Modern Cloud, Modern Threats: Navigating Security Challenges Today

September 2025

Laurent JACQUEMIN

EMEA Field CTO - Enterprise Division

Akamai in Numbers

Unmatched Visibility	We see over 1,056TB of data every day
Global Scale	Over 4200 PoPs in 130+ countries
Security Focused	Recognized leader in cybersecurity
Trusted Partner	Supporting leading brands for over 25 years

Akamai : Protection against the broadest of attacks

Solutions	Zero Trust Security				Application & API Security			Infrastructure Security
	Ransomware	Supply Chain Attacks	Malicious Employee Behavior	Malware, Infection & Spread	API Abuse & Attacks	App Exploits & Abuse	Business Logic Abuse	DDoS & DNS Attacks
	Microsegmentation				App & API Protector			Prolexic
			Enterprise Application Access (EAA)		API Security	Malware Protection	API Security	Network Cloud Firewall
				Secure Internet Access (SIA)		Client-Side Protection and Compliance		Akamai DNS
						Brand Protector		
						Bot Manager		
						Content Protector	Account Protector	
						Prolexic		

Most Common Cybersecurity Challenges

Technical

Data breach

Legacy systems

API Security

IoT Security

DDOS Attacks

App Dependency

Regulatory Compliance

APTs

Cloud Security

Shadow IT

Ransomware

Inadequate Incident Response

Supply Chain Attacks

Zero-day vulnerabilities

Business

Audits

Data Privacy

Third-party risks

Risk management

Demonstrating ROI

Talent shortage

Budget constraints

Cost of breach

Brand reputation

Business Continuity

Regulatory Compliance

Weak authentication

Aligning security with business goals

Cloud Challenges

Identity & Access risks

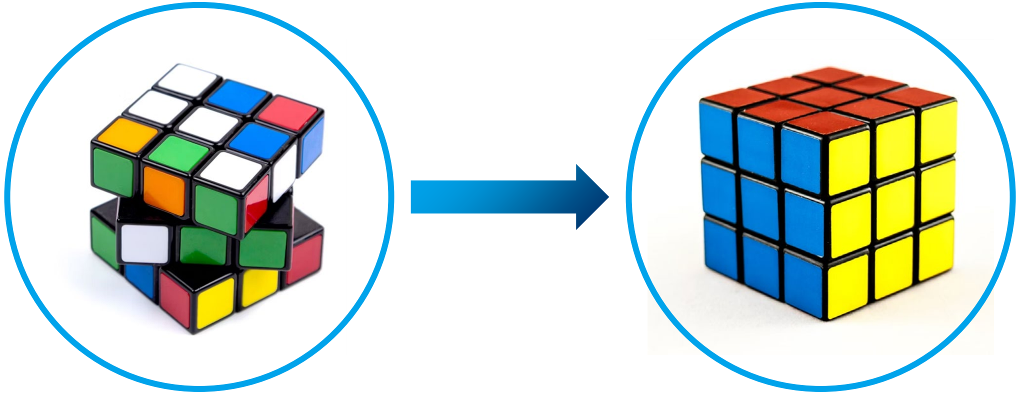
Misconfiguration & poor governance

Supply chain & service exploits

Modern Attacks techniques

Emerging Threats

Security that adapts, protects, and persists



Today's Reality

Flat networks (VPCs)

Security groups (NSGs/ASGs)

Fragmented visibility (Clouds/OnPrem/K8s/PaaS..)

Ideal State:

Segmented

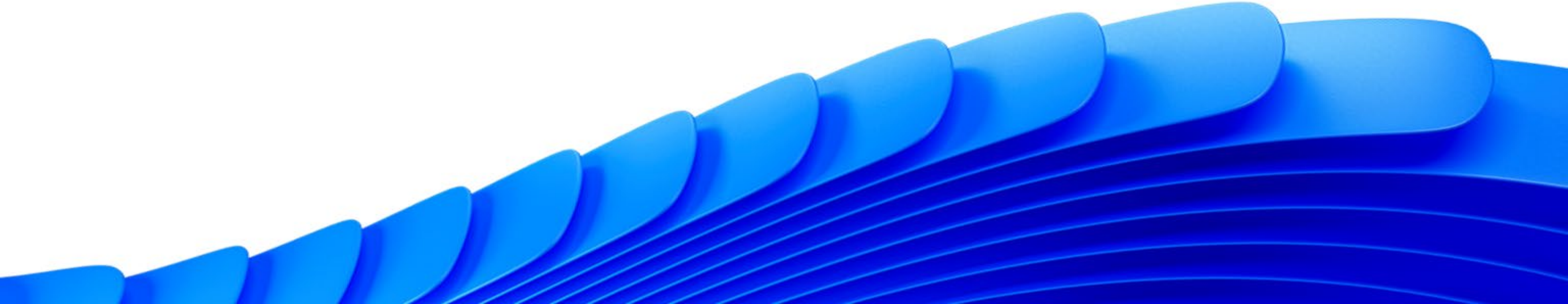
Smart controls

Secured automatically

Akamai

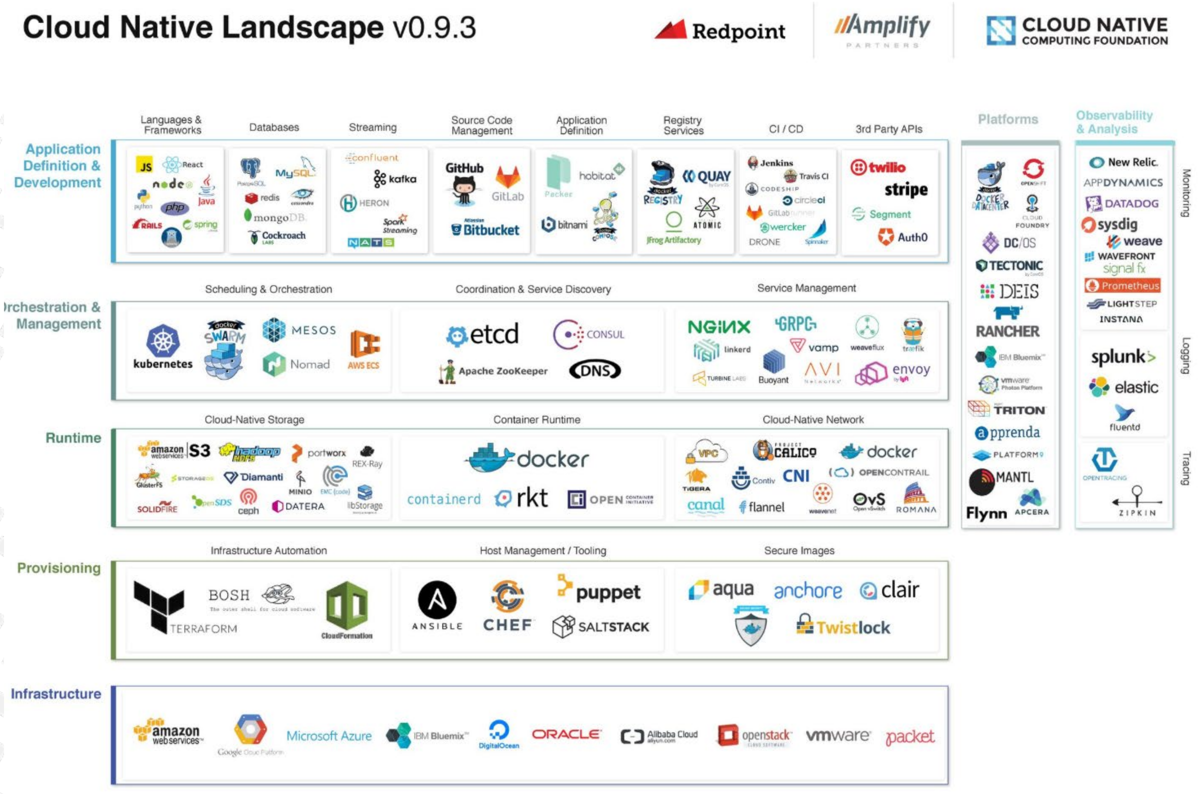
Clouds:

Simplicity or Complexity?

