



Adding Prevention to CNAPP

Shifting Cloud Security Paradigm

YOU DESERVE THE BEST SECURITY



Check Point

CloudGuard

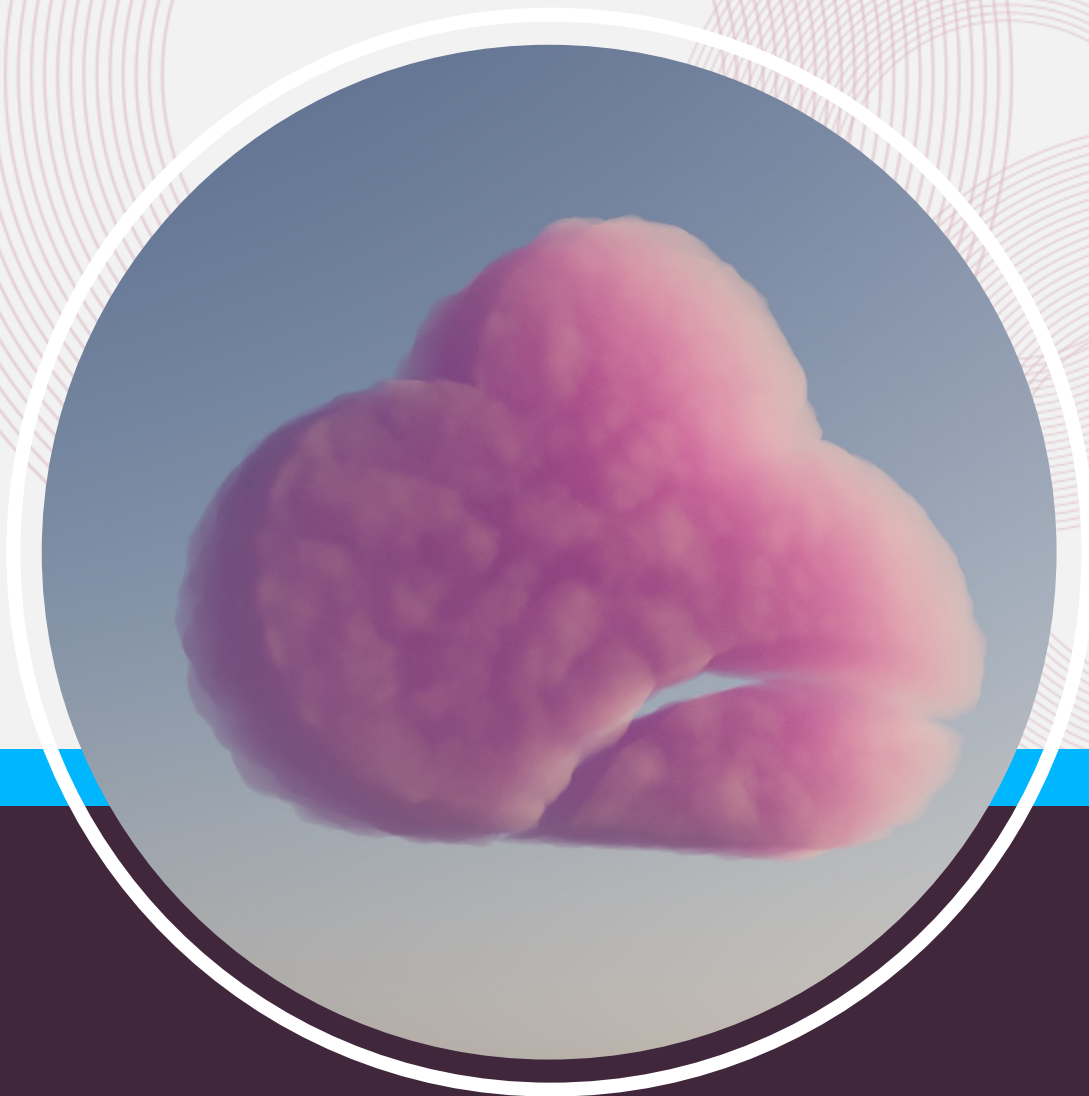
Closing a Successful Year in Cloud

3,700+

CloudGuard
Customers WW

800M+

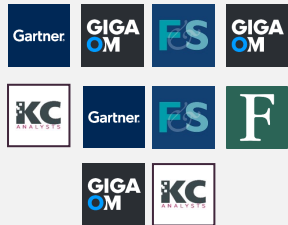
Protected Cloud
Assets Every Day





x10 Cloud Security Recognitions

CNAPP, CSPM, CWPP, WAAP & Network Security



#1 Cloud Network Security & Workload Security Vendor

GigaOm Network Security & CWPP



