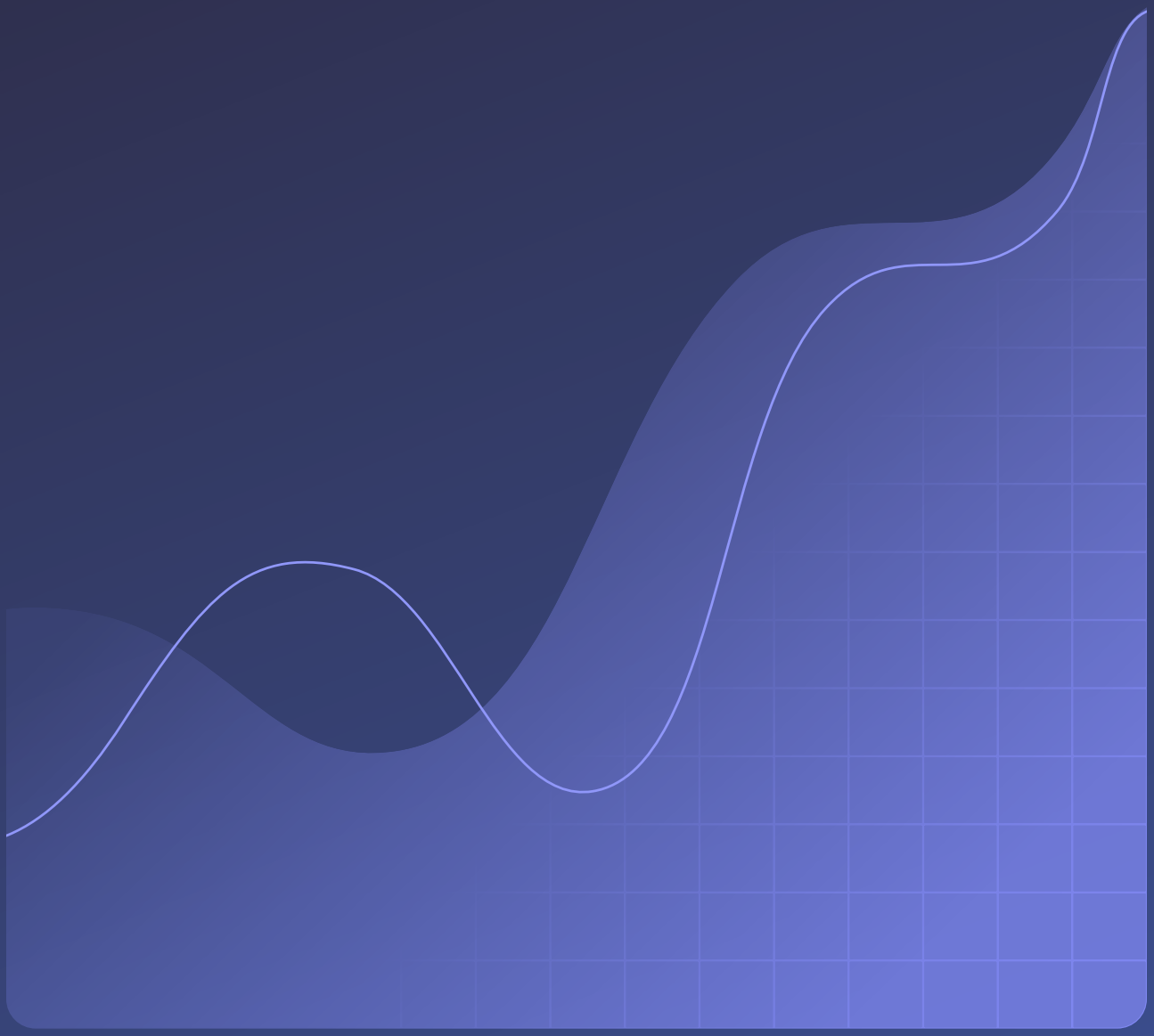
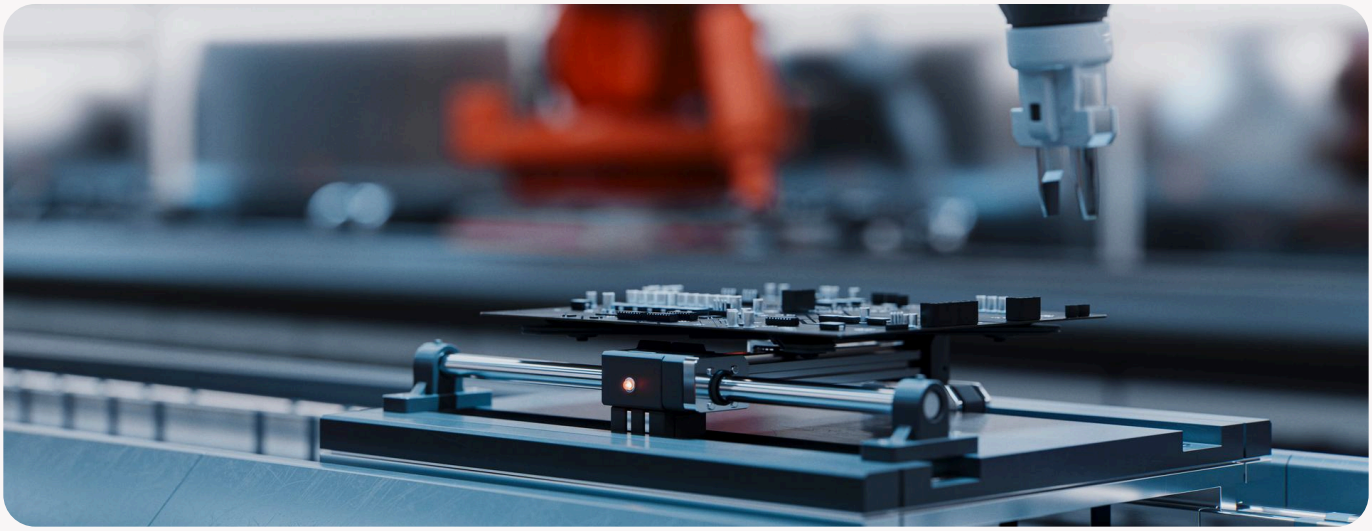
DASHLANE

