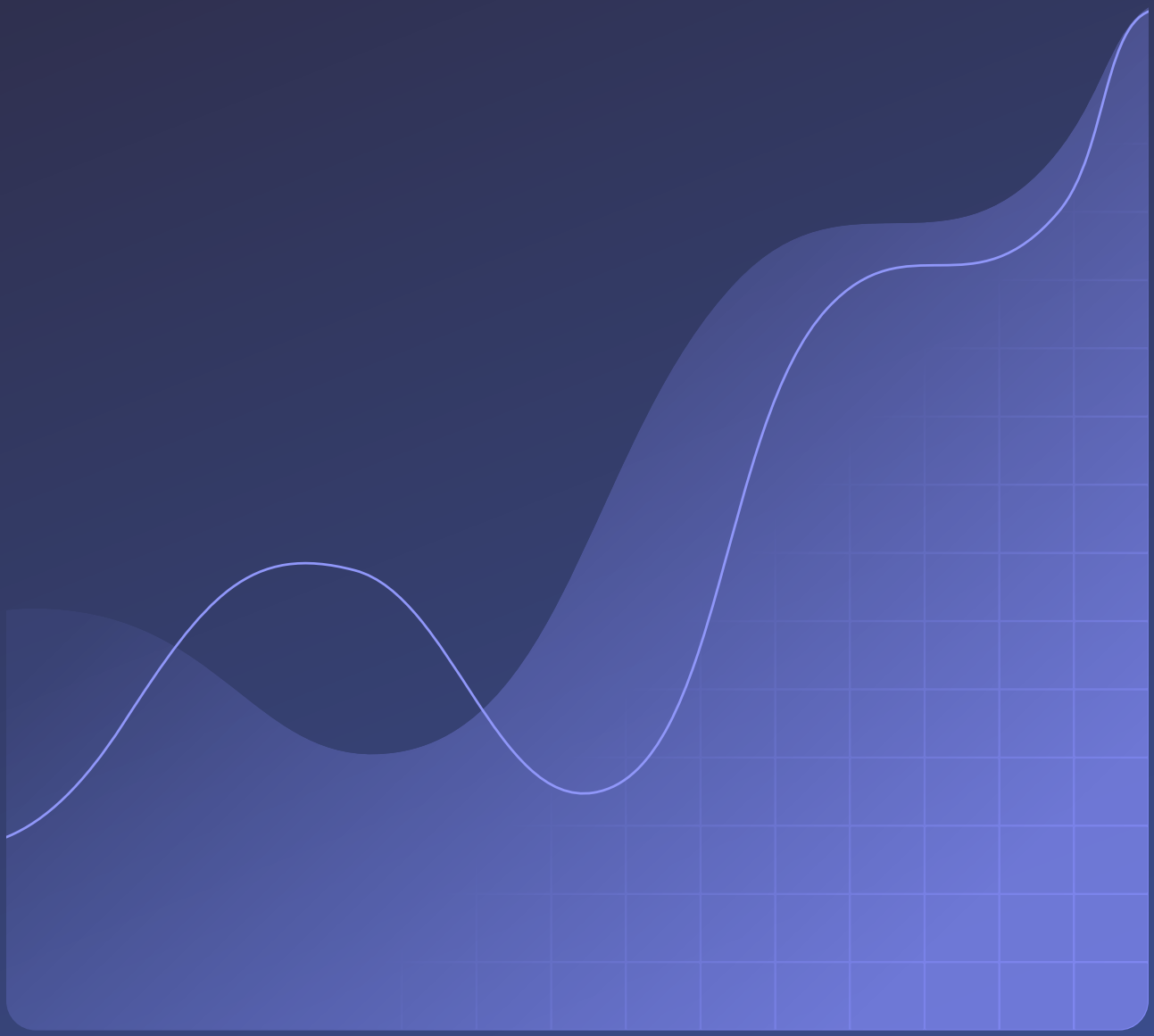
DASHLANE

CASE STUDY

How an HVAC Design Company Saves 5 to 10% of IT Security's Time with Proactive Credential Security



Ambient

Company description

Ambient Enterprises is a U.S.-based HVAC design and implementation company specializing in data centers, service engineering, and government contracts.