#1 Web Application & API Protection Engine

Preemptive Prevention of Zero Day Attacks

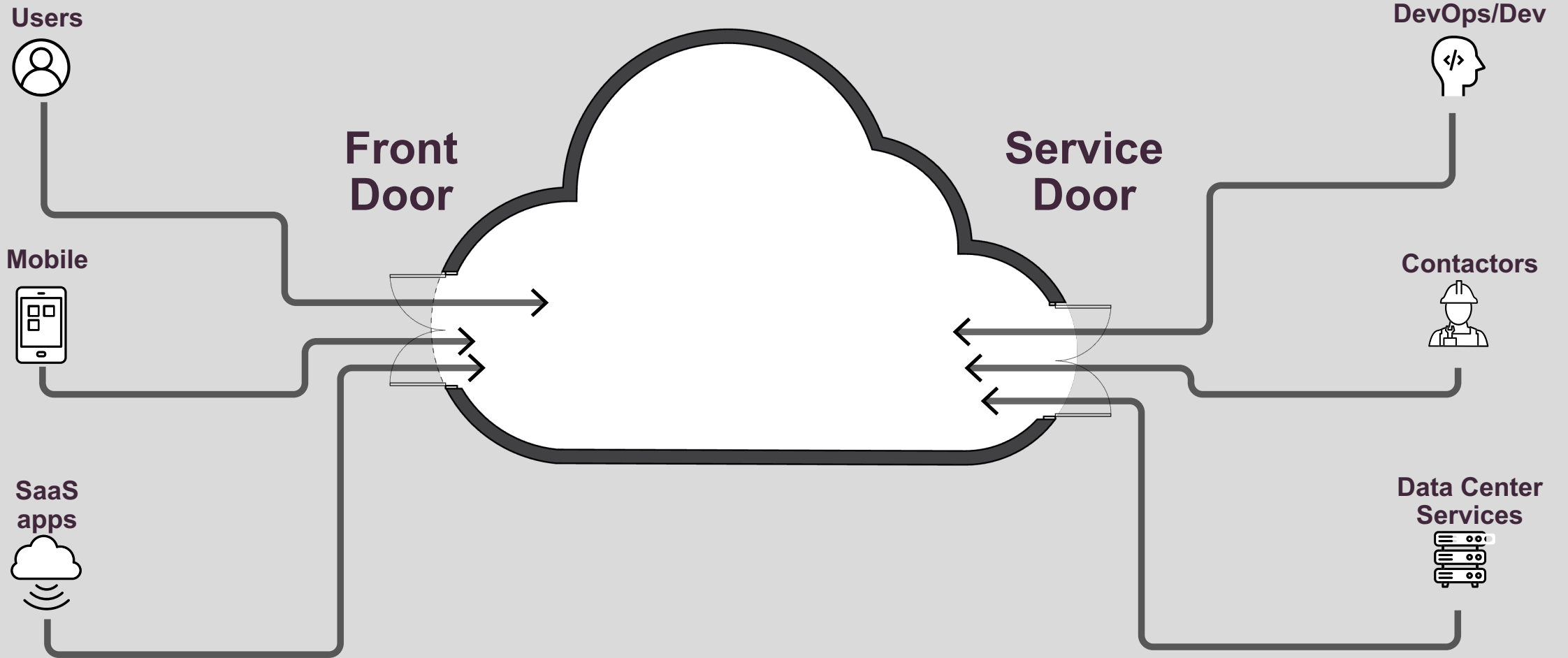
~~Log4Shell~~

~~Sprint4Shell~~

~~Text4Shell~~

~~MOVEit~~

Recognized By Top Analysts

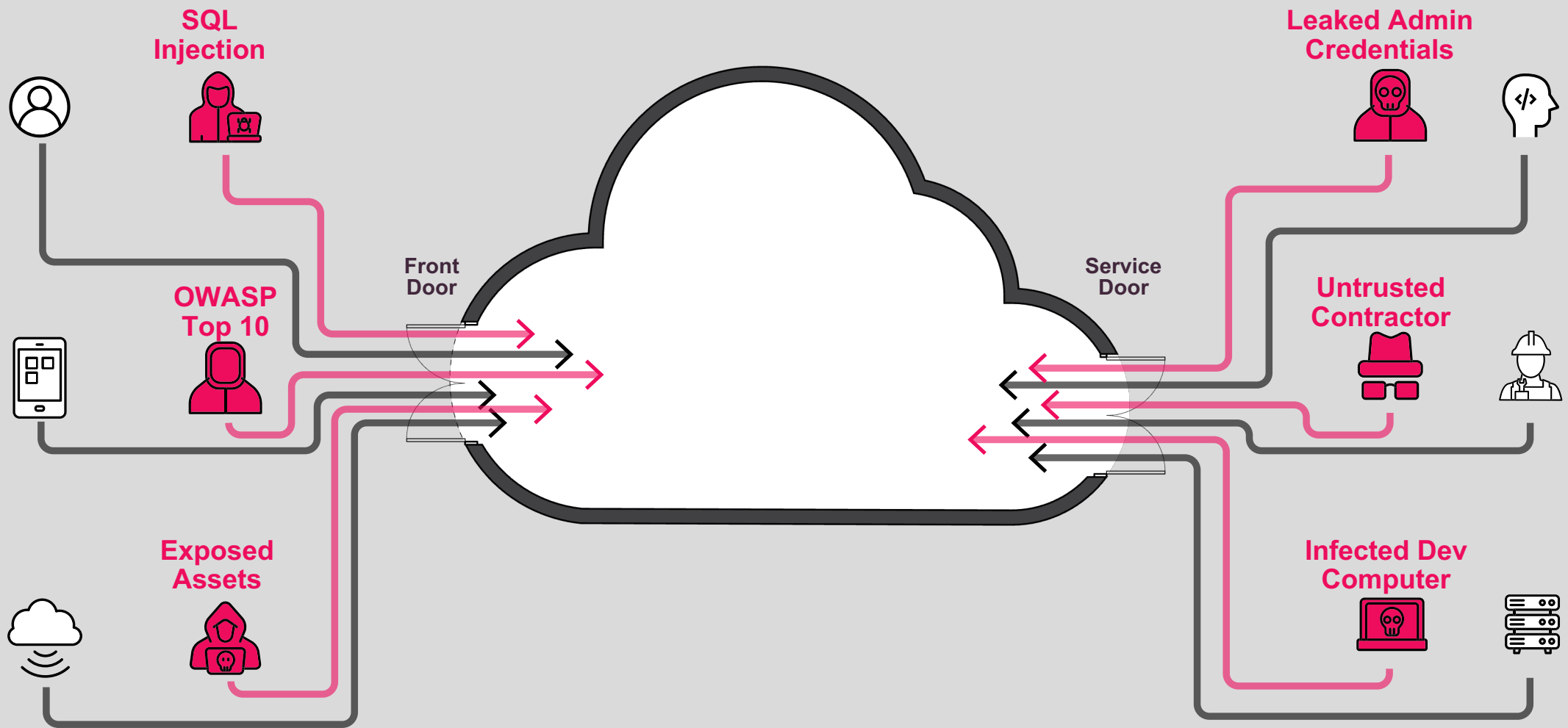


Public Internet

Users Engage with
Web Applications & APIs Services

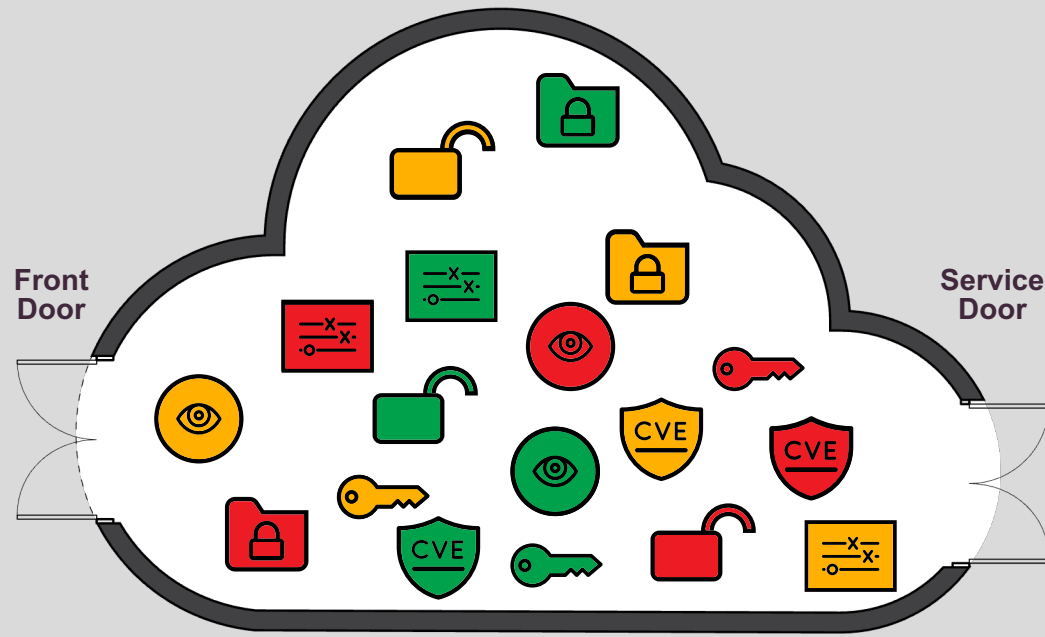
Corporate Network

Internal Teams
& Contractors Maintain
& Update the Cloud

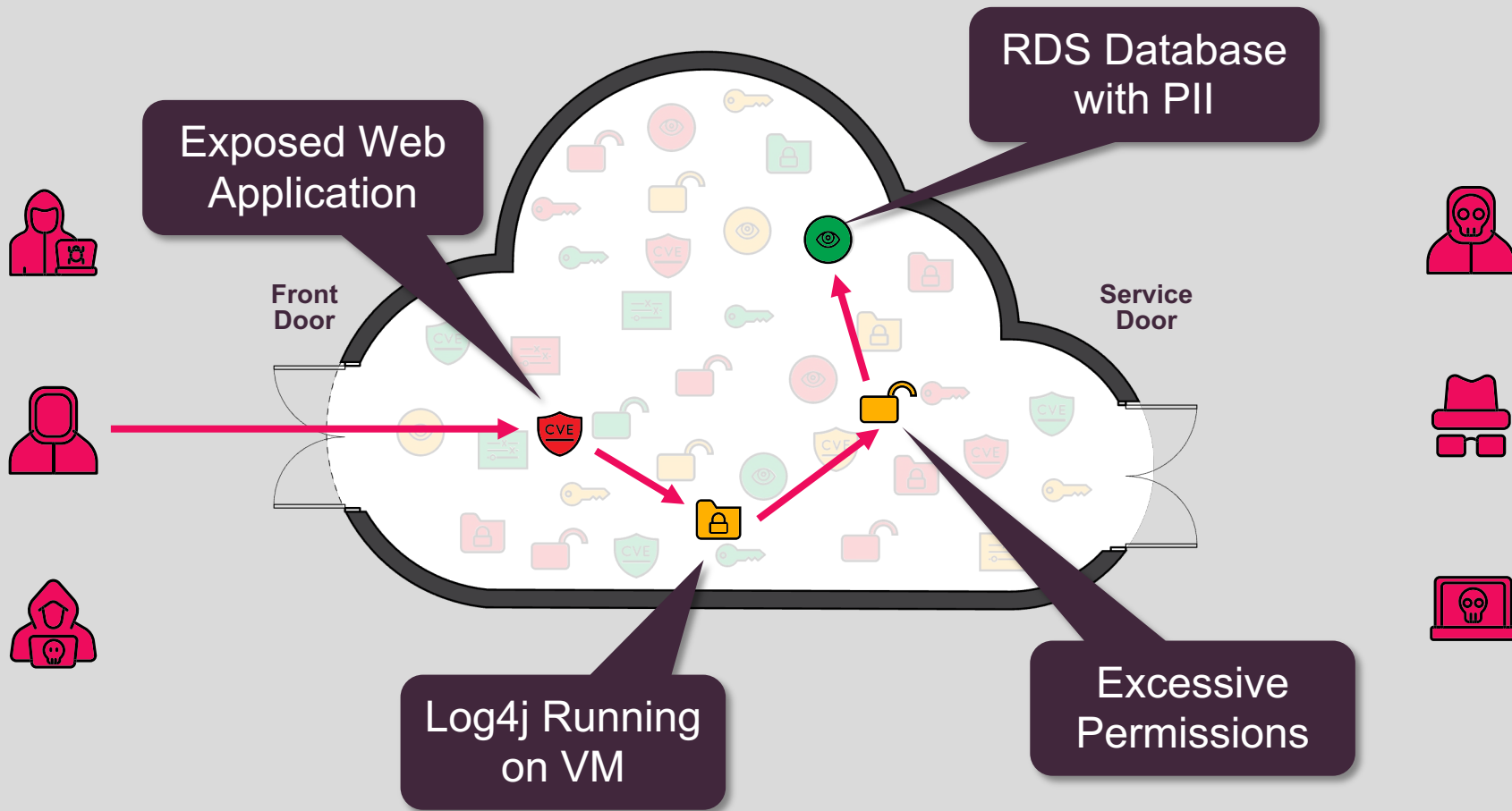


