



# FortiCNP Cloud Native Protection

Kevin Ng

Cyber Security Architect



# Why Fortinet?





# Who is Fortinet?

For over 20 years, Fortinet's mission has been to secure people, devices, and data everywhere.

We have been a driving force in the evolution of cybersecurity and the convergence of networking and security. Our network security solutions are the most deployed, most patented, and among the most validated in the industry.

## Nasdaq 100

Nasdaq: FTNT

Publicly Traded

## S&P 500

Nasdaq: FTNT

GAAP Profitable

## BBB+ Baa1

Security Investment Grade Rating

Financially Stable

## \$4.18B

FY2021 Billing

Top 3

## 50+

Integrated Fabric Products

Broadest Attack Surface Coverage

## ASIC

Security Processing Unit (SPU)

High Performance

# Broad Global Footprint

Majority of our R&D is in North America

1,279

Patents Globally

Top Innovator

11,500+

Employees

Global Leader

595,000+

Customers Worldwide

Massive Customer Input

8.8M+

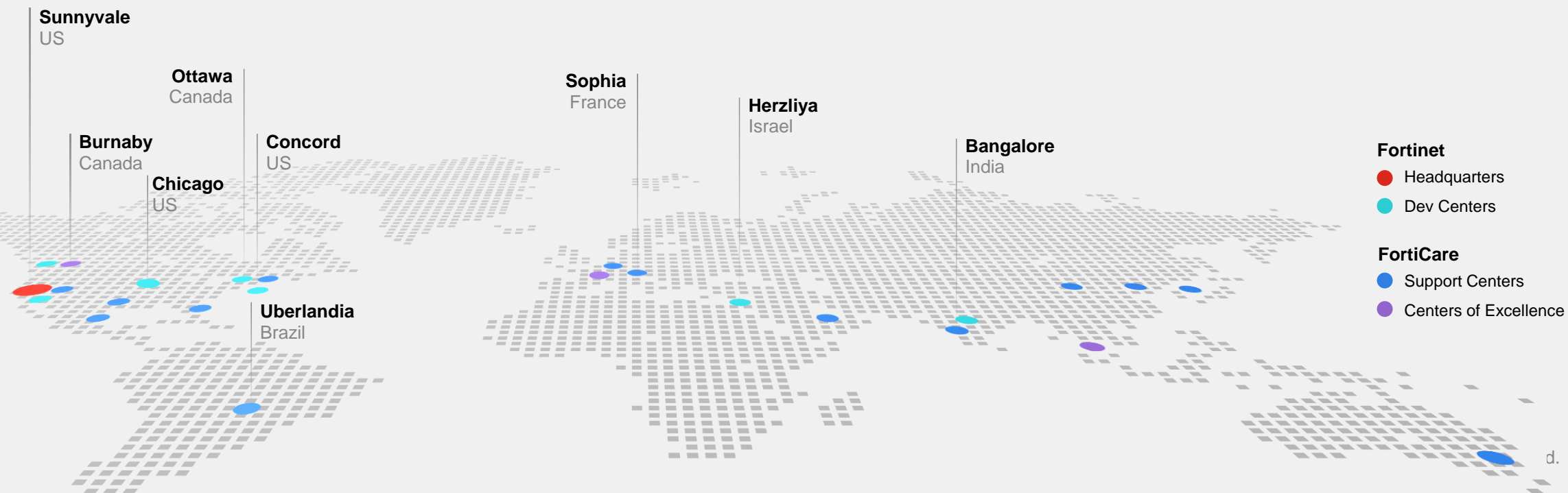
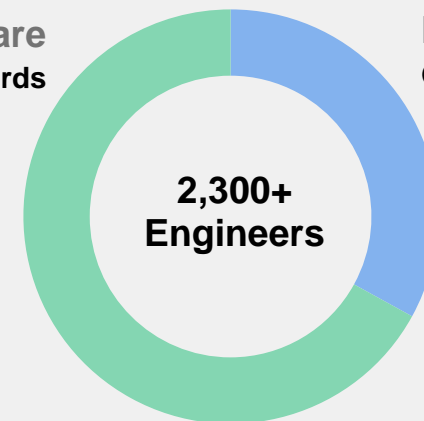
Global Firewall Shipments

