

Rapid Response

For today's technology-dependent businesses, application outages and breaches due to complexity, human error and malicious intent are an unwelcome reality. Swift response to such incidents is critical to avoid tremendous financial and reputational losses. Currently manual troubleshooting and forensic tools are labor intensive and slow remediation times.

5 THINGS TO KNOW ABOUT RAPID RESPONSE

1 IDENTIFY THE ROOT CAUSE

Before any remediation and repair can occur, network operations and security teams need to be able to identify the root cause of any incident or outage. Veriflow pinpoints the cause in a visually intuitive map of network behavior. Zero in on the violating network element within a few clicks and quickly verify remediation changes, drastically decreasing mean time to repair (MTTR).

2 LIMIT THE BLAST RADIUS

Network operations and security teams must be able not only to quickly pinpoint where malicious actors have been and what they have had access to, but also where they may go next to block lateral movement and minimize damage. Veriflow can predict any possible traffic flow, highlighting unwanted back doors into sensitive data based on current state or on changes to that state after an incident.

3 AUTOMATION OF TOOLS LOWERS MTTR

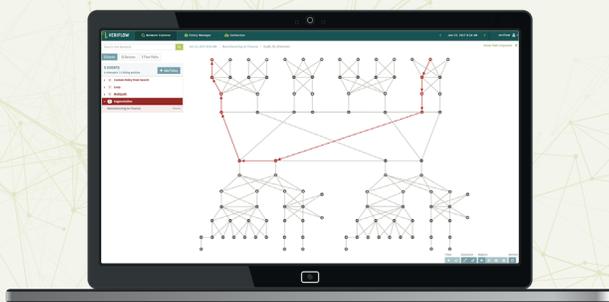
Manual device-by-device tools slow overall remediation efforts. Automation of forensic and response tools is required to get networks back online and protected. Veriflow automatically performs an exhaustive analysis of your entire network to pinpoint the root cause of an incident, lowering mean time to repair (MTTR) and getting teams back to operating and protecting great networks.

4 IT'S NOT JUST ABOUT RESPONSE, IT'S ABOUT LEARNING

Incident response extends beyond the fire drill and should improve an organization's security posture. This requires accurate documentation of the network before and after any incident. Veriflow automatically and at regular custom intervals takes a "snapshot" of the entire network to enable a deep comparative behavioral analysis of the network before and after any incident.

5 RAPID RESPONSE IS NOT REACTIVE

Effective rapid response requires continuous awareness of the network. In addition to identifying your team and action plan, members need to be equipped with the intelligence to quickly move from response to remediation. Veriflow automatically performs an exhaustive mathematical analysis of the network state to give your teams the intelligence they require to overcome any security incident or outage.



Can't Wait?

Book a demo and see how Continuous Network Verification enables Rapid Response in any networking environment.

[REQUEST A DEMO](#)