Attackers Enter The Cloud Through The Front Door

Or Through The Service Door



**There Are Thousands of Risks
Within Your Cloud**



**Once Inside Your Cloud,
Attackers Target Those Risks**

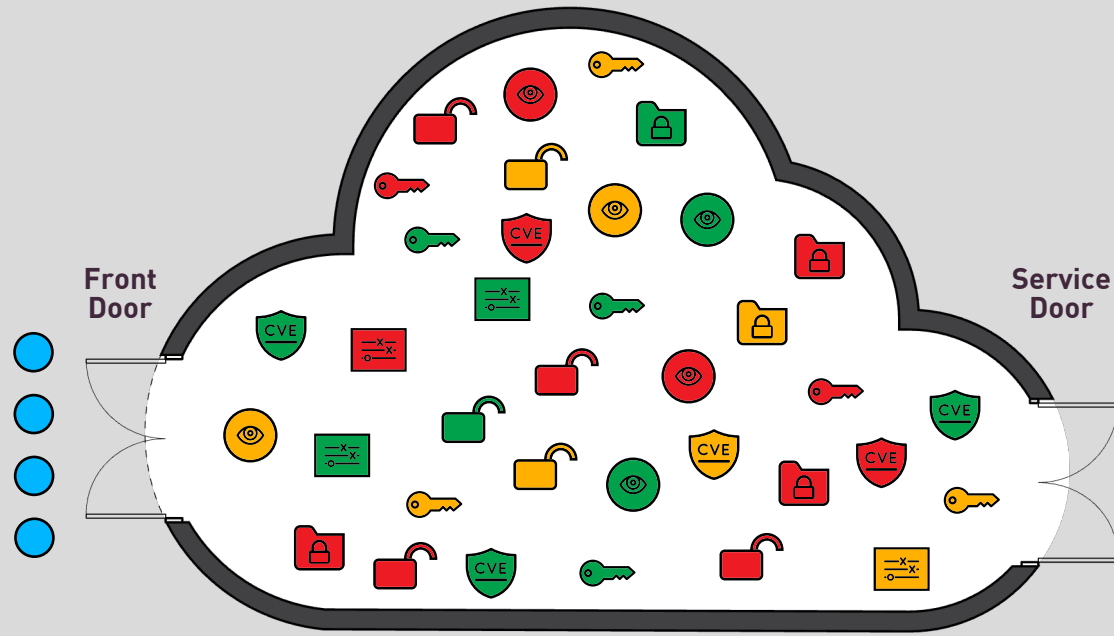


ADDING **PREVENTION** TO YOUR CLOUD SECURITY

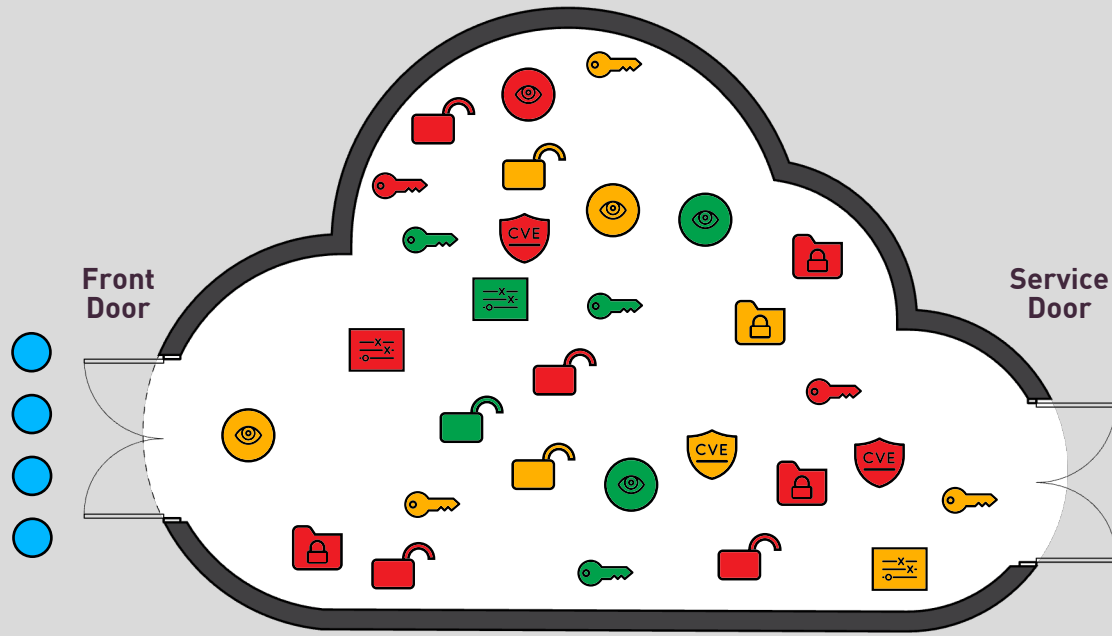


CNAPP+

Cloud Native Application Protection & **Prevention** Platform

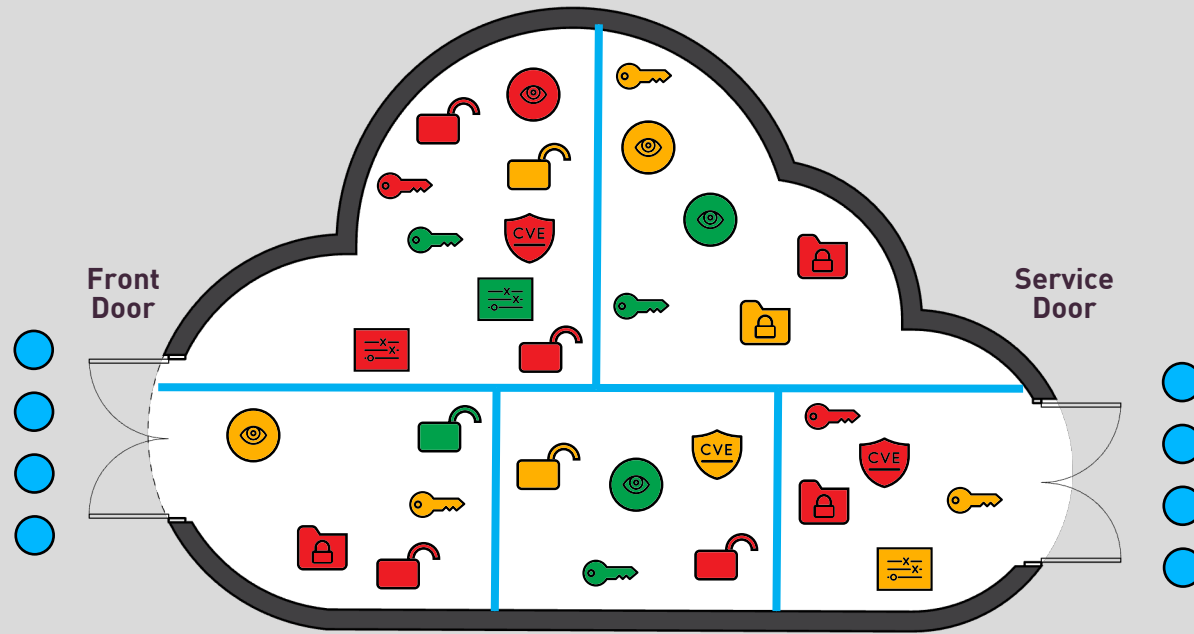


#1 Add **WAF** to Protect Your Cloud Front Door Web Applications And APIs