Huge Scale

Software  
Two-Thirds

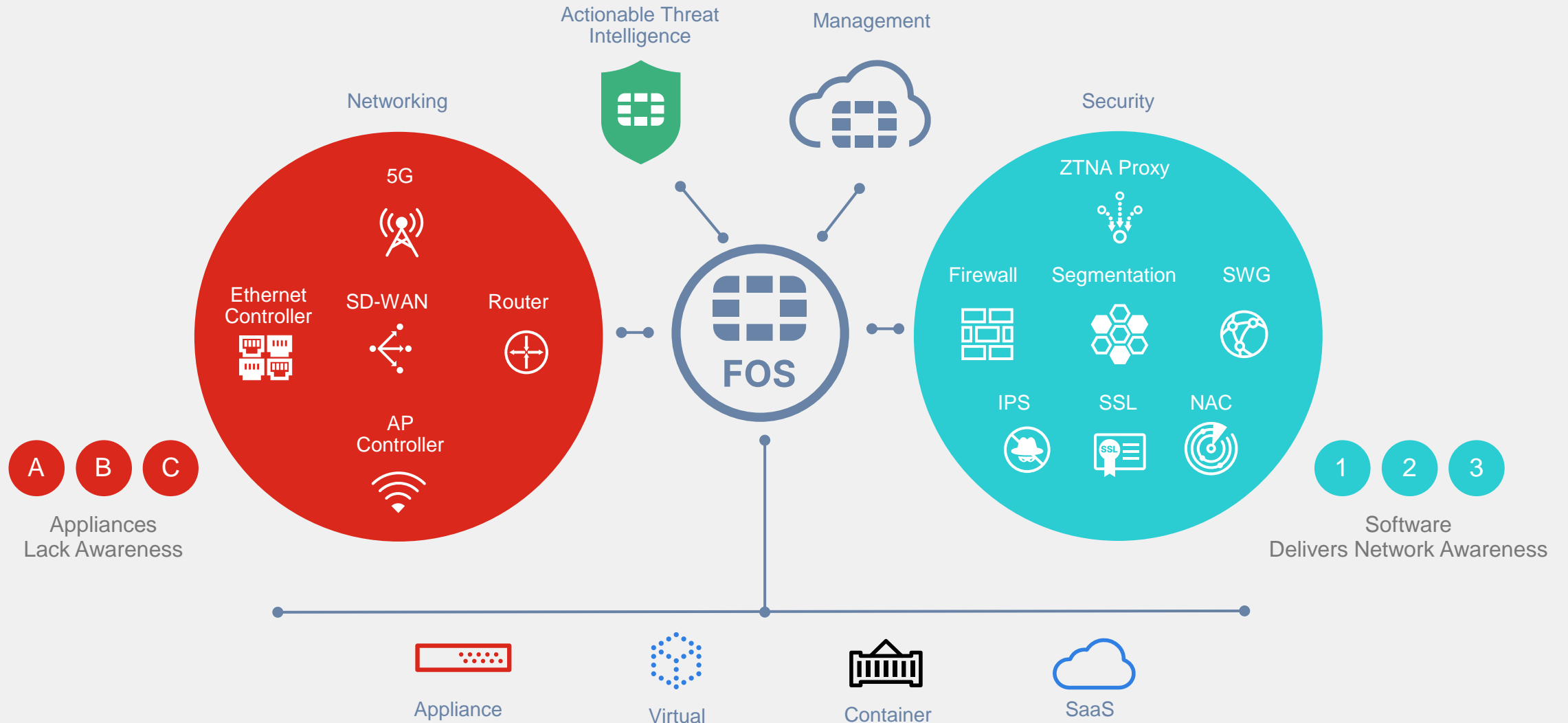
Hardware  
One Third

2,300+  
Engineers

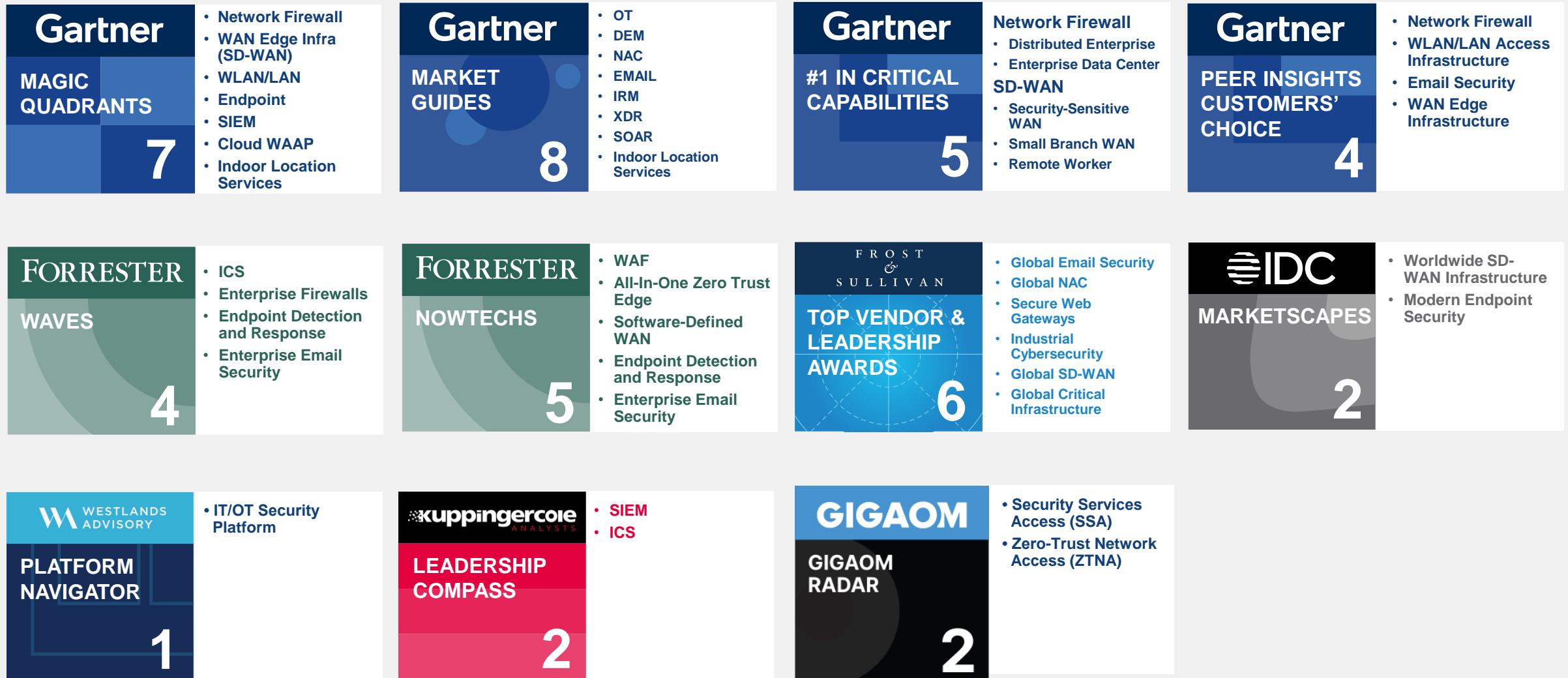


# Convergence of Networking and Security

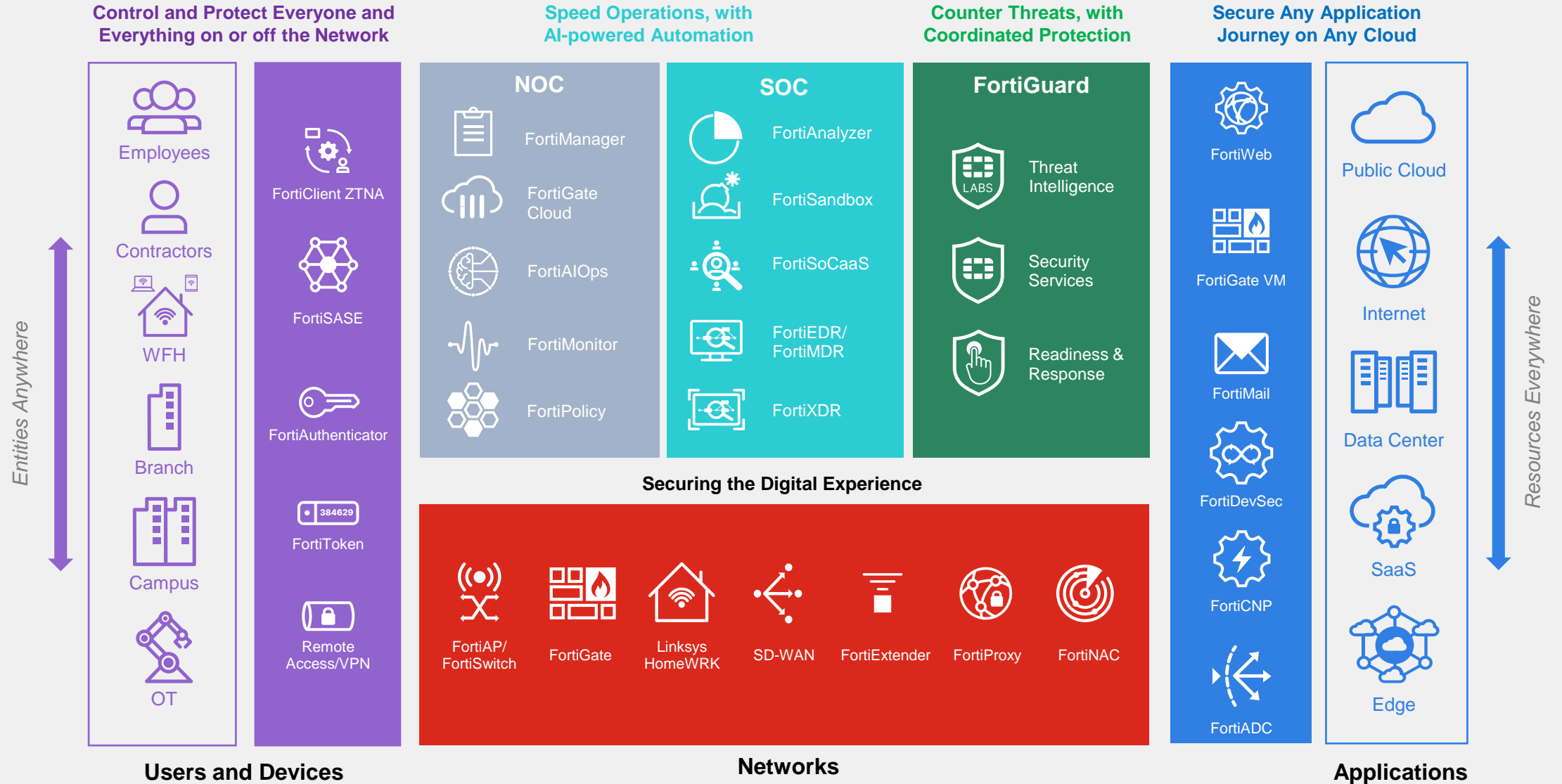
FortiOS Everywhere



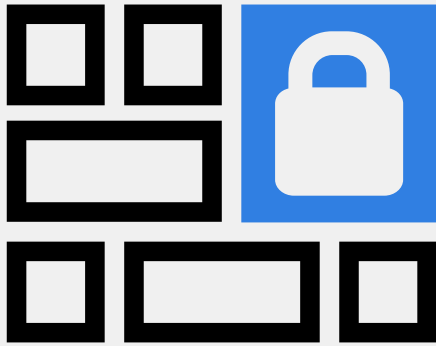
# Fortinet Industry Analyst Recognition



# Fortinet Technology Vision



# AWS and Fortinet deliver comprehensive, consistent security



## Better