SOLUTION NOTE

INFOBLOX AND GENIANS

Security Automation with Real Time Threat Mitigation and Quarantine

THE CHALLENGE

Mitigating risk in today's threat landscape has proven to be an extremely difficult task for security professionals. A recent IBM analysis found that cybersecurity teams use over 80 different security products from 40 different vendors on average in their customers' environments. It also indicated that less than 20 percent of the features in these products are actually used and may not provide the outcomes clients expect because of integration and complexity challenges.

Conceptually, we all know that an integrated approach is the best for detecting and mitigating cybersecurity threats. But how can we orchestrate cybersolutions most effectively? And how can we most efficiently maximize our cybersecurity resources?

SOLUTION OVERVIEW

With Infoblox DDI and Genians Next-Gen Network Access Control (NAC) integration, organizations gain actionable intelligence to mitigate cybersecurity threats in real time. The joint solution extends the enterprise-grade Infoblox DNS Firewall feature with the zero-touch, vendor-agnostic, Layer 2 Address Resolution Protocol (ARP) enforcement capabilities of cloud-managed Genians NAC.

Genians NAC enables administrators to locate and control any non-compliant or compromised devices at the network edge. It serves as the key component necessary for establishing an effective cyberdefense framework. It can also orchestrate an organization's security products by integrating them with a wide range of IT security solutions (IPAM, NGFW, IDS/IPS, SIEM and others) to ensur unified policy enforcement. Combined with Infoblox, the solution is able to isolate network devices using Infoblox DNS Firewall alerts at Layer 2, preventing east-west traffic and optionally displaying information to the end users via a Genians Captive Web Portal (CWP) alerting them to the threat. This capability secures the network at the point of connection in real time when threats are detected and educates end users regarding the security status of their device(s).

KEY FEATURES

Infoblox DDI

- Tracks response policy zone (RPZ) security events
- Hosts indicators of anomalous behavior
- Includes alert generation and notifications

Genians NAC

- Supplies network surveillance and visibility
- Answers the who, what, when and where of cyberthreats
- Has vendor-agnostic enforcement capability

Integration highlights

- Extends Infoblox DNS Firewall capability
- Forwards security threats to Genians NAC
- Provides zero-touch, vendoragnostic, Layer 2 quarantine
- Blocks external and internal traffic in real time

HOW IT WORKS

Legacy threat detection and quarantine methods fail to meet the challenges of most cybersecurity requirements of today (Fig. 1). Once threats are detected, rapidly deploying a vendor-agnostic solution for any environment is key. Dependencies on platform type, network infrastructure or agents/plug-ins are roadblocks that hamper efforts to quickly, easily and effectively quarantine threats.

The Infoblox DDI and Genians Next-Gen NAC integration addresses these concerns and challenges. Based on syslog notifications, the integration can be deployed rapidly without complex API structures. This means the integration can be set up in minutes, not days or weeks (Fig. 2). With no dependency on network infrastructure, the solution can be deployed on any network quickly and easily with only basic networking knowledge. Other methods involving complex network integrations are a burden on IT staff and budgets. The solution also functions without the need for agents, plug-ins or connectors.