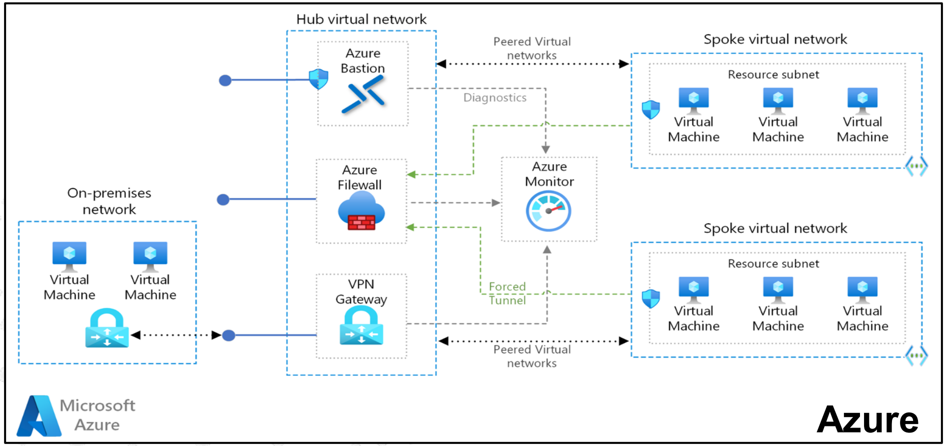


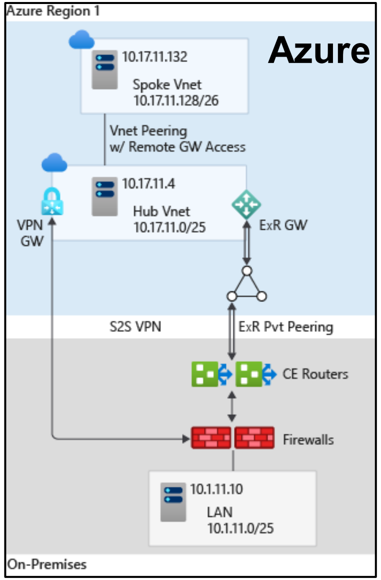
Clouds introduce a wide landscape

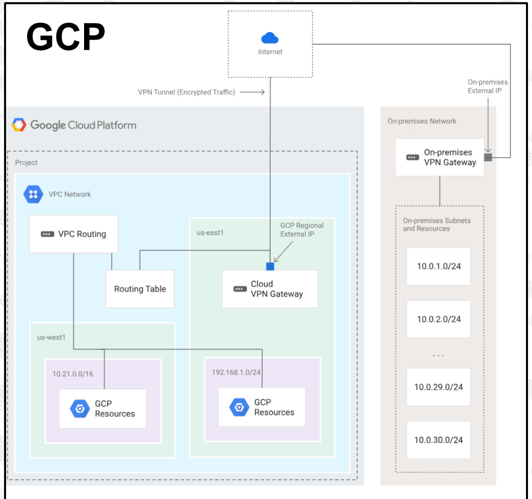
https://landscape.cncf.io/

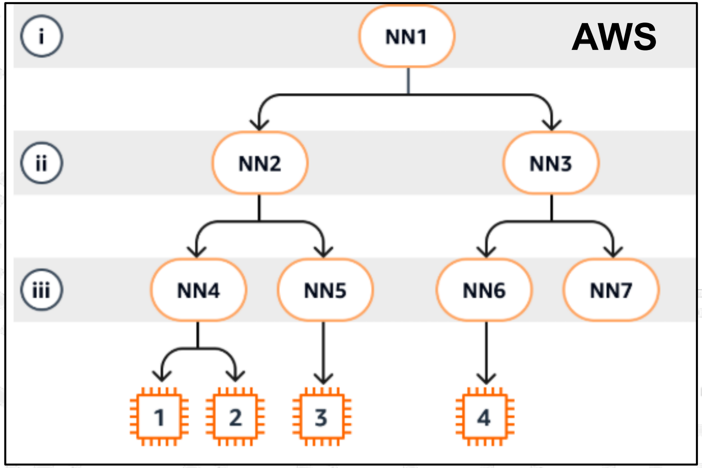


Traditional cloud networking topology

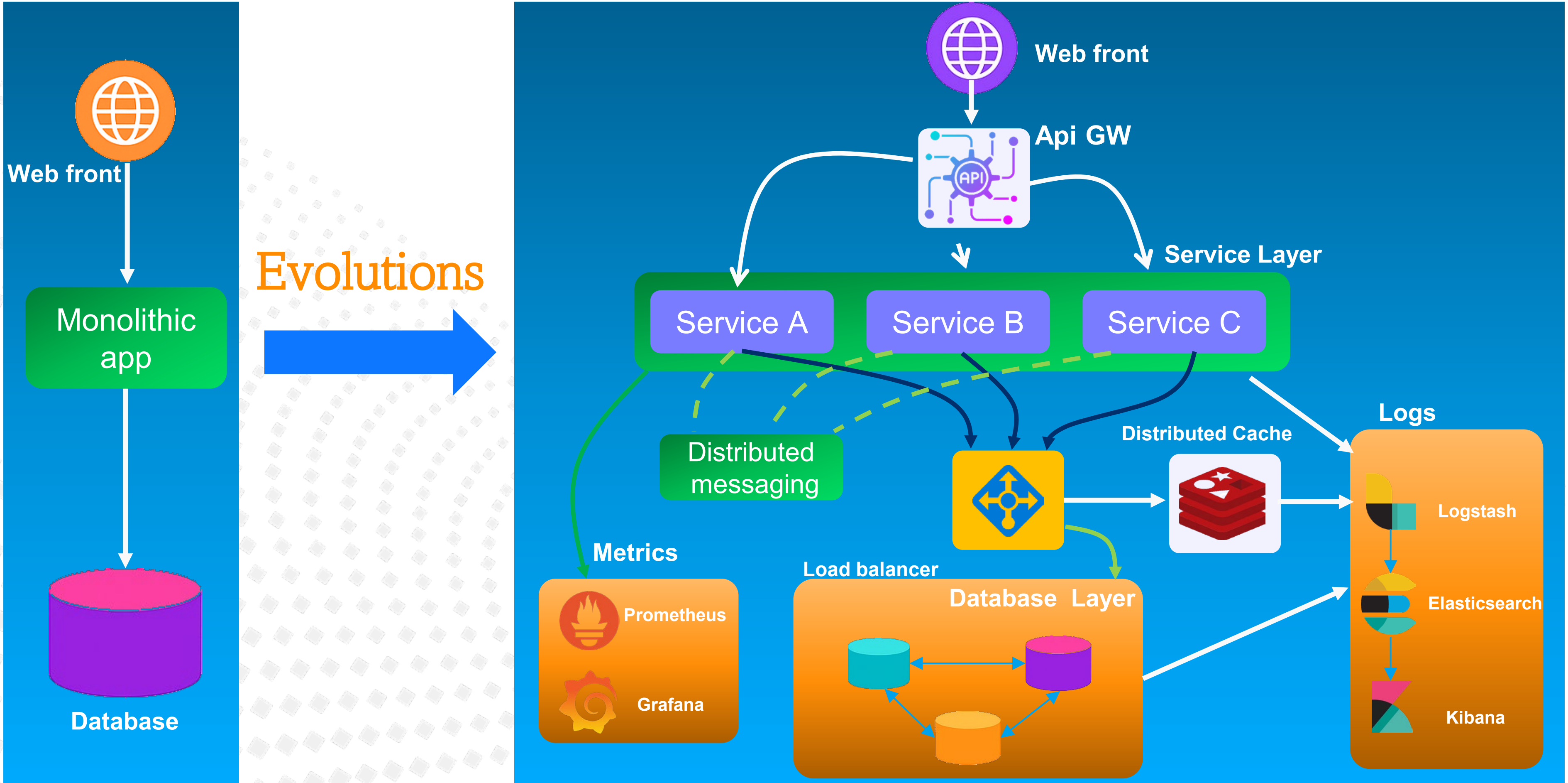








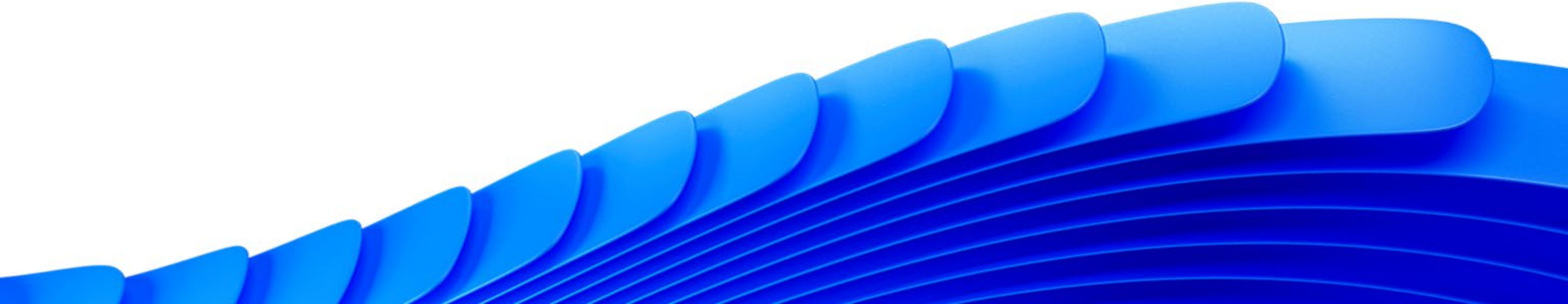
How modern applications are built?



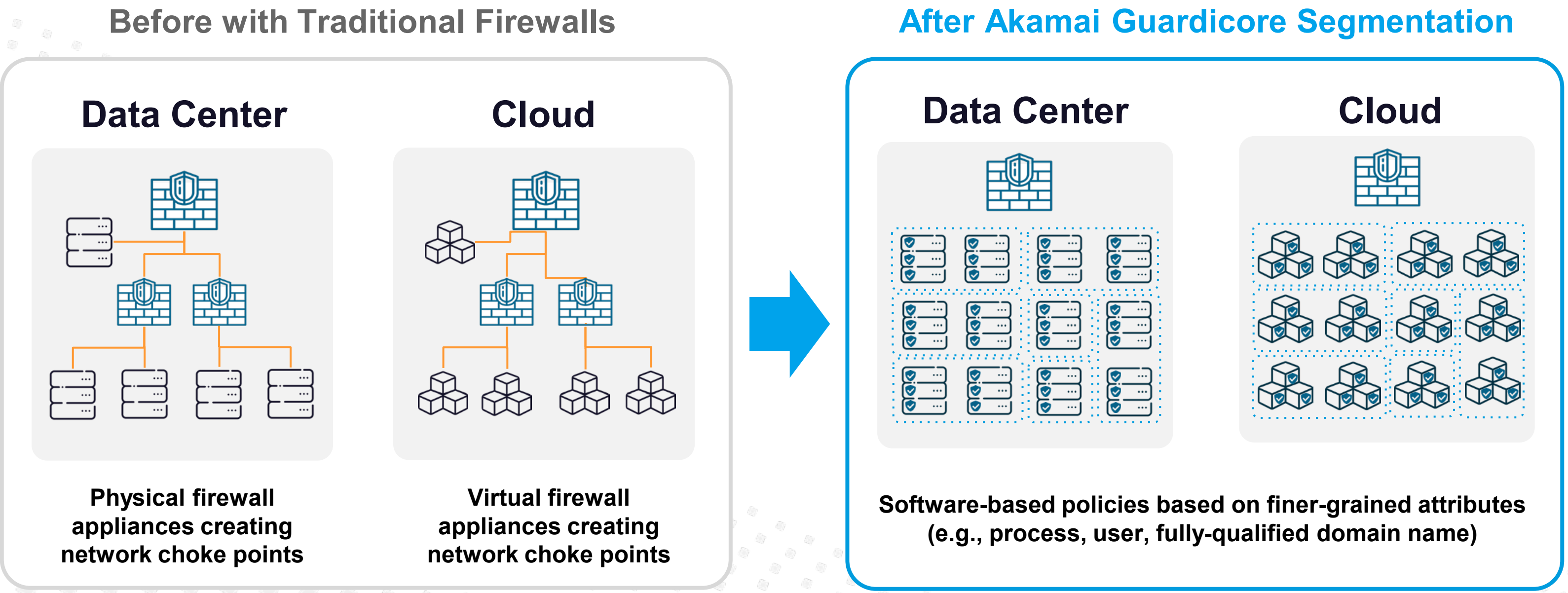
Akamai

Our Solution:

Akamai Guardicore Segmentation