together

Working closely with AWS as an advanced Technology Partner to deliver a unified security experience **since 2014**



## Leading threat intelligence powered by FortiGuard Labs

Safeguarding your dynamic surfaces with security that innovates faster than attackers



## Demonstrated expertise

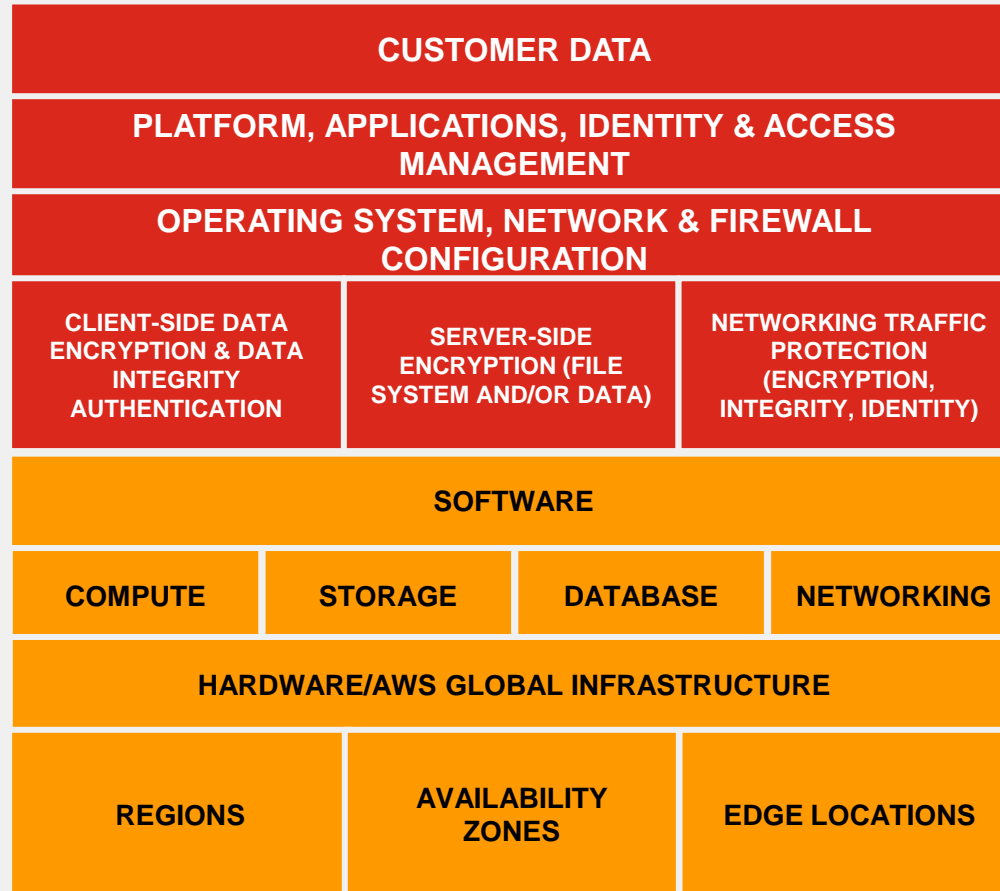
Bringing you security engineered for AWS, the market leading cloud, with more than **20 years** experience



