NUTANIX™

Building Secure Enterprise Clouds

NEIL ASHWORTH | SECURITY SOLUTIONS ARCHITECT

NOVEMBER 2018 | CONFIDENTIAL

Agenda

1 State of the Union

2 What you talkin' bout techie?!

3 Platform Security & Automation

4 More tools in the toolbox

5 Making complicated simple

State of the Union

Data Centre Security

Worldwide spend on InfoSec was expected to reach **$90 billion** in 2017, which would be 7.6%

2018 is projected to hit **$114 billion** up 12.4% p.a.

And 2019, **$124 billion**

2017

143M+	SSN's compromised
150+	Countries hit by Wannacry
1/4	Risk of data breach in U.S.
$3.62M	Avg. cost of a data breach

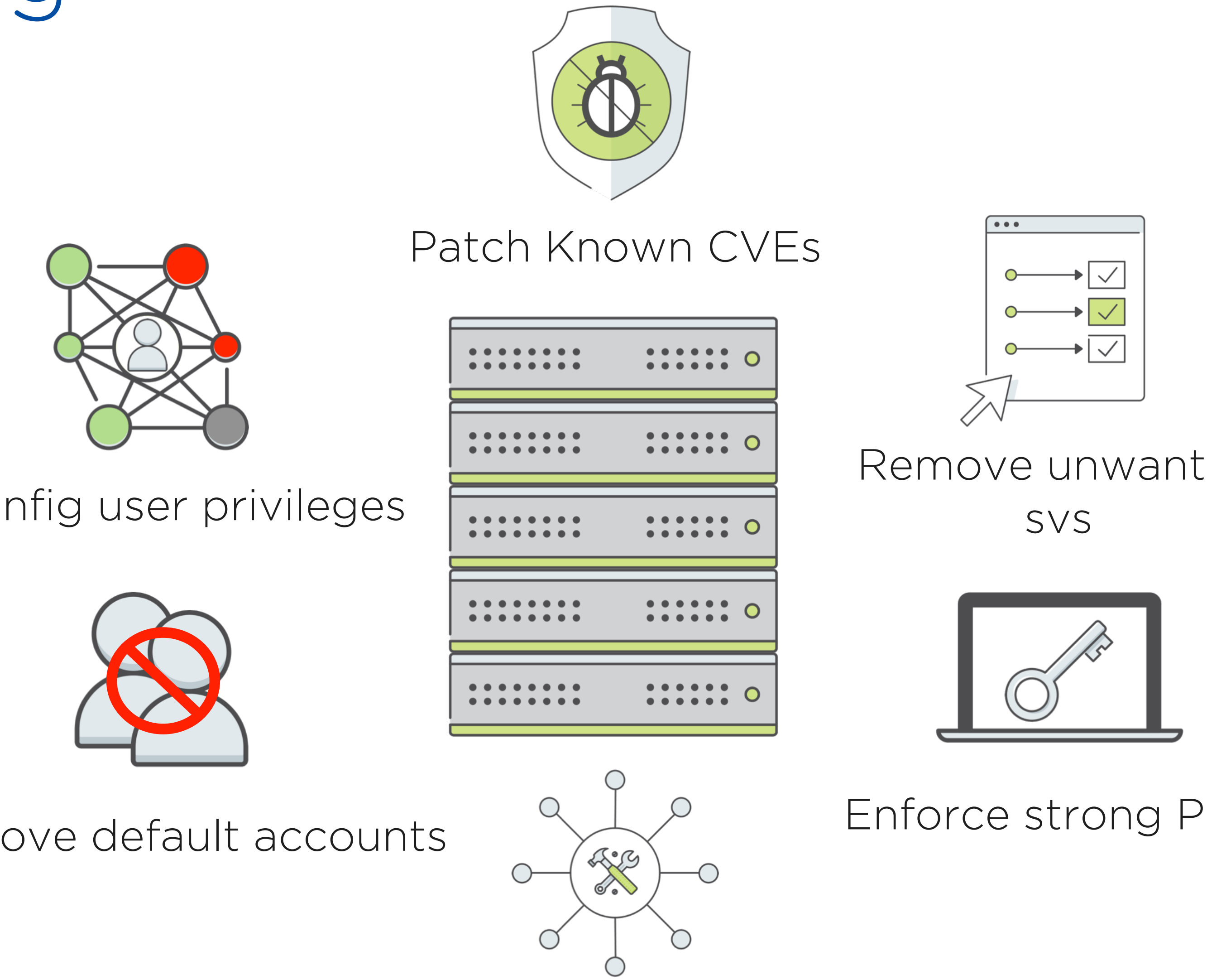
Prevention

Detection

Response

System Hardening

Prevent the possibility of executing vulnerable code by restricting the methods of being able to access certain systems.



Patch Known CVEs

Config user privileges

Remove unwanted svs

Remove default accounts

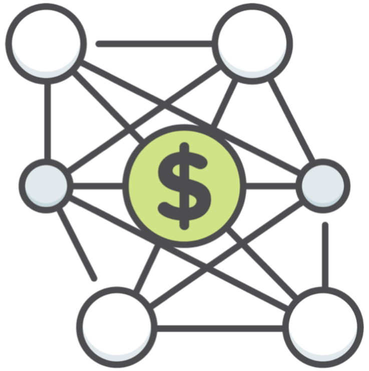
Enforce strong PWs

Close unused ports & protocols

Cloud is my savior!

Continuing complexity

Battling Shadow I.T.



Costs of Technical Debt

FOMO
"You should be in the Cloud."

Benefits of the Public Cloud

Rapid Time to Market

I can deploy my application in five minutes.

Fractional IT Consumption

I use and pay for just what I need, only when I need it.

One-click Simplicity

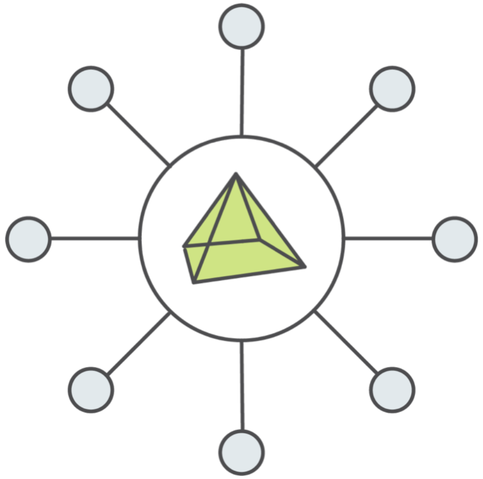
I don’t spend time on low-level infrastructure management.

