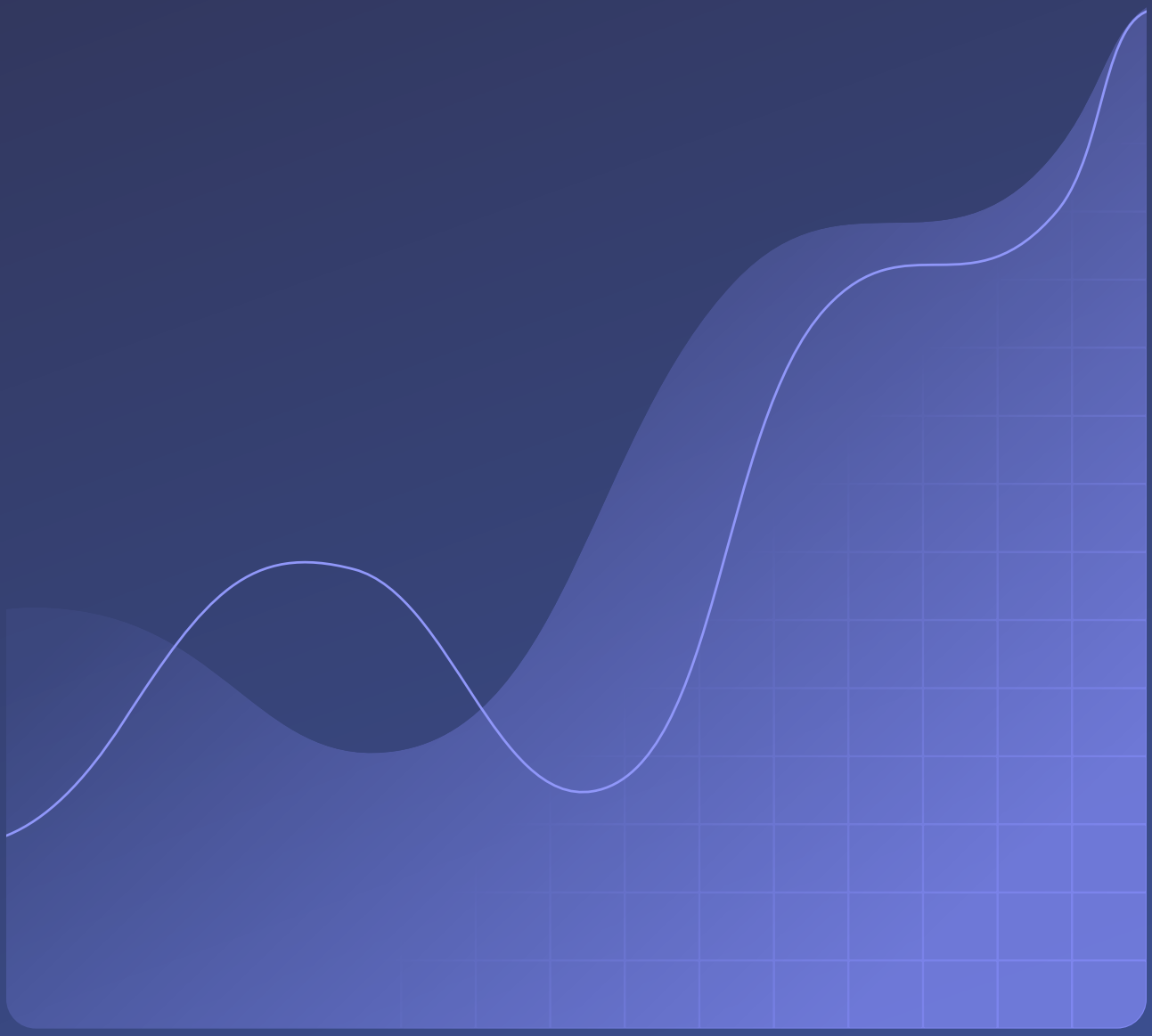
DASHLANE

CASE STUDY

How JFK International Airport's Largest Terminal Defends Their 'Human Firewall' and Secures Operations



JFK INTERNATIONAL AIR TERMINAL

Company description

JFKIAT is the operator of John F. Kennedy International Airport's Terminal 4, which serves 21 airlines and more than 27 million passengers annually.

