



THE ULTIMATE MSSP PLATFORM

Logpoint provides the ultimate platform for managed security service providers (MSSPs) to efficiently deploy and operate our multi-tenant SIEM, SOAR and UEBA solution across customers and geography. The solution has been developed in collaboration with some of the world's largest MSSPs, to ensure the best and most efficient experience for their customers. As the central cybersecurity platform, Logpoint provides a solution with best-in-class analytics to detect breaches, enable threat hunting and manage incidents across customer environments.

MANAGED SECURITY SERVICES IN DEMAND



As the cybersecurity threat evolves and approaches the top of the corporate agenda, the need for efficient cybersecurity-solutions and a highly skilled cybersecurity-workforce is growing. At the same time, the cybersecurity skill gap is increasing dramatically to an estimated 4,07 million people globally, resulting in security analysts being difficult to attract and retain¹. On top of this, cybersecurity is becoming increasingly complex, as IT infrastructures converge towards hybrid deployments between cloud and on-premise, it is more important than ever to have on central security solution.



Businesses across the globe are increasingly turning to MSSPs to acquire efficient and skilled cybersecurity resources. According to Gartner², the key reasons for choosing Managed Security Services includes:

- > An inability to hire enough skilled security personnel (due to budget, regional, cultural or other constraints)
- > An ever-expanding list of security technologies to purchase, manage and operate, to deal with the threat landscape
- > An imperative to accelerate security operations improvements due to changes in the threat landscape or the business
- > Budget constraints that prevent IT from building its own mature security monitoring capabilities and agile security device management
- > A desire to reduce security monitoring complexity by turning over all monitoring controls to a single party
- > The ability to leverage an MSSP's threat intelligence (gained from monitoring many distinct customer networks)
- > Strategic decisions to delegate menial, repetitive tasks to a third party so that valuable security staff can focus on incidents



According to the leading B2B research company MarketsandMarkets, the global MSSP market size is expected to grow from USD 24.05 billion in 2018 to USD 47.65 billion by 2023, at a Compound Annual Growth Rate (CAGR) of 14.7% during the forecast period.

The demand for managed security services is expected to be driven by the factors above, and Logpoint provides MSSPs with state-of-the-art solution, to meet and exceed the demand from end-customers and help them drive business.



The demand for managed security services is expected to be driven by the factors above, and Logpoint provides MSSPs with state-of-the-art solution, to meet and exceed the demand from end-customers and help them drive business.

