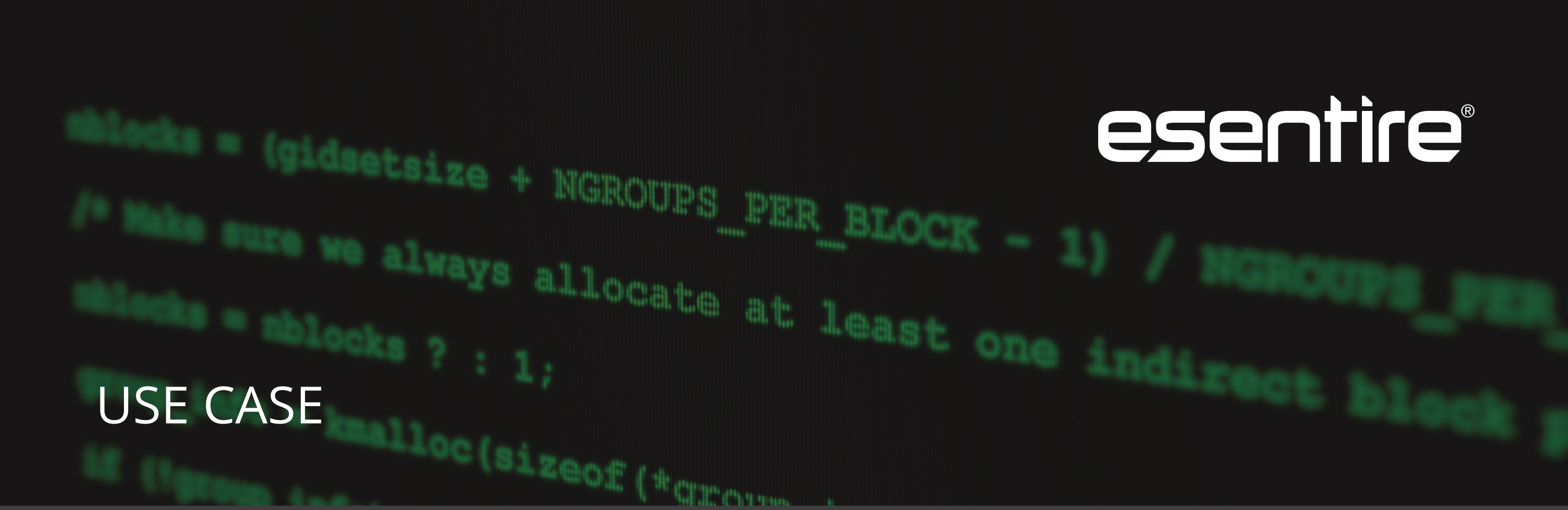

USE CASE

# Incident Report: Shellshock

On September 24, 2014 the world was introduced to Shellshock. Also known as Bashbug, Shellshock is a serious remote code execution vulnerability that affects a large percentage of systems. An eSentire client avoided serious implications from being hit by Shellshock as we were able to catch the attack and isolate it quickly.

## The Attack

Five days after Shellshock was disclosed, the eSentire Security Operations Center (SOC) detected a successful exploitation of a client's public-facing remote access server. The attack caused the client's system to download a script and execute it, releasing the client's IP address and company name back to the attacker.

## Alert and Isolate the Incident

The SOC immediately called and sent a threat intrusion alert to the client, informing them of the breach. Due to the severity of the vulnerability, a call was required to discuss an immediate and appropriate resolution. Analysts received confirmation from the client that the affected system was not mission-critical and could be blocked. Using eSentire Network Interceptor™ service, analysts were able to block all traffic, preventing further exploitation.

## Initiate Human Investigation

SOC analysts investigated the malicious script and determined it was a recon script. The script itself didn't cause any harm to the system, but sent details back to the attacker to confirm its vulnerability for future attacks. Analysts provided the client with necessary information to patch their system.

## A Security Incident Avoided

The client was able to patch their system before any malicious exploitation occurred, which could have led to internal network access by the remote attacker. Two days later, the client advised eSentire that the server was fully patched and the block was removed so they could resume use.

At eSentire, we detect, hunt and investigate threats – 24x7 – so you don't have to. Our security analysts understand the range of threats you face and act as an extension of your team. Contact us to learn more about how eSentire Managed Detection and Response™ service can help protect you.

www.esentire.com