epaton

NUTANIX: THE LAST SECURITY APPLIANCE YOU WILL EVER BUY

About the Author

Rob Jeffery, Technical Director of NG Security (UK) Ltd. is a customer and solution focused IT Security Specialist. After starting his work life in the hospitality industry, Rob gained a 1st class honours degree in Network Infrastructure Technologies and Business Computing Solutions.

During his studies Rob won a number of awards for academic and technical achievement, before joining a security VAR and MSSP in a support role. Rob quickly demonstrated his skills and knowledge, rising through the ranks running large managed services, delivering on site consultancy and working as a solutions specialist on major accounts. Rob then acted in a consultative capacity for a number of years before becoming Technical Director at NGS.

Rob is also a Juniper Networks Ambassador and has authored two Juniper Day One books on migrating from Cisco to Juniper technologies.

Collaboration

In a collaboration between Epaton and NG Security (UK), we are combining years of experience within both the IT infrastructure and Cyber Security fields to deliver the last security appliance you will ever have to buy, utilising Nutanix's hyper-converged infrastructure technology to provide the platform for a virtualised security portfolio to sit on.

Epaton are a value added reseller specialising in infrastructure with a focus on next generation storage and back up solutions. Epaton have been winners of the Specialist Storage Reseller of the Year Awards for 2016, 2017 and 2018, and continue to support customers across the UK by redesigning and transforming their on-premise and cloud infrastructure platforms.

Formed in 2018, NG Security (UK) Ltd, or NGS for short, are independent, vendor agnostic, next generation security trusted advisors, providing all-encompassing solutions from the perimeter to the endpoint.

The Directors, previously at the helm of the Security Reseller of the Year 2013 & 14, bring with them over 60 years of IT security industry experience. Using their broad experience of the Security market combined with the vast knowledge and ability of the wider team, NGS give an unrivalled delivery capability that will help your business develop a strategic architectural blueprint, a business case and a clear roadmap. We translate ideas into actions, delivering significant and measurable value with every element of work undertaken. Unlike many, we're not offering point solutions but providing total security solutions.

Innovation is key, and both companies constantly research the market to advise customers on the most effective technologies and practices to develop their business operations. Partnering with the most innovative and leading technology vendors to drive improved uptime and customer satisfaction. Both Epaton and NGS deliver options to ensure the most informed decisions are made, offering everything from concept to completion.

epaton

INTRODUCTION

Introduction

So it seems a very provocative title, and that is the intention! So why do we think that a HCI vendor produces the last security appliance you will ever buy? Because as far as we're concerned (taking specialist requirements out of the equation) you'll never need to buy a physical security appliance again. Thanks to the proliferation of virtualisation and cloud over the last decade or so we can achieve the same levels of security virtualising security solutions/products as we can deploying dozens of 'branded' appliances which in the majority of cases are just rebadged commodity servers/appliances.

With all the benefits brought forth by virtualisation over the last decade and a half including consolidation, better ROI, higher availability - the threat landscape has expanded, and virtualisation was not designed with security at the forefront. As we see progression towards application mobility and hybrid clouds it's imperative that security is part of every design, enforcing policy for applications at the most granular levels.

In addition to the inherent security hardening and self-remediation capabilities of the Nutanix AHV hypervisor, customers can now easily implement more granular policies leveraging isolated networks and the world class security from 3rd party vendors. Nutanix delivers best-in-class Enterprise cloud to empower its users with the agility and economics of public cloud, without sacrificing the control of on-premise.

The Network is Evolving

How users and organisations access and consume information has and is changing and the network is evolving to meet those demands. The need for elastic storage and compute has driven many organisations to the cloud.

The need for mobility has pulled organisations out of the traditional Data Centre to a SaaS model. But, completely cloud or completely SaaS is a rarity in todays IT environments and the traditional on-premise paradigm has shifted to deliver cloud and SaaS like solutions from the traditional Data Centre. The need to create new networks on the fly, on a per application basis has created a boom in SDN (Software Defined Networking).

The change to the reliability and abundance of cheap internet connectivity is slowly moving organisations away from traditional WAN technologies such as MPLS, towards using commodity connectivity and SD-WAN technologies to not only save costs but provide more flexible and resilient Wide Area Networks. Cloud has created an entire paradigm shift were networking is abstracted and can be defined by intent or scripted up by a software engineer. Even Security itself has evolved beyond the traditional hard-shell model into an application and user centric model.

but it's all just software

Fundamentally when we look at the security solutions we use, 99.9% of them are software running on a piece of tin. Regardless of what that piece of tin is, it is the actual software that is the intelligence behind the security solutions. With the proliferation of virtualisation and cloud computing, security vendors have adapted traditional appliance-based solutions to run solely on the same commodity x86 hardware used by the big cloud providers.