What is microsegmentation and why does it matter?



Before with Traditional Firewalls

Data Center

Physical firewall appliances creating network choke points

Cloud

Virtual firewall appliances creating network choke points

After Akamai Guardicore Segmentation

Data Center

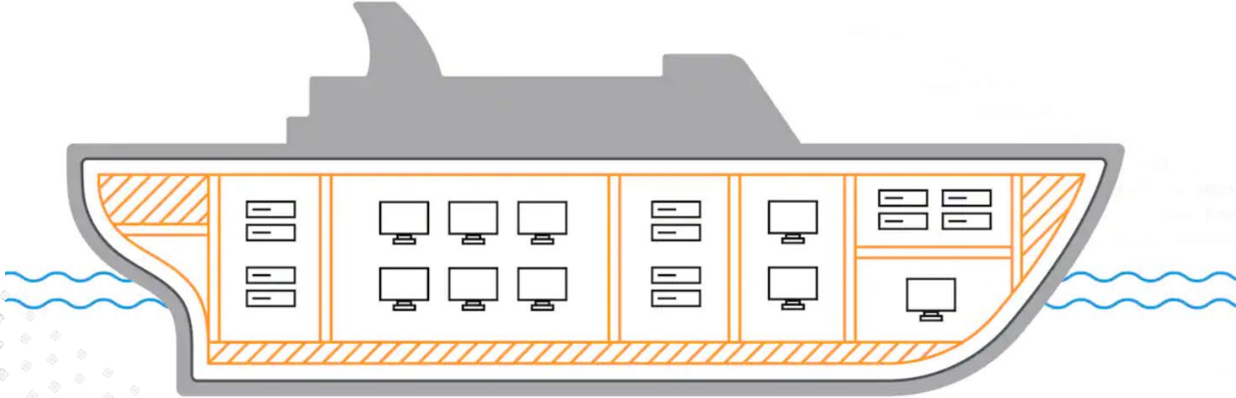
Cloud

Software-based policies based on finer-grained attributes (e.g., process, user, fully-qualified domain name)

It doesn't replace your firewalls — it closes the gaps between them.