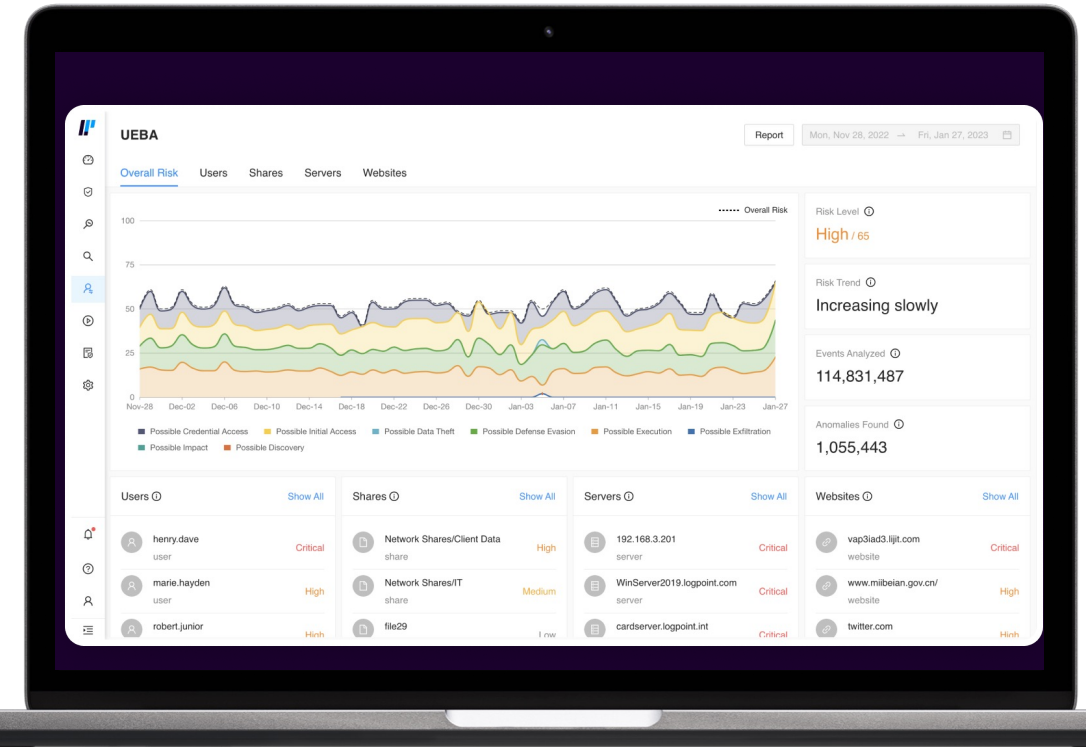


A unique growth opportunity

The MSSP market represents a unique growth opportunity for IT service providers across the globe. At the heart of any MSSP services is a SIEM solution, compiling security data from across the customer IT infrastructure, providing situational awareness of threats and the analytics to detect breaches, enable threat hunting and manage incidents.

Logpoint aggregates data from the entire customer IT infrastructure to provide a centralized security overview, and the analytics to detect breaches, enable threat hunting, and manage incidents.

Logpoint has developed our MSSP solution in collaboration with market-leading providers in Europe and the US. The result is an excellent platform, tailored to enable MSSPs in providing value-adding services and handle security management complexity on behalf of the end-customers.



THE LOGPOINT TECHNOLOGY ADVANTAGE



Efficient analytics for any MSSP



Logpoint delivers a Modern SIEM solution that provides accelerated detection and response to security events or incidents and enables analysts to do efficient threat hunting and forensic investigation. Logpoint provides a wealth of integrations to market-leading security applications, to ensure that the SIEM is a flexible fit to the MSSPs business and technology strategy. With Logpoint as the central security solution, analysts can quickly examine the correlation of events. Integrations with Threat Intelligence solutions allows for quick validation of the output delivered by Logpoint.

The SIEM software collects and aggregates security data generated throughout the infrastructure, from host systems and applications, whether on-premises or in the cloud, from network and security devices, such as firewalls and routers. The SIEM then identifies, categorizes and analyzes incidents and events and delivers real-time alerts, dashboards or reports to the security operations center, enabling efficient analytics across all data sources.





How UEBA enable efficient anomaly detection

With User Entity Behavior Analytics (UEBA) based on advanced, unsupervised, Machine Learning, Logpoint provides extensive anomaly detection capabilities for advanced threat detection, by applying more than 400 Machine Learning models into the solution. It enables analysts to detect cyber-attacks by spotting unusual patterns of activity, eliminate false positives, and increase their effectiveness to reduce the resources required to run security operations.

Logpoint SIEM allows cybersecurity teams and security operation centers to see the bigger picture by collecting security event data from applications, the cloud, and core infrastructure to learn precisely what goes on within the network – creating value from the sum of data which is worth much more than the individual pieces. A single alert from an antivirus filter may not be a cause of alarm on its own. However, if it correlates with other anomalies at the same time, this could be worth investigating by the security analysts.