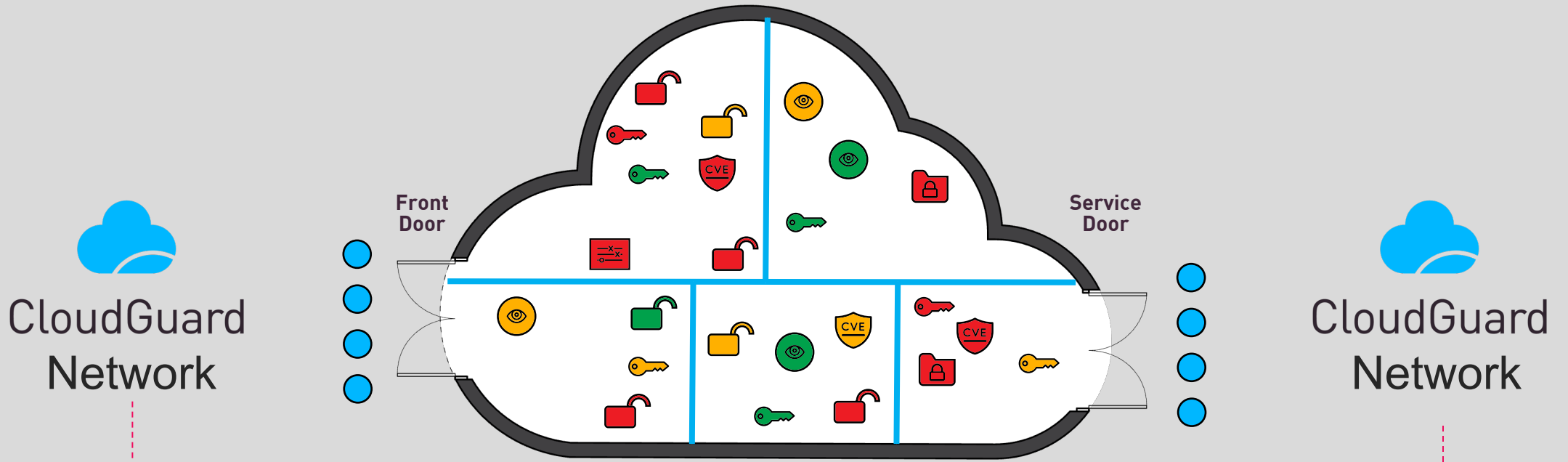




Use Case	CloudGuard WAF	Cloud Native WAF
Zero Day Prevention	✓ Immediate	✗ Avg. 40 days*
Signature Updates	✓ AI	✗ Signature
Accuracy	✓ Highest 97%	✗ 87%*
API Prevention	✓ Yes	✗ Not Provided
Multi-Cloud Support	✓ Yes	✗ Single Cloud

Unmatched AI-Based WAF Prevention



#2 Add **Network Security** to Protect Both Your Cloud Front Door & Service Door & To Macro Segment your Cloud

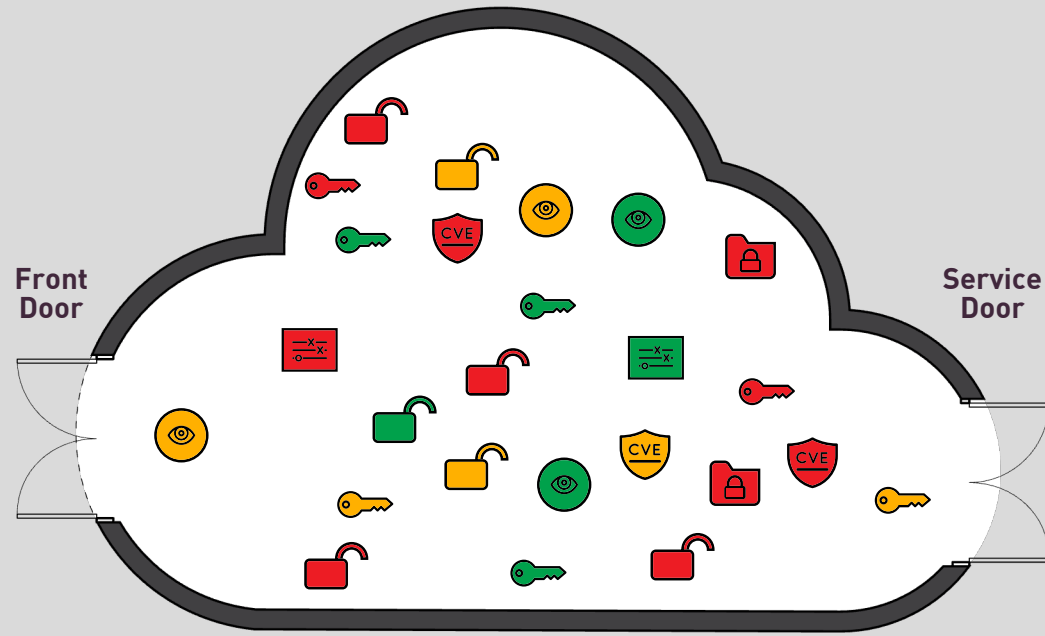


Use Case	 CloudGuard Network Security	 Cloud Native FW
Threat Prevention	✓ Best Security	✗ Limited IPS
Hybrid-Cloud Support	✓ Yes	✗ No On-Prem. Support
Multi-Cloud Support	✓ Yes	✗ Single Cloud
ROI	✓ High 169%	✗ Low <40%

Unmatched Cloud Network Security



CloudGuard
CNAPP



**#3 Use CNAPP with Prevention
To Remediate The Remaining Risks**

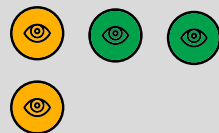
CNAPP+



Workload Protection



Detection & Response



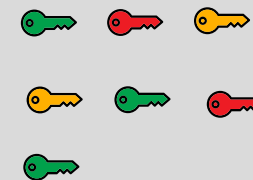
Posture Mgmt.



