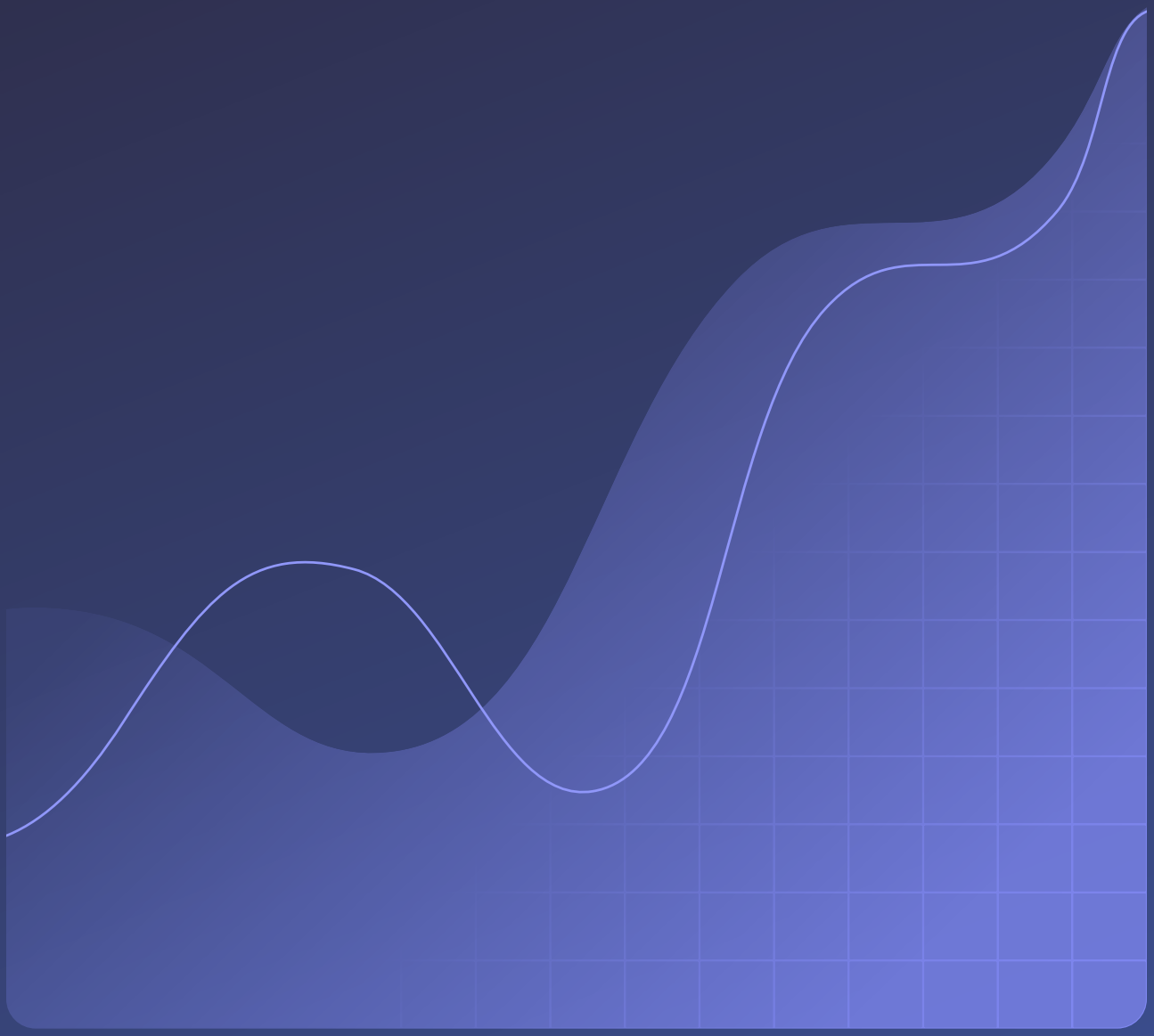
DASHLANE

CASE STUDY

How an AI Biotech Pioneer Strengthened Its Security Foundation with Advanced Password Management



OWKIN

Company description

Founded in 2016, Owkin is transforming biomedical research with agentic AI, helping build diagnostic solutions that improve patient outcomes.

Industry

Biotechnology

Company size

450+ employees in six countries

The challenge: Strengthening security standards and culture amid fast growth

A pioneer in the AI biotech field, Owkin is developing cutting-edge solutions that help biopharmaceutical companies advance drug discovery, development, and diagnostics. Owkin's agentic AI breaks the limits of human intelligence to transform research that requires complex and vast biological data.

Given the highly sensitive nature of medical information, maintaining the highest security standards is paramount to Owkin's mission.

As a rapidly growing company with a globally dispersed, hybrid workforce, Owkin recognized the need to establish enterprise-grade security processes that could scale with their expansion.

"The biotech industry is evolving rapidly, and we knew that staying ahead of emerging threats required a proactive approach to security," says Leo Cunningham, CISO at Owkin.

> "We wanted to establish best-in-class security practices from the ground up."
>
> **Leo Cunningham**, CISO, Owkin

Owkin identified an opportunity to strengthen their password security infrastructure and enhance visibility across their organization. As the company grew, they needed a solution that could provide consistent security standards while supporting their diverse, international team.

"We were at an inflection point where we could either continue with basic security measures or invest in enterprise-level solutions that would support our long-term growth," Leo explains. "We chose to be proactive and implement robust security frameworks early."

