Abnormal Security Protects Famous Retail Brands Like One Kings Lane and Z Gallerie From Costly Invoice Fraud From Compromised Vendors

In the world of retail, the sheer volume of suppliers and invoices processed on a daily basis is central to business operations. For CSC Generation, this challenge is amplified by their aggressive corporate growth strategy. "We might not be a household name but we're a holding company for famous retail brands such as DirectBuy, One Kings Lane, Z Gallerie, and Sur La Table. Our mission is to save retail by leveraging our proprietary technology and operating expertise," says Justin Yoshimura, CEO and Founder.

As organizations like CSC Generation move their business to the cloud, their infrastructure transforms, and so do the attacks. According to the most recent 2020 FBI IC3 Report, the number one threat facing organizations are socially-engineered email attacks from compromised vendors. These novel threats evade traditional defenses and require a new approach to stop them.

Your Vendors' Security Is the Culprit

When it comes to pinpointing where the weak link lies, the culprit is often third-party vendors with lax security controls. If their credentials are phished, the results are dangerous to their own organization and partners.

To add to the frustration, it's common for organizations like CSC Generation to have a robust security stack and internal protocols in place to stop traditional attacks. "As a business, we have thousands of third-party vendors. And when it comes to our security tech stack, we thought we had it covered. CSC uses a lot of software security solutions and we have our own checks in place to protect against fraud," says Yoshimura.

Their approach to security and having a proactive playbook designed to catch invoice fraud before it does any damage stands out as progressive and forward thinking when compared to most organizational policies. "All of our employees use two-factor authentication and log-in via VPNs. We take security seriously," added Yoshimura.

CSC | GENERATION

Sur la table
THE ART & SOUL OF COOKING

Z GALLERIE

ONE KINGS LANE
NEW YORK

DirectBuy

"Since we installed Abnormal, there has been no payment or vendor compromise fraud. None. They've completely removed this headache from our security and fraud teams."

Justin Yoshimura
CEO and Founder

When Traditional Security and Playbooks Fail

However, even the best-laid plans can still fall short. As Yoshimura explains, even though CSC Generation had a thoughtful and aggressive approach to stopping these attacks, it was still defrauded out of a significant sum of money. “Despite all of our security checks, we still got hit with a $100,000 payment fraud attack. It happened through one of our vendors who was compromised. The length the attacker was willing to go was extraordinary. They compromised the vendor account, then changed the phone numbers on the signature and redirected the thread to a lookalike domain where an extra character was added to the email address.”

“So when we went through our payment update playbook, the attacker was able to circumvent all the checks we had in place,” says Yoshimura.

> “Despite all of our security checks, we still got hit with a $100,000 payment fraud attack. It happened through one of our vendors who was compromised.”
>
> **Justin Yoshimura**
> CEO and Founder

The Vendor Security Wake-Up Call

At that point, CSC Generation had come to realize their security is tied to their partner ecosystem, as Yoshimura explained, "the moment you realize you're only as strong as your vendors' security, it's a wake-up call. It was time to look for a solution that is ahead of the times."

That exploration led them to solutions with a differentiated approach to stopping third-party vendor attacks, one that uses AI/ML and behavioral data science to solve the problem. Abnormal Security stood out from the crowd.

"What led us to choose Abnormal Security is their approach and efficacy. They spoke our language, literally. They show you how they use AI/ML to stop vendor attacks right in the dashboard. Their approach gave us confidence that it's the best solution on the market," added Yoshimura.