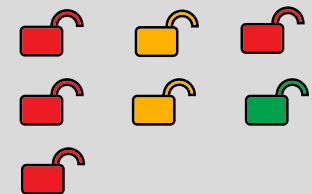
Data Posture



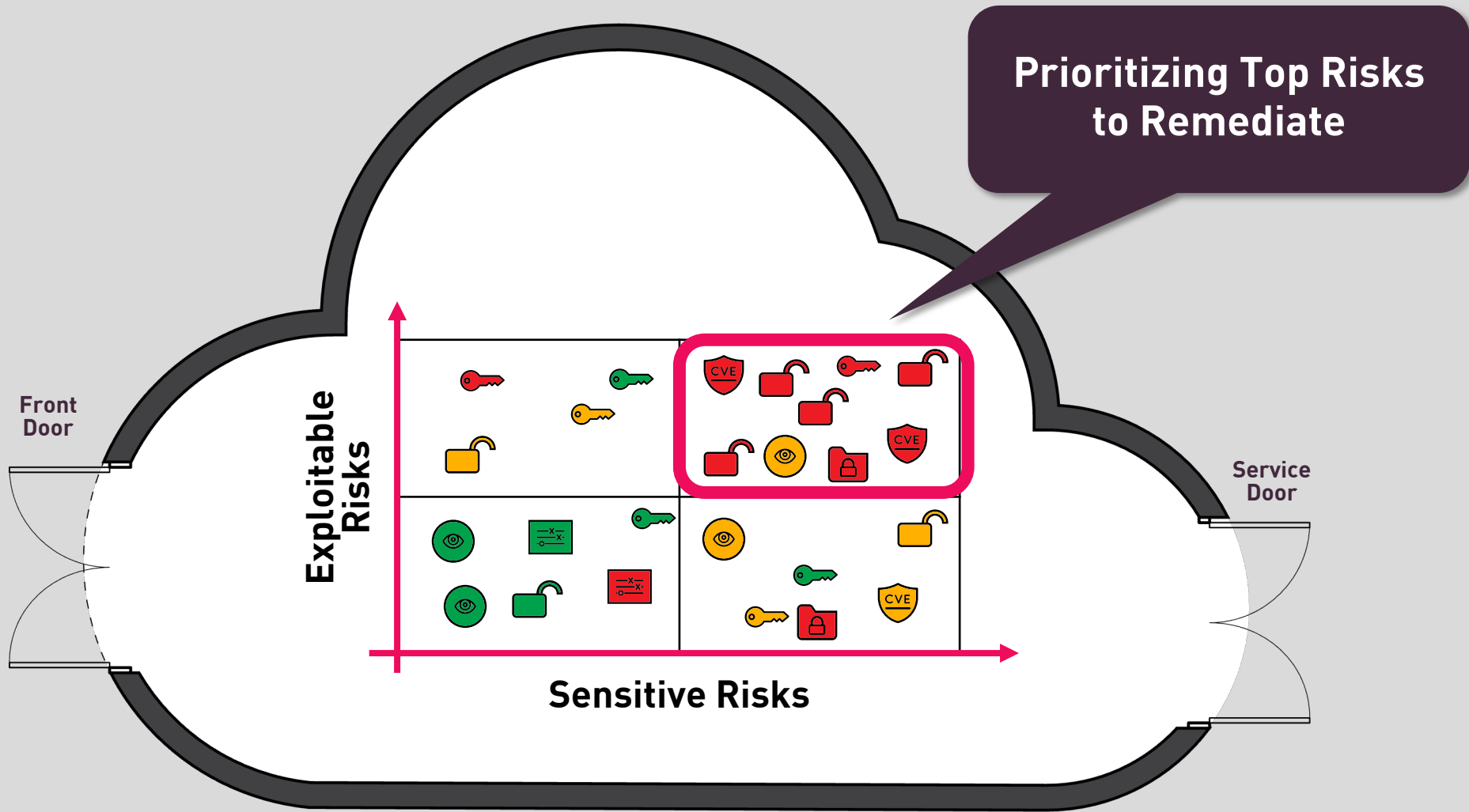
Identity Mgmt.

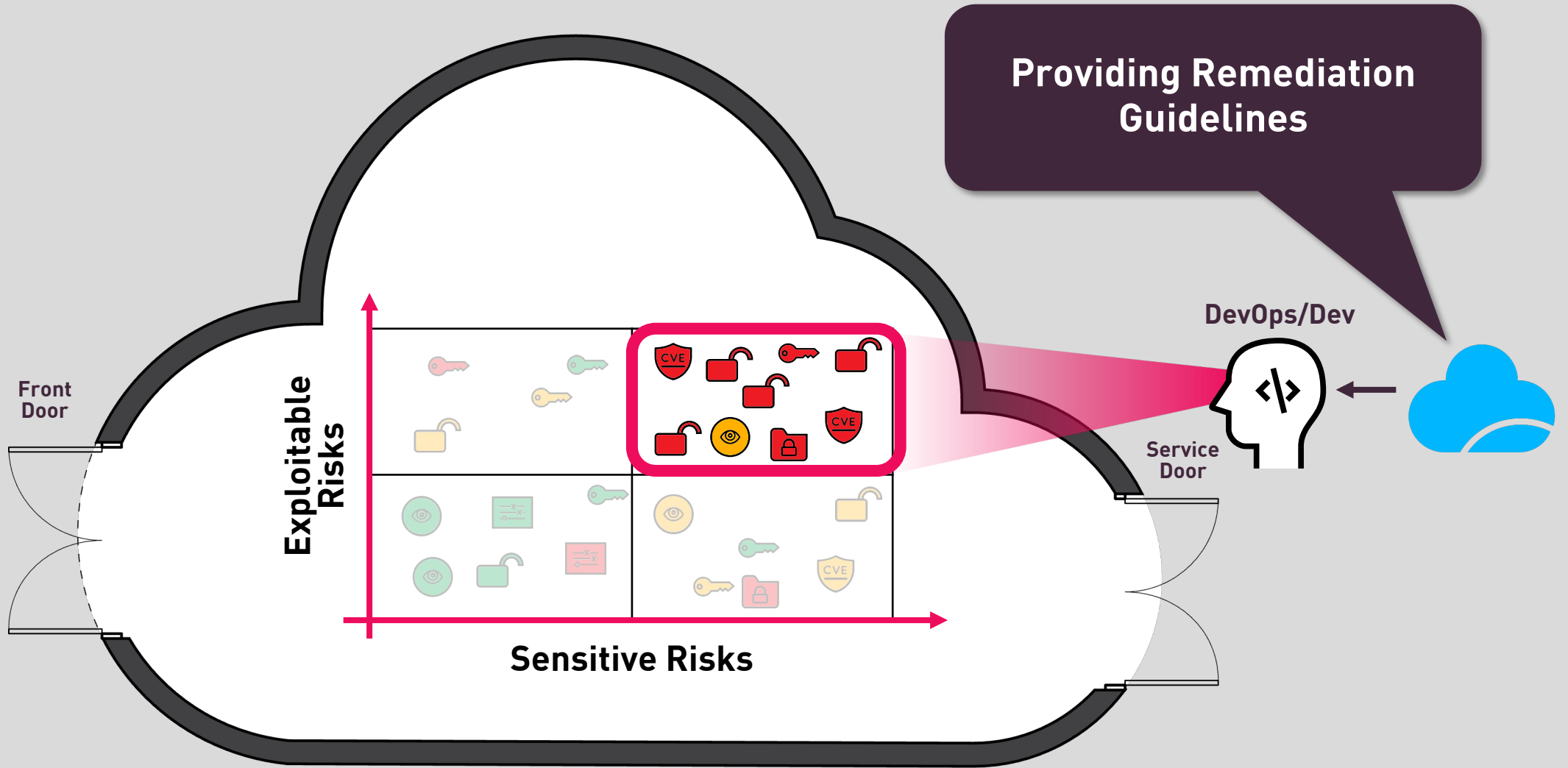


Code Security



Classify Your Cloud Risks Powered by 6 CNAPP Modules



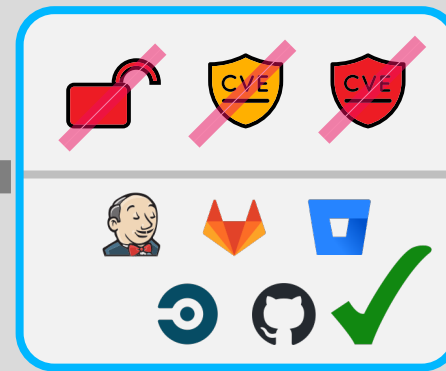


Tight Integration with Dev & DevOps

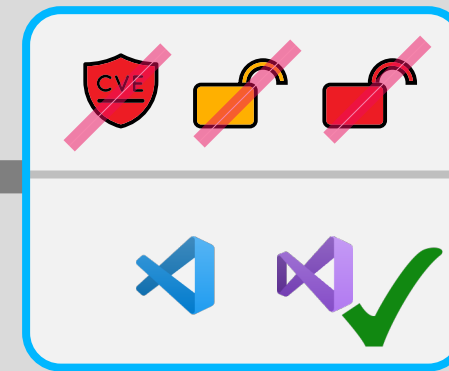
Prevent Unsecured Code from Getting the Cloud



