Case study

Multi-layer protection against unknown threats

Lomma Municipality strengthens its defense against Zero Day-attacks and harmful content with WithSecure™ Elements Collaboration Protection

Customer
Lomma Municipality

Country
Sweden

Industry
Public sector

Solutions
WithSecure™ Elements Collaboration Protection

WITH secure | LOMMA KOMMUN

Lomma Municipality, located on the southern coast of Sweden with 1700 employees, has large amounts of personal data to handle. Their heavy email flows via Microsoft 365 platform were letting malicious content through. Recovering from incidents took its toll on their IT department. Another layer of protection was needed – and they found it in the cloud native solution from long-time cyber security partner WithSecure™.

The Zero Day attack: a wakeup call

Over the past 11 years. Lomma Municipality has used various client protection solutions from WithSecure™ to protect the municipality against various types of cyber-attacks. To strengthen their defenses against targeted cyber threats, something traditional anti-virus solutions simply can't do, Lomma Municipality deployed WithSecure's Rapid Detection & Response solution, which uses automated sensors and machine learning to analyze users and alert them about deviant behavior patterns.

Before deploying WithSecure's RDR solution, Lomma Municipality was subjected to a Zero Day attack. Municipal employees clicked on a link contained in an email, not realizing that the link carried malicious code. The malicious code spread throughout the IT-system by exploiting unknown vulnerabilities in the municipality's software. The breach was not detected by the municipality's existing client protection at the time and caused significant damage, a costly and time-consuming affair to recover from.

In light of this, the municipality, led by IT and service manager Patrik Flensburg, decided to further strengthen its defenses – especially against Zero Day attacks, which have become increasingly common in recent years. These attacks can result in sensitive and valuable data ending up in the wrong hands, if the intrusion is not detected and mitigated at an early stage. In addition they can require time consuming and costly management and restoration afterwards.

These were the main challenges for the municipality:

- A heavy email workload of 1700 employees
- Large amounts of crucial personal data
- An increased number of Zero Day attacks
- Malicious content getting through the built-in protection of Microsoft 365

> **"We realized that we needed to add new layers of protection to our existing client protection as hackers constantly develop their attack methods."**
>
> Patrik Flensburg, IT and Service Manager

> **“Having a solution that can easily control all incoming emails is extremely important. Not least considering the statistics that show 94 percent of all malware spreads that way.”**

Patrik Flensburg, IT and Service Manager

> **“Knowing that our system controls all emails before they are let through means that I can now sleep well at night.”**

Patrik Flensburg, IT and Service Manager

The search for an effortless cloud-based solution

Lomma Municipality needed to strengthen its protection, with a solution that would be easy to manage in the cloud. After testing several different solutions, they chose WithSecure's new cloud-based and future-ready solution WithSecure Elements for Collaboration Protection. It strengthens the municipality's defense against Zero Day attacks as well as its’ Collaboration Protection, as the built-in protection in Collaboration Protection does not safeguard all the properties that users populate it with.

WithSecure™ Elements Collaboration Protection automatically controls the content of all emails and links sent to the municipal employees' email addresses and flags them for any anomalies that break the pattern. Every part of the email is scanned, and the system responds immediately. If it detects a file with a malicious behavior it places that file in a sandbox environment - a virtual environment where suspicious objects are quarantined and executed, to determine how they behave and whether they are malicious or should be allowed to pass through. The system also detects and responds to emails with possible phishing behaviors, as well as ransomware threats. “When WithSecure™ Elements for Collaboration Protection was launched, we felt, after testing the solution, that it was an affordable, comprehensive and user-friendly product that suited our needs very well”, says Patrik Flensburg.

Time and money saved – no more malicious content

In the first two months since the system was deployed, it scanned four million emails, of which 51 objects and 104 web addresses were identified as malicious and flagged. The system selected 626 events, such as emails, calendar invitations, contacts, Outlook groups, etc. and placed them in the sandbox environment to be tested during these first two months.

“This new solution has clearly increased the efficiency of our work which has saved us both time and money. Before, we sometimes had to spend time dealing with the harmful effects and restoration after malicious emails, such as phishing or ransomware emails, had been opened, “ Patrik describes and continues: “We now have a complete solution that guarantees that no malicious emails enter the system.”

Key benefits for Lomma Municipality:

- Time and money saved
- Comprehensive and easy to manage cloud native solution
- Automated discovery of previously unseen threats such as phishing emails, ransomware content and Zero Day attacks
- Faster response to emerging threats

Who We Are

WithSecure™ is cyber security's reliable partner. IT service providers, MSSPs and businesses along with the largest financial institutions, manufacturers, and thousands of the world's most advanced communications and technology providers trust us for outcome-based cyber security that protects and enables their operations. Our AI-driven protection secures endpoints and cloud collaboration, and our intelligent detection & response is powered by experts who identify business risks by proactively hunting for threats and confronting live attacks. Our consultants partner with enterprises and tech challengers to build resilience through evidence-based security advice. With more than 30 years of experience in building technology that meets business objectives, we've built our portfolio to grow with our partners through flexible commercial models.

WithSecure™ is part of F-Secure™ Corporation, founded in 1988, and listed on the NASDAQ OMX Helsinki Ltd.

WITH secure