Industry

Transportation

Company size

12,000+ employees

The mission: Ensuring safe and seamless passenger journeys

Opened in 2001 and operated by JFKIAT, Terminal 4 at John F. Kennedy International Airport is the first privately operated terminal in the U.S. At nearly 2 million square feet (the equivalent of about 35 American football fields), T4 is the largest terminal at the airport.

More than 27 million passengers travel annually through T4, which is home to 21 airlines. Like any critical infrastructure facility, the terminal is a constant target of cyberattackers, and a security breach could impact a variety of essential services.

For example, the disruption from an attack or breach could affect anything from wayfinding displays and baggage-handling systems to the entire "brain" of terminal operations, according to Steve Tukavkin, Vice President of IT and Digital at JFKIAT.

> "There have been a number of unfortunate scenarios in our vertical recently where ransomware has brought down airports."
>
> **Steve Tukavkin**, Vice President of IT and Digital at JFKIAT

"The impact may be huge, depending upon the severity and the type of breach," says Steve, an industry veteran who's been with JFKIAT for 9 years.

The implications of a major incident extend beyond operations and safety.

"It's all about reputation for airports and staying out of the news, but also it impacts airline satisfaction and those passengers who are flying," says Steve. "Those various airlines could be out of considerable amounts of money for flights, along with hotels for passengers, and the list goes on and on."

Regulatory compliance is another consideration. JFKIAT must adhere to mandates such as the U.S. Transportation Security Administration's Cybersecurity Directive for airport operators and New York State's SHIELD Act.

With customer and employee safety and security as one of the organization's core values, cybersecurity is a top priority. For JFKIAT's security leaders, that means staying up to date with security best practices and continuously innovating.

That's why JFKIAT opened a state-of-the-art security operations center (SOC) in 2018 and has adopted the National Institute of Standards and Technology (NIST) Cybersecurity Framework. The aim to align with NIST jump-started the cybersecurity team's search for a robust credential manager.

"We follow best practices and guidelines for cybersecurity as recommended by NIST, and a credential manager aligns with and ticks quite a few boxes in the NIST 'Protect' and 'Identify' capabilities," shares Steve.

> "We did a gap analysis in our technology stack, and we saw credential management as a major gap in opportunity."
>
> **Steve Tukavkin**, Vice President of IT and Digital at JFKIAT

The challenge: Protecting the ‘human firewall’ while lacking consistent credential management

JFKIAT’s IT & Digital and Information Security teams, which share the responsibility for cybersecurity, divide their approach into three pillars. The first—and most vulnerable—layer is people, or what the organization refers to as their human firewall.

“We need to ensure that we have the right controls and processes in place, but also technology to help them make good decisions on how they manage their credentials with multiple systems,” Steve says.

Without centralized credential management, JFKIAT faced risks such as shadow IT, inconsistent policy enforcement, and unauthorized access to data and systems. However, they didn’t have visibility into those risks.

As Steve explains it, “It is really difficult to enforce good, strong password policies across the organization when you don’t have the right tools in place. And there’s a higher risk of credential theft or unauthorized access due to unmanaged credentials.”

While JFKIAT had implemented single sign-on (SSO), they recognized that this technology alone couldn’t fully address their security challenges.

As JFKIAT recognized the need for a proactive approach to risk management, a credential manager presented itself as the ideal solution. A robust tool could bridge the existing gaps and empower the IT & Digital and Information Security teams to manage their risks more effectively.

“Our major objectives were to enable a safer, controlled way of sharing passwords between teams without using unsecure methods like email or spreadsheets, or other ways that I’m not aware of,” Steve says. “It’s all about reducing dependency on manual password tracking, minimizing human error, and improving our overall security posture.”

