SIEM SOFTWARE OVERVIEW

Security information and event management (SIEM) software provides IT security staff both a track record of and insight into the activities in their IT environment. This technology has been around for more than 10 years, initially starting from the log management field. It combines security event management (SEM) – which analyzes event and log data in real time to facilitate incident response, event correlation, and threat monitoring – with security information management (SIM) which gathers, reports on, and analyzes log data.

SIEM software aggregates log info generated in an enterprise’s technology infrastructure including applications, host systems, and security devices like antivirus filters and firewalls. The platform then identifies and classifies events and incidents, and analyzes them.
The FeaturedCustomers Customer Success ranking is based on data from our customer reference platform, market presence, web presence, & social presence as well as additional data aggregated from online sources and media properties. Our ranking engine applies an algorithm to all data collected to calculate the final Customer Success Report rankings. The overall Customer Success ranking is a weighted average based on 3 parts:

**Content Score** is affected by:

1. Total # of vendor generated customer references (case studies, success stories, testimonials, and customer videos)
2. Customer reference rating score
3. Year-over-year change in amount of customer references on FeaturedCustomers platform
4. Total # of profile views on FeaturedCustomers platform
5. Total # of customer reference views on FeaturedCustomers platform

**Market Presence Score** is affected by:

1. Social media followers including LinkedIn, Twitter, & Facebook
2. Vendor momentum based on web traffic and search trends
3. Organic SEO key term rankings
4. Company presence including # of press mentions

**Company Score** is affected by:

1. Total # of employees (based on social media and public resources)
2. Year-over-year change in # of employees over past 12 months
3. Glassdoor ranking
4. Venture capital raised

---

**Customer Success Report Award Levels**

**Market Leader**

Vendor on FeaturedCustomers.com with substantial customer base & market share. Leaders have the highest ratio of customer success content, content quality score, and social media presence relative to company size.

**Top Performer**

Vendor on FeaturedCustomers.com with significant market presence and resources and enough customer reference content to validate their vision. Top Performer's products are highly rated by its customers but have not achieved the customer base and scale of a Market Leader.

**Rising Star**

Vendor on FeaturedCustomers.com that does not have the market presence of Market Leaders or Top Performers, but understands where the market is going and has disruptive technology. Rising Stars have been around long enough to establish momentum and a minimum amount of customer reference content along with a growing social presence.
2019 Customer Success Awards

Check out this list of the highest rated SIEM Software software based on the FeaturedCustomers Customer Success Report.

**Market Leaders**

- AT&T Cybersecurity
- exabeam
- LogRhythm
- Splunk

**Top Performers**

- Alert Logic
- Fortinet
- JASK
- SolarWinds
- Loggly

**Rising Stars**

- Netwrix
- EventTracker
- Logentries
- LOGPOINT
OVERALL BEST
OF SIEM SOFTWARE

BEST IN CATEGORY

AT&T Cybersecurity
ABOUT AT&T CYBERSECURITY

AT&T Cybersecurity’s Edge-to-Edge technologies provide phenomenal threat intelligence, collaborative defense, security without the seams, and solutions that fit your business. Their unique, collaborative approach integrates best-of-breed technologies with unrivaled network visibility and actionable threat intelligence from AT&T Alien Labs researchers, Security Operations Center analysts, and machine learning – helping to enable their customers around the globe to anticipate and act on threats to protect their business.

"Our business must be compliant with all application regulations, i.e. HIPAA, PCI. The USM AiO gives us the tools we need to be compliant and the reporting we need to prove it.”
Daniel Pressner
IT Director, Florida Orthopaedic Institute

"AlienVault gave us a platform that fits perfectly with our managed security service offering and provides our clients with a comprehensive solution for their data security and compliance needs.”