Continuous Innovation

My infrastructure gets better on a regular basis.

Why not go full cloud?

Is Cloud cheaper?



Edge computing

Vendor lock in

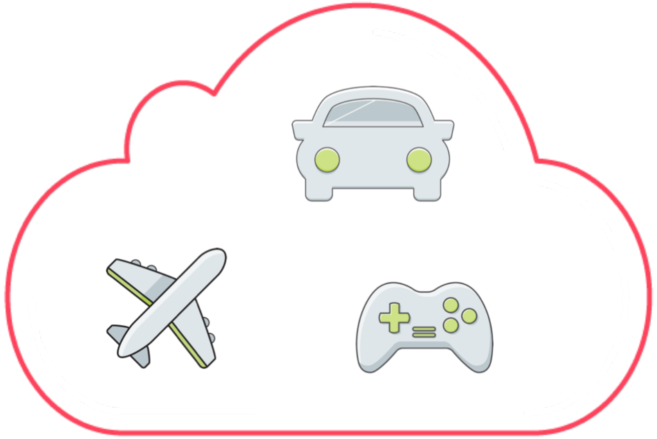
Not a single cloud anymore

Public Cloud

- Scalable and elastic
- Cloud-native applications

Private Cloud

- Predictable and secure
- Performance sensitive
- Mission-critical applications



Distributed Cloud

- Dispersed and small
- ROBO, Edge and IoT applications

What you talkin’ about techie?!

The Theory: A Software vendor makes life easier

Does the vendor understand how customers user their software?

Are the best practices and standards baked into the product?

Do their development lifecycles ensure a repeatable and predictable security baseline in products?

The Practice: Make what matters easier; security & compliance

Full-Stack Security Development Lifecycle

Automated Validation and Self-Healing of Baselines

Detailed Security Documentation for Auditors and IA Teams

What are we talking about?

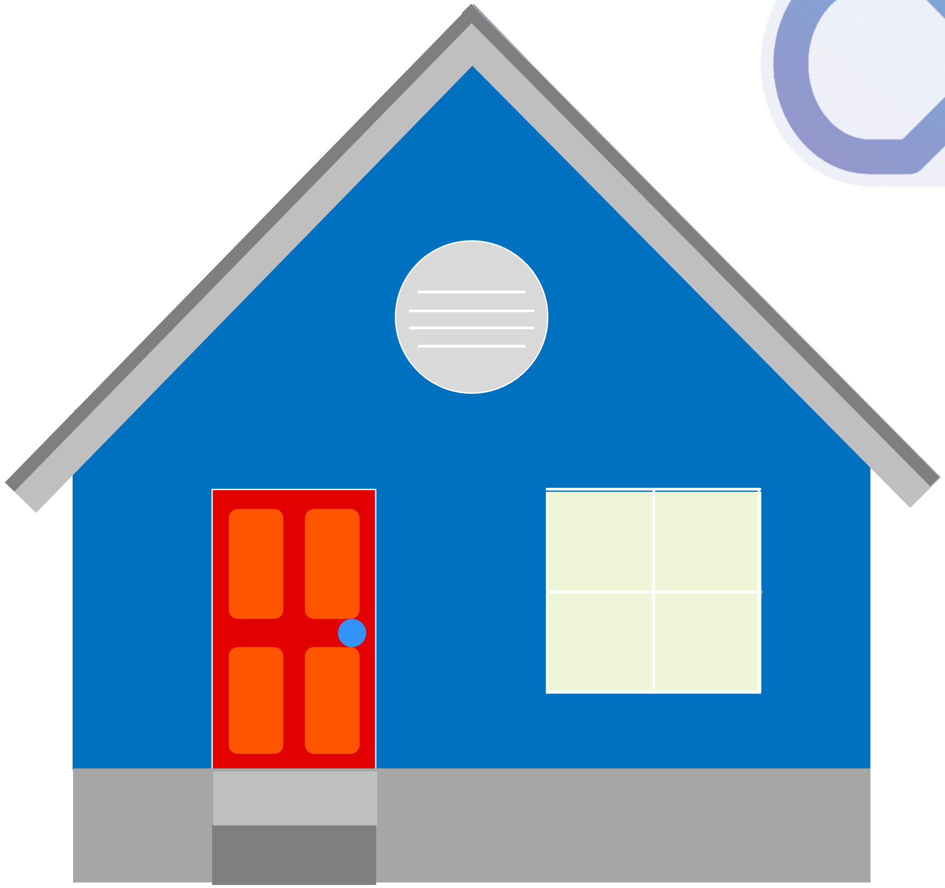
Changing face of technology: The more things change the more they stay the same.

- Virtualization
- Converged / Hyper-converged
- Webscale

Perpetual Legacy: Always securing, assessing, accrediting, never building, innovating or evolving.

A better way: Harden and heal but with automation.