HIGH LEVEL ARCHITECTURE

Firewall

Selecting Palo Alto Networks® or Check Point Software Technologies Next Generation Firewalls gives us the flexibility to deliver a raft of security protections at the border and key network segments. Within this solution the firewalls provide traditional firewall functionality, Intrusion Protection, Anti-Malware and Sandbox, Web filtering and Application control. As per the diagram the firewalls are located at the traditional egress to the internet providing the first line of defense and the last line of user browsing control.

SD-WAN

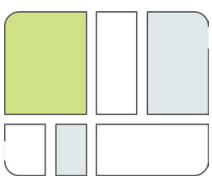
WAN connectivity has changed with the reliability and resiliency of commodity internet connectivity. The need for dedicated WAN solutions such as MPLS is significantly reduced and vast cost savings can be achieved. Utilising SD-WAN and commodity connectivity with flexible resiliency from vDSL and 4G, and with the 5G on the horizon flexible, fast, low latency wire free connectivity will soon become commodity. SD-WAN future proofs the solution against any changes in interconnectivity between sites.

Remote Access

Whilst Palo Alto Networks Global protect is an excellent solution, looking at the bigger picture, where the solution as a whole can be expanded to integrate additional technologies such as VDI. With the capability to provide SSO to web and SaaS application the Citrix Gateway provides a huge amount of flexibility and security.

Application Delivery Control

Citrix ADC provides a market leading application delivery platform fit for the modern world easily scalable to the cloud both private and public. Designed for an application centric work flow it allows DevOps teams to automate ADC delivery along with Applications through API's or through deep integration with Nutanix flow, whilst delivering enterprise class security.



Micro-segmentation

When using AHV Nutanix Flow allows us to take security to the next level with application centric micro segmentation to isolate application resources preventing east-west spread of malicious code and preventing attacker pivots further into the network.

Illumio provides the same benefits and functionality but, with cross hypervisor platform compatibility.

SIEM

AlienVault® USM delivers not only SIEM functionality backed by the OTX Threat Exchange but, provides IDS, vulnerability scanning and more, although more importantly for its place here is that it integrates and collects logs from AWS and Azure. This allows organisations to not only build out a private cloud with Nutanix but, also where required extend out onto public clouds without compromising security.

AV\AM

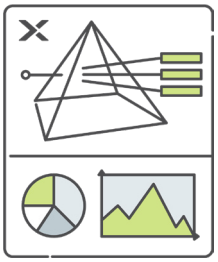
Bitdefender provides hypervisor level anti-virus and anti-malware protection ensuring that all virtual machines within the organisation are protected from known and unknown threats.

Key Management

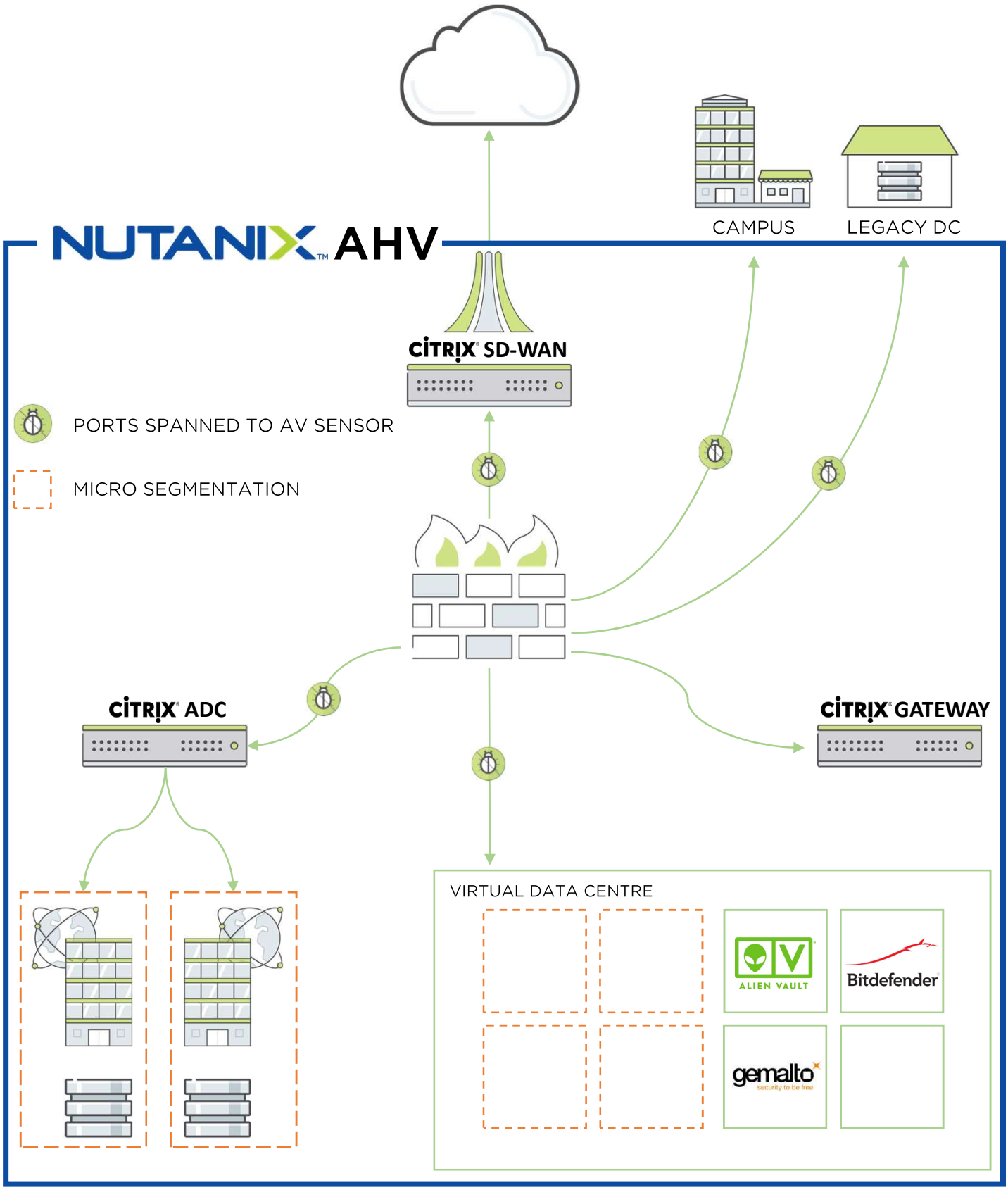
Securing your data center and campus whilst critical, securing your virtual infrastructure is just as important and managing encryption keys effectively and securely is likely one of the most critical security controls you can put in place. Whilst Nutanix provide self-encrypting drives, with the Nutanix solution the key managament is held on box and in some cases could be a failure of compliance.