Mike Kerem
Chief Technology Officer, TrustNet

"AlienVault USM provides the insight of what’s happening where, when and by whom and gives us the ability to review and capture incidents that were previously undetected and therefore unknown.”
Philip Clarke
Security Manager, Randall & Quilter

"The #1 best benefit of AlienVault USM is the all-in-one [platform] and not having to switch to different products to check on different issues/reports. Running everything from a single interface gives me the ability to become an expert with one product, but with a full picture view.”
Eric Shaver II
Security Officer, The Plateau Group
2019 MARKET LEADERS

exabeam

LogRhythm

splunk

sumo logic
Exabeam provides security intelligence and management solutions to help organizations of any size protect their most valuable information. The Exabeam Security Intelligence Platform uniquely combines a data lake for unlimited data collection at a predictable price, machine learning for advanced analytics, and automated incident response into an integrated set of products. The result is the first modern security intelligence solution that delivers where legacy SIEM vendors have failed. Built by seasoned security and enterprise IT veterans from Imperva, ArcSight, and Sumo Logic.

"It wasn’t that we didn’t have the logs; we had those. But they were in many divergent locations, and it took our analysts lots of time to actually dig into those logs and find them and put a story together. With Exabeam, it actually provides us with a story.”

Chris Hymes
Director of Information Security, Hulu

“We collect eight to 12 billion events per day. With Exabeam, almost overnight, we gained an immense operational efficiency.”

V.Jay LaRosa
Vice President, Global Security Architecture, ADP

"With Exabeam’s minimal configuration and low maintenance, a SOC can autonomously detect insider threats and suspicious activity. And they’re able to do this without having to create static correlation rules, those often being ineffective.”

Martin Jakobsen
Managing Director, Cybanetix

"Having Exabeam’s unlimited data lake and attractive pricing model made the difference for our large organization.”

Hiroshi Honjo
Head of Cyber Security and Governance, NTT DATA Corporation
ABOUT LOGRHYTHM
LogRhythm provides enterprise-class log management, log analysis and event management in an integrated solution that empowers organizations to comply with regulations, secure networks, and optimize IT operations. LogRhythm was positioned by Gartner Inc. in the visionaries quadrant of the Security Information and Event Management Magic Quadrant report for 2007. LogRhythm is privately held and based in Boulder, Colorado.

"LogRhythm enabled us to see logs from our switches and firewalls that previously would have been missed, and would have resulted in the University’s data processing systems being out of action for an extended period of time.”
Paul Kennedy
Security and Compliance Leader, University of Nottingham

“We used to collect and manage log data manually, but with LogRhythm we can now automate this process and have a single view of the entire infrastructure. This means we can now spot even the tiniest of events, including those which would have been missed in the past.”
Jason Collins
IT Development Centre Manager, Endsleigh Insurance Services

“The intelligence provided by [LogRhythm's] advanced correlation not only allows us to identify current threats, but also predict what might happen in the future. In addition to assisting with security monitoring, the LogRhythm solution has also proved useful in both identifying and resolving any networking errors that arise.”
Michael Brown
Group Head of Security and Fraud Management, Callcredit

“I would absolutely say we have gotten a good ROI on this product. We have that comfort level that we’re monitoring these systems and meeting that PCI compliance for our franchisees. LogRhythm has enabled us to achieve PCI compliance two years in a row now since we’ve started on this path.”
Rik Steven
Manager in the Corporate Project Management Office, CARA
ABOUT SPLUNK

Splunk provides the leading software platform for real-time Operational Intelligence. Splunk software and cloud services enable organizations to search, monitor, analyze and visualize machine-generated big data coming from websites, applications, servers, networks, sensors and mobile devices. Splunk is the leading software platform for machine data that enables customers to gain real-time Operational Intelligence.

522
Customer references from happy Splunk users

VIEW ALL REFERENCES

“My colleagues are amazed when I pull up an instance of Splunk and show logs, performance data, and application data, in one location, sortable by time.”
Shaun Butler
Sr. Technology Specialist, Infrastructure, Corporate Express

“With our operations already in the cloud, Splunk Cloud is ideal for us. We get the full functionality of Splunk Enterprise, which means the real-time data and insights to optimize our services, refine our processes and rapidly put software into production. But now, someone else minds the servers and addresses capacity.”
Software Engineer
MindTouch

“Splunk helped us establish the baseline for our company’s operational model and helped us identify and understand anomalies to that baseline. And as the business has evolved and changed, Splunk has helped us understand how the baseline is changing.”
Mark J. Day
Executive Vice President, Research and Development, iRhythm Technologies