The Security concept



Micro-Segmentation

DAR-Encryption

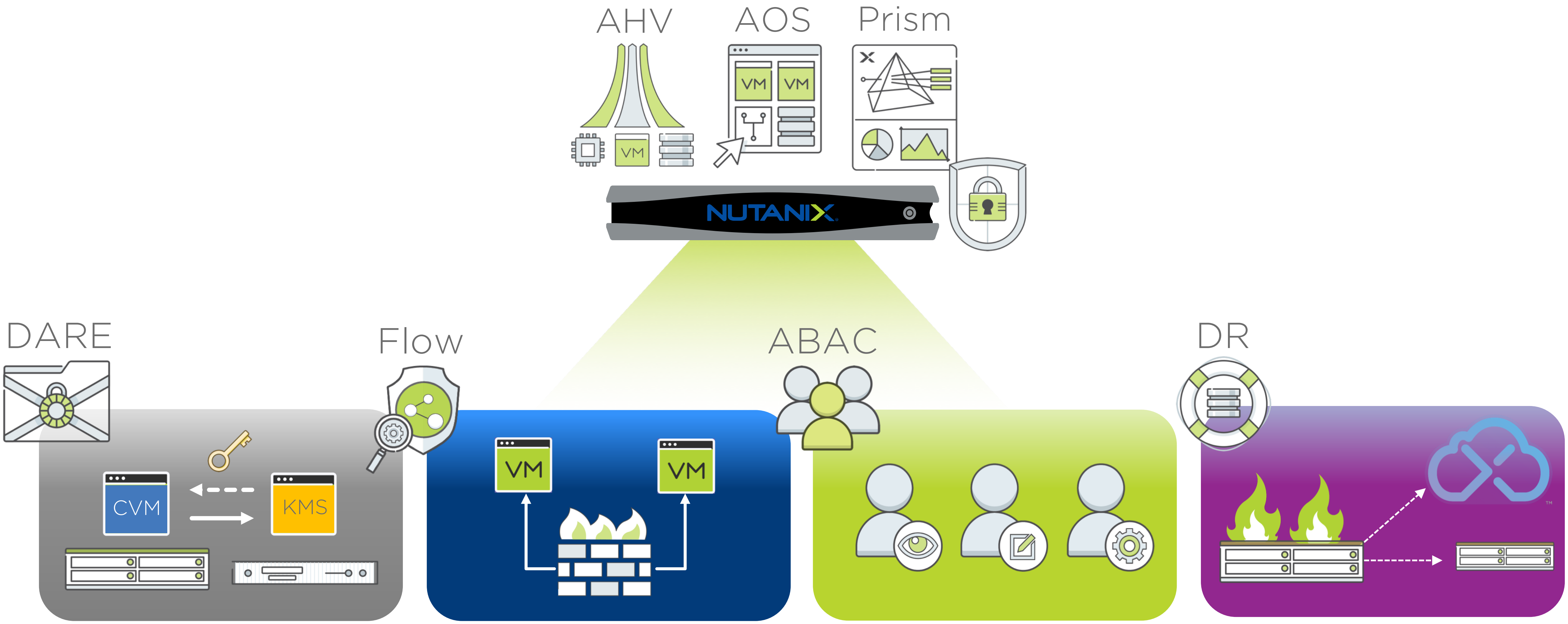
IAM with ABAC
& SAML

STIGs & SCMA

Security Development
Lifecycle

More tools in the toolbox

Secure foundation for securing data

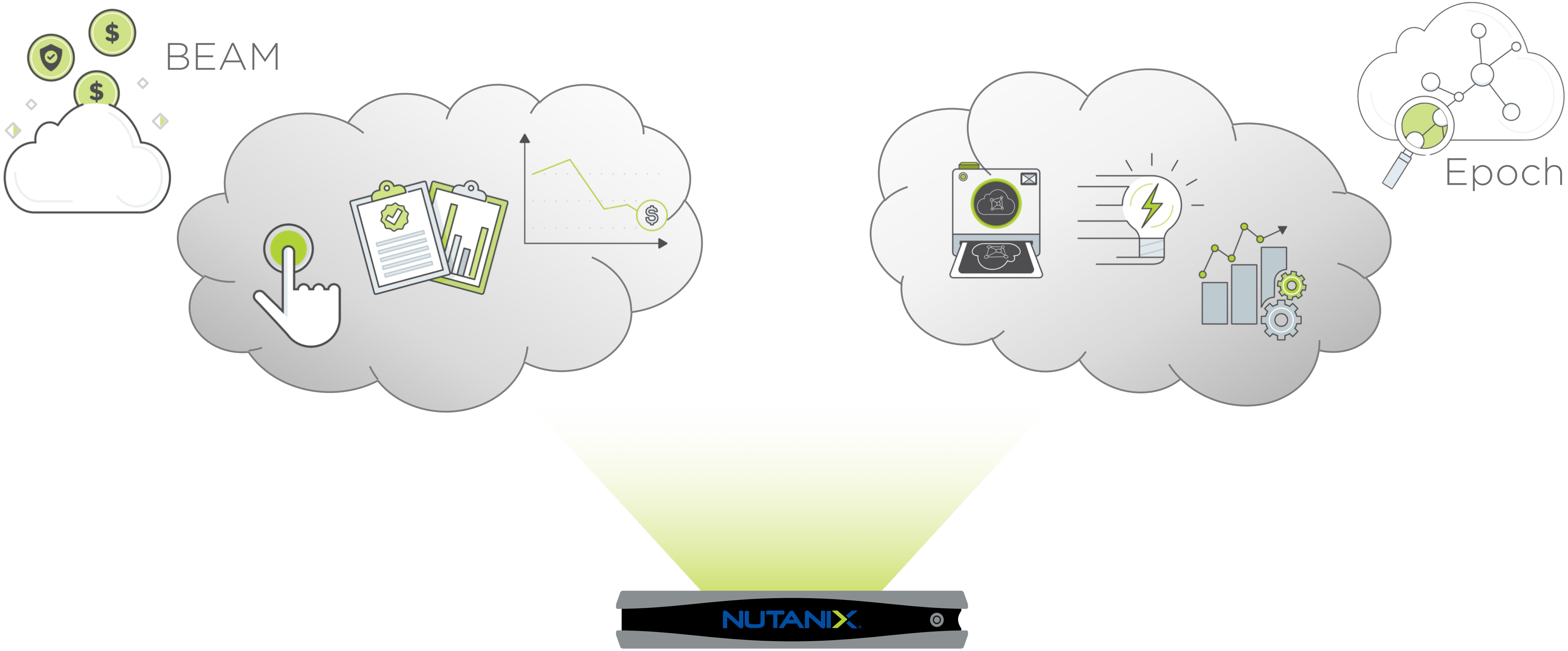


Cloud services

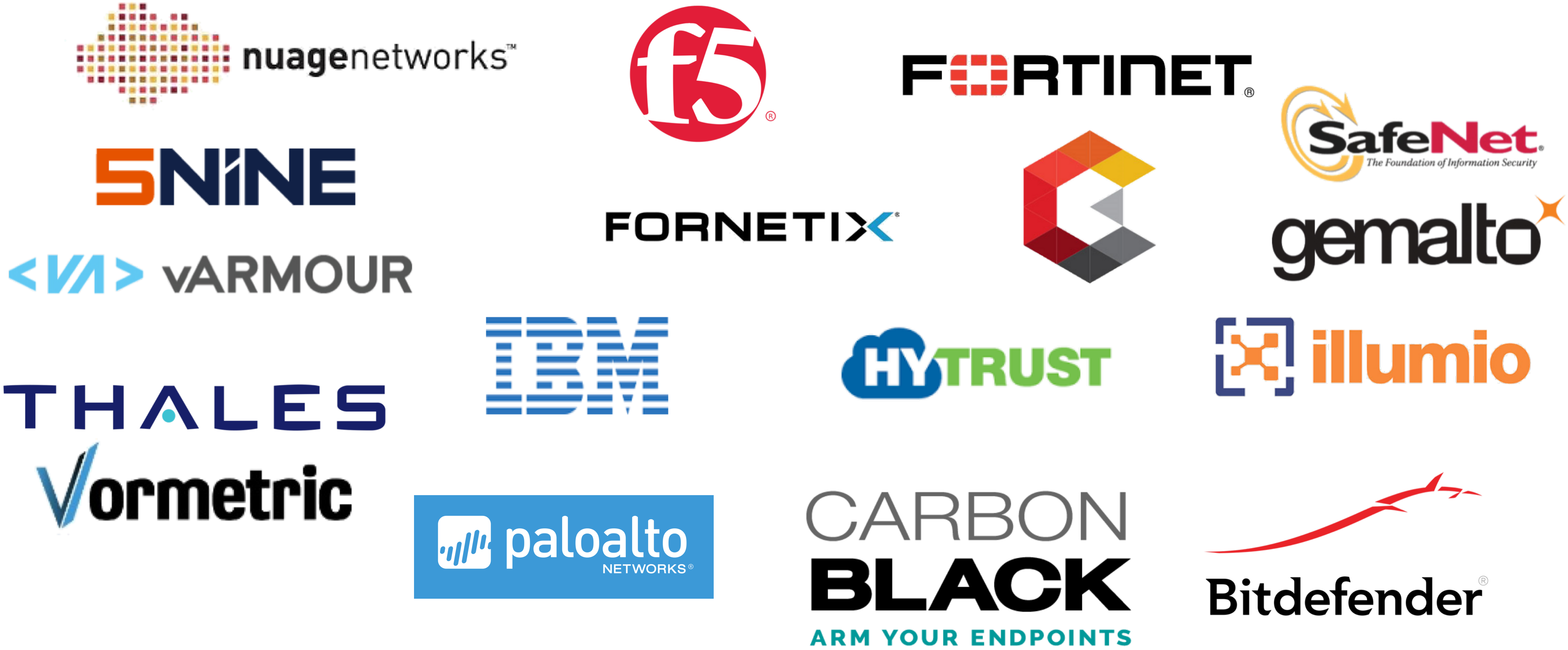
amazon web services

Microsoft Azure

Google Cloud Platform

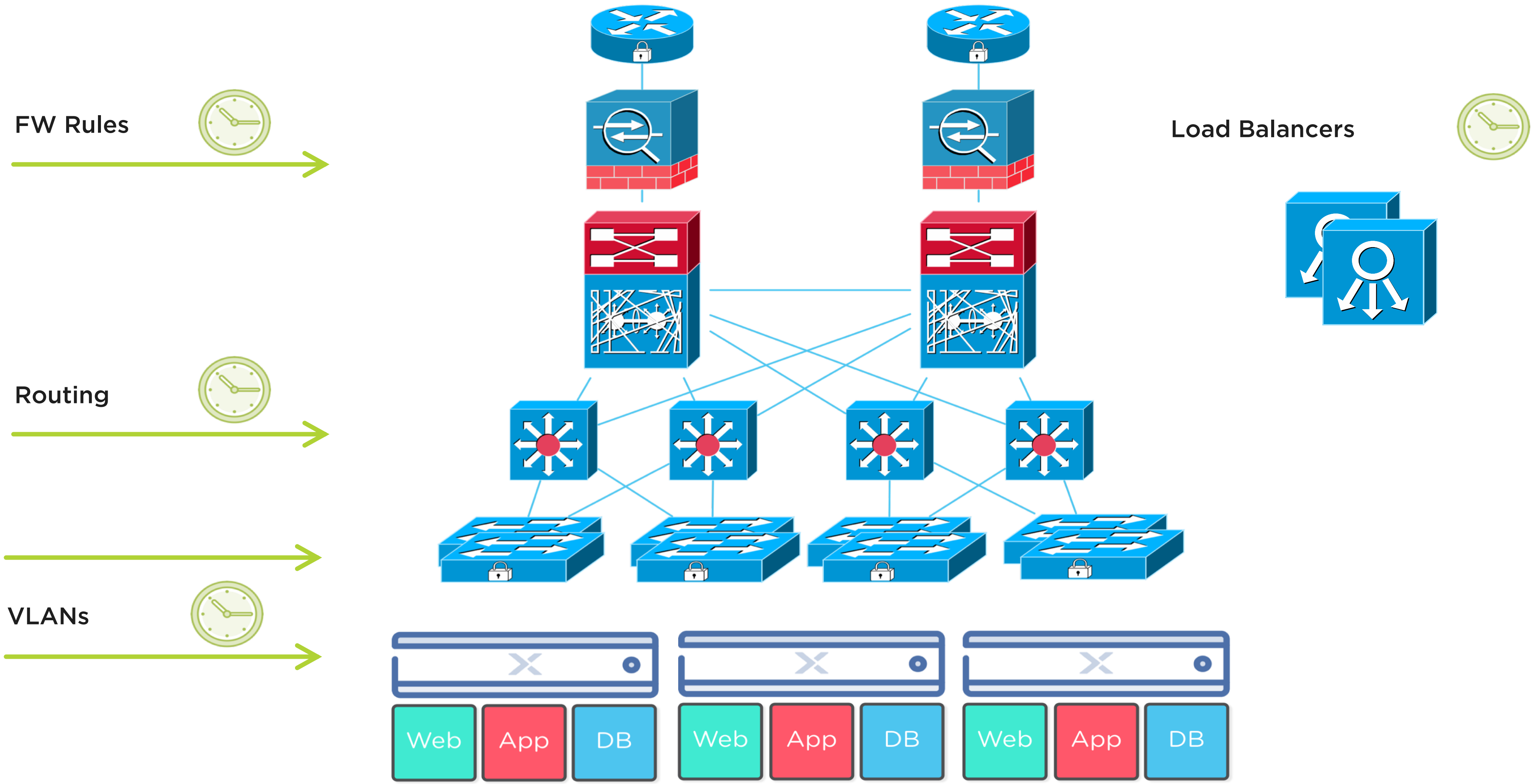


Security Ecosystem



Making complicated simple

The problems with Networking



FW Rules

Routing

VLANs

Load Balancers

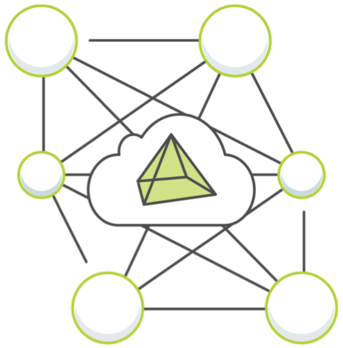
Web App DB

Web App DB

Web App DB

Application Centric Networking

VISUALIZE



- Visualize your application topology
- Analyze your application flows

AUTOMATE

- One-click connectivity for your applications
- Automate Firewall and load balancing policies

