VISIBILITY AS A SERVICE

You cannot secure what you cannot see. In today's ever-changing environment, the need to understand what is on your network is paramount to having confidence in the security posture of your enterprise. It is so important, that SANS ranks Hardware Asset Management (HWAM) as number one on its list of the top 20 CIS Critical Security Controls. Offered through the Northwest Regional Data Center (NWRDC), Visibility as a Service by ForeScout CounterACT® is an agentless, network-connected device discovery solution that provides rapid visibility of devices as they connect to your network whether wired, wirelessly, or via a VPN connection. CounterACT automatically determines the user, owner, operating system, device configuration, software, services, patch state and the presence of security agents, all while providing continuous remediation, control and monitoring of these devices.

You cannot track what you cannot see. All discovered data can be integrated into and used with IT Service Management (ITSM) solutions to provide asset intelligence and context to other processes. Your organization's ability to track assets, where they reside and what is installed on them is reliant upon an accurate representation of the connected endpoints and devices. SANS also cites Software Asset Management, Configuration Management and Vulnerability Management as critical security controls. Each of these areas depend on an accurate understanding of the devices themselves upon which to use as targets.

AGENTLESS AND RAPIDLY DEPLOYED

CounterACT can be quickly deployed in a number of days, giving visibility into various infrastructure technology environments. Its agentless design makes implementation easy, with minimal configuration changes required. Once deployed, CounterACT begins watching the traffic, events, connections and disconnections, all while analyzing the devices, categorizing them by type, ascertaining manageability, assessing for compliance against established policies, and determining whether to allow or deny access privilege. All of these functions are performed agentlessly and continuously, ensuring the complete visibility of all IP-connected devices at the moment they connect, with context around their posture and compliance.

RICH, CONTEXTUAL DISCOVERY DATA

CounterACT discovers and aggregates hundreds of data points on the discovered endpoints. Additionally, when integrated with third party solutions such as vulnerability scanning or advanced threat detection technologies, many of the properties associated with the endpoints as scanned or analyzed by those solutions are also brought into CounterACT, adding to the robustness of the device repository. Each of those individual property elements can be used in policies for analysis to determine compliance, or simply for basic asset querying and reporting purposes.

FEATURES

Open interoperability: CounterACT works with popular switches, routers, VPNs, firewalls, endpoints, operating systems (Windows®, Linux, iOS, OS X and Android), patch management systems, antivirus systems, directories and ticketing systems) without infrastructure changes or equipment upgrades.

Out-of-band deployment: Deploys out-of-band on your network without adding latency or a potential network failure point.

Scalability: Proven in customer networks exceeding 1,000,000 endpoints with current support for 2,000,000 endpoints in a single deployment. CounterACT appliances are available in a variety of sizes.

Flexible control options: Unlike "old school" NAC products that employ heavy-handed controls and disrupt users, CounterACT provides a full spectrum of enforcement options that allow you to tailor the response to the situation.

Reporting: A fully integrated reporting engine helps you monitor your level of policy compliance, fulfill regulatory audit requirements, and produce real-time inventory reports.

Policy management and enforcement: Create security policies that are right for your enterprise. Configuration and administration are fast and easy thanks to built-in policy templates, rules and reports. Enforce network access control, endpoint compliance, and movable device security.

THE NWRDC ADVANTAGE

The Northwest Regional Data Center (NWRDC) is pleased to partner with ForeScout Technologies to provide its VaaS solution at competitive rates. Serving public and not-for-profit entities for over forty-five years, NWRDC is one of Florida's leading computing providers for government and educational communities. Their status as an auxiliary of Florida State University allows public entities to contract directly with them for a number of IT support solutions without engaging in a lengthy procurement bid process. Contact NWRDC today to see how ForeScout's VaaS can benefit your organization.

CONTACT US

For more information about NWRDC's VaaS Partnership with ForeScout please contact them at info@nwrdc.fsu.edu or 850-645-3500. For complete service offerings and rates, please refer to http://www.nwrdc.fsu.edu/servicecatalog. To learn more about CounterACT, visit: https://www.forescout.com/products/counteract/

Agentless. No endpoint agents required for authentication and network access control.

Exceptional visibility. See devices that other solutions can't:
- Desktops, laptops, servers, routers, smartphones and tablets
- Wired/wireless LANs and printers
- IoT devices (projectors, industrial controls, healthcare, manufacturing, POS devices and more).

Role-based access. CounterACT leverages your existing directory to ensure the right people with the right devices gain access to the right network resources.

Automated control. Automate an extensive range of actions:
- Grant, deny or limit network access based on device posture and security policies
- Quarantine and remediate malicious/high-risk endpoints

Reliability. Improve network stability by identifying and removing rogue infrastructure.

Productivity. Grant appropriate network access to persons and devices—without intrusive intervention or staff involvement.

Cost savings. Eliminate manual labor associated with opening/closing network ports for guest access.

Compliance. Automatically identify policy violations, remediate endpoint deficiencies and measure adherence to compliance mandates.

ForeScout®

NWRDC