The need for enhanced password management became particularly important as Owkin pursued ISO 27001 compliance, demonstrating their commitment to international security standards. This compliance initiative reinforced Owkin's dedication to building a strong security culture from the foundation up.

Given their focus on innovation and rapid scaling, the Owkin security team prioritized solutions that would be intuitive for their research-focused workforce while providing comprehensive security benefits. That led the Owkin team to the Dashlane Omnix™ platform.

> “User experience was critical in our selection process. We needed a solution that would enhance security without creating friction for our team members who are focused on groundbreaking research.”
>
> **Leo Cunningham**, CISO, Owkin

The solution: A platform that integrates seamlessly and elevates security standards

Omnix is an AI-accelerated, proactive credential security platform that gives IT and security leaders the power to detect, respond to, and protect against credential-based threats across the entire organization. It's designed to cover the full lifecycle of a credential-based threat: From detecting a compromised credential, to alerting employees and driving remediation, to ongoing credential management.

Efficiently implementing enterprise security solutions like Omnix is crucial for growing companies like Owkin. The SSO integration with a broad range of Identity Providers (IdPs) enabled seamless deployment, streamlining onboarding for existing employees and automating the process for new hires.

Omnix also simplified password management for administrators, reducing administrative overhead.

"The implementation experience exceeded our expectations," says Adrian Vasile Ciorba, IT Engineer at Owkin.

> "The intuitive interface and seamless SSO integration made deployment incredibly smooth. Getting new employees up and running takes just a few minutes, which has been transformative for our scaling organization."
>
> **Adrian Vasile Ciorba**, IT Engineer, Owkin

Throughout the implementation process, Adrian valued the collaborative relationship with the Dashlane team.

"The support from the Dashlane team during rollout was exceptional," he shares. "Their responsiveness, technical expertise, and proactive approach made the transition seamless. The level of partnership we experienced set a new standard for vendor relationships."

Omnix enabled Owkin to establish comprehensive password security standards while providing the security team real-time visibility into Password Health scores across the organization. With high adoption rates among employees and contractors—and automatic onboarding of new team members—Owkin gained valuable insights into their overall security posture.

"The automatic onboarding capability is particularly powerful—it ensures consistent security practices while giving us visibility into adoption patterns across our teams," Leo shares.

Advanced features like individual Password Health scores, Dark Web Monitoring, and automated alerts empower employees to maintain excellent security hygiene. For example, Dashlane's real-time alerts automatically provide in-browser or Slack notifications to guide employees toward optimal password practices.

When employees have tools that integrate seamlessly into their workflows, they become active participants in organizational security. For Owkin, Dashlane's Omnix platform provided the ideal combination of robust security, user-friendly design, and operational efficiency.

"Omnix streamlines access management across our various platforms and locations," Leo says. "Whether someone needs to access shared systems or connect to Wi-Fi at our New York office, we have centralized secure access. The shared vault functionality for different systems and locations has significantly improved operational efficiency."

> “Omnix has become our standardized intelligent credential management solution across the organization.”
>
> **Leo Cunningham**, CISO, Owkin

Owkin has partnered with Dashlane since 2017, and Leo emphasizes that scalability and sustained high adoption rates remain priorities as the company continues to grow. He conducts annual reviews of their security stack, evaluating tools based on ROI and strategic value. He appreciates that Dashlane continuously enhances functionality and introduces new features like automated alerts based on customer input.

"Partnership and continuous innovation are essential when selecting security vendors," Leo explains. "Dashlane consistently demonstrates their commitment to customer feedback, turning our suggestions into valuable features that benefit the entire user community."

The results: Elevating security culture as a strategic advantage

Leo and Adrian agree that Dashlane has proven to be a strategic partner for Owkin, supporting both security objectives and operational excellence.

"Our experience with Dashlane has been exceptional," Leo says. "Their collaborative approach and commitment to customer feedback creates a productive partnership that directly benefits our security posture."

By implementing Omnix, Owkin has achieved their dual objectives of proactively strengthening credential security and cultivating a security-conscious culture. The platform has become integral to daily operations, with their company-wide Password Health score of 86.3 percent reflecting strong security practices. Leo notes continued improvement in this metric throughout his tenure with the company.

> “Dashlane has elevated security awareness across our organization. The real-time visibility and health scores have transformed password management from a background concern into an active component of everyone's security responsibility.”
>
> **Adrian Vasile Ciorba**, IT Engineer, Owkin

According to Adrian, Dashlane has become a cornerstone of Owkin's security infrastructure. Key features include:

- **SSO integration:** providing seamless access across the organization while maintaining IT oversight and control
- **Dark Web Monitoring:** enhancing employee awareness of potential security threats and enabling proactive responses
- **Credential Risk Alerts & Notifications:** Automate risk response with in-browser alerts and Slack notifications that encourage employees to immediately close security gaps.

"The [Credential Risk Alerts & Notifications] feature has been remarkably effective," Adrian says. "They provide the right level of guidance without creating friction, and employees respond positively. We've seen consistent improvement in password strength and reduction in credential reuse since implementing this feature."

He emphasizes that Omnix represents "one of those exceptional solutions that enhances both IT efficiency and end-user experience." Most importantly, it has reinforced Owkin's commitment to security excellence.

> “We've seen measurable improvements in strong password adoption, 2FA usage, and reduction in credential reuse. Security has evolved into a shared organizational responsibility rather than solely an IT concern—and Omnix has been instrumental in driving this cultural transformation.”
>
> **Adrian Vasile Ciorba**, IT Engineer, Owkin

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