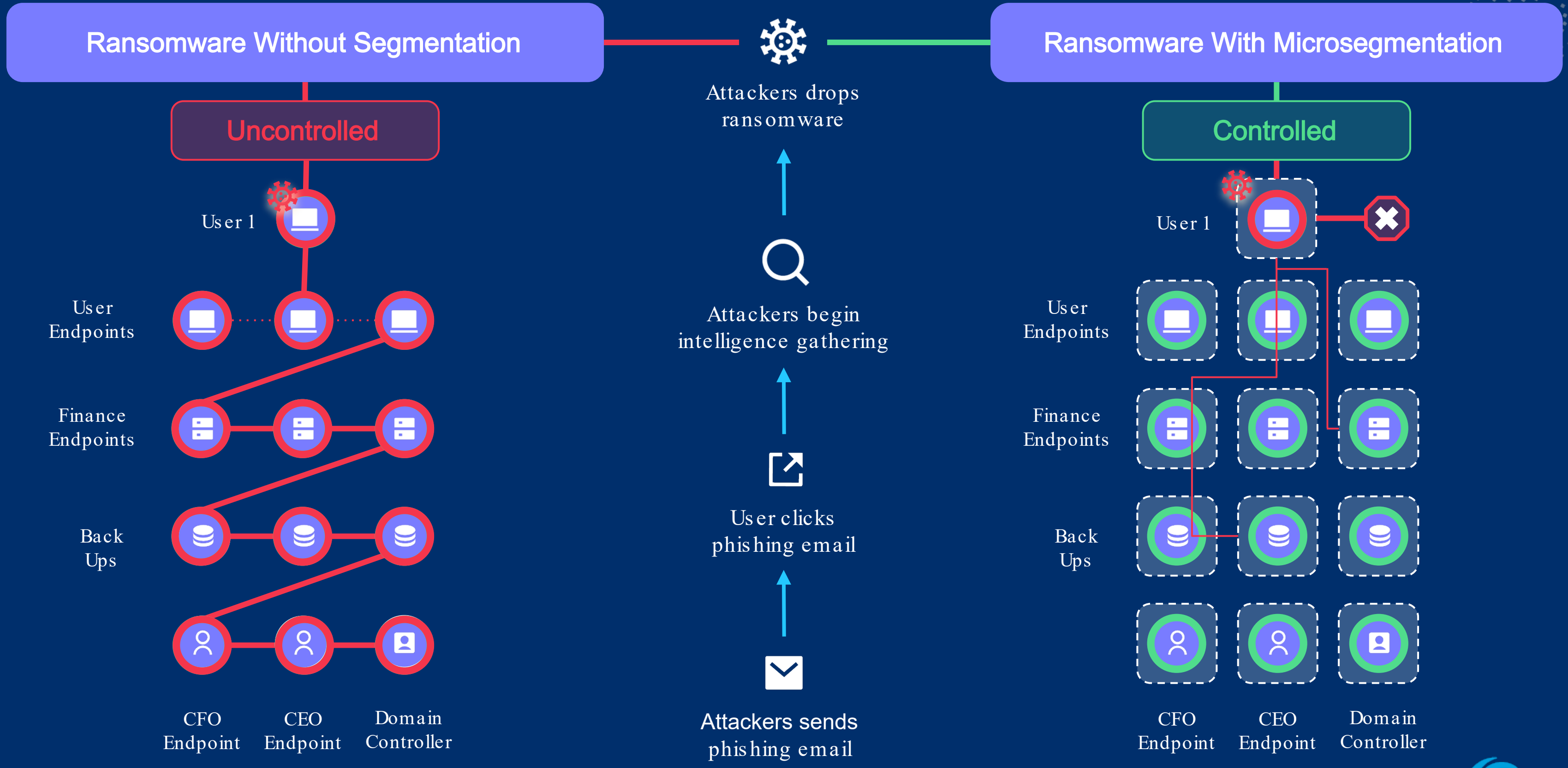
What is microsegmentation and why does it matter?

***Microsegmentation** is the practice of creating fine-grained security policies that control how individual workloads, applications, and devices communicate – regardless of their location of underlying infrastructure.*



It doesn’t replace your firewalls — it closes the gaps between them.

Microsegmentation: Controlling Lateral Movement



Ransomware Without Segmentation

Uncontrolled

Attackers drops ransomware

Attackers begin intelligence gathering

User clicks phishing email

Attackers sends phishing email

Ransomware With Microsegmentation

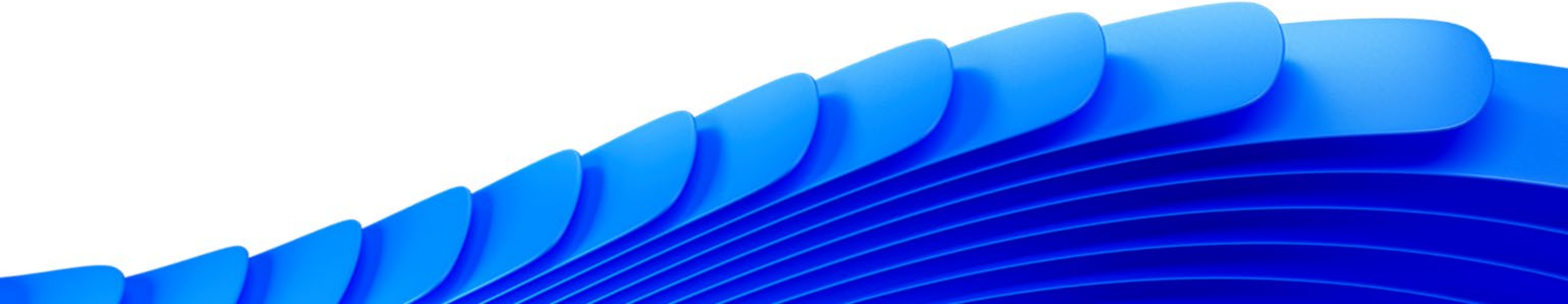
Controlled

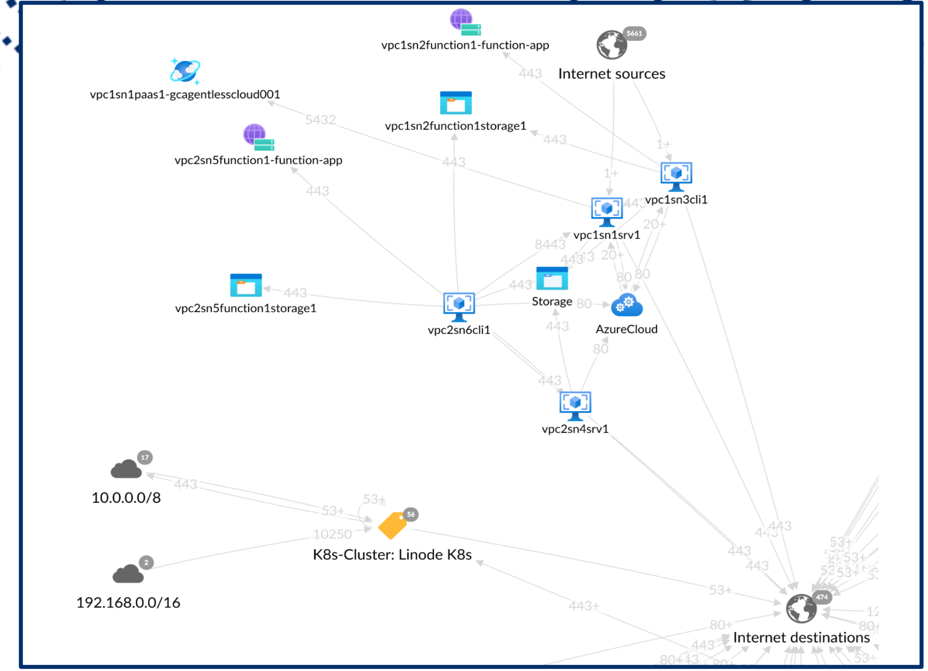
Benefits if Software-Based Approach vs Infrastructure Approach