Gemalto SafeNet KeySecure™ integrates with Nutanix via the Key Management Interoperability Protocol (KMIP) to store the encryption keys for each self-encrypting drive. By consolidating the policy and key management of application servers, databases, and file servers, security administration is streamlined. Centralised key management improves security in a number of ways, most notably by making key surveillance, rotation, and deletion easier while separating duties so that no single administrator is responsible for the entire environment. Additionally, unifying and centralising policy management, logging, and auditing makes information more readily accessible and demonstrating compliance with data governance requirements simple.

Automation & Orchestration



Nutanix Prism powered by AI and Machine learning provides a single pane of glass to manage resources and provisioning. Coupled with Nutanix flow, users can expand into service chaining, and orchestration, automatic configuration changes as services are added and removed from the environment. When working alongside Prisms built in service catalogue the deployment of services whether long lived or ephemeral can be provisioned with all the required security controls and micro segmentation already in place without any user interaction. This means that security teams develop gold standards for pre-defined services types reducing not only their work load but, allows security and compliance teams to enable rather than hinder DevOps teams.


NUTANIX AHV
CAMPUS
LEGACY DC
CITRIX SD-WAN
PORTS SPANNED TO AV SENSOR
MICRO SEGMENTATION
CITRIX ADC
CITRIX GATEWAY
VIRTUAL DATA CENTRE
ALIEN VAULT
Bitdefender
gemalto

SECURITY PRODUCTS

For the purpose of this paper we have focused on providing a template for what we feel would be the minimum security controls that the majority of organisations would have in place. We have done this with the aim of keeping the number of vendors to a minimum.

Firewall

Both Palo Alto Networks® and Check Point Software Technologies Next Generation Firewalls detect known and unknown threats, including in encrypted traffic, using intelligence generated across many thousands of customer deployments. That means they reduce risks and prevent a broad range of attacks. For example, they enable users to access data and applications based on business requirements as well as stop credential theft and an attacker's ability to use stolen credentials.

SD-WAN

The traditional WAN was not designed to tackle today's application traffic. Citrix SD-WAN, offers a scalable, reliable, and cloud-ready approach. Citrix SD-WAN combines packet-level, real-time path selection, WAN optimisation, firewall, routing, and application analytics into one comprehensive solution. Whether accessing SaaS applications, virtualised desktops, or traditional data centers, Citrix SD-WAN ensures an always-on, high-quality experience and a simpler, more agile branch network.

Remote Access

People today need to access their apps from anywhere and on any device. Citrix Gateway provides best-in-class security and a seamless user experience by providing secure access and SSO across enterprise, VDI, web, or SaaS app hosted on any data center or cloud through a single URL.

Citrix Gateway consolidates multiple remote access solutions, provide Single Sign-On (SSO), multi-factor authentication, end-to-end monitoring across all application traffic and contextual access control across on-premise VDI, web, cloud and SaaS apps. It helps reduce costs, simplify management, and improve the user experience.