“The HIPAA-compliant version of Splunk that we use gives us a BAA that is very advantageous and critical for any vendor we work with. If some report stops running or the scheduler slows down, we don’t have to go figure out why. We let the experts at Splunk do it.”
Manager, Cloud Platform Team
Imprivata
ABOUT SUMO LOGIC

Sumo Logic is the next generation log management and analytics company that leverages Big Data for real-time IT insights. Sumo Logic cloud-based service provides customers with real-time interactive analytics at unprecedented petabyte scale. The Sumo Logic service is powered by patent-pending Elastic Log Processing™ and LogReduce™ technologies, and transforms log data into actionable insights for IT operations, application management, and security and compliance teams. Unlike expensive and complex premise-based solutions, the Sumo Logic service has a low TCO, can be deployed instantly, scales elastically and requires zero maintenance. Sumo Logic is based in Silicon Valley and is backed by Greylock Partners and Sutter Hill Ventures.

“Sumo Logic provides us instant visibility into AWS services. We were able to get AWS ELB dashboards in a few minutes, which was very impressive.”
Alex Zadorozhnyi
Director of Technology, Hootsuite

“Sumo Logic has allowed McGraw-Hill Education to move to AWS with confidence, enable real-time visibility across the entire stack, all at reduced TCO.”
Shane Shelton
Sr. Director of Application Performance & Development Operations, McGraw Hill Education

“With Sumo Logic, we put the power in the hands of the people who can actually fix the problem. Our average response times have reduced from hours to minutes and we can detect and resolve any irregularities before they have the potential to impact customers.”
Michael Ridgway
Director of Engineering, Carsales

“What Sumo Logic does for Hearst is open the data funnel up in such a way that everyone has access to the value that the data provides.”
Pauly Comtois
VP of DevOps, Hearst
2019 TOP PERFORMERS

- Alert Logic
- Fortinet
- JASK
- SolarWinds
- Loggly
Alert Logic offers Security-as-a-Service in the cloud a platform of fully managed products and services to keep their data safe and compliant. Whether Alert Logic IT infrastructure is on-premise, in the cloud or anywhere in between, Alert Logic portfolio of solutions and deployment options allows unprecedented visibility into their environment, saving their business time, money and worries about data compliance and security.

“"The company’s solutions are specifically engineered for cloud deployments instead of taking older architectures and forcing them to work – this is exactly what we were looking for.””
Mieke Koolj
Security Director, Trainline

“Alert Logic provides the perfect mix of artificial intelligence from their product suite and human intelligence from their security operations center to give us fast remediation actions that keep us secure and compliant.”
Marcus Kern
Chief Technology Officer, Fonix

“One of the key benefits of the partnership is the agility of the Alert Logic service, whether it is an on-premises deployment, cloud integrated deployment or a hybrid, and the rate that can be executed.”
Seamus Macloughlin
Group Head of Information Security, Connect Group

“We saved thousands of dollars and many hours every week by choosing this cost-effective technology with experts included. Alert Logic ensures that our cloud security extends being the reactive to a truly proactive stance – allowing us to continue successfully growing the Hillarys brand.”
Julian Bond
Head of Information, Communications and Technology, Hillarys

142
Customer references from happy Alert Logic users

VIEW ALL REFERENCES
ABOUT FORTINET
Fortinet protects the most valuable assets of some of the largest enterprise, service provider and government organizations across the globe. Fortinet's fast, secure and global cybersecurity solutions provide broad, high-performance protection against dynamic security threats while simplifying the IT infrastructure. Fortinet has strengthened the industry's highest level of threat research, intelligence and analytics. Unlike pure-play network security providers, Fortinet can solve organizations' most important security challenges, whether it be in networked application or mobile environments - be it virtualized/cloud or physical.