- No infrastrcuture changes required and no application downtime.
- Faster Time-to-value
- Less resources required to deploy and manage
- Significantly lower costs
- Process-Level visibility and enforcement
- Infrastructure Agnostic and Broad OS Coverage

vmware
ubuntu
Google Cloud
Core OS
IBM
AIX
RED HAT OPENSHIFT
Azure
docker
amazon web services
debian
kubernetes
SUSE
ORACLE Cloud
redhat LINUX
Akamai

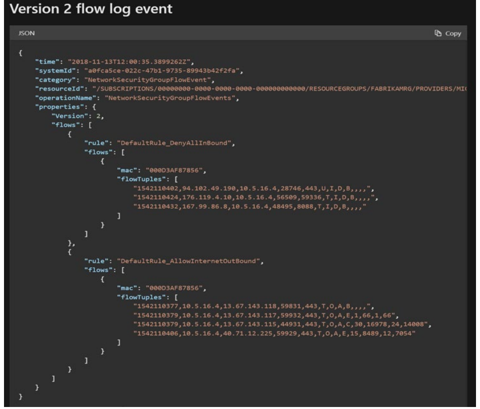
Security steps





Discover all connections

No matter where the assets seat and the type of assets

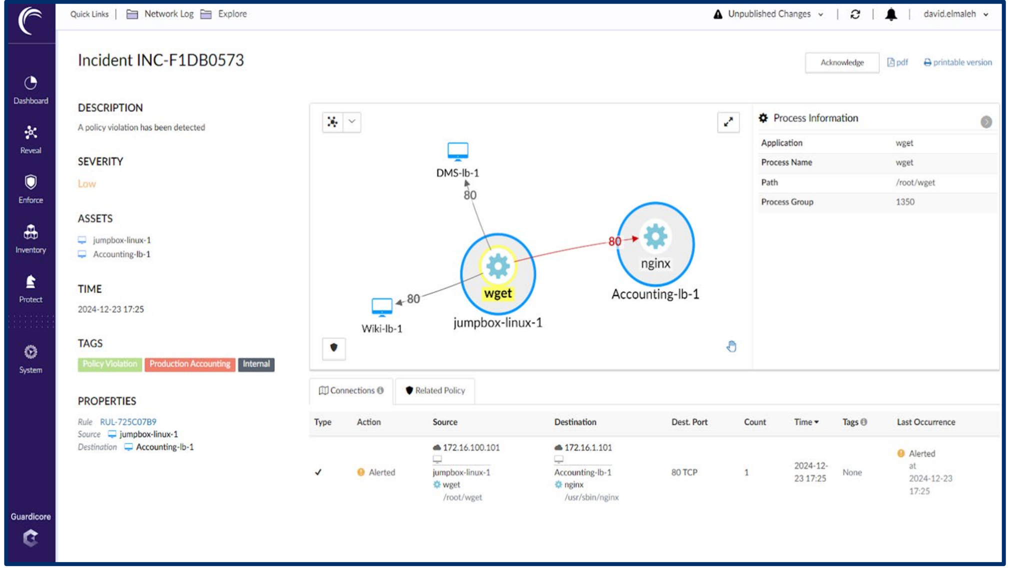


Version 2 flow log event

```
{
    "time": "2018-11-13T12:00:35.3899262Z",
    "systemId": "a0fca5ce-022c-47b1-9735-89943b42f2fa",
    "category": "NetworkSecurityGroupFlowEvent",
    "resourceId": "/SUBSCRIPTIONS/00000000-0000-0000-0000-000000000000/RESOURCEGROUPS/FABRIKAMRG/PROVIDERS/MI
    "operationName": "NetworkSecurityGroupFlowEvents",
    "properties": {
        "Version": 2,
        "flows": [
            {
                "rule": "DefaultRule_DenyAllInBound",
                "flows": [
                    {
                        "mac": "000D3AF87856",
                        "flowTuples": [
                            "1542110402,94.102.49.190,10.5.16.4,28746,443,U,I,D,B,,,,",
                            "1542110424,176.119.4.10,10.5.16.4,56509,59336,T,I,D,B,,,,",
                            "1542110432,167.99.86.8,10.5.16.4,48495,8088,T,I,D,B,,,,"
                        ]
                    }
                ]
            },
            {
                "rule": "DefaultRule_AllowInternetOutBound",
                "flows": [
                    {
                        "mac": "000D3AF87856",
                        "flowTuples": [
                            "1542110377,10.5.16.4,13.67.143.118,59831,443,T,O,A,B,,,,",
                            "1542110379,10.5.16.4,13.67.143.117,59932,443,T,O,A,E,1,66,1,66",
                            "1542110379,10.5.16.4,13.67.143.115,44931,443,T,O,A,C,30,16978,24,14008",
                            "1542110406,10.5.16.4,40.71.12.225,59929,443,T,O,A,E,15,8489,12,7054"
                        ]
                    }
                ]
            }
        ]
    }
}
```

Discovering

Analysing



Incident INC-F1DB0573

DESCRIPTION

A policy violation has been detected

SEVERITY

Low

ASSETS

- jumpbox-linux-1
- Accounting-lb-1

TIME

2024-12-23 17:25

TAGS

Policy Violation | Production Accounting | Internal

PROPERTIES

Rule RUL-725C07B9
Source jumpbox-linux-1
Destination Accounting-lb-1

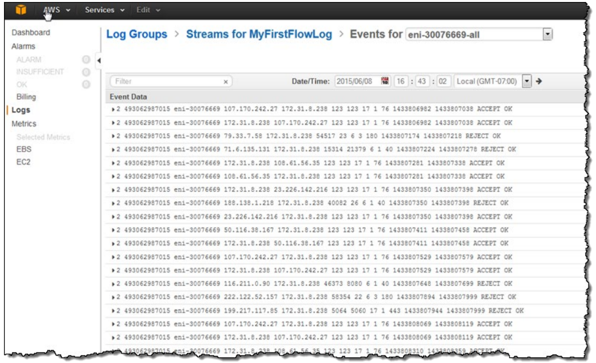
Process Information

Application	wget
Process Name	wget
Path	/root/wget
Process Group	1350

Type	Action	Source	Destination	Dest. Port	Count	Time ▾	Tags	Last Occurrence
✓	Alerted	172.16.100.101 jumpbox-linux-1 wget /root/wget	172.16.1.101 Accounting-lb-1 nginx /usr/sbin/nginx	80 TCP	1	2024-12-23 17:25	None	Alerted at 2024-12-23 17:25

Analyze all the connections between assets.