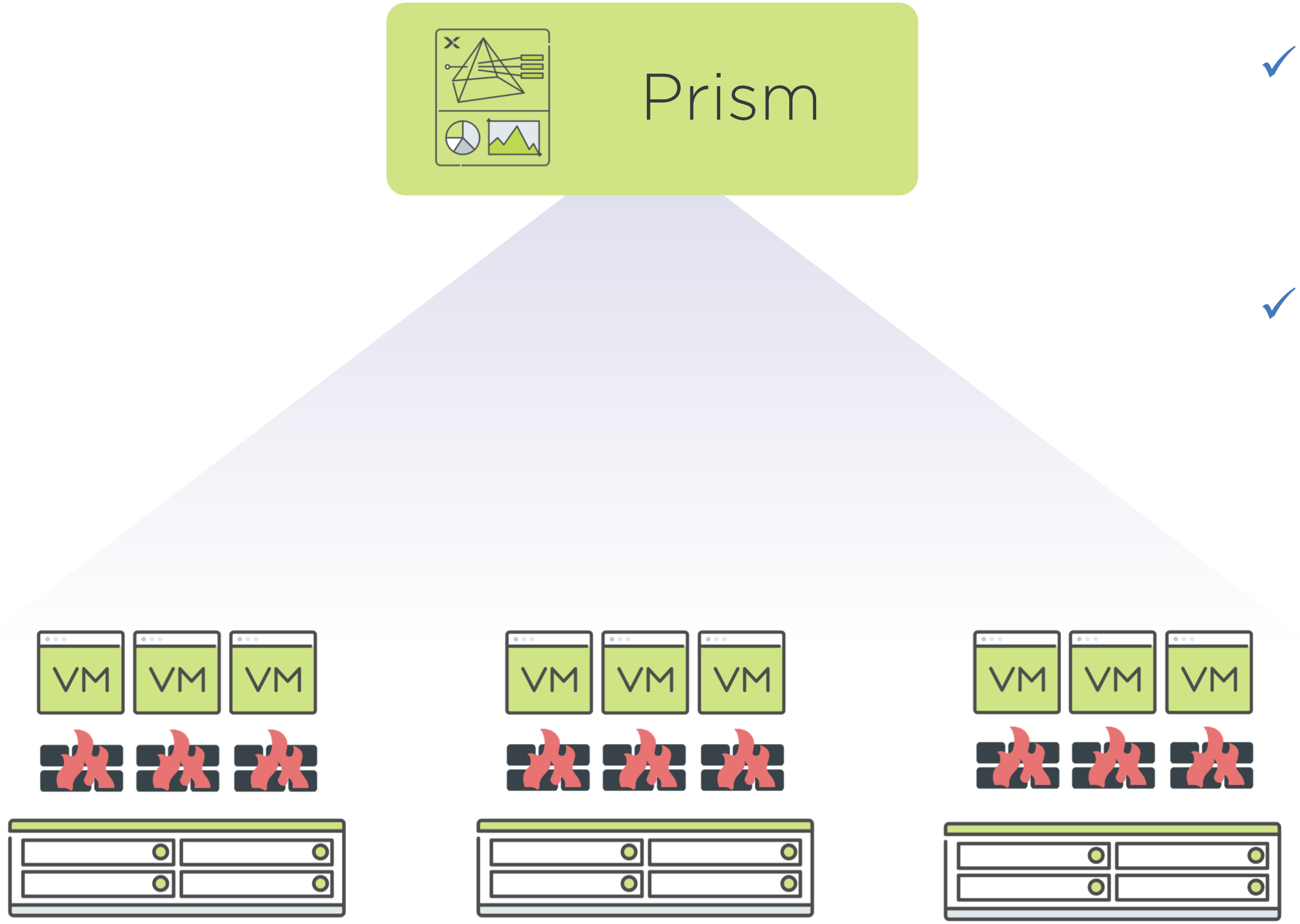
SECURE

- Maintain fine-grained control of your application flows
- Protect against threats that originate from the inside

Something different

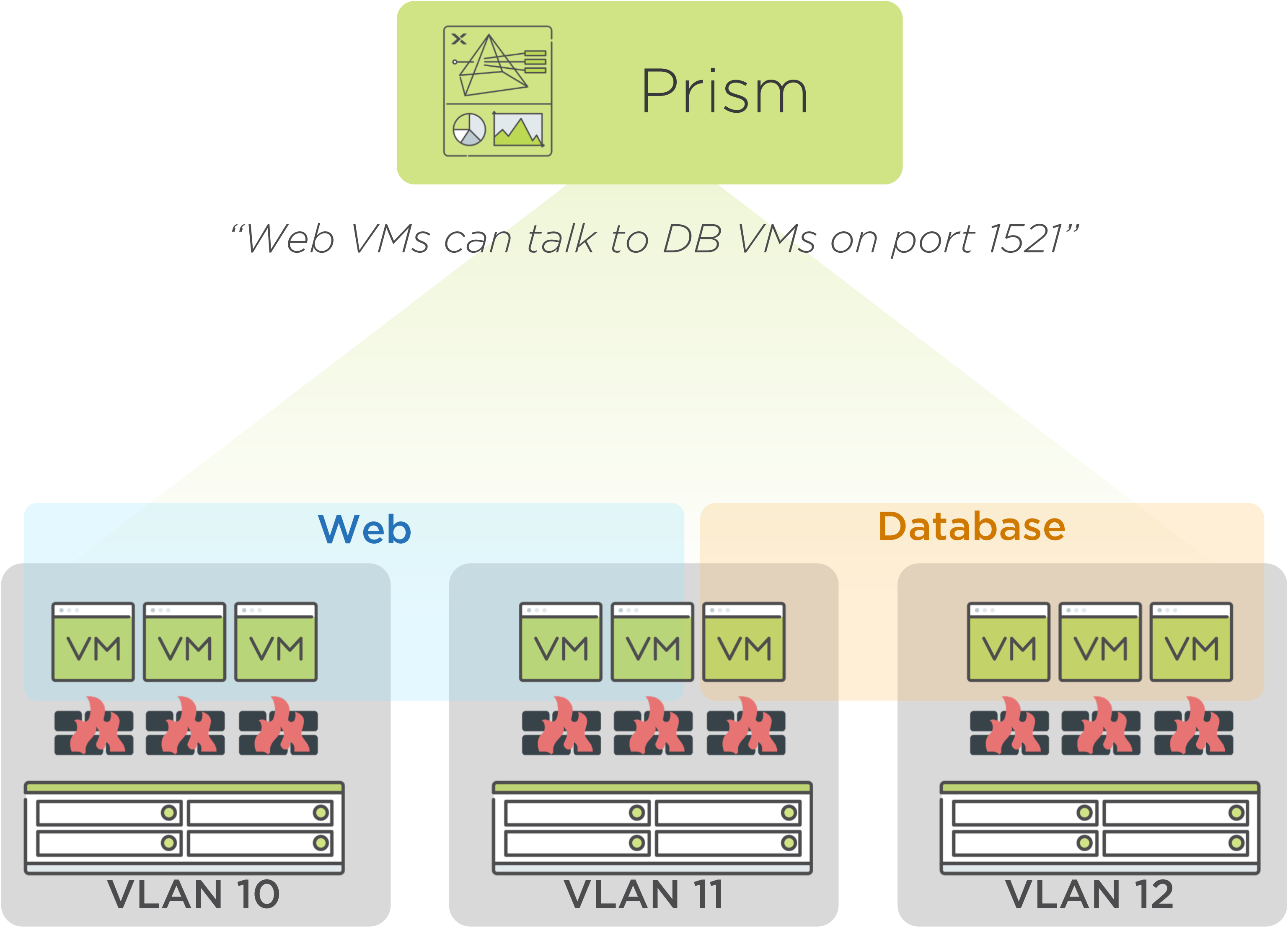
Currently	What is Needed
Perimeter based approach	Security enforcement everywhere
Static, manual security policy	Automated and centralized policies
Network-based segmentation, decoupled from applications	App-based segmentation, decoupled from network
Poor application visibility	Real-time visibility into workload interactions