Key Logpoint SIEM and UEBA benefits

- Accelerated detection and response by source agnostic SIEM and UEBA across every application in the enterprise infrastructure
- Market-leading data privacy and protection capabilities, enabling security analytics while safeguarding Personally Identifiable Information
- Logpoint normalizes data from the entire network infrastructure into a single Common Taxonomy at ingestion, enabling efficient analytics across all data sources
- Hundreds of data source integrations make the Logpoint SIEM and UEBA truly source agnostic, to perform best in class correlations and cross-application analytics
- Incisive analytics provides instant insights to enable security analysts to prioritize efforts and accelerate root-cause analysis
- The lowest hardware footprint of any Modern SIEM deployment on the market, including GDPR compliant, cloud based, UEBA
- Prioritization of alerts with ML-based incident scoring reducing false positives
- Transparent and True Predictable Pricing means licensing is not a limiting factor when planning how and which data to analyze.
- Correlation across applications with a wealth of integrations, enabling faster and more efficient Threat Hunting and Security Orchestration, Automation and Response (SOAR)

THE ULTIMATE MSSP PLATFORM



As an MSSP, monitoring the customer's cyber-security incidents, analyzing security data, and responding to threats is where the focus should be. Time is valuable and maintaining a cumbersome SIEM solution shouldn't be on the top of the to-do list. Logpoint is the solution to help with that.



Logpoint Director is the ultimate tool for MSSPs offering managed services based on our SIEM and UEBA solution. In collaboration with some of the largest MSSPs in the world, we have developed a unique multi-tenant SIEM platform that leverages the needs for a modern management fabric, fully integrated on top of the Logpoint SIEM and UEBA solution.

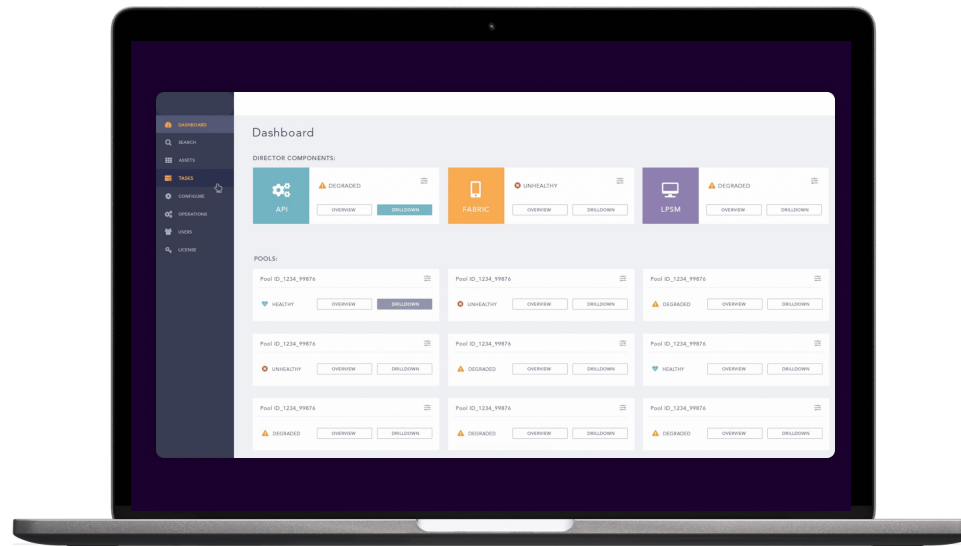


A centralized console for cybersecurity log monitoring

With the Director, MSSPs are able to orchestrate and automate many management tasks that would otherwise tie up the ops-team. From a single pane of glass, the Director gives MSSPs a tool to easily update, manage, operate, and monitor large multi-tenant and single-instance SIEM deployments.

The Logpoint Director is a centralized point for orchestration of the entire Logpoint environment, allowing easy, simplified deployment and management of Logpoint instances (pools) while allowing segregation of information across the MSSP customer base.

The Director Console is used to push configurations to a pool of Logpoint servers (deployments). This can be done if an organization has several subsidiaries, or customers, whom must not view the other customer's Logpoint data, while providing full access to the MSSP. Multi-tenancy enables MSSPs to separate customer deployments, making it easy and secure to manage the different Logpoint pools, made convenient by centralizing server configuration from the Director





Investigate widely or deeply

For MSSPs fielding large deployments, where different teams or different regions have their own analytics needs, deployments may contain more than one analytics node. Centrally managing these nodes is done through the Logpoint Search Master, which can connect an analyst to a decentralized analytics node, conduct investigations, or assist a local user with an incident. The Search Master allows a central team of security analysts to view data across multiple analytics nodes.