CloudGuard
Code Security



Git & CI/CD



Dev Workstation



Open-Source
Components



The Only **CNAPPP** with **Prevention**



Giving the Power Back to the Security Experts



The Challenge

- Securing 100+ dynamically scaling security gateways across regions and clouds.
- Tight development timelines impacted the ability to ensure products' security.
- Securing multi hybrid-cloud with physical and cyber assets resulted in extreme management overhead.

27K employees & \$5B in revenue

1,200+
Physical Stores

100's
Of websites

  
Azure, AWS, and on-prem

8
Regions across the globe

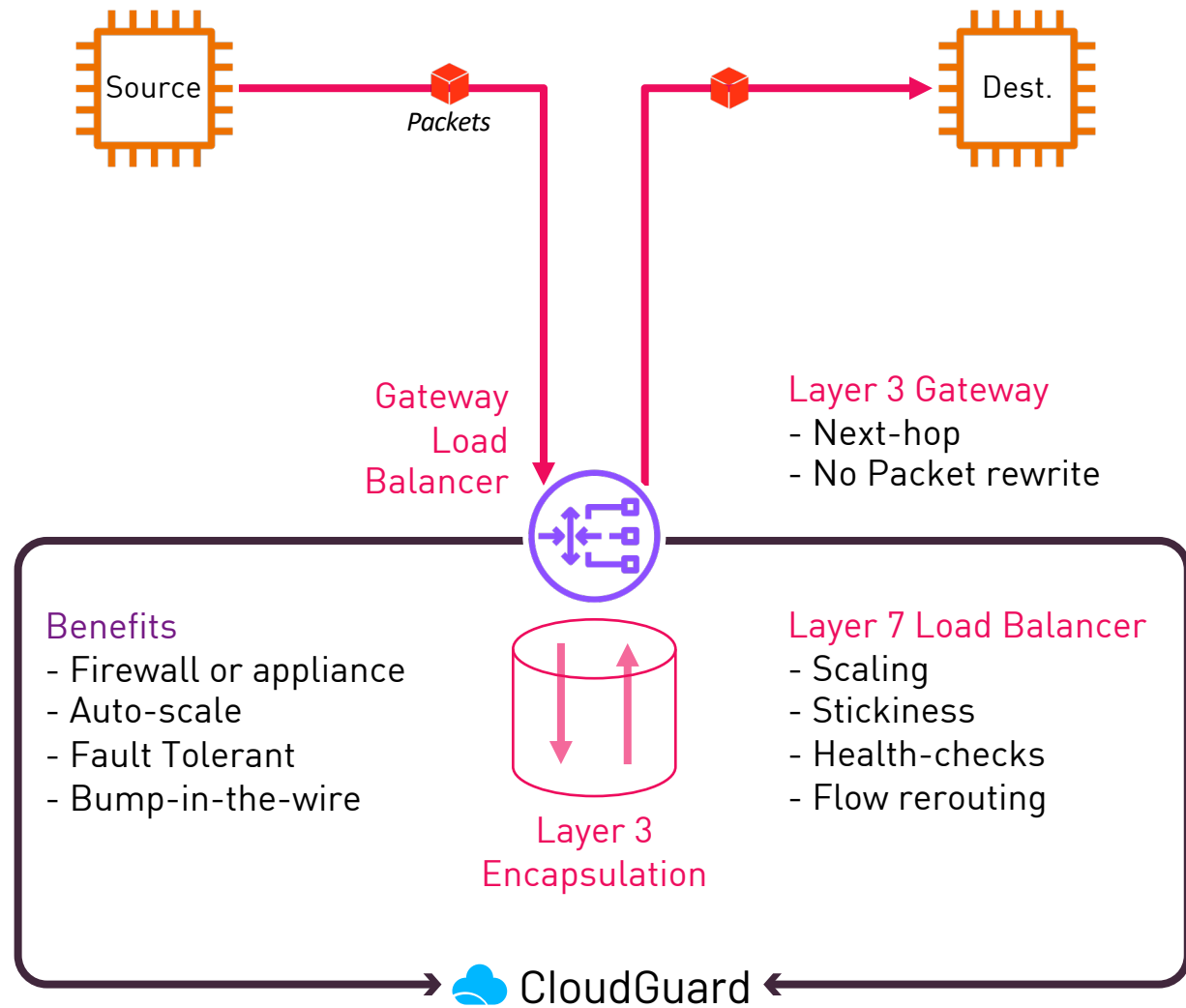
100+
Security Gateways



Solution: CloudGuard Network Security

- Automatically scaling network security inspecting traffic, including DLP, Threat Extraction and Emulation.
- East-West and North-South and Egress traffic protection across environments.
- Eliminated the need to manually monitor and manage resources.

Outcome: Simplified security architecture across all environments with world-class threat prevention.



A very large Swiss financial organization

The Challenge

- Released code was full of secrets.
- Secrets were left in git history after removal.
- Impossible to enforce compliance at code-level.
- Existing code scanner was a bottleneck due to slow scan speed and code base size.
- Existing code scanner sent code to be scanned in the cloud, exposing the company to possible exfiltration.

50K employees & \$3B in revenue

Over 1,600

Developers, Security & Managers

10s of Thousands

Of code repositories in

 GitLab &  Bitbucket

Millions

Of lines of code

Hundreds

Of daily commits

A very large Swiss financial organization

Solution: Code Security

- 2,800 lang-agnostic secret detectors.
- Secret and compliance scans ran on commit, so issues never entered the git.
- Remediation playbooks in IDE.
- Entire code base scanned in minutes.
- Code never left the on-prem env.

Outcome: Clean and compliant code with full CISO control and no risk for 3rd-party code exfiltration.