CASE STUDY

# How a Manufacturing Company Improves Employee Security Habits Without IT Effort





OPTIMA

## Company description

Headquartered in Canada, Optima Manufacturing makes precise metal and mechanical parts using computer-controlled machines, supporting highly regulated industries such as oil and gas and aerospace.

## Industry

Manufacturing

## Company size

80 employees

## The challenge: Protecting sensitive data with a small IT team

Like many growing organizations, Optima Manufacturing faced the challenge of maintaining strong credential security amid rapid change.

A three-person IT team supported approximately 80 employees across multiple systems, many of which required local passwords. As the organization grew, so did the risk of password reuse, weak credentials, and phishing attacks—threats that can be especially dangerous in regulated manufacturing environments.

“Manufacturing is a very sensitive space,” explains Paul Bahga, System Analyst for Optima Manufacturing. “You need to be very careful with all of the information and make sure that all the data is protected. We have a lot of on-prem storage files, servers, that kind of thing, and hundreds of local passwords to track.”

Before switching to Dashlane, Optima had lost confidence in its previous password manager due to its security weaknesses and lack of credential risk visibility. The IT team was also still spending time helping users recover lost passwords, which should’ve been unnecessary with their previous password manager.

In addition, that password manager had a non-intuitive user interface, and adoption never exceeded 50%.

As Optima pursued new cybersecurity certifications and focused on password hygiene and audit readiness, the IT team recognized the organization needed a new credential security solution.

“A lot of the password managers, they just store your passwords, but they don’t really protect them,” Paul shares.

## The solution: Switching to Dashlane for proactive credential and phishing protection

The organization now leverages Dashlane Omnix™, an AI-accelerated credential security platform, to secure employee credentials—even if they're not stored in a vault.

The platform includes:

- **Credential Risk Detection:** Get complete credential visibility across the organization and enable IT to proactively uncover credential risks and respond to threats faster
- **Credential Risk Alerts:** Prompt employees to immediately fix weak and compromised passwords with clear guidance and no extra IT work required
- **AI Phishing Alerts:** Notify employees in real time when they're visiting a suspicious site and before they can enter any data

Instead of relying solely on stored credentials, Omnix actively warns users when risky behavior occurs, even for credentials not stored in Dashlane. Plus, admins get centralized visibility into credential risk and can set security and access policies.

Deployment was fast and straightforward for Optima. SSO and provisioning were completed in just a few days, with the IT team prioritizing the high-risk users who manage Optima's most critical systems. Despite a workforce with mixed technical skill levels, adoption was immediate.

> "Dashlane was approved instantly after seeing the flaws that the other password managers had. We didn't want anything overly complicated for the users. It should just be very simple, like how Dashlane is."
>
> **Paul Bahga**, System Analyst, Optima Manufacturing

## The results: Stronger security, fewer IT interruptions, and measurable impact

Since deploying Dashlane, Optima Manufacturing has seen immediate and measurable improvements across security, productivity, and user behavior.

“Dashlane is helping everyone improve security at our organization,” Paul shares. “And we have the visibility we need now.”

Password-related support requests dropped to zero, eliminating several monthly resets and allowing the IT team to reclaim an estimated two to three hours per month previously spent on credential recovery.

Adoption is significantly higher than with their previous password manager, and overall password hygiene has improved drastically.

In addition, Omnix insights reinforce better security habits automatically. The platform delivers approximately 30 to 40 Credential Risk Alerts per week, guiding users away from risky behavior. Meanwhile, AI Phishing Alerts trigger only when necessary—just once or twice in the past month—to add protection at critical moments without overwhelming users.

> “With the AI Phishing Alerts, employees have that extra bit of security at the final checkpoint where they’re entering credentials.”
>
> **Paul Bahga**, System Analyst, Optima Manufacturing

Together, these improvements have strengthened Optima's security posture and reinforced long-term compliance goals by embedding security awareness directly into everyday workflows.

> "The biggest impact would be the security that Dashlane offers. I definitely do feel more secure with Dashlane than another password manager."
>
> **Paul Bahga**, System Analyst, Optima Manufacturing

See for yourself how Omnix delivers complete credential security.
Request a demo