Noname Advances Its API Security Mission with Abnormal Email Protection

Fast-growing API protection provider protects its email ecosystem from advanced impersonation threats.

Noname Security has made a name for itself since 2020 when it launched its full-lifecycle API security platform. Since then, Noname has added several hundred employees, achieved unicorn status, and works with a quarter of the Fortune 500. Noname now protects more than 10 million APIs and close to $3 trillion in revenue streams for financial services, healthcare, retail, and public sector enterprises.

The Noname Email Security Challenge

Noname's CISO, Karl Mattson, wanted to stop advanced spear phishing and BEC attacks that were evading the company's Google Workspace security tools. “Early on, when a bad actor impersonated a member of Noname, we all knew each other so we'd call or text if an email seemed off. Now, we have a global team that hasn't met in-person, so we need security systems we can trust. We also have to protect our email to prevent sophisticated threats to connected applications.”

An API-based solution was the logical choice for Noname. “As a cloud-first company, we didn't want to go back in time to a legacy approach. We believe API-based security solutions based on AI and ML offer a huge advantage in terms of ease of implementation and adaptability,” Mattson said.

“Generative AI poses a remarkable threat to email security. Abnormal is uniquely positioned to stay ahead of attackers who are using sophisticated AI to deliver malware and socially-engineered messages to our email inboxes. We’re leaning into Abnormal for that expertise.”

Karl Mattson
CISO

<table>
<thead>
<tr>
<th>Industry</th>
<th>Headquarters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer and Network Security</td>
<td>San Jose, California, USA</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Employees</th>
<th>Protected Mailboxes</th>
</tr>
</thead>
<tbody>
<tr>
<td>300+</td>
<td>500+</td>
</tr>
</tbody>
</table>
Customer Case Study

The Abnormal Security Solution

Noname's proof of value with Abnormal exceeded Mattson's expectations for ease and speed of implementation. It also surpassed his expectations for results,— showing 10 times more impersonation attacks than the team had expected based on user reports.

Abnormal also provided unique insights in the initial POV. “We saw trends emerge in terms of which employees were being targeted and which were being impersonated. It wasn't always C-level executives. For example, it might be an employee with a lot of LinkedIn followers and a visible email address. Abnormal delivered a new depth of insight on our email attack surface,” Mattson said.

Why Noname Chose Abnormal

Abnormal's ease of use, efficacy, and attack insights freed the security team from an unscalable manual investigation and remediation workload. “We want our analysts and engineers focused on product security. Abnormal gives us faith in our email security, so we can bring our time and energy back to our product. It's been a pleasant surprise to have a platform that I don't feel compelled to log into very often because I know it's doing what it's supposed to do.”

Mattson added that Abnormal's AI and ML expertise gives Noname confidence that their email will be safe from emerging attacks. “The degree of attack sophistication is going to significantly increase as bad actors leverage generative AI to create novel campaigns. It's not reasonable that each company can become an AI security specialty shop, so we're putting our trust in Abnormal to lead the way in that kind of advanced detection.”

A Security Partner Now and for the Future

With Noname's email more secure today and positioned against future threats, Mattson views Abnormal as a sophisticated and supportive ally. “The partnership with Abnormal has been fantastic from the beginning. Our touchpoints with the Abnormal customer success team are high-fives. The technology has been stable and very effective. So our journey with Abnormal has been remarkably positive the whole way.”

“We expected to see some impersonation attempts in our Abnormal POV. Abnormal showed that impersonation rates were 10 times higher than we knew. Before the week was over, there was nothing else to test. We had solved it, and everything was in place—production, deployment, configuration—so there was no rationale to look any further. Abnormal hit it out of the park from the beginning.”

Karl Mattson
CISO

abnormalsecurity.com

© 2023 Abnormal Security Corporation. All rights reserved.