Industry

HVAC services

Company size

1,800 employees

The challenge: Securing rapid growth without slowing the business

Ambient Enterprises is a fast-growing national collective of HVAC design and implementation firms. With approximately 1,800 employees and a 35% annual growth rate, the company expands primarily through acquisition, completing an average six to nine mergers per year.

Each acquisition introduces new users, systems, vendors, and credentials, often from smaller, family-owned companies that haven't previously needed enterprise-grade security controls. For Chris Scalise, IT Security Manager at Ambient Enterprises, the challenge is integrating those organizations quickly and securely.

"Once acquisition announcements go out, the attacks start," Chris explains. "So I try to be proactive, not reactive."

Employees average 50 to 75 passwords each, and Chris is well-aware that weak or reused credentials remain one of the most common causes of security incidents.

"Almost all reports of breaches come back to around 80% being insider-related, usually unintentional," says Chris.

At the same time, security controls can't become a bottleneck. Many employees are sales engineers or service technicians focused on customer work, not IT tools. Shadow IT—including personal password managers—creates additional risk and visibility gaps.

With Cybersecurity Maturity Model Certification (CMMC) requirements on the horizon for government contracts, Ambient Enterprises needed a solution that strengthened credential security, improved visibility, and supported a proactive strategy, all without overwhelming users or disrupting day-to-day work.

The solution: Ease of use and proactive security for all

Chris evaluated three or four credential management solutions before selecting Dashlane. Ease of use quickly emerged as the deciding factor.

“A consistent user experience builds confidence,” Chris says. “Changes are most successful when they align with existing workflows and minimize disruption. We’re designing security to enable productivity—protecting the organization without getting in the way of how people work.”

Dashlane stood out by combining strong security controls with an intuitive, user-friendly experience. Built-in guidance helps employees improve password hygiene, while enterprise visibility gives security teams insight without requiring much time or effort.

To support his long-term, proactive security strategy, Chris chose Dashlane Omnix™, the intelligent credential security platform designed to reduce credential risk before it becomes an incident.

In addition to enterprise password management, Omnix provides:

- Credential Risk Detection for uncovering credential risks across all employees, even if they don’t have a vault
- Credential Risk Alerts that automatically prompt employees to fix at-risk passwords
- AI phishing alerts to warn employees in real time when they visit a suspicious site, providing last-mile phishing defense
- Advanced security dashboards that give admins visibility into credential risk organization-wide

Ambient Enterprises deployed Dashlane across the organization, and onboarding was smooth and low-friction, even at scale.

The results: Measurable security improvements and saved time

Since rolling out Omnix, Ambient Enterprises has seen tangible improvements across security posture, efficiency, and the user experience.

Chris estimates Dashlane saves him “probably five to ten percent” of his time. For example, Omnix sends 60 to 90 Credential Risk Alerts per day across the organization, guiding employees to address at-risk credentials on their own. For Chris, that automation adds up quickly.

“Recently, there were 91 Credential Risk Alerts sent in one day,” he says. “If it would’ve taken a minute to manually send each reminder, that’s over an hour of work every day we’ve saved.”

And while Chris was happy with Ambient Enterprise’s existing phishing software, Omnix adds a critical final layer of defense. In just a 30-day period, Omnix’s AI phishing alerts detected 87 potentially risky site visits, warning the employees who made those visits and providing actionable domain-level data that Chris can cross-check against email filtering rules to stop threats before they spread.

In addition, Omnix provides added security controls so IT and security personnel can set permissions, enforce policies, and monitor security hygiene, all in one place. And this hasn’t increased support overhead or user frustration.

> “Recently, there were 91 Nudges sent in one day. If it would’ve taken a minute to manually send each reminder, that’s over an hour of work every day we’ve saved.”
>
> **Chris Scalise**, IT Security Manager

Employees benefit from seamless access across multiple systems and tenants, as well as a strong mobile experience, which is especially valuable for their high-travel workforce.

Omnix has also given Chris risk visibility he previously didn't have the bandwidth to achieve manually. The security team now has insight into duplicate credentials, dark web exposure, and more.

"You can't solve credential risks if you don't know where they are," Chris explains. "With Omnix, now we have that visibility."

Today, Omnix has become a foundational part of Ambient Enterprises' security strategy, supporting rapid growth, ongoing M&A integration, and compliance readiness without slowing the business.

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