The Director Fabric is the infrastructure that ties together the Director Console and Search Master with the Logpoint SIEM servers. The Fabric is a full API used internally and exposed to administrators, enabling easy orchestration, providing authentication methods, and managing licenses. Director Fabric also makes it easy to streamline Logpoint and summarize all the Logpoint servers' health data – positioning the MSSP to control their environment more efficiently.



The Director

– takes the hassle out of managing SIEM by simplifying time-consuming tasks. It allows MSSPs to focus on the value-adding services and work efficiently across large Logpoint installations. Logpoint provides several advantages for MSSPs:

- > A true multi-tenant platform and a strong emphasis on resiliency and High Availability
- > Augment and connect the Logpoint solution to existing automation and orchestration platforms for both provisioning and managing incidents, playbooks, and workflows
- > The Director features serve as an addition to the Logpoint solution, delivering a centralized, easy to use interface for deployment, maintenance and integration tasks
- > Through a strong product architecture, Logpoint allows for extensions, normalizations and plugins to be written with short turnaround time by Logpoint or the MSSP
- > Logpoint allows MSSPs to scale while maximizing ROI through easy scaling of hardware and software while keeping costs in control through predictive, node-based licensing

HOW IS LOGPOINT WORKING WITH MSSPS



Logpoint is working with MSSPs across Europe and the US, providing our modern SIEM, SOAR and UEBA solution in complex infrastructures across customers, geography, divisions, and subsidiaries.

We provide a centralized, unified solution for management, correlation, and analysis of security data, translating data into valuable intelligence, enabling MSSPs to make informed decisions



Super-compliance and business expansion

RAM Infotechnology is a Dutch IT services company specializing in IT outsourcing, managed services, and cloud-based services. Logpoint enables RAM Infotechnology to stay compliant with an impressive array of industry standards, while at the same time boosting cybersecurity and opening a new revenue stream providing managed SIEM services to end-customers.

“The bottom line is that Logpoint enables us to document compliance with a wide variety of standards and boost security as well. The SIEM solution enables us to provide our customers with better services and support. We are already delivering Logpoint-based services to two customers and are planning on expanding the installation. Logpoint is now a part of our service offering and is generating revenue”



