IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

In Conversation

In Conversation with Jesper Zerlang

Carol Baker

As cybersecurity provider Logpoint continues to dominate the SIEM vendors market in Europe, we catch up with Jesper Zerlang, CEO, Logpoint for his views on what changes we can expect to see in the technology this year.

Jesper Zerlang has been CEO of Logpoint (https://www.Logpoint.com) since 2009, and has led Logpoint to become the dominate Security Information and Event Management (SIEM) vendor in Europe.

He has more than 25 years' experience in the IT industry and has held top management positions at Telia Company, Dell Computer and Compaq.

His strong customer and partner focus, passion for his employees and great entrepreneurial spirit helps to spark innovation and growth at Logpoint.

Jesper has supplemented his leadership skills with executive management programs at Harvard Business School.

Tell our readers what sets Logpoint apart from its competitors?

Logpoint was originally founded as an IT security consultancy which really sets us apart from our competitors, many of whom were founded in big data analytics and have then later pivoted into the cybersecurity domain. Having deep roots in cybersecurity has provided us with the essential knowledge, understanding and capabilities to deal with the cyberthreat landscape. Everything we do, and everything in our DNA, is centred around providing genuine cybersecurity solutions to end customers.

We started out in the Nordic region and initially had around 70 large Swedish and Danish customers whom we were providing cybersecurity consultancy to as well as providing them with different solutions to suit their needs.

However, within three or four years we began to realize that many of our customers in the region were looking for an efficient way to manage their logs, as the exponential growth of data was leading to chaos. Then, at the back end of the financial crisis, a lot of technologies started to appear in the USA, but there were no European vendors in this space. So, we saw that there was a big opportunity for us to focus in this area.

We acquired a small start-up from a university near Copenhagen which we then built out to focus upon SIEM and log management. The funny part is that even today, several years later, we remain the only non-US vendor in this domain, which is unusual.

It is still a puzzle to me why there are no European competitors, when there is easily room for more. The simple answer is that it is an extremely complex market to enter, in part due to the difficulties in managing the massive data volumes involved. To do this requires a large organization, with incredibly advanced technology – making the entry barrier quite high.

Growing out of Copenhagen and the Nordics, we expanded across Europe to London, Paris, and Munich. We've since added offices in Boston to serve the US market, and in Nepal to serve the Asian market. Along with Europe, these areas are our key focus as a company. We now have customers all over the world, and have just passed the 300 employees' mark. We hired more than 140 people last year, almost doubling the existing number, and we are now serving almost all industries across Europe and the US, which is testimony to just how fast the company is growing.

There are, of course, some areas in which we are stronger than others such as business critical application security and protecting SAP environments. These customers and functional domains are where we have seen a pocket of opportunity to gain traction ahead of our competitors because our cybersecurity foundation allows us to navigate the complex processes of ERP systems.

What is happening in the market right now?

There is currently a big transition from general IP protection to actually protecting more of your deeper IP, financial and operational data. This data often resides in the SAPs and Oracle's of this world – and it is an area where CFOs and CEOs are taking much more of an interest than just protecting the broader IT infrastructure. Cyber topics are now considered a board issue for many of our customers.

How is Logpoint developing to its solutions to handle the transition?

From a product perspective, we are moving our products into the cloud. A third of our portfolio is already fully SaaS native, and by the end of 2022 we will have full-blown availability in the cloud. It is a very complex undertaking and one that takes us back to our security roots.

Going into the cloud is not necessarily the answer to the world's problems, especially from a cybersecurity perspective because when you have all your data in the cloud, you can also lose control. Therefore, we are particularly cautious with the way we are transitioning into the cloud. Our focus is on security and ensuring that the data of our customers remains secure.

Another issue is that there are a lot of organizations in the world who do not, and will not, go into the cloud. Defence organizations, the police, the intelligence services, and NATO, for example, are reluctant to send data to Microsoft or Amazon as they want to maintain control of the data, and they still require an on-premise system for managing security.

We are very proud to be the only cybersecurity vendor to have our solution certified to the Common Criteria EAL Level 3+. This means that if you are a defence force or part of a critical infrastructure organization in Europe, Logpoint have the only product trusted at this level. Again, I believe that our background in cybersecurity consultancy has given us this advantage over our competitors.

How do you explain Logpoint to non-technical corporate leaders?

Sometimes when I have had to explain Logpoint to a non-technical person, I compare it to blood sampling. For a company, all your logs are actually your company's blood or DNA. By analyzing the logs, we can basically see the state of health of the patient, only it's not based on the occasional sample, but goes on in real time. It allows us to continuously monitor how exposed you are to disease from a cybersecurity perspective. When companies realize this, it is an eye-opener. But this type of log analysis goes even further as it also gives them the ability to analyze data and predict their future exposure from a security perspective.

Cybersecurity as a Service is trending now, what can we expect to see moving forward?

Cybersecurity as a Service is going to be a huge topic in the years to come. The big players such as the likes of Deloitte, PwC, Accenture, even Telcos, are going to be much more active in providing protection for companies, especially companies who do not have the internal cybersecurity capabilities or are not able to attract employees with the necessary expertise. Let's not forget that the biggest challenge we probably have today is lack of skilled cyber people. Right now, there are more than two million cyber security people missing from the marketplace, and it is impossible to close this gap in due time. The only way to do this is by leveraging the efficiencies of Cybersecurity as a Service, and implementing automation, machine learning and artificial intelligence.

Cybersecurity is now top of the agenda for corporates, and we see more CISOs on the executive boards because cybersecurity is becoming such a complex issue. Cybersecurity is no longer just an appendix to a Request for Proposal (RFP) when you do a digital transformation project.

So, for a cybersecurity vendor like Logpoint, you have to be able to articulate how you add value to a company's true business focus. It is not just a matter of buying a commoditized product and then expecting everything to work. It's about understanding what the business issues are from the customer perspective and then applying a solution that addresses those and adds value from day one.

Speed is also important and this is something that is often overlooked. Many companies spend one or two years (especially if they are a very large company) just trying to articulate what they need from a cybersecurity solution. But, by the time they have implemented the solution, they have more than likely already been compromised. Companies need to apply a much more agile approach to keeping them secure during the digital transformation journey.

How do businesses create a holistic approach to security?

In my view, the most important factor is securing business-critical applications. If you look at SAP for instance, this application has become the backbone of digital transformation for many companies. But management are not paying enough attention to incorporating it into the overall security strategy – and they should. Instead, it just becomes a question of ticking a compliance box, rather than actually securing the business-critical application in the most efficient way.

I always recommend any company who is operating in a SAP environment to step outside of the box and look at the security aspect separately. Although many network and security teams are addressing this by deploying cybersecurity platforms across the product lifecycle, SAP is often an area that falls through the security gap. With all the business-critical information stored in a SAP system, and the dramatic consequences to an organization if it is compromised, SAP security should be one of the first considerations on your digital transformation journey.