CASE STUDY FOCUS | ARCHITECTURE & URBAN DESIGN

Studio Gang Strengthens Data Security With BlackFog's Last Line Of Defense

Founded and led by Jeanne Gang, Studio Gang is an international architecture and urban design practice with offices in Chicago, New York, San Francisco, and Paris. The firm brings together architects, designers, and planners to deliver innovative projects across architecture, interiors, planning, and exhibitions. With a highly collaborative and globally connected workforce, Studio Gang relies on secure systems to support creativity, communication, and the exchange of ideas across teams and regions.

INDUSTRY	HEADQUARTERS	OFFICES	EMPLOYEES	WEB
Architecture & Urban Design	**Chicago, IL**	**Chicago, NYC, SF, Paris**	**135**	**studiogang.com**

OVERVIEW

Adding The Missing Layer Of Cybersecurity

Like many modern organizations, Studio Gang faces an evolving cybersecurity landscape, from phishing and ransomware to increasingly sophisticated data harvesting threats. While traditional security tools are effective at detecting and preventing attacks, they often lack control over what happens once a threat gets through. To close this gap, Studio Gang turned to BlackFog to gain control over outbound data and stop data exfiltration, establishing a true last line of defense.

THE CHALLENGE

Closing The Gap In Outbound Data Protection

Studio Gang's IT team was already managing a wide range of threats, including phishing, malware, ransomware, and data harvesting. However, their existing security stack was primarily focused on detection and prevention, not on what happens to data once a system is compromised.

"As an industry we face the same threats as everyone else, phishing, malware, ransomware, but the bigger concern is data harvesting and what leaves the environment," said Danny Graham, Principal and Chief Information Officer at Studio Gang.

Without visibility and control over outbound data activity, the organization remained exposed to the risk of sensitive data being exfiltrated.

> "As an industry we face the same threats as everyone else, phishing, malware, ransomware, but the bigger concern is data harvesting and what leaves the environment."
>
> **DANNY GRAHAM** · PRINCIPAL & CHIEF INFORMATION OFFICER, STUDIO GANG

THE SOLUTION

Stopping Data Exfiltration With ADX Protect

Studio Gang initially deployed BlackFog's ADX Protect across all company endpoints to stop data exfiltration in real-time, establishing control over outbound data and preventing unauthorized data transfers. This added a critical layer of protection to their existing security stack, ensuring that even if a threat bypassed traditional defenses, sensitive data could not leave the environment.

"For me, it's about stopping the problem before it happens. Once I saw a demo, I could see data leaving our environment and our other solutions weren't capturing it. I knew then that a proactive approach to preventing data exfiltration was a necessary part of our tech stack," Graham said.

EXPANDING VISIBILITY

Addressing AI And Application Risk With ADX Vision

Months after deploying ADX Protect, Studio Gang expanded its use of BlackFog by implementing ADX Vision, to gain visibility into how applications and AI tools were being used across the organization. "Instead of sending out surveys and guessing, we can actually see what tools are being used and how often. That saves a huge amount of time," Graham said. This visibility enabled the team to identify unexpected data activity and potential risks.

"For example, we saw WeChat transmitting data externally, which raised a flag. But we also knew many of our staff in Asia rely on it to communicate with family," he said. Rather than removing the application entirely, Studio Gang took a balanced approach, allowing its use while maintaining control over data movement. "We didn't want to take it away completely. BlackFog gave us the confidence to allow it, while still protecting the environment," Graham explained.

ADX Vision also provided insight into AI usage across the organization, helping the team better understand how data was being shared with external tools. "We found that one model, Cohere, was responsible for about 20% of our AI traffic. That's something we wouldn't have known otherwise," he noted. With this level of visibility, Studio Gang was able to make informed decisions around AI usage. "It allows us to put guardrails in place and make informed decisions, rather than reacting blindly," Graham added.

THE RESULTS

From Detection To Prevention

BlackFog has become a core component of Studio Gang's cybersecurity strategy, enabling a shift from detection-based security to a more proactive, prevention-first approach. By focusing on stopping data exfiltration and gaining visibility into data exposure, Studio Gang has strengthened its overall security posture and reduced risk across the organization.

"If you can stop the data leaving, you're already in a much better position. That's the layer that was missing before. BlackFog fills a gap that other solutions fail to address," Graham said.

A Partnership Beyond the Product: Beyond the technology itself, Studio Gang emphasized the importance of its relationship with BlackFog.

"The product is important, but the team behind it matters just as much. Having people who are honest and willing to work through challenges makes a big difference," Graham said.

This collaborative approach has helped ensure the solution continues to evolve alongside Studio Gang's needs.

> "The product is important, but the team behind it matters just as much. Having people who are honest and willing to work through challenges makes a big difference."
>
> **DANNY GRAHAM** · PRINCIPAL & CHIEF INFORMATION OFFICER, STUDIO GANG

CONCLUSION

A True Last Line Of Defense

For Studio Gang, cybersecurity is no longer just about preventing threats, it's about controlling what happens when a threat gets through.

"It's not just about stopping threats from getting in. It's about making sure that even if something does get through, the data doesn't leave," Graham said.

By first implementing ADX Protect to prevent cyberattacks and later expanding with ADX Vision to gain visibility into application and AI-driven data exposure, Studio Gang has established a true last line of defense, ensuring sensitive data remains protected in an increasingly complex threat landscape. When asked what advice he would give to other organizations considering ADX technology.

"Run a demo. Once you see the data your current tools are missing, the value is obvious. That's what pulled us in," Graham said.

ABOUT BLACKFOG

Real-Time, On-Device, Data Exfiltration Prevention

BlackFog helps organizations reduce modern cyber risk by stopping data exfiltration, the common factor behind ransomware, insider threats, zero day attacks, and Shadow AI exposure. Our anti data exfiltration (ADX) platform delivers real-time, on-device prevention. It stops sensitive data from leaving endpoints and networks without authorization and blocks ransomware communication, data theft, and AI driven leakage before damage occurs. By focusing on prevention instead of just detection, BlackFog helps organizations strengthen compliance, protect privacy, and improve operational resilience.