476
Customer references from happy Fortinet users
VIEW ALL REFERENCES

“With a network like ours and the demands that are placed on it, there is no room for second-best security. Fortinet delivers high-performance enterprise firewalling that enables us to drop malicious traffic and allow legitimate traffic in so the business can keep running.”
Mark Graff
Global Chief Information Security Officer, Nasdaq OMX

“When we added up the features that Fortinet brought to the equation and looked at the price/performance, the decision was clear-cut. Fortinet's FortiGate 1000C Next Generation Firewalls were, dollar-for-dollar, the most costeffective and function-rich enterprise solutions on the market.”
Hammad Akbar
Network Consultant, Advent One

“Fortinet's solutions are helping us to manage a large, often difficult network that comes with many different use cases. The result is that we're protecting Cambridge University's students, staff, research, data integrity, and, ultimately, its reputation.”
Ashley Culver
Network Services Manager, University of Cambridge

“Fortinet didn't only supply us with great security and massive reliability, but also gave us the flexibility to implement their solutions in our business helping us develop and transition from the legacy network into a powerful SD-WAN.”
Jonathan Merrell
Chief Information Officer, Alorica
ABOUT JASK

JASK is modernizing security operations by delivering an advanced SIEM platform that provides better visibility, better automation, and a better architecture. Built on cloud-native technologies, the JASK ASOC platform streamlines security analyst workflows by automating many of the repetitive tasks that restrict productivity, including data ingestion, normalization, parsing, and triaging alerts. JASK frees SOC analysts to focus on investigative and response efforts and perform higher-value roles like threat hunting and vulnerability management, while addressing the escalating talent shortage.

"Using JASK, BHG has improved the efficiency and efficacy of security operations all while using JASK’s predictable pricing model. Their support model has surpassed the typical and is more like a partnership than a typical support vendor.”

Fred Hamilton
Information Security Manager, Bankers Healthcare Group

"As we add technologies to our security toolbelt, the flexibility that JASK provides will be incredibly valuable. We look forward to adding data sources for JASK to correlate for us in the future, and continuing to reap the benefits of its powerful automation abilities.”

Kevin Vadnais
Manager of Information Management and Security, University of Lethbridge

"We can’t possibly add or train enough staff to manage this deluge of data, and AI is the only viable answer. We’ve had an incredible experience – the JASK team provides an unheard of level of customer support - and my security team is more effective than ever before.”

Lewis Brodnax III
Chief Security Officer, GreenSky

"JASK’s automation process and machine learning capabilities have helped us implement a threat hunting process that often doesn’t even need a human involved. Based on profiles that have been established by industry leaders on the JASK team -- guys who really understand how to analyze a threat -- threat hunting is applied in our environment through AI..."

Mitch Thomas
Chief Security Officer, Encompass Health

18 Customer references from happy JASK users
VIEW ALL REFERENCES

TRUSTED BY

Encompass Health
University of Lethbridge
GreenSky
Veeva
ABOUT LOGGLY

Loggly aims to empower the creators and operators of cloud-based services to operate flawlessly and deliver great user experiences by knowing what's going on with their applications and why. Loggly's cloud-based log management solution shows you what matters by crunching through huge volumes of log data that no human could possibly read. Loggly is the world's most popular cloud-based, enterprise-class log management solution, used by more than 6,000 happy customers. Founded in 2009 and based in San Francisco, the company is backed by Harmony Partners, Trinity Ventures, True Ventures, Matrix Partners, Cisco, Data Collective Venture Capital, and others.

“Loggly was a smarter choice for our cloud-based business, offering a painless adoption path with virtually no effort on our part and allowing us to accomplish the same things we had from our Splunk solution at a fraction of the cost.”

Brock Haywood
Director of Platform, SendHub

“The type of fast diagnosis, to find out if issues are one-off or systemic, is something that we haven’t found outside of Loggly.”

Bryan Tinsley
Site Reliability Engineer, Peloton

“I know from practical experience that the type of performance I get from Loggly would require a $1-2 million Splunk infrastructure. We have no capital expenditures, low recurring costs, and the ability to grow quickly.”

Jorge De La Torre
DevOps Engineer, Stanley Black & Decker

“Log management is critical for running an operational service like a game. If we didn’t have Loggly, there would be days where our revenue would be affected by as much as 70 percent.”

Albert Ho
Engineer, Rumble Entertainment
2019 RISING STARS

Netsurion™ EventTracker

LOGPOINT

logentries by RAPIDD
ABOUT EVENTTRACKER

EventTracker is a Netsurion company, empowers organizations to successfully predict, prevent, detect, and respond to cybersecurity threats. The EventTracker SIEM platform unifies machine learning, behavior analytics, and security orchestration, and has been recognized for 10 straight years by Gartner on the Magic Quadrant for SIEM. EventTracker offers a suite of SIEM solutions built for any size company or budget. More and more organizations are seeking SIEM-as-a-Service to realize optimal security results. SIEMphonic builds on the EventTracker platform by delivering a Co-Managed SIEM service complete with 24/7 global Security Operations Center (SOC), powered by threat intelligence.