Centralized Policy with Ubiquitous Enforcement



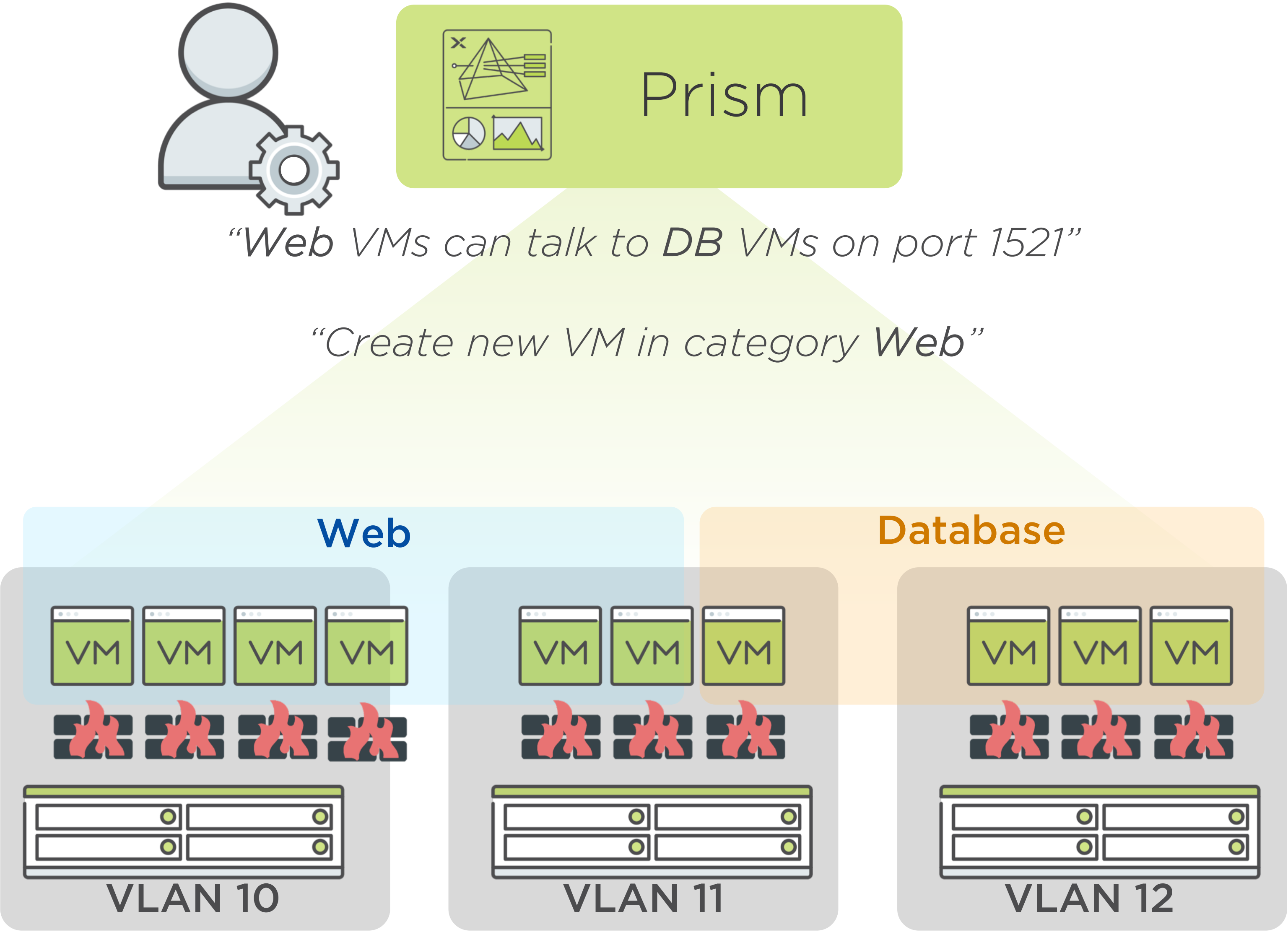
- ✓ One single point of control for all east-west communication
- ✓ Stateful distributed firewall protects every single VM