The solution:
An innovative credential manager that's easy to integrate, manage, and use

JFKIAT had an extensive list of requirements for a credential manager, starting with integration with an enterprise-managed browser and visibility into password health and credential risks. For Steve's small team, the ability to manage the tool easily was at the top of the list, along with simple onboarding and offboarding.

Cost was another consideration so they could scale the tool cost-effectively as the organization grew.

After a thorough evaluation process, Dashlane emerged as the clear winner.

"We looked at two or three other solutions. When we did the feature-rich matrix comparison, we found Dashlane had more ticks in boxes than others in terms of their capability and feature-rich functionality," Steve says.

Dashlane did much more than deliver on all of JFKIAT's criteria. The IT & Digital and Information Security teams were also swayed by Dashlane's commitment to innovation and to customers.

"Dashlane is quite an innovative organization," explains Steve. "That's an important part of our selection process—Dashlane doesn't just deliver a solution, they keep on looking at new ways and new capabilities as part of their roadmap."

Dashlane provided not only a platform for secure, centralized credential management, but also additional security layers like a VPN, which enables employees to connect to data and systems securely outside of the corporate network.

> “Dashlane really introduced visibility into our credential risk and Password Health monitoring. As an added benefit, the Dark Web Monitoring alerts help to proactively understand if there were any compromised accounts in the past, and also to detect new compromised events based on different email accounts.”
>
> **Steve Tukavkin**, Vice President of IT and Digital at JFKIAT

The recent upgrade to Dashlane Omnix™—a proactive credential security platform—further expanded their teams’ capabilities with features such as:

- **Credential Risk Detection**, which delivers complete visibility, enabling IT and security teams to uncover credential risks proactively—even for employees not logged into Dashlane—and respond faster
- **Credential Risk Alerts & Notifications**, which send employees smart, automated notifications to encourage them to mitigate risky credentials
- **AI Phishing Alerts**, which warn employees about potential phishing attempts in real time to prevent them from entering data on suspicious websites

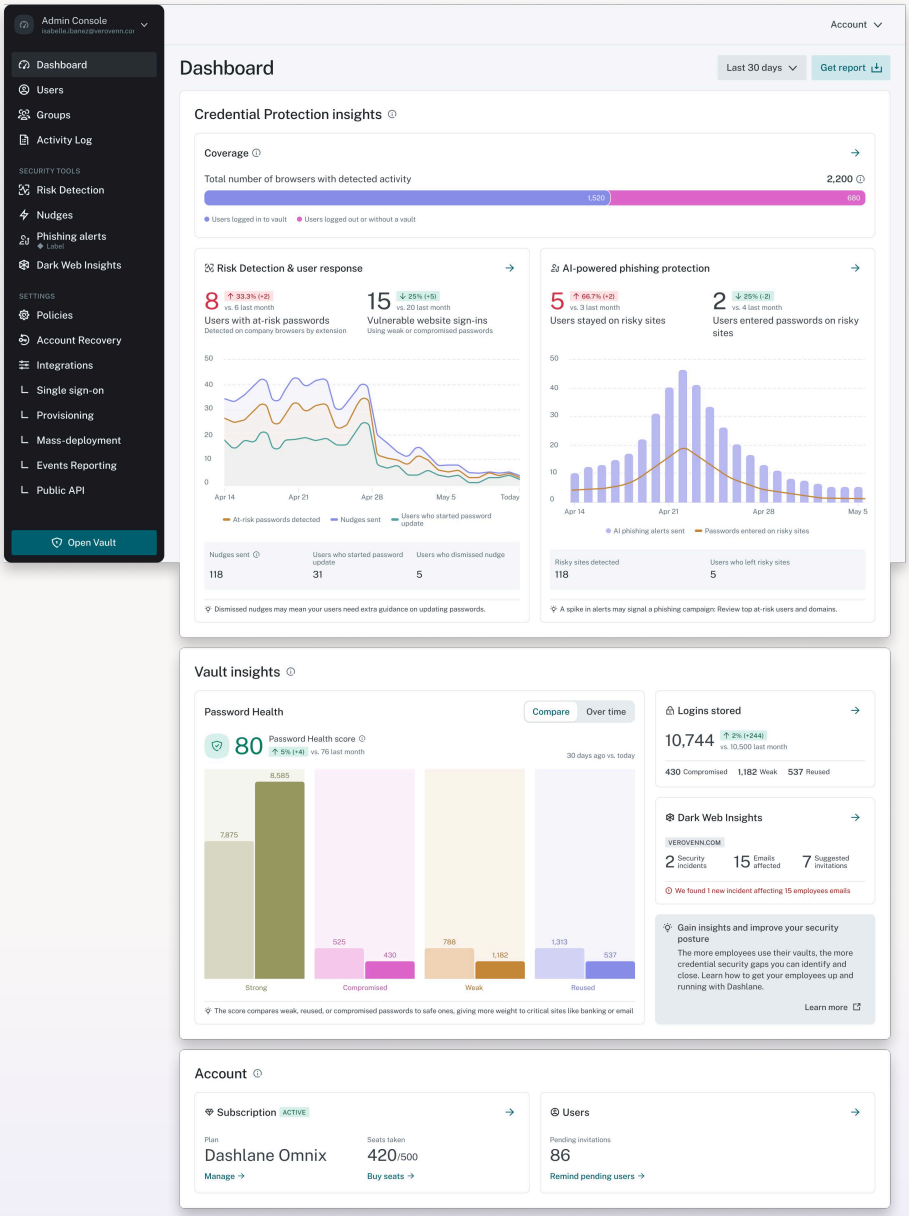
“We’re quite excited about [Credential Risk Alerts & Notifications], to see how that might help us further improve our user resiliency,” Steve says.