No matter where the assets seat and the type of assets



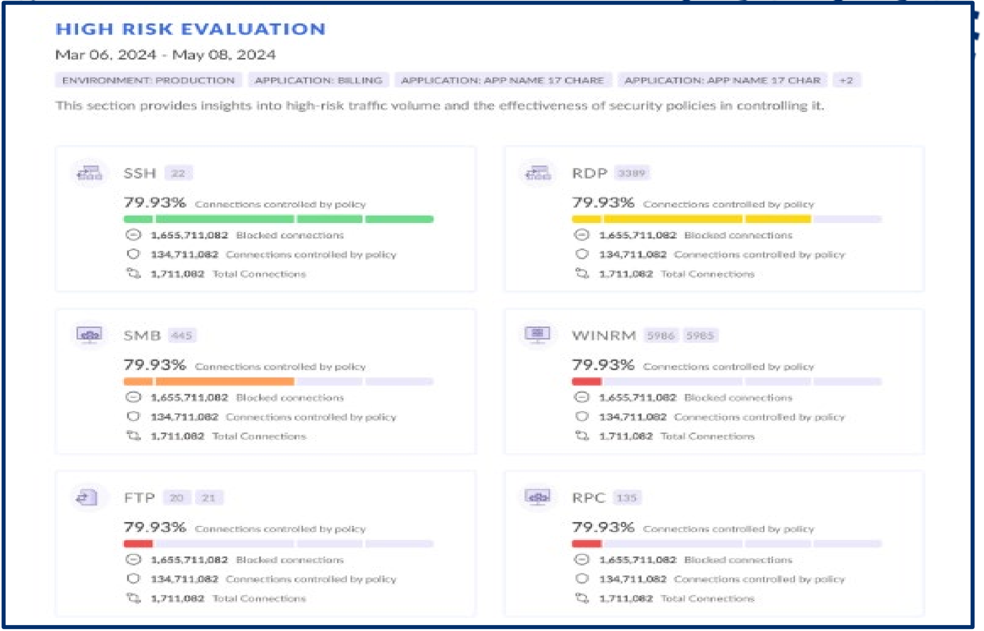
Log Groups > Streams for MyFirstFlowLog > Events for eni-30076669-all

Filter

Date/Time: 2015/06/08 16 : 43 : 02 Local (GMT-07:00)

Event Data

```
2 493062987015 eni-30076669 107.170.242.27 172.31.8.238 123 123 17 1 76 1433806982 1433807038 ACCEPT OK
2 493062987015 eni-30076669 172.31.8.238 107.170.242.27 123 123 17 1 76 1433806982 1433807038 ACCEPT OK
2 493062987015 eni-30076669 79.33.7.58 172.31.8.238 54517 23 6 3 180 1433807174 1433807218 REJECT OK
2 493062987015 eni-30076669 71.6.135.131 172.31.8.238 15314 21379 6 1 40 1433807224 1433807278 REJECT OK
2 493062987015 eni-30076669 172.31.8.238 108.61.56.35 123 123 17 1 76 1433807281 1433807338 ACCEPT OK
2 493062987015 eni-30076669 108.61.56.35 172.31.8.238 123 123 17 1 76 1433807281 1433807338 ACCEPT OK
2 493062987015 eni-30076669 172.31.8.238 23.226.142.216 123 123 17 1 76 1433807350 1433807398 ACCEPT OK
2 493062987015 eni-30076669 188.138.1.218 172.31.8.238 40082 26 6 1 40 1433807350 1433807398 REJECT OK
2 493062987015 eni-30076669 23.226.142.216 172.31.8.238 123 123 17 1 76 1433807350 1433807398 ACCEPT OK
2 493062987015 eni-30076669 50.116.38.167 172.31.8.238 123 123 17 1 76 1433807411 1433807458 ACCEPT OK
2 493062987015 eni-30076669 172.31.8.238 50.116.38.167 123 123 17 1 76 1433807411 1433807458 ACCEPT OK
2 493062987015 eni-30076669 107.170.242.27 172.31.8.238 123 123 17 1 76 1433807529 1433807579 ACCEPT OK
2 493062987015 eni-30076669 172.31.8.238 107.170.242.27 123 123 17 1 76 1433807529 1433807579 ACCEPT OK
2 493062987015 eni-30076669 116.211.0.90 172.31.8.238 46373 8080 6 1 40 1433807648 1433807699 REJECT OK
2 493062987015 eni-30076669 222.122.52.157 172.31.8.238 58354 22 6 3 180 1433807894 1433807999 REJECT OK
2 493062987015 eni-30076669 199.217.117.85 172.31.8.238 5064 5060 17 1 443 1433807944 1433807999 REJECT OK
2 493062987015 eni-30076669 107.170.242.27 172.31.8.238 123 123 17 1 76 1433808069 1433808119 ACCEPT OK
2 493062987015 eni-30076669 172.31.8.238 107.170.242.27 123 123 17 1 76 1433808069 1433808119 ACCEPT OK
2 493062987015 eni-30076669 172.31.8.238 108.61.56.35 123 123 17 1 76 1433808310 1433808359 ACCEPT OK
```



HIGH RISK EVALUATION

Mar 06, 2024 - May 08, 2024

ENVIRONMENT: PRODUCTION | APPLICATION: BILLING | APPLICATION: APP NAME 17 CHARE | APPLICATION: APP NAME 17 CHAR | +2

This section provides insights into high-risk traffic volume and the effectiveness of security policies in controlling it.