# Delivering security in the cloud requires close collaboration

Fortinet provides comprehensive security configurations **IN** the Cloud

AWS is responsible for the security **OF** the Cloud



Network Security



Application Security



Platform Visibility & Control

**FORTINET**®

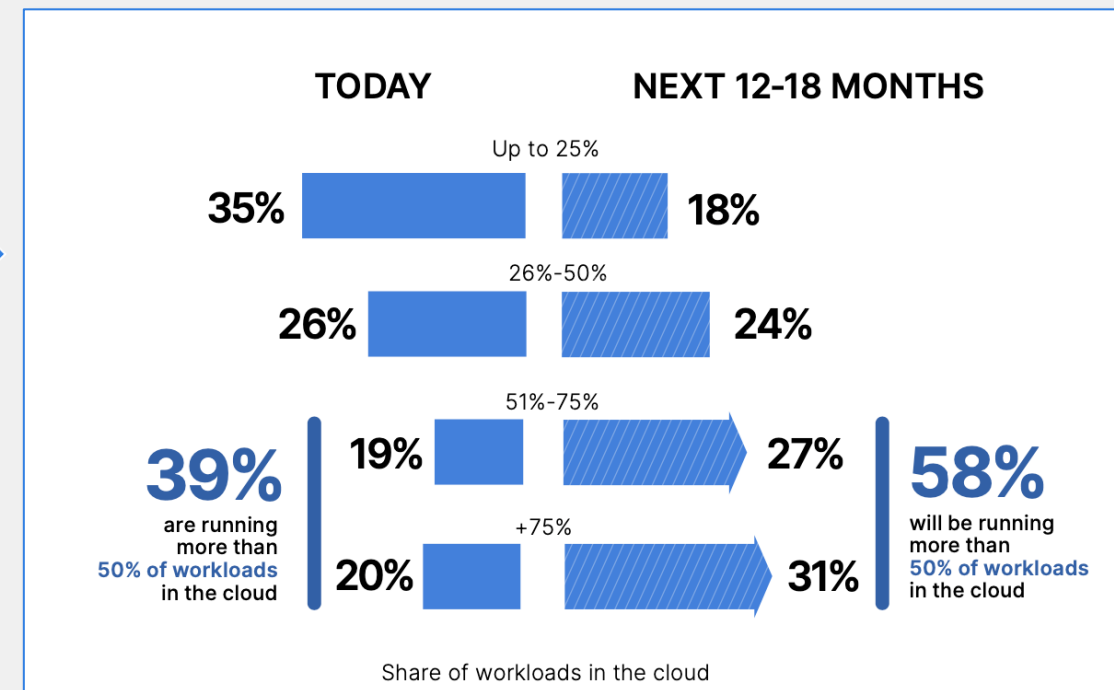
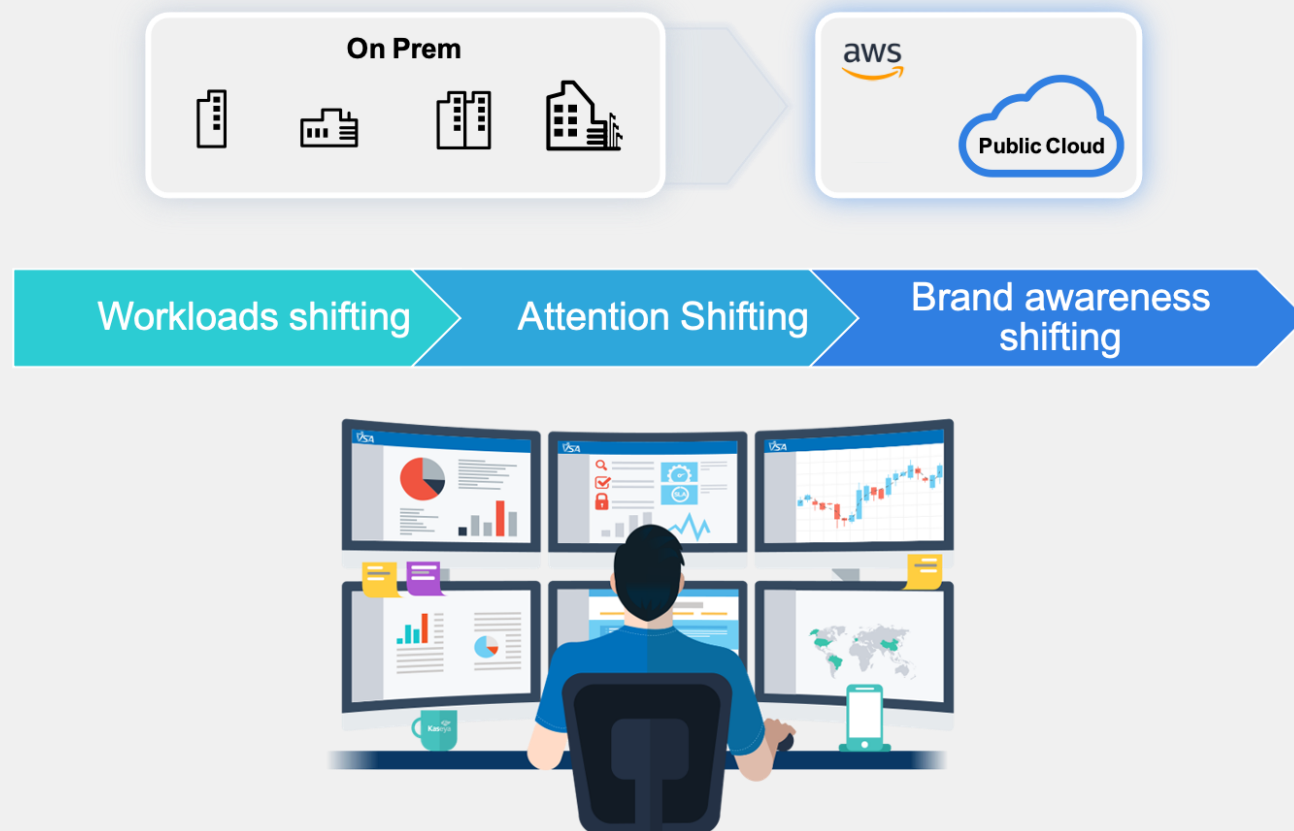




# Cloud Native Protection



# Security Operations is shifting to the Cloud



# Accelerated Cloud Adoption Brings New Challenges

*Customers are moving more of their workloads to the cloud*

## Insufficient Security Coverage



**62%** of IT executives say they are having difficulty keeping up to manage its increased cloud adoption.

*"The rush to cloud-everything will cause many security holes, challenges, misconfigurations and outages"*

2022 State of Security Posture  
Balbixeciprocity

## Too Many Security Tools to Manage



59% of Enterprise organizations have more than **50** separate security tools deployed

*"volume of disparate security tools and a lack of native interoperability ...biggest challenges facing cybersecurity operations today"*

Cyber Resilient Organization 2021  
IBM  
7 top challenges of security tool integration  
CSOnline

## Alert Fatigue



On an average day, security tools can generate over **700** cyber security alerts

*"cloud computing has led to an increase in the amount of security data to analyze. "*

Help Net Security  
Top Strategic Technology Trends for 2022  
Gartner

## Mitigation & Remediation



**60%** of organizations are manually prioritizing alerts or not at all

*"Many alerts don't contextualize potential cybersecurity threat... "*

Top Security Predictions for 2022  
Forbes



# Cloud-native or Third-Party Cloud Security?



Developer/Application  
Owner Focused Persona



Quick and  
easy to deploy



Availability of security  
service offerings



Scalable  
Flexible



Increased efficiency  
Reduced costs

Availability of  
integrated Security  
service offerings



Features limited  
to CSP offerings



Requires uncommon  
skill sets



Advanced  
security  
limitations



Security Operations  
Focused Persona



Single dashboard  
manages consistent  
workflows

Broad, Integrated and  
Automated Security Suite



Advanced security  
capabilities and  
depth of coverage



Security across  
multi-cloud  
environments



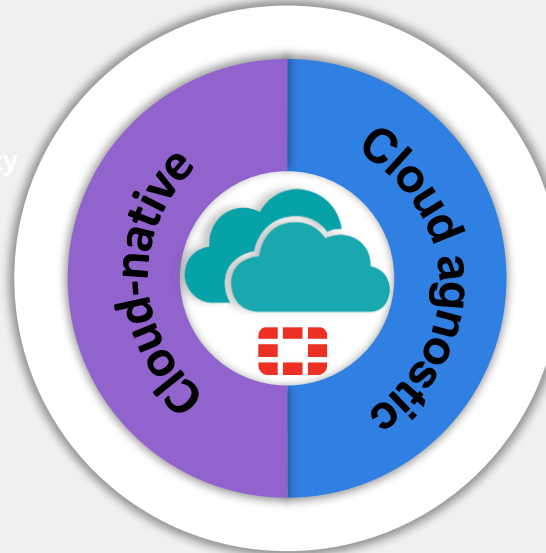
Minimizes full  
consumption of  
cloud capabilities