Legacy threat detection and quarantine

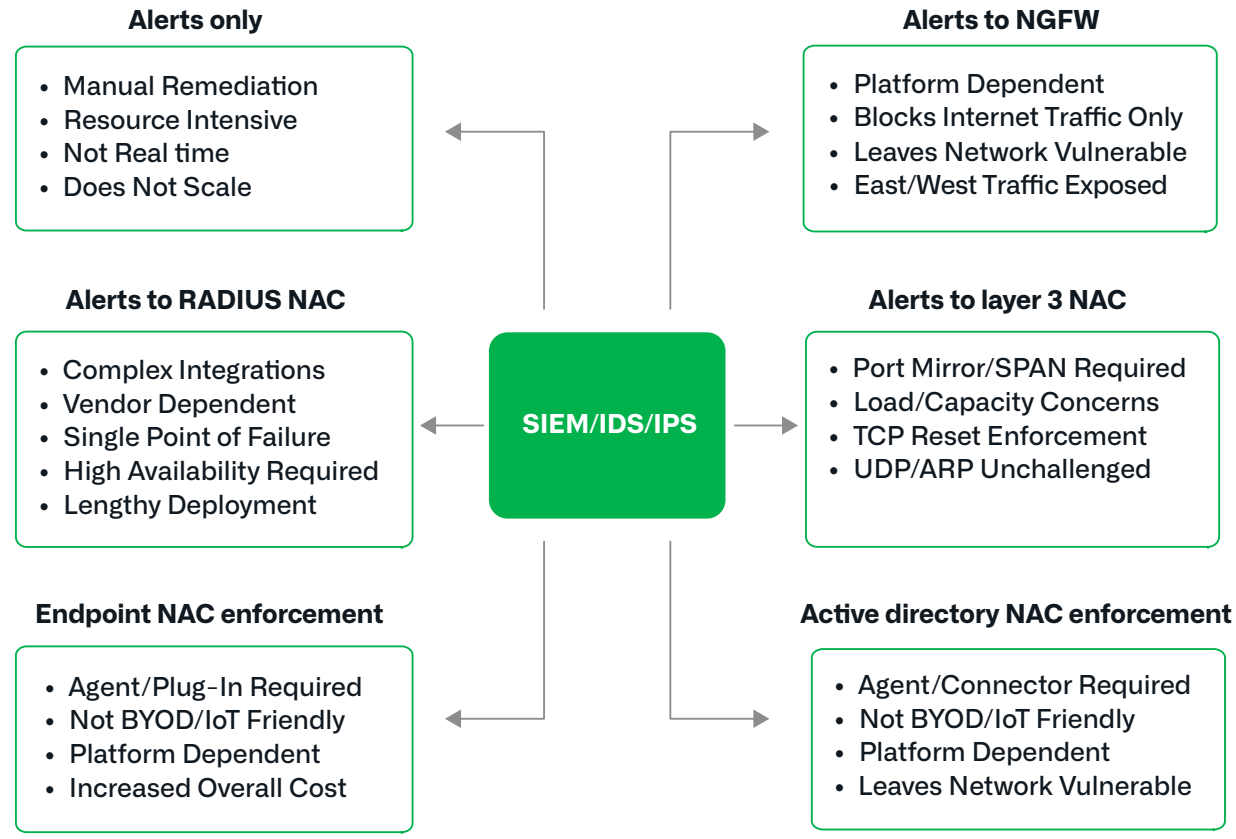

Figure 1: Dependencies involving legacy threat detection and quarantine solutions hamper mitigation.

Genians and Infoblox security automation

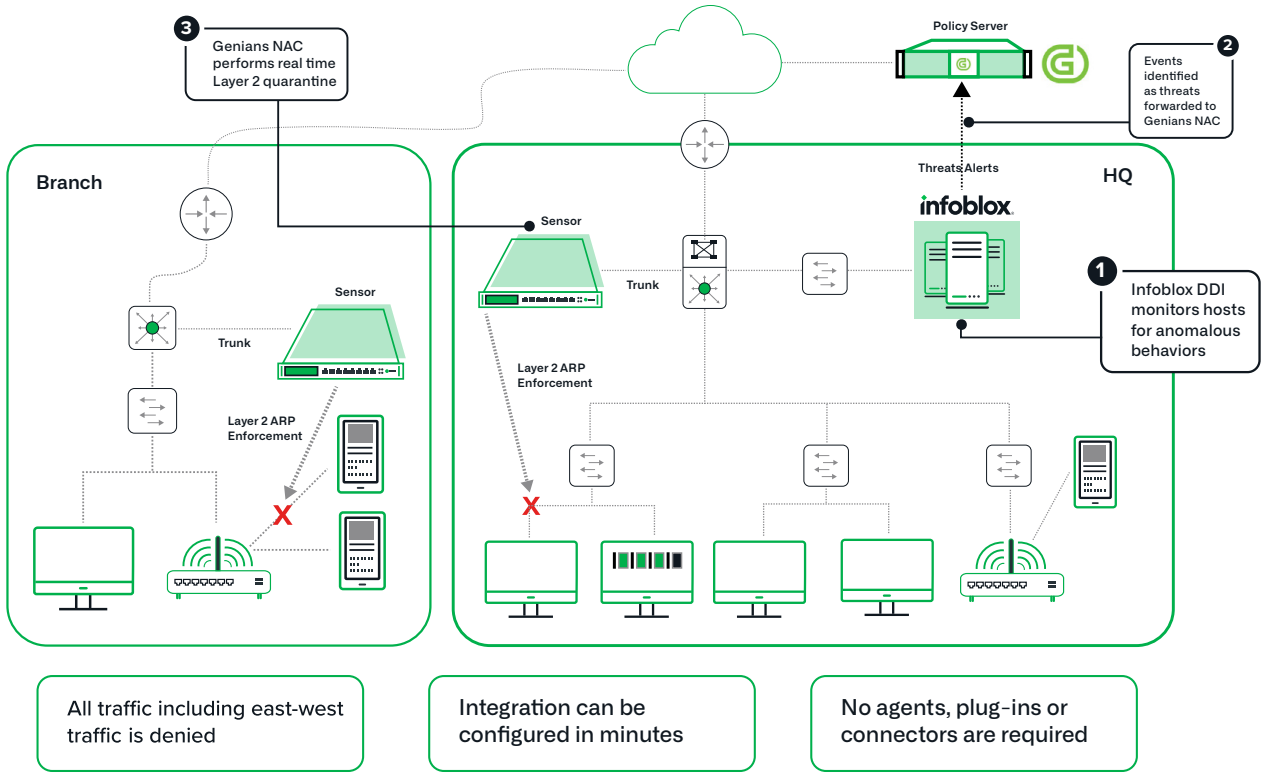

Figure 2: The joint Infoblox-Genians solution accelerates threat response

CONCLUSION

Legacy approaches to mitigating the ever-changing threat landscape of the BYOD, IoT era and beyond are simply failing to meet the demands of cybersecurity teams today. New approaches that can be easily adopted, rapidly deployed into any network environment and added to existing cybersecurity ecosystems on time and on budget are necessary. Infoblox DDI with RPZ monitoring and cloud-managed Genians Next-Gen NAC with truly vendor-agnostic enforcement capability meet these stringent demands and answer the call.

MORE INFORMATION

To speak to an engineer to learn more about how to rapidly deploy this integration into your network environment, as well as discuss best practices and deployment scenarios, contact Infoblox or Genians today.

info@infoblox.com
hello@genians.com

Corporate Headquarters
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com

Version: 20231031v1