Bombardier Enhances Security with Zscaler™ Advanced Cloud Sandbox to Stop Patient-Zero Attacks

Bombardier

www.bombardier.com/en

Location: Montréal, Canada

Industry: Aviation

Customer Size: 13,000 employees across 12 countries

Bombardier is a global aviation leader, creating and supporting business jets that set new standards in passenger comfort, energy efficiency, reliability, and safety. The company supports a worldwide fleet of more than 4,900 aircraft and serves customers ranging from multinational corporations and charter providers to governments and private individuals.

Visibility need prompts recalibration

Having built its brand on providing high-end business aircraft to discerning customers, Bombardier perennially leads the aviation market by constantly innovating its operations, including IT security.

"We embarked on a Zero Trust journey to provide us with a solution that gives us visibility and mitigates threats rapidly," explained Mark Ferguson, CISO at Bombardier.

Expanding Zero Trust for competitive advantage

As a provider of sophisticated products to an elite group of customers, Bombardier is responsible for keeping aircraft and purchaser data secure for passenger and crew safety. Simultaneously, the company needs to operate efficiently, effectively and with the highest integrity to maintain its competitive edge, all of which is codified in the company's extensive Environmental, Social, and Governance (ESG) plan.

These imperatives led Bombardier to consider how it could enhance its Zero Trust approach.After reviewing the options for improving threat mitigation and risk reduction, Bombardier decided to expand its deployment of the cloud-native **Zscaler Zero Trust Exchange™ platform**. "In addition to offering superior protection, we determined the Zscaler solution was the easiest to deploy and operationalize," Ferguson said. "There's no heavy lifting for IT."

CHALLENGE

Reduce risks from patient-zero threats while minimizing IT overhead

SOLUTION

- Zscaler Internet Access™ (ZIA™)
- Advanced Cloud Sandbox

OUTCOMES

- Obtained the highest level of protection against known and unknown threats, including patient-zero attacks
- Significantly improved situational awareness and risk reduction posture to increase security for modern and legacy IT technologies
- Gains granular data and AI-powered analytics for instant threat mitigation and optimizing the entire security stack
- Contributes to meeting worldwide ESG goals by helping ensure data privacy is embedded in systems and processes and assisting with reducing the energy IT consumes
- Obtained a rapidly deployed and expanded platform, with the initial 70K users onboarded in less than six weeks

Instantly mitigating patient-zero threats

Having previously adopted **Zscaler Internet Access (ZIA)**, a fundamental building block of the Zero Trust Exchange platform, Bombardier elected to deploy the Zscaler **Advanced Cloud Sandbox**, which protects against patient-zero attacks.

Using real-time, AI-powered analysis, Advanced Cloud Sandbox conducts inline inspections of suspicious files and issues an instant verdict, quickly allowing benign traffic to continue. The remaining traffic is quarantined and receives further AI analysis. Concurrently, this suspicious traffic is blocked for every Zscaler user. As an integrated Zscaler service, protections are updated in real time from billions of transactions per day.

"Advanced Cloud Sandbox is significantly widening our range of situational awareness," Ferguson said. "We not only have modern systems to protect, but also various legacy solutions that are more vulnerable. Advanced Cloud Sandbox is helping keep all of those systems safe, which is improving how we sleep at night."

Integrations and data help optimize security framework

Adopting Advanced Cloud Sandbox is also adding data to the insights Bombardier is already gathering from ZIA and combining it with other solutions to help optimize enterprise security.

"Along with expanding our Zscaler platform, we're in the process of moving to **Sailpoint** as our cloud-based identity governance and administration (IGA) platform," Ferguson said. In addition, Bombardier is using VMware **Carbon Black** for endpoint security.

"We appreciate Zscaler's tight integration with both of those solutions as it enables us to collect and analyze threat data for optimizing our entire security framework," Ferguson said. "With good data, we can also educate our business users more effectively, as well as make data-driven decisions, like evaluating which legacy solutions we should prioritize for retirement."

Hiding assets from external threats

By deploying Zscaler, Bombardier reduces exposure points and commonly known attack surfaces in the first place, because Zero Trust can't be achieved while relying on legacy firewalls and VPNs. With the Zero Trust Exchange platform connecting Bombardier's users and devices to applications, rather than to the network, it prevents lateral movement of infections while making users and applications invisible to external threats.