SSH 22

79.93% Connections controlled by policy

1,655,711,082 Blocked connections

134,711,082 Connections controlled by policy

1,711,082 Total Connections

RDP 3389

79.93% Connections controlled by policy

1,655,711,082 Blocked connections

134,711,082 Connections controlled by policy

1,711,082 Total Connections

SMB 445

79.93% Connections controlled by policy

1,655,711,082 Blocked connections

134,711,082 Connections controlled by policy

1,711,082 Total Connections

WINRM 5986 5985

79.93% Connections controlled by policy

1,655,711,082 Blocked connections

134,711,082 Connections controlled by policy

1,711,082 Total Connections

FTP 20 21

79.93% Connections controlled by policy

1,655,711,082 Blocked connections

134,711,082 Connections controlled by policy

1,711,082 Total Connections

RPC 135

79.93% Connections controlled by policy

1,655,711,082 Blocked connections

134,711,082 Connections controlled by policy

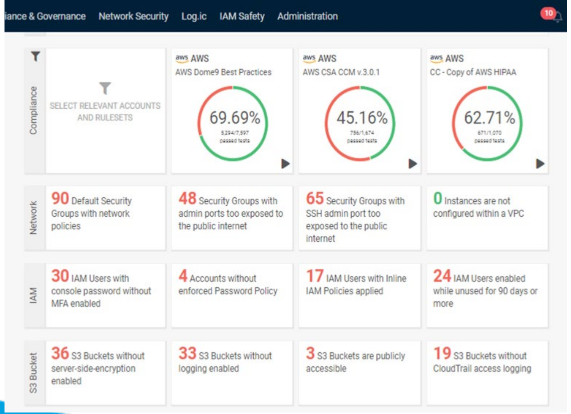
1,711,082 Total Connections

Suggest optimal policies

Create policies easily

Suggesting

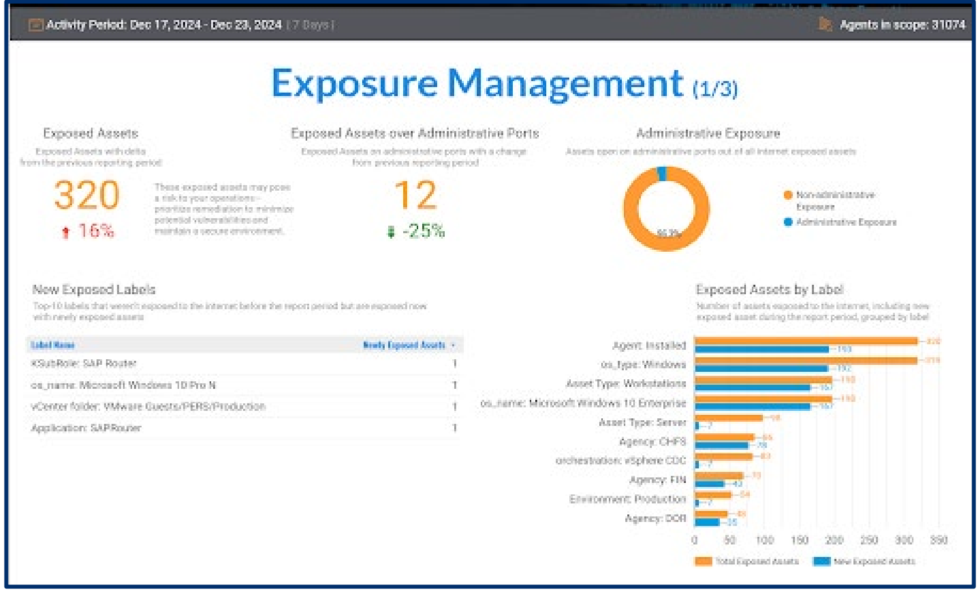
Akamai



SELECT RELEVANT ACCOUNTS AND RULESETS

AWS	AWS	AWS
AWS Dome9 Best Practices	AWS CSA CCM v.3.0.1	CC - Copy of AWS HIPAA
69.69% 5294/7,597 passed tests	45.16% 756/1,674 passed tests	62.71% 671/1,070 passed tests

90 Default Security Groups with network policies	48 Security Groups with admin ports too exposed to the public internet	65 Security Groups with SSH admin port too exposed to the public internet	0 Instances are not configured within a VPC
30 IAM Users with console password without MFA enabled	4 Accounts without enforced Password Policy	17 IAM Users with Inline IAM Policies applied	24 IAM Users enabled while unused for 90 days or more
36 S3 Buckets without server-side-encryption enabled	33 S3 Buckets without logging enabled	3 S3 Buckets are publicly accessible	19 S3 Buckets without CloudTrail access logging



Activity Period: Dec 17, 2024 - Dec 23, 2024 (7 Days) Agents in scope: 31074

Exposure Management (1/3)

Exposed Assets

Exposed Assets with delta from the previous reporting period

320 ↑ 16%

These exposed assets may pose a risk to your operations—prioritize remediation to minimize potential vulnerabilities and maintain a secure environment.

Exposed Assets over Administrative Ports

Exposed Assets on administrative ports with a change from previous reporting period

12 ↓ -25%

Administrative Exposure

Assets open on administrative ports out of all internet exposed assets

New Exposed Labels

Top-10 labels that weren't exposed to the internet before the report period but are exposed now with newly exposed assets

Label Name	Newly Exposed Assets
KSubRole: SAP Router	1
os_name: Microsoft Windows 10 Pro N	1
vCenter folder: VMware Guests/PERS/Production	1
Application: SAPRouter	1

Exposed Assets by Label

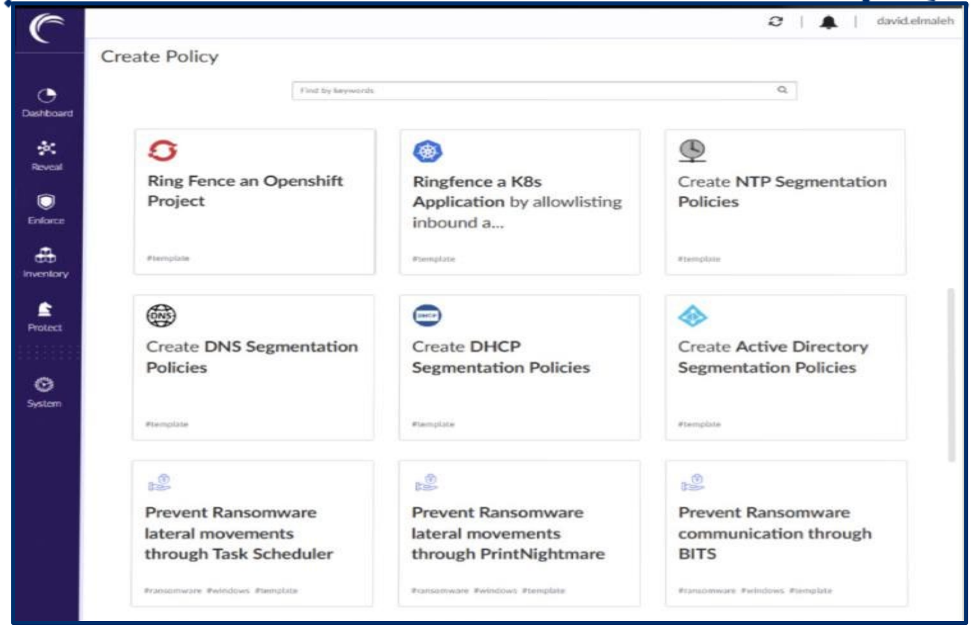
Number of assets exposed to the internet, including new exposed asset during the report period, grouped by label

Limiting

Limit the scope of a Breach

Manage critical exposures first

Deciding



Create Policy

Ring Fence an Openshift Project
#template

Ringfence a K8s Application by allowlisting inbound a...
#template

Create NTP Segmentation Policies
#template

Create DNS Segmentation Policies
#template

Create DHCP Segmentation Policies
#template

Create Active Directory Segmentation Policies
#template

Prevent Ransomware lateral movements through Task Scheduler
#ransomware #windows #template

Prevent Ransomware lateral movements through PrintNightmare
#ransomware #windows #template

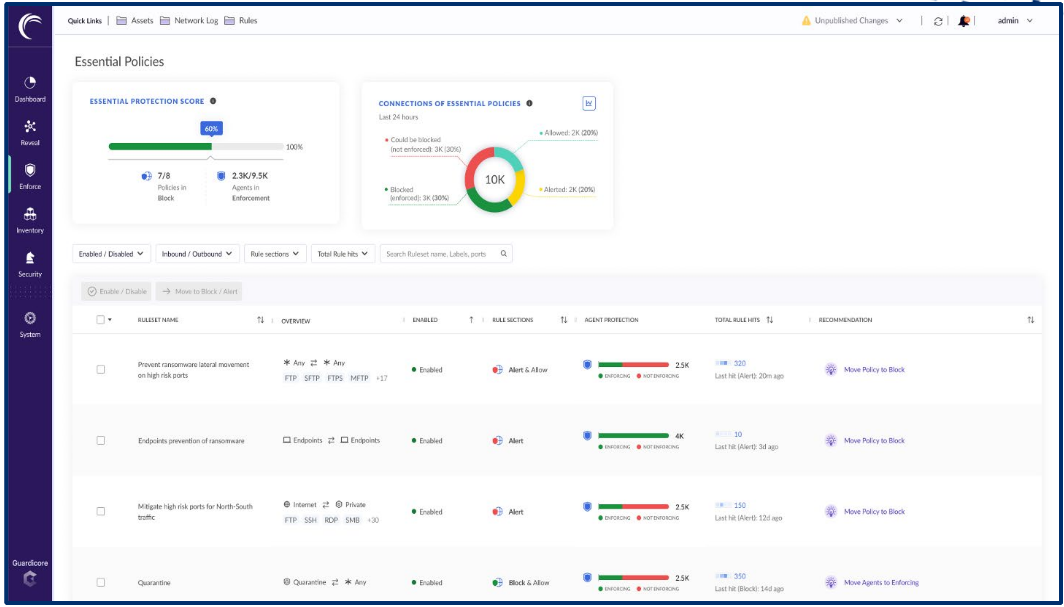
Prevent Ransomware communication through BITS
#ransomware #windows #template

