



How Netwrix scales securely on AWS with Bugcrowd

Netwrix accelerates identity-based threat detection and response



Industry:

Tech

Founding date:

2006

Number of employees:

500-1,000

Headquarters:

Frisco, Texas, USA

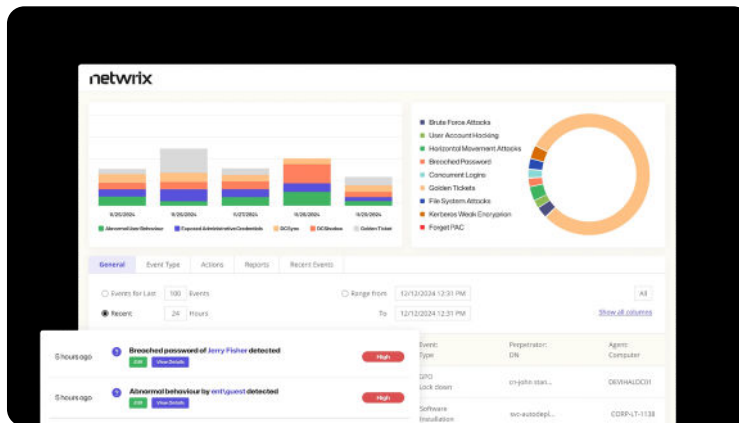
Website:

netwrix.com

The situation and challenge

Netwrix delivers data and identity security solutions so organizations of all sizes always know where their sensitive data lives and whether it's secure.

Netwrix wanted to put its products to the test through actual real-world attack scenarios to see if they can catch attackers looking to compromise the organization's identities and data.



Key takeaways

100%

of attacks from users and IT admin accounts can now be detected

Gained a competitive edge in threat detection and response

Can ship products faster, with a higher bar for accuracy and quality



The Bugcrowd solution

Netwrix decided to run a Managed Bug Bounty engagement with Bugcrowd via Amazon Web Services (AWS).

Bugcrowd gave Netwrix the ability to connect with actual ethical hackers who can perform the same types of attacks that they'd run into in a real data breach scenario. AWS provided additional strength, stability, and scalability.

"The Bugcrowd Platform, hosted on AWS, was extremely powerful to connect us with the very specific type of hackers that we wanted to gain access to our platform.

It was very efficient in connecting us with the exact right type of hackers that we needed," said Jeff Warren, Chief Product Officer at Netwrix.

Netwrix had a series of hackers come into its hosted lab environment and simulate real world active directory attacks. Netwrix was able to closely monitor what worked, what didn't work, what was detected, and what wasn't detected. Bugcrowd's ethical hackers brought novel creativity and above-and-beyond engagement.

The outcome

After that first phase, Netwrix was able to harden and improve the product protections and run through another simulated test with the hackers. It went from a 70% detection rate up to 90%. Netwrix plans to continue to work through Bugcrowd via AWS to keep raising that bar higher and higher.

"This approach gives us an advantage over the competition because we're able to simulate what a real world attack scenario looks like. Rarely do you get to work with real world hackers, looking closely over their shoulder, seeing what they are doing, and monitoring what works for them and what doesn't," Warren said. "Because we now have battle-tested this through the mindset of real attackers, we know that it's more ready for the real world environment."

Netwrix can now not only ship more quickly and reliably, but also raise the bar in the accuracy and quality of our releases by bringing in that diversity of perspectives to help test their products from all different angles and bring in different viewpoints.

By the end of the engagement with Bugcrowd, we are able to successfully detect and prevent 100% of attacks performed by regular user and IT administrator accounts.

Jeff Warren, Chief Technology Officer, Netwrix



"By the end of the engagement with Bugcrowd, we are able to successfully detect and prevent 100% of attacks performed by regular user and IT administrator accounts," Warren said.

Netwrix plans to continue to engage in programs like this that raise the bar for the security of its platform to give customers a product that they can be confident in.