

Borlänge Municipality



“The solution provides excellent reporting capabilities and is easy to manage.”

— Jan Stegaras, IT Operations Manager, Borlänge Municipality

INDUSTRY
Government

COUNTRY
Sweden

PRODUCT TYPE
Forcepoint Web Security and
Forcepoint Email Security

SIZE
12,000 Users

SECURITY ISSUE
Meeting Compliance
Regulations for Data Security

OVERVIEW

[Borlänge Municipality](#)—in Dalarna County in Sweden— has a population of around 48,000 people. The local government is the town’s largest employer with around 3,800 employees. The IT department supports these employees as well as employees at related city organizations, all of which total 4,500 employees on a wide variety of applications.

CHALLENGE

For quite some time, data theft prevention and data security had been on the agenda for the IT team at Borlänge Municipality. As a government organization, it was especially crucial that Borlänge meet strict compliance regulations. When the existing information security solution in Borlänge had reached end of support, the IT team started a serious search for a new and more advanced platform.

SOLUTION

After a thorough selection process, Borlänge selected Forcepoint solutions. Since then, Borlänge’s ability to protect its data has improved significantly without increasing pressure on IT management.

“We needed to determine if we wanted to continue with our existing supplier or look for an alternative. As our existing system was not able to meet all of our needs—especially with regard to data theft prevention—we turned to the market. We evaluated a variety of solutions and it turned out that Forcepoint TRITON was the best match for our requirements.”

— Carl Söderström, Information Security Officer,
Borlänge Municipality

Forcepoint’s unified approach is one of the reasons why Borlänge selected the Forcepoint solution. The Forcepoint Web and Email solutions with Hybrid and DLP modules integrate to offer data theft



prevention applied to web and email channels, unified security intelligence and unified policy and reporting. Modern phishing attacks succeed primarily because phishing emails now contain embedded links that point to dynamic-IP botnets or web pages that host dynamic code. With Forcepoint, email is protected by Point-of-Click Threat Analysis URL Sandboxing which isolates suspicious links embedded in emails and analyzes the payload of the corresponding web page at the recipient's point-of-click. In addition, the platform blocks malware in real-time with SSL-inspection. Another reason for choosing Forcepoint was the advanced data theft prevention capabilities:

“For us, it is very important that privacy related information does not leave the organization.”

— Söderström

With Forcepoint solutions, an organization can create policies that prevent employees from sending specific information externally, such as social security numbers, in an email. TRITON Architecture will stop the email and send an alert to the user. This also applies to specific documents which can be stopped by TRITON Architecture when they are attached to an email.

The third major reason for Borlänge selecting the Forcepoint platform was its granular policy-setting and filtering capabilities. According to Carl Soderström, this provides much more control of the organization's data and is very useful for educating staff on data privacy. For Bengt-Ake Soderberg, IT Security Officer in the IT team at Borlänge, manageability was an important feature during the selection process.

“Forcepoint solutions provides one single interface which has considerably improved the manageability of all our security efforts. We can manage all functions for web and data security and data theft prevention through one single and user-friendly interface. This saves us time.”

— Bengt-Ake Soderberg, IT Security Officer, Borlänge Municipality

In Soderberg's opinion, the TRITON Architecture also plays an important role in supporting ISO 27001 initiatives at Borlänge. Several city departments are ISO 27001 compliant and Forcepoint's reporting capabilities particularly help in meeting these tough compliance requirements.

RESULTS

According to Jan Stegaras, IT Operations Manager at Borlänge, the IT department has been able to lay a strong foundation for IT and data security.

“Up until now we were very much focused on providing maximum security in a reactive manner. Now we are ready to take the next step and secure our systems more proactively. Forcepoint provides the tools necessary for this process.”

— Jan Stegaras, IT Operations Manager, Borlänge Municipality

Stegaras and his colleagues are unanimous in their evaluation of Forcepoint as the right choice for Borlänge.

“With Forcepoint, we have a greatly enhanced insight into the security risks which have been mitigated. The solution provides excellent reporting capabilities and is easy to manage. Also, the support from Forcepoint always provides exactly what we need, when we need it. We are very happy with this platform and convinced we have made the right choice.”

— Stegaras

Borlänge Municipality has relied on Forcepoint solutions since 2013.

CONTACT

www.forcepoint.com/contact

ABOUT FORCEPOINT

© 2017 Forcepoint. Forcepoint and the FORCEPOINT logo are trademarks of Forcepoint. Raytheon is a registered trademark of Raytheon Company. All other trademarks used in this document are the property of their respective owners.

[CASESTUDY_BORLÄNGEMUNICIPALITY_EN] 300070.021317