

RESOURCE CENTER

ATEA onboarding playbook

4000+ employees to Bitwarden across 88 offices

Get the full interactive view at
<https://bitwarden.com/ja-jp/resources/atea-onboarding-playbook/>



Overview

Founded: 1968

Industry: IT infrastructure

Location: Northern Europe

Size: 8,500 employees

A country-by-country phased rollout that mandated no browser-extension password saving. Here are details on ATEA's proven blueprint for enterprise onboarding success.

ATEA is a Nordic and Baltic IT infrastructure company with 8,500 employees and 88 offices across seven countries (Sweden, Norway, Denmark, Finland, Lithuania, Latvia and Estonia). ATEA offers a variety of hardware, software, and services that enable organizations to manage their IT operations. The company prides itself on specializing in the entire lifecycle of information technology.

Table of Contents

Situation: Need for password management solution with self-hosting capabilities and strong security features

Solution: Implemented Bitwarden Password Manager with phased country-by-country rollout

Result: Measurable security improvements

Situation: Need for password management solution with self-hosting capabilities and strong security features

Understanding that the size of ATEA, nature of its work, and reach across Northern Europe necessitated use of an enterprise-wide password manager, its security team developed and engaged in a thoughtful and detailed evaluation process for identifying the most appropriate solution.

Password management risk analysis

To narrow down its options, ATEA created a comprehensive risk analysis analyzing 10 different risks potentially present in enterprise-wide password management deployment. The team explored the potential implications of a server going down in one country, how it may impact users in other countries, or what might happen if employees opted not to use the password management solution. Other considerations included weighing what would happen if customer support was not speedy or robust.

Narrowing down key features

Concurrently, ATEA also identified what it considered the most important security features to look for in an enterprise-wide password manager and settled on the following must-haves:

- Self-hosted solution
- Active Directory integration for authentication and group access management
- Multi-factor authentication
- Separation of private credentials and work credentials
- Encryption and password policy enforcement
- Logging of credential usage
- Offline access
- Compatibility with browser extensions, desktop, and mobile apps
- Dark web monitoring
- Single-sign on (SSO) integration
- Passwordless authentication capabilities

Solution: Implemented Bitwarden Password Manager with phased country-by-country rollout

Ultimately, ATEA narrowed down its selection to three solutions, with Bitwarden standing out from the pack for its passwordless authentication architecture. The same thoughtful and detailed approach that marked the ATEA selection process also extended to its deployment strategy.

Preliminary pilot program

ATEA kicked off its deployment by initiating a pilot program that enabled interested and engaged employees to test-drive the product. By starting with smaller user groups, ATEA was able to handle any issues before a larger-scale deployment, with ongoing updates and improvements made based on user feedback. It also coupled this with training calls with the Bitwarden customer support team, all with the goal of making the larger deployment process smoother and more seamless for employees.

Country-by-country rollout

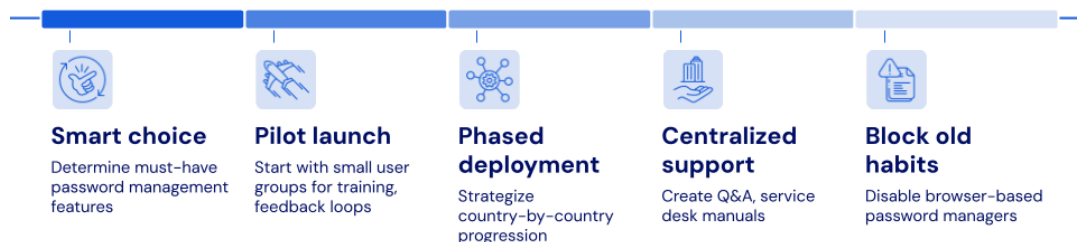
Next, ATEA segued into the most important part of its deployment strategy: rolling out Bitwarden on a country-by-country basis. After implementing the password manager, it observed users interacting with the product and encouraged employees to ask questions about utilizing Bitwarden. The first week proved very successful, with disruptions primarily consisting of employees forgetting their master passwords and having to reset their accounts. ATEA prioritized rolling out Bitwarden to smaller countries first, with a focus on ironing out any technical or logistical issues, before offering the solution to larger countries.

"It was very important to us that we have one single source of truth for employees that needed more information about how to set up their account or had other questions about deployment."

Ieva Pudure

ATEA onboarding playbook

4000+ employees. 7 countries. 88 offices.
All on Bitwarden.



Internal Q&A and service desk manual

Simultaneously, ATEA facilitated a Bitwarden-related Q&A. Additionally, ATEA created a knowledge-based manual for its service desk to ensure its IT team was well-equipped with all the information needed to answer Bitwarden-related questions from employees. The content for these materials was pulled from the Bitwarden website and ascertained from the Bitwarden support team.

"It was very important to us that we have one single source of truth for employees that needed more information about how to set up their account or had other questions about deployment," said Ieva Pudure, cybersecurity officer and product owner, ATEA.

Disabling browser-based password saving accelerated Bitwarden adoption

In an effort to incentivize adoption across the organization, ATEA limited its employees from defaulting to browser-based password managers by permanently disabling the option to save passwords in a browser.

"We don't allow employees to save passwords in browsers," said Mats Sundberg, cybersecurity officer, ATEA. "Even before we removed this option, employees were still opting to use Bitwarden. Overall, employees understand the benefits, which include add-ons such as a free family plan. They are also hearing positive feedback through word-of-mouth and getting good information about the product. People like Bitwarden."

Result: Measurable security improvements

Since the completion of its initial rollout, ATEA has seen considerable benefits, including:

- Fewer credential-related security incidents
- Significant decrease in service desk tickets
- Enhanced sharing capabilities among team members
- An overwhelmingly positive reception from its Bitwarden employee users
- Smooth transition and implementation for non-technical users

"Since deploying Bitwarden, we haven't experienced negative employee feedback," said Mats Sundberg. "We believe the employees are happy."

"After having used Bitwarden for a year, I'd highly recommend the product," said Ieva Pudure. "It's easy to use, easy to update, and highly secure."

"After having used Bitwarden for a year, I'd highly recommend the product. It's easy to use, easy to update, and highly secure."

Ieva Pudure

Recommendations for a successful multi-country enterprise password management deployment

"For organizations interested in deploying an effective enterprise-wide password manager, I would advise them to research their options, conduct a thorough risk analysis to prepare for the risk, implement a pilot program to test-drive the product, and create a comprehensive Q&A to help answer questions," said Ieva Pudure. "It would be wise for organizations to create one single source of truth where they can access information, instead of expecting employees to visit multiple sources or articles. Scattered, disorganized information will result in people giving."

Ieva Pudure also strongly recommends a phased rollout approach, as it helps instill confidence, offers peace of mind, and isn't too overwhelming for IT support teams and service desks.

Get started with Bitwarden

Learn more about what Bitwarden can do for your business and sign up for a [free 7-day trial](#).