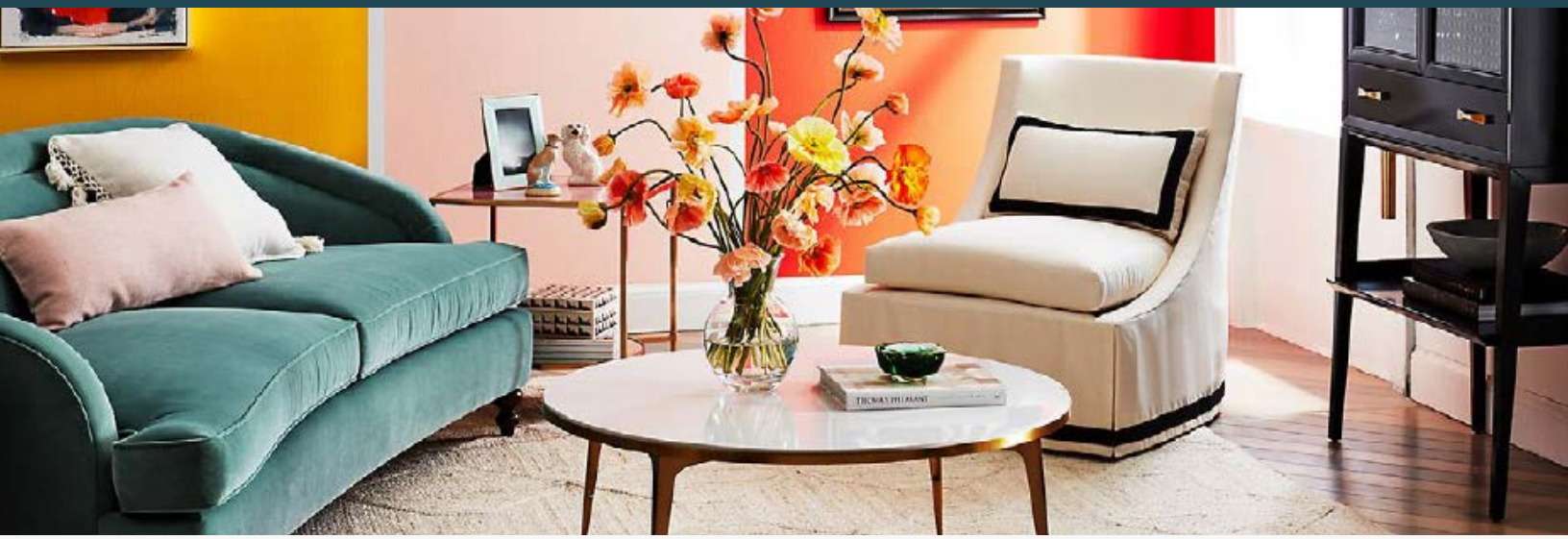
"The moment you realize you're only as strong as your vendors' security, it's a wake-up call."

Justin Yoshimura
CEO and Founder

Abnormal Delivers Results for CSC Generation

Once Abnormal was added to CSC Generation's security stack, the results spoke for themselves. Yoshimura stated, "Since we installed Abnormal, there has been no payment or vendor fraud. None. They've completely removed this headache from our security and fraud teams."

"Before Abnormal, the amount of vendor and payment fraud attempts that would come into our company was sky high. We now know it's because traditional security solutions still use domain blocking and rule-based security to try to stop these attacks. But it's not predictive and it doesn't work, and that's where the problem lies. Abnormal solves that problem completely."



How Abnormal Security Stops Vendor Fraud

Before CSC Generation added Abnormal to the mix, they relied on the now considered "old approach" employed by gateways that uses threat intelligence and looks for known bad or indicators of compromise, like bad reputation, suspicious links or malicious attachments in an email. But because vendor compromise attacks do not make use of these tactics, they evade conventional defenses.

The API-driven approach pioneered by Abnormal Security uniquely leverages behavioral data science to profile and baseline good behavior to detect anomalies and stop attacks. Abnormal Security delivers this breakthrough approach through a cloud-native email security platform that can be deployed instantly through a one-click API integration and can be used to extend and complement existing secure email gateways. "With the one-click API installation, we were able to get up and running in just one day," added Yoshimura.

Abnormal's behavioral data science approach is based on three pillars of technology: identity modeling, behavioral and relationship graphs, and deep content analysis. With these pillars, we're able to profile the known good of an organization and then use it to detect and stop abnormal behavior to stop a broad range of attacks.

When it comes to advice for C-level executives looking for an answer to the problem, Yoshimura says, "Evaluate your existing security solutions and scrutinize how they handle vendor security. It's the biggest threat you face."

> "Without Abnormal's approach to vendor security, we would be open to these kinds of attacks."
>
> **Justin Yoshimura**
> CEO and Founder

ABNORMALSECURITY.COM →