AV\AM

Engineered for HCI, Bitdefender GravityZone Datacenter Security is a server- and VDI-workload protection platform that delivers award-winning next-generation defenses while facilitating IT agility, operational efficiency and infrastructure-cost containment. A single-console, single-agent solution, GravityZone unifies security management for physical, virtual and cloud workloads, enabling single-pane-of-glass visibility and consistent policy enforcement across the enterprise cloud.

Application Delivery Control

Citrix ADC was created to transform traditional networks into next-gen, app-driven enterprises. Designed for use in virtualised networks, it's ideally suited to integrate with SDN and cloud orchestration systems. The platform combines the flexibility of virtualisation with the resiliency, reliability, and performance of purpose-built network appliances. Eliminating the need for multiple physical devices, a single Citrix ADC can be deployed in a multi-tenant environment, while also offering traffic isolation and dedicated resources per tenant.

Administrators can rightsize instances based on the workload required per tenant, with fine-grained control over the CPU, memory, and SSL hardware resources, to achieve performance goals.

Micro-segmentation

Nutanix Flow simplifies network and policy management with a focus towards applications – enabling applications and environments to be governed independent of the physical infrastructure. Delivering advanced networking and security services that allow enterprises to gain visibility and granular control of their enterprise applications, leading to better application function and security posture.

Nutanix can provide additional network functions by enabling partners and other 3rd party virtual networking solutions to integrate directly into the virtual network. Tightly integrated with Calm, Prism and AHV virtualisation, Nutanix Flow delivers the power of software defined virtual networking with the simplicity and elegance of the Enterprise Cloud OS.

**Nutanix Flow only works on the Nutanix AHV (Acropolis) hypervisor Were you wish to use either HyperV or vSpere hypervisors we would recommend Illumio for Micro segmentation.

Illumio ASP delivers micro-segmentation that is enabled by combining vulnerability data with real-time traffic visibility. This powerful combination enables organisations to understand how their applications work, see where they are most vulnerable, and use that visibility to create and enforce micro-segmentation policies.

Rather than purchasing more infrastructure (firewalls, hypervisors upgrades, or switches), organisations use Illumio ASP to turn every workload into a point of traffic visibility, a point of micro-segmentation enforcement, and a sensor that detects any connectivity policy violations.

With a patented, software-only architecture, Illumio ASP is the new foundation for data centre and cloud security, offering a range of micro-segmentation options.

SIEM

AlienVault® USM Anywhere delivers powerful threat detection, incident response, and compliance management in one unified platform. It combines all the essential security capabilities needed for effective security monitoring across your cloud and on-premises environments: asset discovery, vulnerability assessment, intrusion detection, endpoint detection and response, behavioral monitoring, SIEM log management, and continuous threat intelligence. Built for today's resource-limited IT security teams, USM Anywhere is more affordable, faster to deploy, and easier to use than traditional solutions. It eliminates the need to deploy, integrate, and maintain multiple point security solutions in your data center. USM Anywhere offers a low total cost of ownership (TCO) and flexible, scalable deployment options for teams of any size or budget.

Key Management

Gemalto SafeNet Virtual KeySecure™ is a hardened virtual security appliance that provides organisations with a more operation and expense friendly alternative to using a hardware appliance for secure key management and meeting security and compliance requirements. By using a virtual key manager instead of a hardware appliance, organisations can scale key management in private or public cloud infrastructures, and eliminate the cost for additional rack space.

SafeNet Virtual KeySecure allows organisations to utilise a secure virtual appliance to manage keys as well as data encryption, and enforce access control across cloud infrastructures. It also ensures that organisations maintain ownership of their encryption keys at all times by hardening the appliance OS and encrypting the entire virtual appliance for enhanced key security and protection against snapshot attacks.

There is no Limit

We have discussed what we see as the basics of any security environment within this paper however, there are no limits to the solutions that can be put in place other than the resource limits of the Nutanix environment.

Expanding the solution could include technologies such as:

- Identity & Access Management
- Data Loss Prevention
- Cloud Access Security Broker
- Mobile Device Management
- Web and Email

epaton

specialists in **next-gen storage**

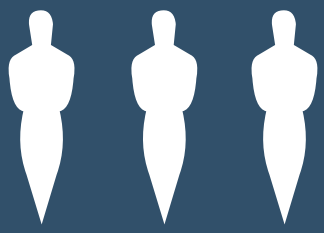
STORAGE AWARDS

THE STORRIES XIII

WINNER

Specialist Storage Reseller of the Year

2016 | 2017 | 2018



Ludgate House
107-111 Fleet Street
London
EC4A 2AB

Fountain House
4 South Parade
Leeds
LS1 5QX

03333 111001 | sales@epaton.co.uk | epaton.co.uk