Frank Waarsenburg,
CISO at RAM Infotechnology.
The Netherlands



SoC and CERT services

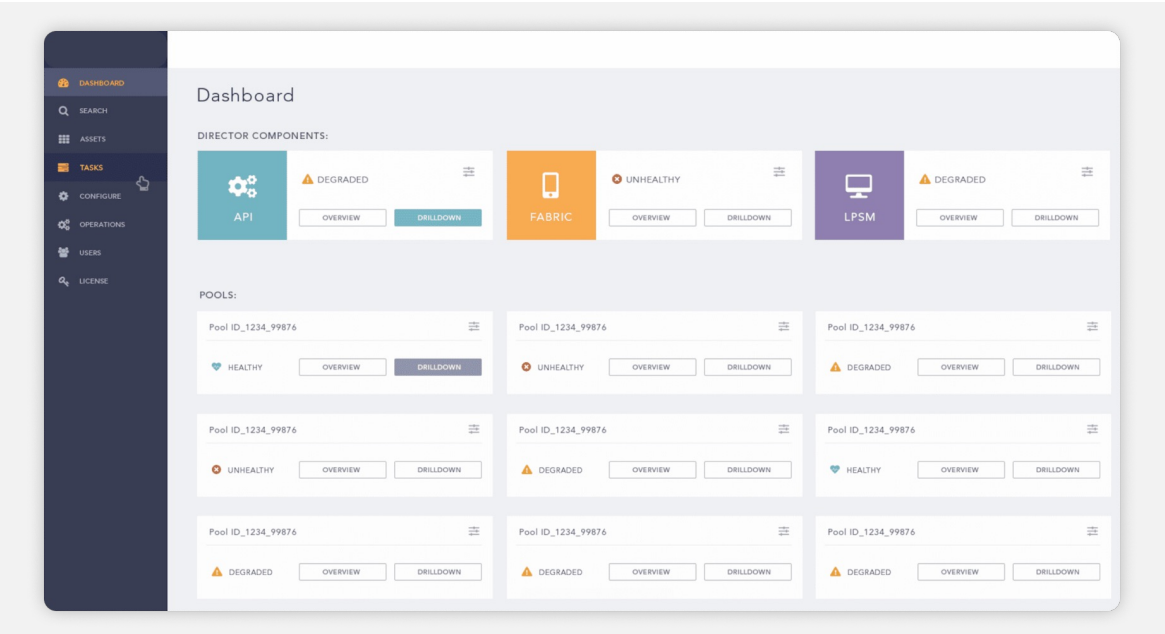
Founded in 2004, 8com is a full-service cybersecurity provider, employing 55 cybersecurity specialists. Since 2010, 8com has operated its own Cyber Defense Center, a Security Operations Center (SoC), and the Computer Emergency Response Team, providing 24-7 cybersecurity services to more than 40 customers. The 8com SoC relaunched in 2019 with Logpoint at the center of operations.

“Following extensive evaluations, we have selected Logpoint for 5 main reasons. Logpoint is made in Europe, and It's the only EAL 3+ certified SIEM solution around. While other vendors focus on the Cloud, Logpoint remains dedicated to on-premises solutions and provides the perfect platform for Managed Security Services. And finally, the Logpoint licensing model is very attractive”

