings to come up with the product score in use cases.

The critical capabilities Gartner has selected do not represent all capabilities for any product; therefore, may not represent those most important for a specific use situation or business objective. Clients should use a critical capabilities analysis as one of several sources of input about a product before making a product/service decision.