Integration friction  
and reduced  
security coverage

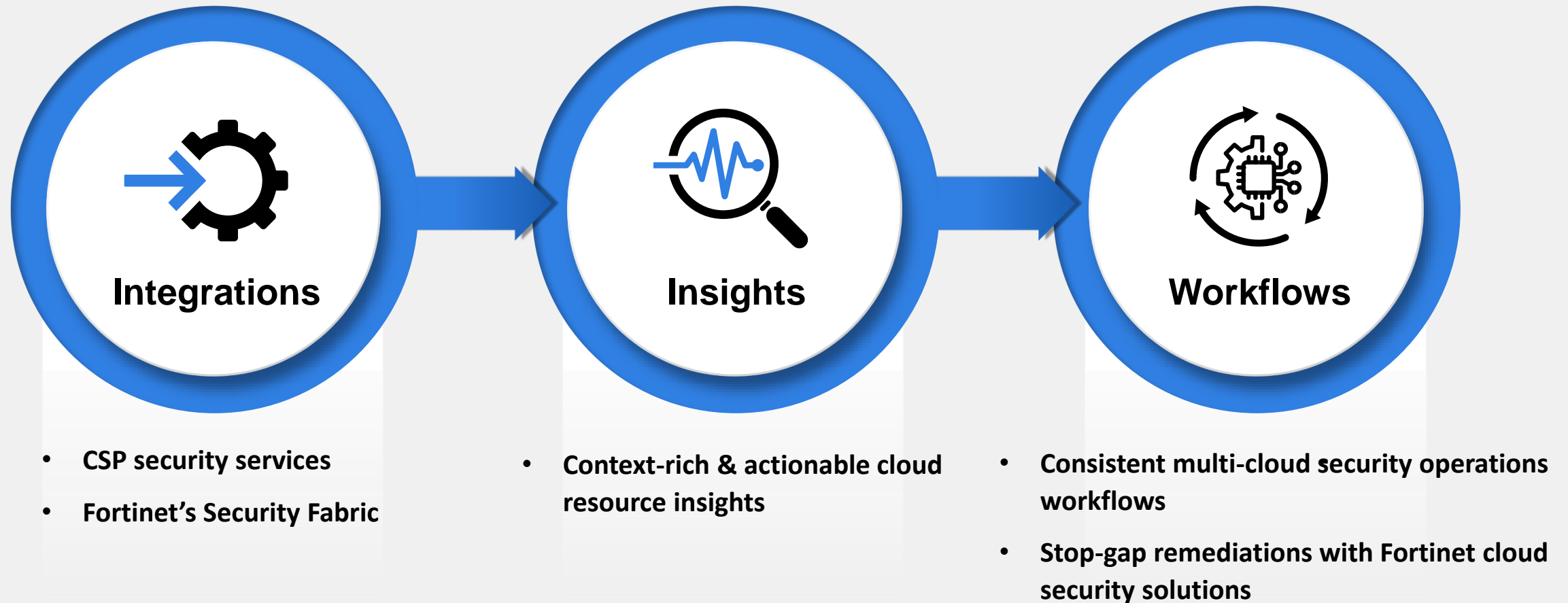


Setup complexity  
can delay  
deployment



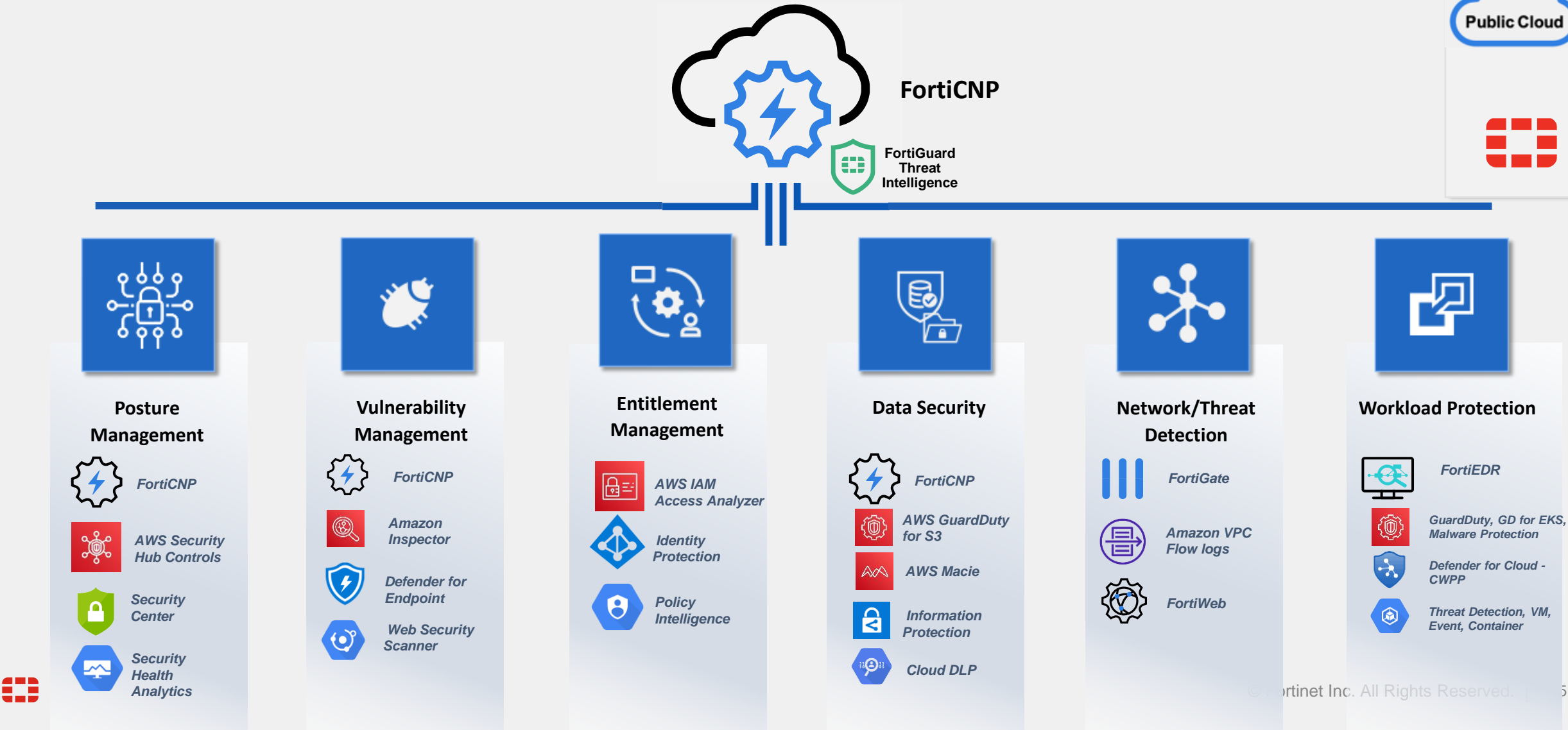
# FortiCNP's approach:

## *Context-Rich, Insight Driven Risk Management*

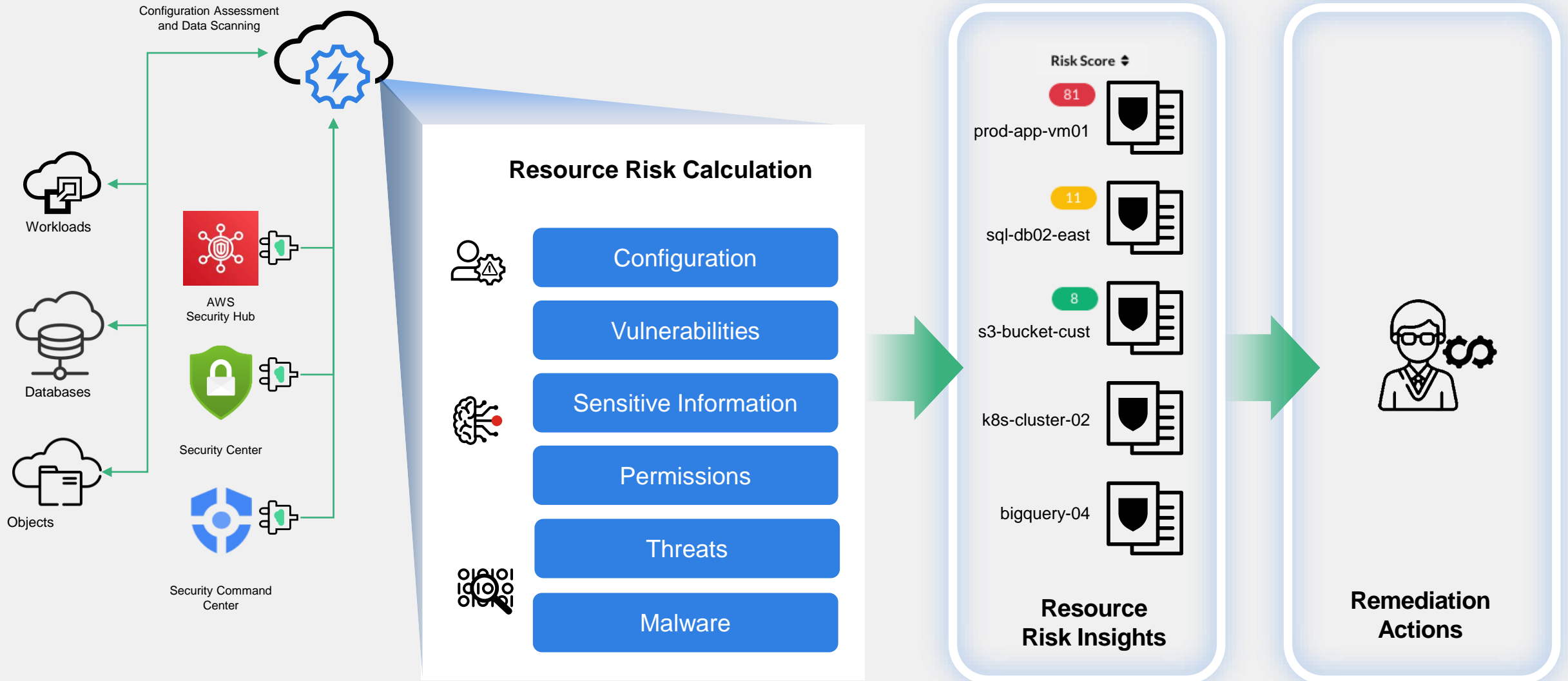


# FortiCNP Cloud-native Security Vision

Cloud-native integrations deliver real-time threat protection with zero-permission malware scanning capabilities

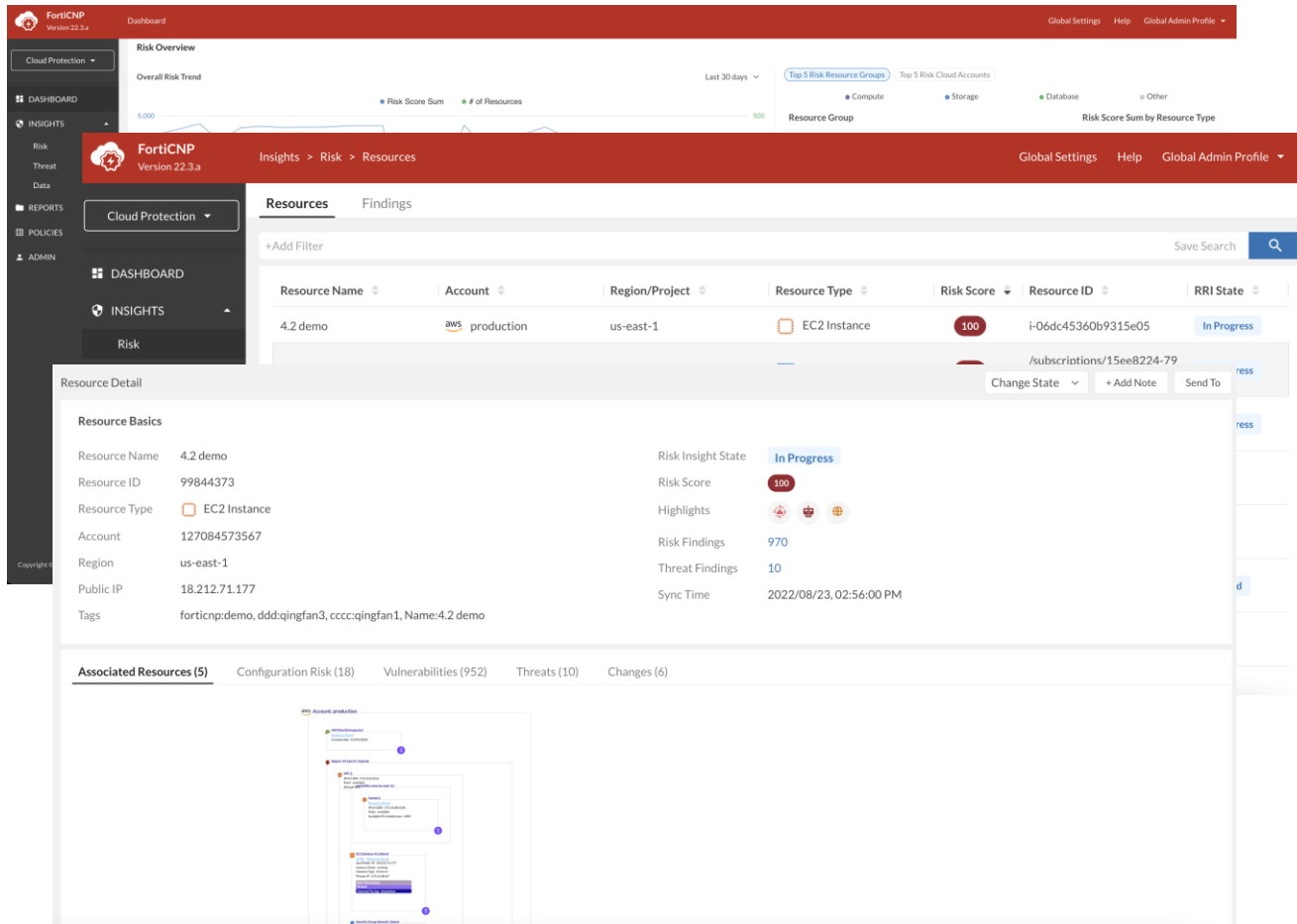


# Managing Risk with Resource Risk Insights (RRI)





# Use Case: Centralized Cloud Posture Management



## Customer Challenge

- Multi-cloud environments, multiple management tools and fragmented visibility
- Too many cloud native services and configurations management
- Challenging risk prioritization over multi-cloud environments
- Lack of actionable insights with rich context and remediation approaches

## FortiCNP Benefits

- **Single pane of glass** for multi-cloud environments
- **Prioritize risky resources by normalized risk score** for cloud-native services and Fortinet security fabric findings
- Allow Security Team to identify associate resources with risks, mis-configuration under same pane of glass, **reduce the Mean Time To Response (MTTR)**
- Provide actionable insights with rich context and remediation recommendations
- Automate workflow with your existing tools such as Jira and ServiceNow



# Use Case: Data Security

The screenshot displays the FortiCNP interface, version 22.3.a. The top navigation bar includes 'Policies > Data Scan > Policies'. The left sidebar shows a menu with 'Cloud Protection', 'DASHBOARD', 'INSIGHTS', 'Risk', 'Threat', 'Data', 'REPORTS', 'POLICIES', 'Risk Management', 'Threat Detection', 'Data Scan', 'Collection', and 'ADMIN'. The main content area is titled 'Policies' and 'Data Patterns'. It contains a description of the Compliance Standard and a table of predefined policies. The selected policy is 'DLP Birthdate Policy' with a severity of 'Low'. Below this, the 'Resource Detail' section shows information for an S3 Bucket resource, including its name, ID, type, account, region, and scan status. The 'Configuration Risk' section lists four risks, with the highest being 'High' for 'S3 buckets should not be publicly editable'.

