



We are helping companies detect and respond faster than ever before. But looking ahead, we'll see that without a proper security foundation, even the best tools won't help companies detect or respond faster, says LogPoint CTO Christian Have

Jan 29, 2021 13:10 CET

## LogPoint: Security foundation must be solid to benefit from new cybersecurity technology

**While deploying new technologies is a critical element to effectively respond to cybersecurity threats, a strong security foundation should be on top of the agenda, says LogPoint CTO Christian Have in 2021 Outlook.**

**COPENHAGEN – January 29, 2020** – [LogPoint](#), the Modern SIEM and UEBA company, today published its 2021 Cybersecurity Outlook, providing strategic guidance for customers and partners on the year ahead. The Outlook concludes on developments in the past year and identifies trends LogPoint

CTO Christian Have believe will shape Cybersecurity in 2021.

“In 2021, the industry will present automation and orchestration of incidents as a panacea. Looking at where critical decisions are made during triage and response and looking at how detection takes place, AI and ML have a place, and so does automation. But most important to enable accelerated detection and response is the foundation,” says Christian Have.

“We are helping companies detect and respond faster than ever before. But looking ahead, we'll see that without a proper security foundation, even the best tools won't help companies detect or respond faster,” says Have.

In the 2021 Cybersecurity Outlook, Christian Have anticipates four significant trends:

- We expect more organizations to take a hard look at their existing architecture. Rather than implement a lot of new technology, they'll find ways to adopt simple measures that limit breaches' impact.
- Robust controls anchored in a security architecture framework will free up analysts' time to focus on what's essential: risk models and gathering supporting evidence to triage effectively.
- To achieve security automation or orchestration capabilities, security teams must finely tune the security architecture and controls, or else run the risk that systems either miss or act insufficiently to manage the breach, leading to a false sense of security for the teams relying on these capabilities.
- The attack graph is real, and point solutions add more complexity than net security increases unless the foundation and architecture are firmly defined and followed.

The full [LogPoint 2021 Cybersecurity Outlook](#) by CTO Christian Have is at LogPoint.com

For more information, visit [www.logpoint.com/press](http://www.logpoint.com/press)

The attached photos can be used by the media free of charge.

---

## About Logpoint

Logpoint safeguards society in a digital world by helping customers and Managed Security Service Providers (MSSPs) detect cyberattacks. Combining reliable technology with a deep understanding of cybersecurity challenges, Logpoint makes security operations easier, giving organizations the freedom to progress. Logpoint's [SIEM](#) and [NDR](#) technologies improve visibility and give a multi-layered approach to cybersecurity that helps customers and MSSPs in Europe navigate the complex threat landscape. Headquartered in Copenhagen, Denmark, Logpoint has a European foundation and is the only European SIEM vendor with a Common Criteria EAL3+ certification. This demonstrates Logpoint's strong focus on data protection and cybersecurity regulations. For more information, visit <http://logpoint.com>.

## Contacts



### **Maimouna Corr Fonsbøl**

Press Contact

Head of PR

PR & Communications

[mcf@logpoint.com](mailto:mcf@logpoint.com)

+45 25 66 82 98