App-Centric policy decoupled from NT



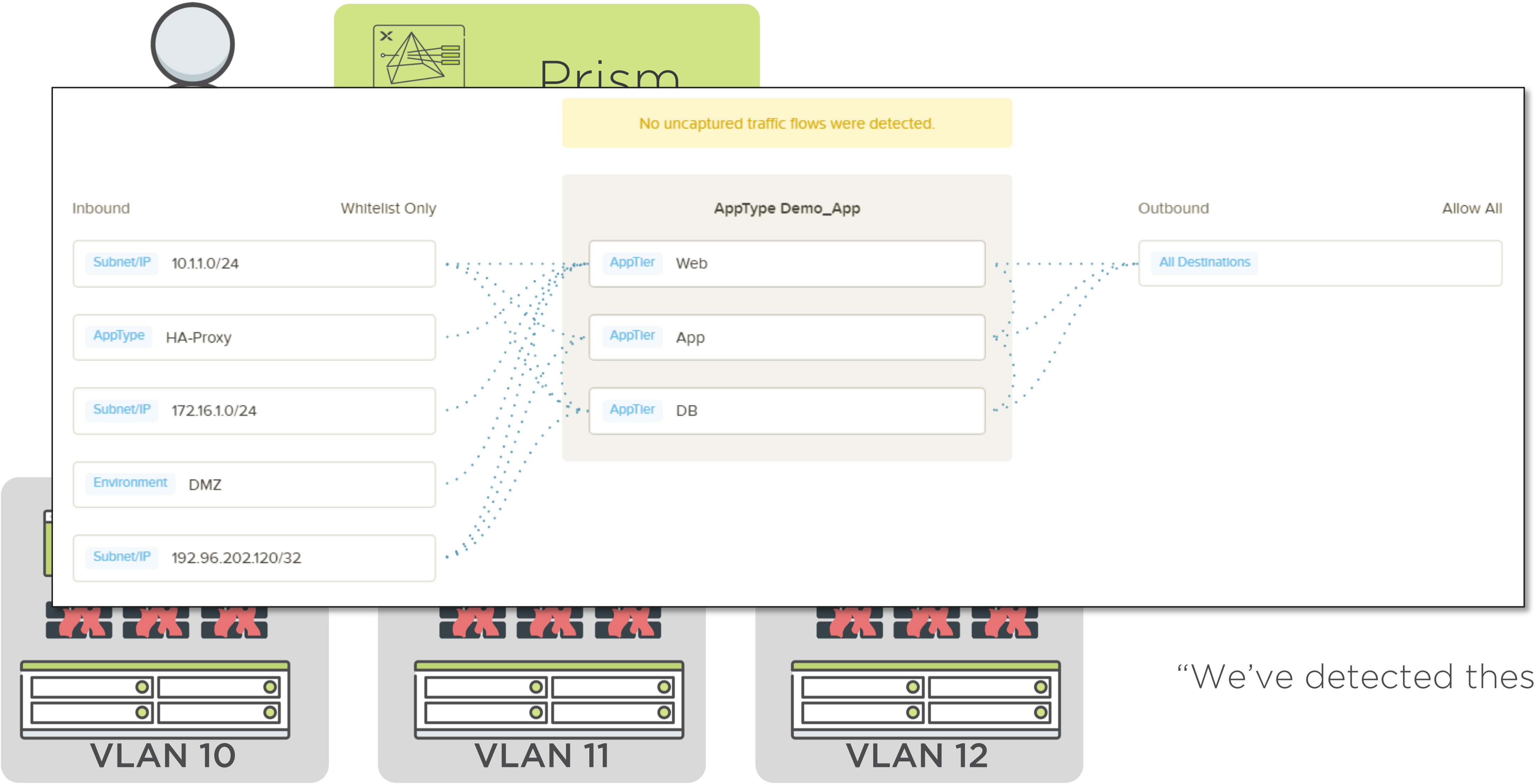
- ✓ Simple and intuitive policy model meant for virtualization teams
- ✓ Networking complexities (VLANs, subnets, routes) removed from policy language
- ✓ Enforcement follows VM lifecycle and is independent of network topology

Auto Updates for Simplified Change Management


Prism
"*Web* VMs can talk to *DB* VMs on port 1521"
"Create new VM in category *Web*"
Web
Database
VM
VM
VM
VM
VM
VM
VM
VM
VM
VM
VLAN 10
VLAN 11
VLAN 12

- ✓ Policies specified on logical groups
- ✓ Security rules are updated real time based on group membership changes
- ✓ Adaptive security enforcement auto-detects IP address changes and updates rules

Rich Flow Visualization to Aid in Policy Authoring



No uncaptured traffic flows were detected.

Inbound Whitelist Only

- Subnet/IP 10.1.1.0/24
- AppType HA-Proxy
- Subnet/IP 172.16.1.0/24
- Environment DMZ
- Subnet/IP 192.96.202.120/32

AppType Demo_App

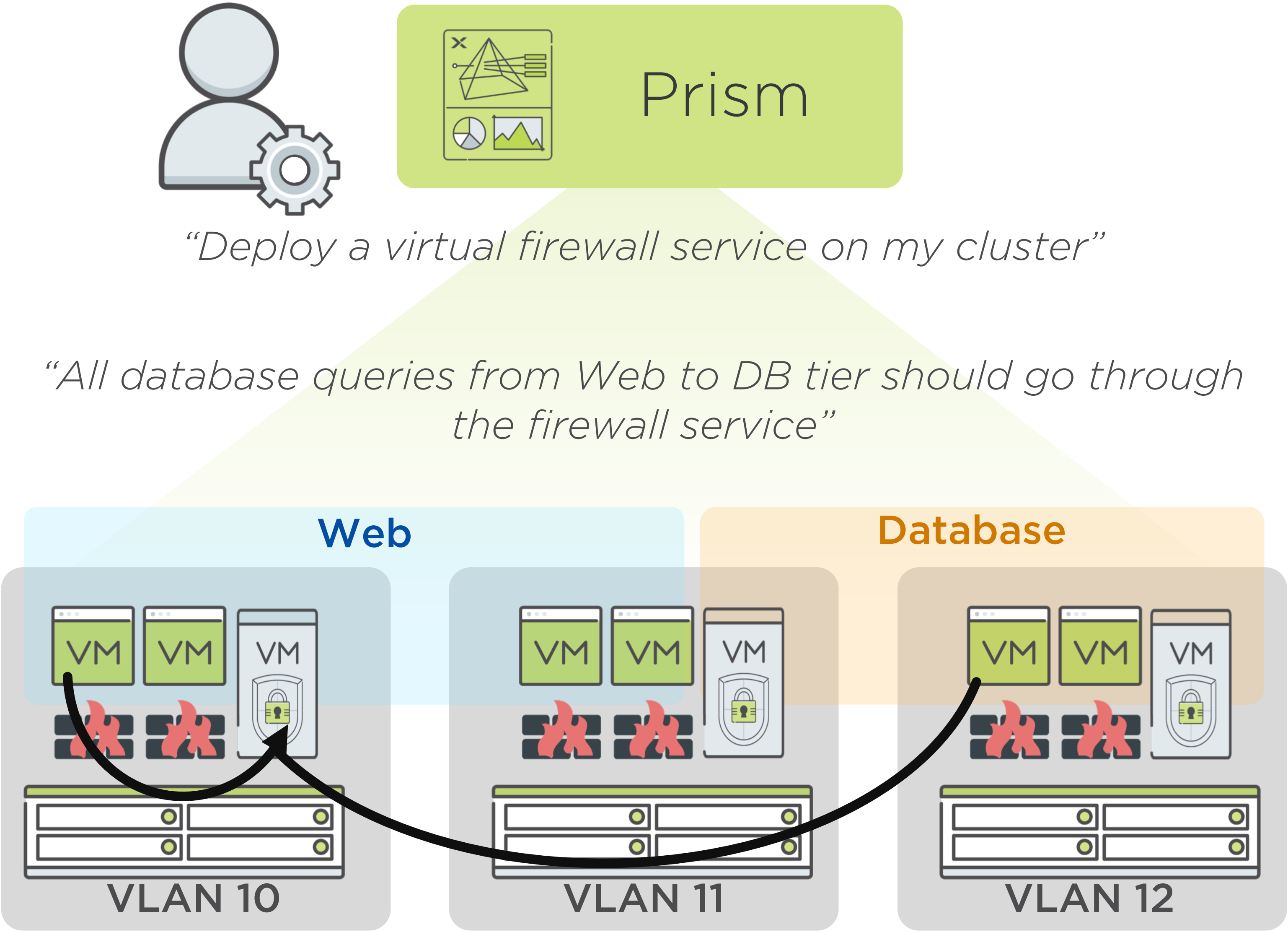
- AppTier Web
- AppTier App
- AppTier DB