He expects the AI Phishing Alerts to strengthen resiliency even more, and notes that the feature is another example of how Dashlane innovates with its roadmap. The roadmap is critical to JFKIAT and T4 because two departments govern information security, and they must collaborate and align their needs.

The impact: Proactive credential risk management and improved cyber resiliency

Since implementing Dashlane, JFKIAT has significantly improved their visibility into credential risk, better aligning their security capabilities with the NIST Cybersecurity Framework.

Centralizing credential management enables JFKIAT to address their human-driven risk more effectively, while Dashlane is easy to use and manage for admins. The improved insights and visibility that Omnix delivers in a simple, high-level dashboard in a centralized location are “a big key differentiator,” according to Steve. Other new Omnix features provide additional value.



“Credential Risk Detection gives us more visibility into areas of risk that we need to focus on,” Steve shares. “We can see how many risks are coming from the same domains and determine an action plan.”

With Dashlane, JFKIAT can consistently reinforce their password policies through robust technology controls and improve overall posture. The platform is part of their onboarding and efforts to enhance user awareness, helping educate employees about cyber resilience, dark web threats, and the importance of improving Password Health.

“We do phishing training, but training is only one aspect,” Steve says. “We do simulations and monthly campaigns, and our phish-prone percentage has decreased significantly. The new AI Phishing Alerts from Dashlane will give us additional proactive protection and help us with further mitigation in this area.”

Dashlane plays a crucial role in improving the effectiveness of JFKIAT’s cybersecurity program. Perhaps the most important outcome is their enhanced ability to manage their most considerable risk—people.

“Dashlane has really helped us improve our cybersecurity posture around the human firewall element and enhance the end-user education about credential management, not only for business usage but also leveraging the personal partition as well,” Steve says.

The organization constantly advances their security approach. Part of this ongoing effort includes continually integrating Dashlane’s Dark Web Insights into their phishing defense and incident response playbooks.

The IT & Digital and Information Security teams continue to test new Dashlane features to determine the best use cases for improving their security posture. Dashlane enables them to stay current with the latest security practices and state-of-the-art technology capabilities.

"From an organizational perspective, having very good credential management software that's easy to use, onboard, and manage effectively across the enterprise is a major benefit," Steve says.

> "Dashlane is providing the right level of end-user credential risk insights and management across the enterprise. It fits into our culture of innovation."
>
> **Steve Tukavkin**, Vice President of IT and Digital at JFKIAT

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