Fewer avenues for breaches means reduced risk and fewer incidents for Bombardier: Hackers can't attack what they can't see. In addition, the platform inspects all traffic, including encrypted traffic, for the effective prevention of threats and data loss.

> "With the Zscaler Advanced Cloud Sandbox, there's no heavy lifting for IT, which is critical as today's talent market is so tight that hiring is extremely challenging."
>
> – **Mark Ferguson**
> CISO
> **Bombardier**

"When everyone went remote during the first wave of COVID-19, we learned that many of our employees completed the majority of their job functions using Microsoft 365 [M365]," Ferguson said. "By adopting ZIA, employees using M365 no longer need to utilize our virtual private network [VPN] to log into our data center only for us to send traffic back out to the Microsoft cloud."

Connecting users directly to M365 has significantly reduced remote worker traffic to Bombardier's data center. "This reduces the risk of lateral infections, as well as decreases various other known security vulnerabilities associated with VPNs," Ferguson said.

Boosting private app security on deck

Moving forward, Bombardier is also planning to adopt **Zscaler Private Access™ (ZPA™)**, which can eliminate its dependence on VPNs altogether. Like ZIA, ZPA connects users to applications, providing secure access to private applications residing in Bombardier's data center and in its **Microsoft Azure** environment.

"Adding ZPA would assist with fully implementing a least-privileged access model," says Ferguson. "This will confine user access to only the applications they require for their jobs. It fits in with our IGA transformation as it requires building upon least-privilege principles and policies."

Given Bombardier's smooth ZIA implementation, Ferguson also looks forward to an easy ZPA deployment. "We adopted ZIA at the beginning of the pandemic but before our recent divestiture, when we had about 70,000 employees," Ferguson explained. "We added about 10,000 employees to the platform a week, with the entire deployment lasting less than six weeks."

Further innovation to address ESG and other goals

With a significant application migration to Azure on the horizon, Bombardier will consider other Zscaler solutions, including **Zscaler Workload Segmentation** and the **Zscaler Cloud Protection** suite. Both solutions help alleviate challenges related to migrating legacy solutions to cloud platforms, such as Azure, **Amazon Web Services (AWS)** and **Google Cloud Platform**, due to Zscaler's tight integration with each cloud provider.

Bombardier's continued expansion of Zero Trust and the Zscaler platform is a vital component for meeting the company's ESG goals, including establishing systems and processes that embed data privacy best practices worldwide and achieving a 20% reduction in energy consumption.

"Zscaler is another tool in our cyber controls that gives us confidence our IT environment is operating securely," Ferguson said. "In addition, Zscaler's commitment to using 100% renewable energy in its operations aligns with our ESG priorities of improving our cybersecurity and driving positive environmental impact by reducing our security appliances."

> "We never get any phone calls about Zscaler – that's a huge win for us."
>
> **– Mark Ferguson**
> CISO
> **Bombardier**

Strong partnership + robust pipeline = success

Overall, Bombardier will continue to benefit from Zscaler's strong partnership culture, according to Ferguson. "IT and security technologies are constantly evolving," he said. "So, our emphasis isn't on determining which company is the current leader, it's on selecting providers that demonstrate a commitment to partnership and have a strong innovation pipeline."

"In Zscaler, we have a partner that dedicates resources to closely examining our situation and making a variety of suggestions based on accumulated insights and expertise," he continues. "Zscaler's intense dedication to forming value-added partnerships is what differentiates it from the rest."

Most importantly, adopting Zscaler has significantly improved user and IT experiences. "Our users love our Zscaler deployment because it's transparent to them," Ferguson said. "They appreciate not using a VPN and we never get any phone calls about Zscaler – that's a huge win for us."

> "Zscaler's intense dedication to forming a value-added partnership is what differentiates it from the rest."
>
> – **Mark Ferguson**
> CISO
> **Bombardier**

Toward More Sustainable Flight

An innovator for over 100 years, Bombardier's commitment to excellence extends to its comprehensive ESG efforts, including dedicating a substantial amount of its R&D investments towards greener aircraft, and is a signatory to the United Nations' Global Compact. With Zero Trust protecting the integrity of its data, Bombardier can rely on the insights it gathers to ensure its workplaces are becoming more inclusive, it's business more responsible and its aircraft greener for a more sustainable and financially resilient future.

Zscaler, Inc.
120 Holger Way
San Jose, CA 95134
+1 408.533.0288
www.zscaler.com