Outbound Allow All

- All Destinations

“We’ve detected these flows”

Service Chaining / Network Functions


Prism
"Deploy a virtual firewall service on my cluster"
"All database queries from Web to DB tier should go through the firewall service"
Web
Database
VM
VM
VM
VM
VM
VM
VM
VM
VM
VLAN 10
VLAN 11
VLAN 12

- ✓ Cluster wide deployment of service chains
- ✓ A single service chain can consist of 1 or more sequence of services
- ✓ User can selectively redirect specific flows to a service chain for advanced processing

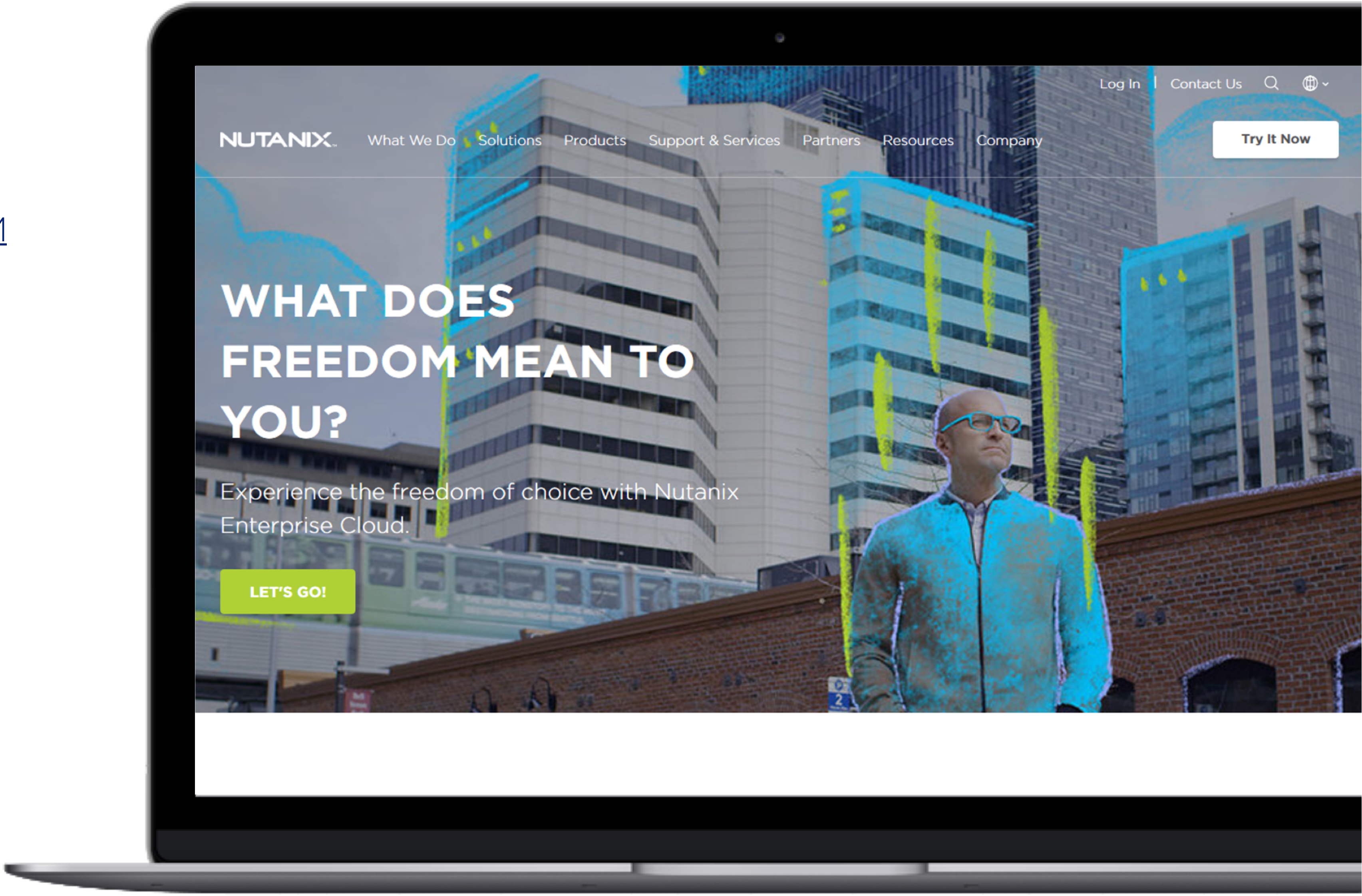
Demo

Get in touch

NEIL.ASHWORTH@NUTANIX.COM

SECURITY@NUTANIX.COM

HTTPS://WWW.NUTANIX.COM



WHAT DOES FREEDOM MEAN TO YOU?

Experience the freedom of choice with Nutanix Enterprise Cloud.

NUTANIX™

Thank you