“...we let other coops know. We’ve been thrilled with what we get from EventTracker and we were thrilled enough to share the great results.”

Tim Peede
Vice President of IT and CIO, South River EMC

“There are hundreds of attacks against our internet connection every day, but with EventTracker I feel safer knowing that I have alerts and a secure audit trail in the event there is an incident.”

Shan Venable
Vice President Incharge of IT, Darby Bank & Trust Company

“We were impressed with EventTracker since it provided us with far better functionality than other log management solutions at a much more affordable price and also delivered tremendous value in terms of increased efficiency and savings in time.”

Michel Vereshchatsky
Senior Application Analyst, College of Humanities, The University of Arizona

“Our log-on failure report generally runs 10 pages. One day it ran to over 3,000 pages. This quickly alerted me to an issue with our passwords, and helped me prevent potential security threats. I would never have caught this, if it hadn’t been for EventTracker.”

Robert Sheridan K. Smith
Information Technology Manager, Arch Reinsurance Ltd.
ABOUT LOGPOINT

LogPoint enables organizations to convert data into actionable intelligence, improving their cybersecurity posture and creating immediate business value. Their advanced next-gen SIEM, UEBA and Automation and Incident Response solutions, simple licensing model and market-leading support organization empowers their customers to build, manage and effectively transform their businesses.

27
Customer references from happy LogPoint users

"The operational cost savings we've seen have been impressive, and the support we've received from LogPoint before, during, and after implementation has really been fantastic. We're now upgrading to the latest version of LogPoint and looking to leverage its analytics to assess other areas such as asset utilization and more detailed profiling of the...

Chris Newby
Systems Infrastructure Manager, University of Bedfordshire

"LogPoint allows Computerome administrators to quickly detect unusual behavior in the system and to prevent misuse and data breaches. It provides that extra layer of security on top of the established security controls, which is required when handling vast amounts of data. It also allows us to provide our users with full insight and transparency."

Peter Løngreen
National Life Science Supercomputing Center, Computerome

"The strength of the LogPoint solution is that we don't have to spend unnecessary time on investigating false positives and that we check all logs. Not only logs chosen at random. This way, we comply to the legal requirements of effective log auditing."

Joakim Bengtzon
IT Security Manager, Region Värmland

"A highly responsive support in deploying the solution plus total control over costs were decisive criteria in validating the LogPoint solution. The savings generated by the LogPoint solution allowed us to upgrade the quality of service offered to our organization, which is an unexpected but much-welcomed benefit."

Cédric Chevrel
CISO, Matmut
ABOUT LOGENTRIES

Logentries (by Rapid7) is the leading real-time log management and analytics service built for the cloud, making business insights from machine-generated log data easily accessible to development, IT and business operations teams of all sizes. With the broadest platform support and an open API, Logentries brings the value of log-level data to any system, to any team member, and to a community of more than 35,000 worldwide users. While traditional log management and analytics solutions require advanced technical skills to use, and are costly to set-up, Logentries provides an alternative designed for managing huge amounts of data, visualizing insights that matter, and automating in-depth analytics and reporting across its global user community.

30
Customer references from happy Logentries users

苗

"At Boxever our systems are mission critical. Logentries helps us keep them up and running 24X7, and provides our operations and development teams with the actionable information we need to stay ahead of complications before they arise.”

Dave O’Flanagan
CEO, Boxever

"I used to settle for knowing there were certain insights I simply wouldn’t uncover because I couldn’t interrupt our dev team. Logentries now enables me to identify problems and patterns I couldn’t see before.”

Sean McGlinchey
Chief Data Officer, Yummly

"We made a great decision - Logentries’ ability to display production logs across the entire architecture with read-only access for developer and QA teams has been a huge boost to productivity. And the support has been fantastic.”

Colin Ebert
Operations, Innotas

"We were constantly running into the same issue - pinpointing specific events when errors arose was difficult and time-consuming. We knew there was a better solution out there.”

Nick Andren
Developer, TrackIf