nuagenetworks
From Nokia

Partner Solution Brief

SDN-based threat response with CounterTack Endpoint Detection and Response integration

SOLUTION OVERVIEW

CounterTack® Sentinel Endpoint Detection and Response solution and Nuage Networks Virtualized Services Platform (VSP) work together to provide advanced threat detection for your datacenter. Through deep server and workload system-level visibility, the solution enables an integrated SDN response that facilitates detection, remediation and diversion of threats.

CounterTack Sentinel solution is certified to interoperate with Nuage Networks VSP.

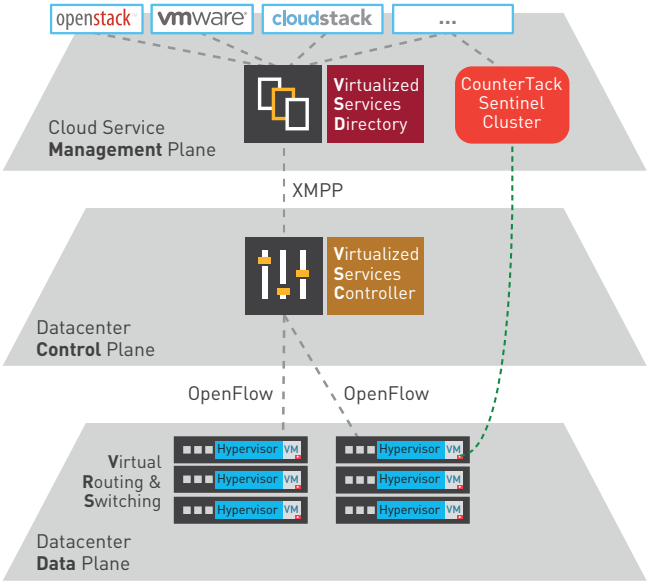
SOLUTION FOR

Application Service Providers with Internet facing datacenters

Enterprise /Internal Datacenters with connectivity to private networks (VPN)

Telecommunication Providers offering clean Internet services

CounterTack | ManTech Cyber Solutions International



- Delivers authoritative server and workload visibility for detecting insider threats, advanced threats and policy breaches within your datacenter
- Extends the speed and efficiency of a Nuage Networks-enabled network to the detection, containment and isolation of advanced attacks
- Tight integration with Nuage Networks APIs allows for diverse use-cases including visibility, isolation, and diversion and deception

Together, Nuage Networks and CounterTack have created the abilty to seamlessly bring next-generation endpoint visibility, detection and response capability into your datacenter.

As a datacenter manager, you are under pressure to protect your infrastructure and applications from increasingly sophisticated, stealthy and targeted threats.

It is all too common for stealthy attacks to seep through the existing perimeter and network-based datacenter protections. You need a highly scalable and efficient system for detecting and responding to advanced threats (known and unknown) only visible from deep within the server or desktop operating system.

The CounterTack Sentinel Endpoint Detection and Response solution offers you unprecedented visibility, control and detection capabilities using big data analytics to discover both known and unknown (zero-day) malware lurking in your organization.

When deployed alongside the Nuage Networks VSP, the Endpoint Detection and Response solutions can trigger real-time network policies to isolate/quarantine and take diversionary actions that render advanced threats and insider attacks impotent.

Endpoint insight and detection is a critical strategy augmenting the network security capabilities inside your datacenter. It simultaneously provides you with deep, endpoint context to enable better and faster incident response. It also detects advanced threats that would have previously lingered for days, weeks or months, providing you with an essential strength in combating today's advanced and targeted threats.

Integration with the Nuage Networks VSP allows for an automated, fine-grained response to isolate the impacted workload during remediation as well as advanced diversion for further intelligence gathering and deception.

UNPRECEDENTED ENDPOINT CONTEXT WITH NETWORK RESPONSE

Today's advanced threats can only be reliably detected and validated with deep, endpoint analysis. Combining this analysis with policy-based automation features from Nuage Networks VSP gives you an advantage in detecting and responding to advanced, targeted and insider attacks across your organization including your critical datacenter assets.

SECURING THE DATACENTER NETWORK

With Nuage Networks VSP and CounterTack, security becomes an integral part of the datacenter fabric.

ABOUT COUNTERTACK

CounterTack | MCSI is the leading provider of real-time, big data endpoint detection and response technology for the enterprise. The company provides unprecedented visibility and context around operating system and in-memory behaviors to detect zero-day attacks, rootkits, targeted malware and advanced persistent threats.

CounterTack | MCSI solutions dramatically reduce the impact of the most advanced attacks in real-time, giving teams an opportunity to defend the enterprise before incidents escalate.

Learn more:
www.countertack.com

Solution features and benefits

With the CounterTack Sentinel solution deployed throughout your organization, including your datacenter assets, you immediately begin to gain rich endpoint context including:

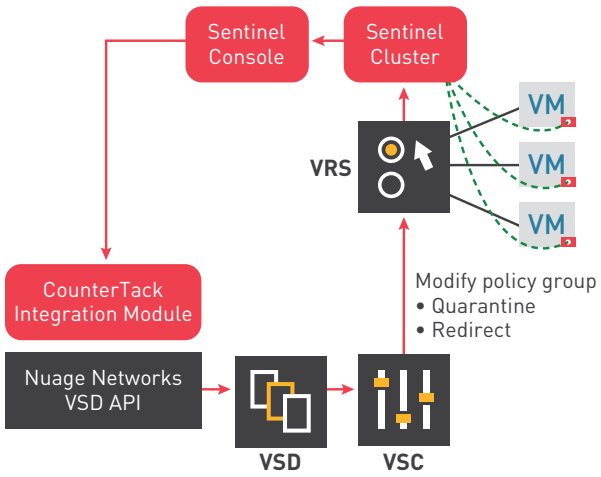
- Processes including execution, termination and related activity
- File information including remote and local file access and details
- Memory allocations for processes and executions
- Networking connections tied to above
- Registry values (Windows® Server OS)

By performing stateful, system-level, behavioral analyses, advanced threats, insider attacks and policy breaches are discovered in real-time.

The CounterTack Endpoint Detection and Response solution can be deployed on servers and workloads alongside the Nuage Networks VSP.

Integration between CounterTack Sentinel Endpoint Detection and Response allows for fine-grained control of Nuage Networks VSP micro-segmentation policies. This in turn provides intermediary isolation (while the infected asset undergoes incident response) as well as network diversion for the purpose of either further investigation or deception.

Leveraging the automated micro-segmentation policies and API capabilities of the Nuage Networks VSP you have flexibility around integrating network policy decisions with advanced endpoint threat detection and response.



About Nuage Networks

Nuage Networks (www.nuagenetworks.net) brings a unique combination of groundbreaking technologies and unmatched networking expertise to the enterprise and telecommunications industries. The Silicon Valley-based business has applied radically new thinking to the problem of delivering massively scalable and highly programmable SDN solutions within and across the datacenter and out to the wide area network with the security and availability required by business-critical environments. Nuage Networks, backed by the rapidly growing IP/Optical Networks business of Nokia, has the pedigree to serve the needs of the world's biggest clouds. The cloud has made promises — the mission of Nuage Networks is to help you realize them.

Discover more at www.nuagenetworks.net/partners and follow us @nuagenetworks

nuagenetworks
From Nokia