Policy Name	Policy Code	Supported Cloud	Severity	Multi-Contexts	Enabled Contexts	Action
DLP Birthdate Policy	FC-ACT-018	AWS, Azure, GCP	Low	—	1 / 1	

Resource Basics	Risk Insight State
Resource Name: daiweidavidip	In Progress
Resource ID: 99850178	Risk Score: 41
Resource Type: S3 Bucket	Highlights: 1
Account: 127084573567	Risk Findings: 4
Region: us-east-1	Threat Findings: 6
Files Scanned: 0	Sync Time: 2022/08/23, 02:56:00 PM
Public IP: —	
Tags: forticnp:demo	

Configuration Risk (4)	Threats (6)	Changes (7)	Permissions
Policy	Severity	Last Seen	
S3 buckets should not be publicly editable	High	2022/08/23, 02:58:19 PM	
S3 buckets should have access logging enabled	Medium	2022/08/23, 02:59:02 PM	
S3 Object Versioning should be enabled	Medium	2022/08/23, 02:58:45 PM	
S3 buckets should not be publicly available	Informational	2022/08/23, 02:58:24 PM	

## Customer Challenge

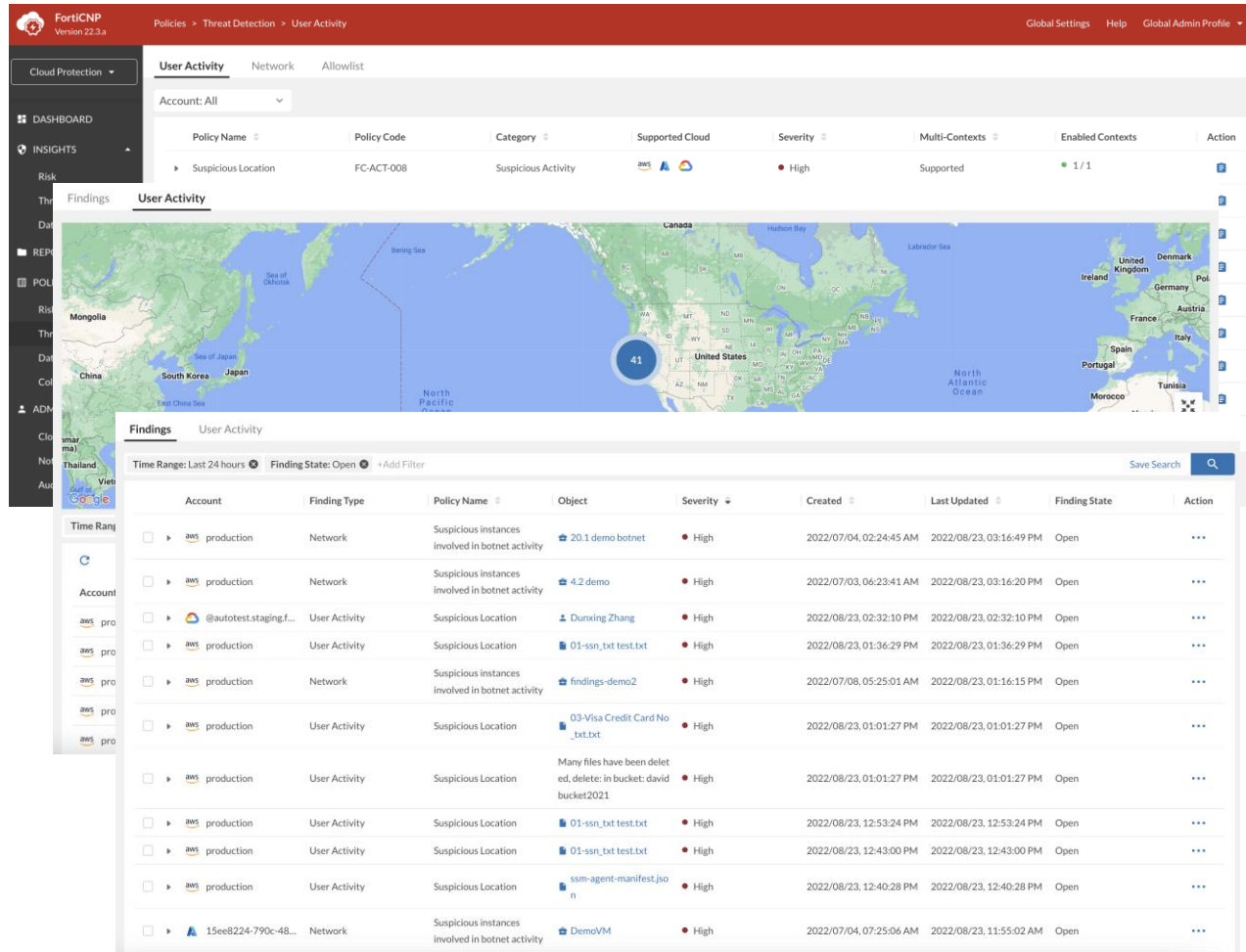
- Misconfigurations of data storage services
- Unaware of sensitive data or incompliance of cloud storage service usage
- Lack of virus and malware protection

## FortiCNP Benefits

- Detect misconfiguration of cloud storage with best practice and compliance standard
- Identify sensitive data, pre-configured **DLP engine** conform to compliance standards powered by FortiGuard
- **Customizable pattern** for sensitive data detection
- **Virus and malware detection** for AWS and other public cloud storage powered by FortiGuard



# Use Case: Threat Protection



The screenshot displays the FortiCNP User Activity interface. At the top, the navigation bar shows 'Policies > Threat Detection > User Activity'. The left sidebar contains a 'DASHBOARD' and 'INSIGHTS' section. The main content area is titled 'User Activity' and shows a map of the United States with a blue circle highlighting a specific location. Below the map, there is a table of findings with columns: Account, Finding Type, Policy Name, Object, Severity, Created, Last Updated, Finding State, and Action. The table lists several findings, including suspicious instances involved in botnet activity and suspicious locations.

Account	Finding Type	Policy Name	Object	Severity	Created	Last Updated	Finding State	Action
aws production	Network	Suspicious instances involved in botnet activity	20.1 demo botnet	High	2022/07/04, 02:24:45 AM	2022/08/23, 03:16:49 PM	Open	...
aws production	Network	Suspicious instances involved in botnet activity	4.2 demo	High	2022/07/03, 06:23:41 AM	2022/08/23, 03:16:20 PM	Open	...
@autotest.staging.f...	User Activity	Suspicious Location	Dunxing Zhang	High	2022/08/23, 02:32:10 PM	2022/08/23, 02:32:10 PM	Open	...
aws production	User Activity	Suspicious Location	01-ssn_txt test.txt	High	2022/08/23, 01:36:29 PM	2022/08/23, 01:36:29 PM	Open	...
aws production	Network	Suspicious instances involved in botnet activity	findings-demo2	High	2022/07/08, 05:25:01 AM	2022/08/23, 01:16:15 PM	Open	...
aws production	User Activity	Suspicious Location	03-Visa Credit Card No _txt.txt	High	2022/08/23, 01:01:27 PM	2022/08/23, 01:01:27 PM	Open	...
aws production	User Activity	Suspicious Location	Many files have been deleted, delete in bucket: david bucket2021	High	2022/08/23, 01:01:27 PM	2022/08/23, 01:01:27 PM	Open	...
aws production	User Activity	Suspicious Location	01-ssn_txt test.txt	High	2022/08/23, 12:53:24 PM	2022/08/23, 12:53:24 PM	Open	...
aws production	User Activity	Suspicious Location	01-ssn_txt test.txt	High	2022/08/23, 12:43:00 PM	2022/08/23, 12:43:00 PM	Open	...
aws production	User Activity	Suspicious Location	ssm-agent-manifest.json	High	2022/08/23, 12:40:28 PM	2022/08/23, 12:40:28 PM	Open	...
15ee8224-790c-48...	Network	Suspicious instances involved in botnet activity	DemoVM	High	2022/07/04, 07:25:06 AM	2022/08/23, 11:55:02 AM	Open	...