Decide what to block / Allow

Wizard to build policies (Zero Trust template)

Akamai

Increasing



Essential Policies

ESSENTIAL PROTECTION SCORE

60%

100%

7/8 Policies in Block

2.3K/9.5K Agents in Enforcement

CONNECTIONS OF ESSENTIAL POLICIES

Last 24 hours

10K

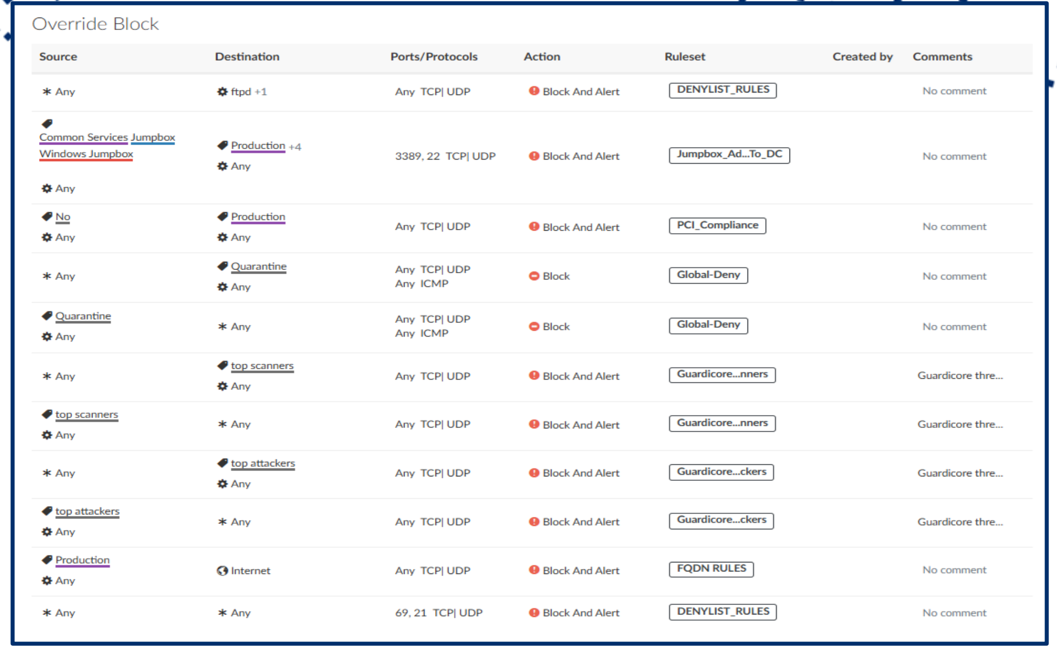
- Could be blocked (not enforced): 3K (30%)
- Allowed: 2K (20%)
- Blocked (enforced): 3K (30%)
- Alerted: 2K (20%)

□	RULESET NAME	OVERVIEW	ENABLED	RULE SECTIONS	AGENT PROTECTION	TOTAL RULE HITS	RECOMMENDATION
□	Prevent ransomware lateral movement on high risk ports	✱ Any ⇄ ✱ Any FTP SFTP FTPS MFTP +17	● Enabled	Alert & Allow	2.5K ● ENFORCING ● NOT ENFORCING	320 Last hit (Alert): 20m ago	Move Policy to Block
□	Endpoints prevention of ransomware	Endpoints ⇄ Endpoints	● Enabled	Alert	4K ● ENFORCING ● NOT ENFORCING	10 Last hit (Alert): 3d ago	Move Policy to Block
□	Mitigate high risk ports for North-South traffic	Internet ⇄ Private FTP SSH RDP SMB +30	● Enabled	Alert	2.5K ● ENFORCING ● NOT ENFORCING	150 Last hit (Alert): 12d ago	Move Policy to Block
□	Quarantine	Quarantine ⇄ ✱ Any	● Enabled	Block & Allow	2.5K ● ENFORCING ● NOT ENFORCING	350 Last hit (Block): 14d ago	Move Agents to Enforcing

Inscrease security posture

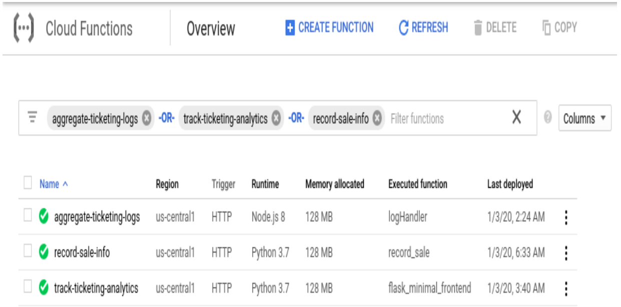
Apply suggestions to improve security

Akamai



Override Block

Source	Destination	Ports/Protocols	Action	Ruleset	Created by	Comments
✱ Any	⚙ ftpd +1	Any TCP| UDP	Block And Alert	DENYLIST_RULES		No comment
Common Services Jumpbox Windows Jumpbox ⚙ Any	Production +4 ⚙ Any	3389, 22 TCP| UDP	Block And Alert	Jumpbox_Ad...To_DC		No comment
No ⚙ Any	Production ⚙ Any	Any TCP| UDP	Block And Alert	PCI_Compliance		No comment
✱ Any	Quarantine ⚙ Any	Any TCP| UDP Any ICMP	Block	Global-Deny		No comment
Quarantine ⚙ Any	✱ Any	Any TCP| UDP Any ICMP	Block	Global-Deny		No comment
✱ Any	top scanners ⚙ Any	Any TCP| UDP	Block And Alert	Guardicore...nners		Guardicore thre...
top scanners ⚙ Any	✱ Any	Any TCP| UDP	Block And Alert	Guardicore...nners		Guardicore thre...
✱ Any	top attackers ⚙ Any	Any TCP| UDP	Block And Alert	Guardicore...ckers		Guardicore thre...
top attackers ⚙ Any	✱ Any	Any TCP| UDP	Block And Alert	Guardicore...ckers		Guardicore thre...
Production ⚙ Any	Internet	Any TCP| UDP	Block And Alert	FQDN RULES		No comment
✱ Any	✱ Any	69, 21 TCP| UDP	Block And Alert	DENYLIST_RULES		No comment



Name	Region	Trigger	Runtime	Memory allocated	Executed function	Last deployed
aggregate-ticketing-logs	us-central1	HTTP	Node.js 8	128 MB	logHandler	1/3/20, 2:24 AM
record-sale-info	us-central1	HTTP	Python 3.7	128 MB	record_sale	1/3/20, 6:33 AM
track-ticketing-analytics	us-central1	HTTP	Python 3.7	128 MB	flask_minimal_frontend	1/3/20, 3:40 AM

Blocking

Block communications

Based on real trafic, define accurate policies

Akamai

Questions?