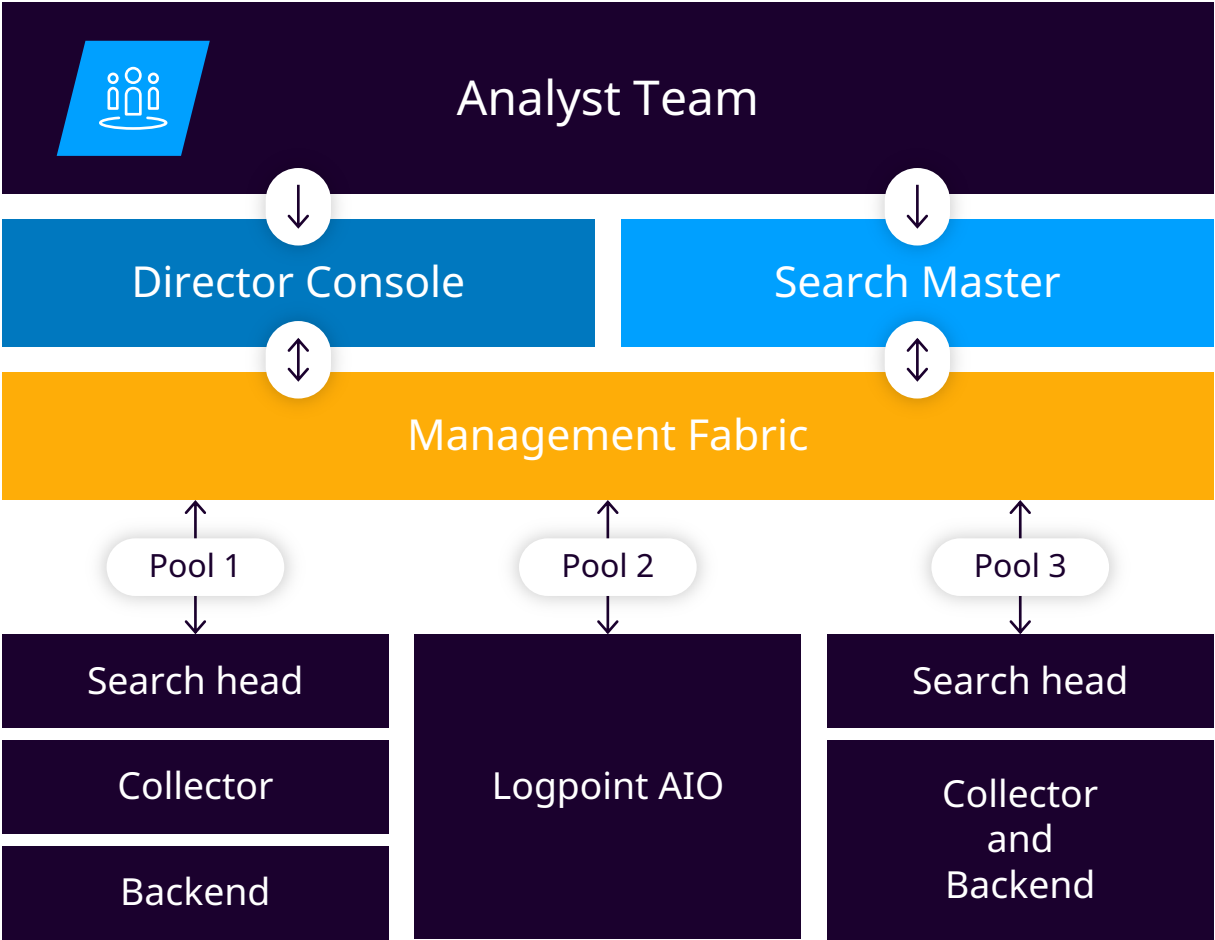


Götz Schartner,
Founder and CEO of 8com,
Germany.

LOGPOINT DIRECTOR ARCHITECTURE



Full support for multi-tenancy



LOGPOINT BUSINESS ADVANTAGE



Logpoint is committed to providing the ultimate SIEM, SOAR and UEBA solution for MSSPs. We are a true partner-centric SIEM, SOAR and UEBA vendor, selling only through certified resellers and MSSPs, offering a permanent commission on the Logpoint portfolio that each partner accumulates. In addition to 2nd and 3rd level support for partners, we also contribute actively to system integration needs as a natural part of the partnership.



We offer a simple, transparent, and powerful go-to-market model for MSSPs, including:

- > Transparent pricing (node-based pricing vs. volume-based licensing)
- > Licensing follows the “pay-as-you-grow” principle – pay only for what is consumed, no upfront payments for the MSSP
- > Quarterly licensing with full flexibility, including enterprise licensing agreements for very large customers.
- > Partner centric: We have a direct professional touch to end customers and generate high quality leads to all our certified partners.
- > Our service and support stand out as the best in the industry
- > And don’t just take our word for it: Take a look at our credentials



**98% Consistent
Customer
satisfaction**



**Only European and
only new SIEM
vendor in the 2018
Gartner SIEM Magic
Quadrant**



**2019 Gartner
Peer Insights
Customers' Choice
for SIEM**



**Gold Medalist in the
2019 Data Quadrant
Report for SIEM by
SoftwareReviews**

ABOUT LOGPOINT



Trusted by more than 1,000 enterprises

KONICA MINOLTA

CAPTIVATE



GoSecure

RÉMY COINTREAU

Awards and honors



Gartner Peer Insights

Gartner

Gartner
Magic
Quadrant



For more information, visit www.logpoint.com

Logpoint is the creator of a reliable, innovative cybersecurity operations platform — empowering organizations worldwide to thrive in a world of evolving threats.

By combining sophisticated technology and a profound understanding of customer challenges, Logpoint bolsters security teams' capabilities while helping them combat current and future threats.

Logpoint offers SIEM, UEBA, and SOAR technologies in a complete platform that efficiently detects threats, minimizes false positives, autonomously prioritizes risks, responds to incidents, and much more.

Headquartered in Copenhagen, Denmark, with offices around the world, Logpoint is a multinational, multicultural, and inclusive company.