## Customer Challenge

- Lack of user activity monitoring and suspicious activity detection
- Malicious traffic, c&c communication

## FortiCNP Benefits

- **User behavior analysis** with pre-config policies
- Export user activities for further analysis
- **Detect compromised instances and malicious traffic** with FortiGuard IOC and Anti Botnet databases



# Use Case: Compliance

FortiCNP Version 22.3.a

Reports > Compliance > Reports

Global Settings Help Global Admin Profile

Cloud Protection

DASHBOARD

INSIGHTS

Risk

Threat

Data

REPORTS

Compliance

Reports Standards

Compliance Reports on incontinent findings are generated automatically on a monthly, quarterly, and yearly basis. You can also click the Generate button to generate one-time reports with a custom date range.

+Add Filter

Generated

Created Date	Report Title	Action
2022/08/23, 06:15:58 AM	CWP3 ISO 27001 Compliance Report Aug 15 22:15:58 - Aug 22 22:15:58 UTC.zip	...
2022/08/23, 06:15:58 AM	CWP3 NIST800-171 Compliance Report Aug 15 22:15:57 - Aug 22 22:15:58 UTC.zip	...

The out-of-the-box compliance standards automatically inspect and identify cloud account misconfigurations and user activities that are incontinent.

SOX-COBIT PCI-DSS HIPAA GDPR NIST SP 800-53 rev4 NIST SP 800-171 ISO 27001

Account: All

Policy Name	Policy Code	Supported Cloud	Severity	Multi-Contexts	Enabled Contexts	Action
PCI - Cloud KMS key rotation should be enabled	FC-ACT-278	Google Cloud	Medium	—	1 / 1	...
PCI - MFA(Multi-factor Authentication) should be enabled for IAM users	FC-ACT-275	AWS	Medium	—	1 / 1	...
PCI - Access keys should be disabled for the root account	FC-ACT-067	AWS	Medium	—	1 / 1	...
PCI - Failed Access Attempt Detection	FC-ACT-056	AWS, Azure, Google Cloud	High	Supported	1 / 1	...
PCI - Privileged Account Activity	FC-ACT-057	AWS, Azure, Google Cloud	High	Supported	1 / 1	...
PCI - Security groups should not allow all internet traffic without restriction	FC-ACT-060	AWS	Medium	—	1 / 1	...
PCI - Cloud Storage buckets should not be publicly available	FC-ACT-110	Google Cloud	High	—	1 / 1	...
PCI - Firewall rules should not allow all internet traffic without restriction	FC-ACT-108	Google Cloud	Medium	—	1 / 1	...
PCI - Retain audit trail history	FC-ACT-085	AWS, Azure, Google Cloud	High	—	1 / 1	...

## Customer Challenge

- Challenging compliance enforcement in multi-cloud environments
- Lack of cross platform tools to apply consistent policies and monitor if any compliance violations
- Hard to find out the incontinent resources and remediation approaches
- Lack of compliance reporting tools for cloud environments

## FortiCNP Benefits

- Pre-config policies for different compliance standards including PCI, HIPPA, GDPR, ISO 27001, NIST, etc.
- On-demand and periodical report generation
- **Actively monitoring compliance violation** with remediation recommendations
- For example, in PCI DSS compliance, pre-defined policy is available to identify inactive users for 90 days, saving Security Team resources to deal with manual reporting

# FortiCNP Consumption Models

Flexible procurement options to fit your needs

AWS Marketplace

From Fortinet Distributors

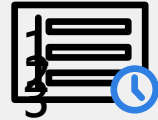


## Monthly

Pay for software and compute capacity monthly

**Ideal for temporary projects and baseline workloads**

**14-day Free Trial Available**



## Annually

Make an annual payment

**Ideal for long-term cloud posture management**



## BYOL

Negotiate a custom price with a Fortinet seller

**Available for 1Y, 3Y and 5Y, stackable**

**60-day Free Trial Available**



# Case Study

## Brazilian Bank Enhances On premises and Cloud-based Network Security With Fortinet



### Customer Overview

BK Bank is a Brazilian financial services company founded in 2015. The bank started out in the meals voucher segment, before moving on to issuing prepaid credit cards and offering payment services such as card machines & e-commerce. In 2020, the company created Conta Digital BK, a digital account that today gives 20,000 users access to banking services including transfers, payments, and prepaid credit card management.

### Business Impact with Fortinet Security Solution

- Secure, integrated network management and visibility
- Blocks almost all 80,000 fraudulent intrusion attempts the bank receives every five minutes
- Complete visibility into the cloud ecosystem for easier, more proactive operation management
- Integrated and dynamic protection for AWS Cloud
- Automated reporting of instant users do and do not meet the 90-day rule

### Challenges

- Compliance with **PCI DSS** for banks' end-to-end credit card processing systems
- Received an average of **80,000 fraudulent intrusion** attempts every five minutes
- BK Bank migrated its operations to Cloud, ensured cloud security model was **compliant with all relevant industry regulations & support multi-Cloud**
- Require a deep levels of information on their cloud platform's functionality or information flows
- **Manual check of inactive users** who had not logged in during the past 90 days

### Solution Components

- FortiGate Next- Generation Firewall
- FortiWeb
- FortiAnalyzer
- FortiCNP
- Fortinet Cloud Consulting Services



# Cloud Security Posture Assessment

Aligned with AWS *Well Architected Framework* Best Practice

**Objective:** Cloud Partner will use a Fortinet's tool & monitors enterprise public cloud environments to identify and report on deviations of an enterprise's security posture against best practices. This assessment includes deviations based on:



Compute instances for compromises



Network traffic for suspicious traffic flows



Storage buckets for vulnerabilities and misconfigurations



Sensitive data exposure



Malware



Compliance deviations

# How CSPA works?

To perform the assessment outlined above, Partner uses Fortinet's CSPA tool with the following methodology:



Establish connectivity  
to the customer's  
cloud environment



Assess compute  
instances, network  
traffic, and data  
stores for anomalies



Generate  
best-practice  
report and  
recommendations



Once the prerequisite steps are established to gain visibility into the cloud resources across AWS, other Cloud Platforms, the service utilizes global threat intelligence on zero-day threats, botnets, viruses, and indicators of compromise to report on the risks and exposures



# CSPA Results



Your assessment will provide results in these areas:

- Identification of misconfiguration of the cloud resources for exposure to threats
- Reporting on data stores containing sensitive information
- Reporting on data stores for content infected with malware
- Highlighting open alerts by severity to help prioritize actions
- Highlighting suspicious data flows and user behavior
- Reporting on compliance with industry standards
- Recommendations to remediate issues found in the environment



# FortiCNP Key Takeaways

01

**Cloud-native integrations reduces complexity**

- Integrations with CSP security services and Fortinet Security Fabric provide broad visibility across cloud footprint
- Native integration enables zero-permission security coverage

02

**Patented Resource Risk Insights (RRI) simplify cloud security**

- RRI insights prioritizes high risk resources and provides context rich, and actionable insights
- RRI enables cloud neutral workflows that scale security to manage and remediate risk

03

**Streamlines Security Operations**

- Takes findings and alerts into actionable insights
- Integrations with digital workflow solutions automate processes to manage and remediate risk
- Stop-gap remediations enabled with Fortinet cloud security solutions to protect from threats



**FORTINET®**