Pre-commit hook scanning



404

Average daily code scans

68,535

Unique Repos Scanned

657,282

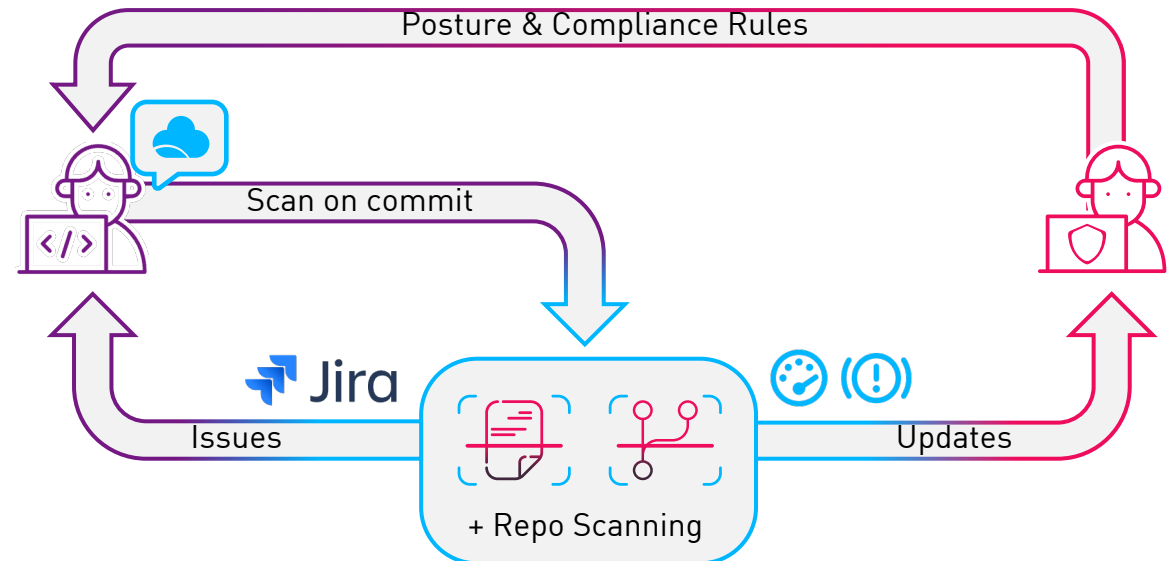
Secrets and Issues Fixed



Decreased R&D Strain



Increased Sec Control



The Challenge

- Enforcing compliance on the US's largest university system with the largest PeopleSoft deployment.
- Repeatable consistency in hybrid multi-cloud environment.
- 9M PII records subject to multiple stringent Federal compliance requirements.
- Increased attacks on higher-ed institutions.



500,000
Students



9,000,000
Student & Staff Records



2 PB
Sensitive Data



HIPAA



FERPA

Family Educational Rights & Privacy Act



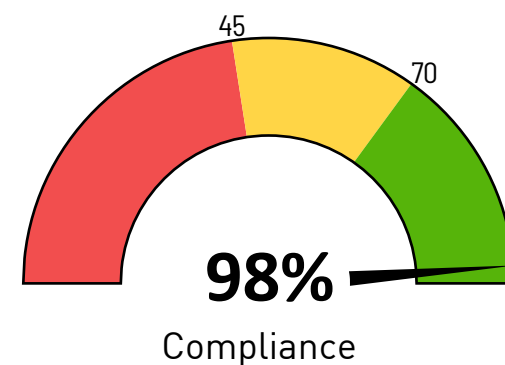
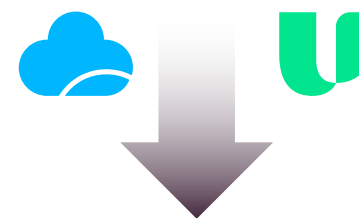
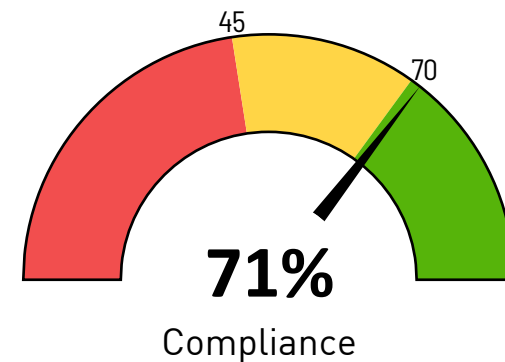
NIST
800-171



Solution: Cloud Security Posture & Workloads Protection

- Automatic assessments with built-in compliance framework scanners.
- Methodical remediation instructions based on prioritization.
- Tailored dashboards for different stakeholders ensure constant improvement and oversight over CSU infra. by Check Point partner - Unisys.

Outcome: CSU achieved 98% compliance in 90 days!



In 90 days!



Secure the Cloud

2024 Roadmap



Network



Data



Identity



Workloads



Code

Network Security

Web Application Firewall

CNAPP

CloudGuard Network Security

Integrating with Cloud Native WAN Services

RELEASED
IN 2023

**Integrating to
Azure vWAN**



RELEASED
IN 2023

**Integrating to
AWS
CloudWAN**



COMING IN
2024

**Integrating To
GCP Packet
Intercept**

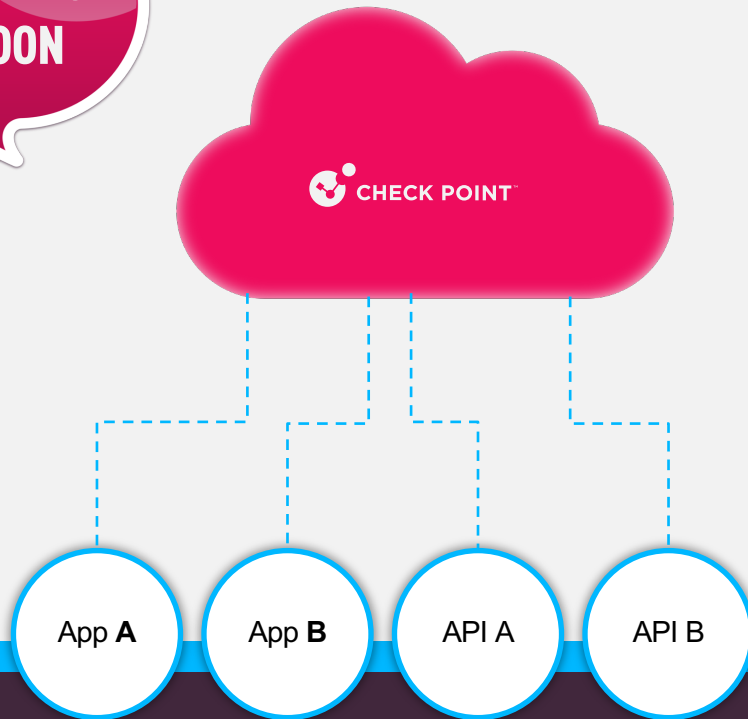


CLOUD NETWORK SECURITY & SEGMENTATION
IS NOW EASY THAN EVER

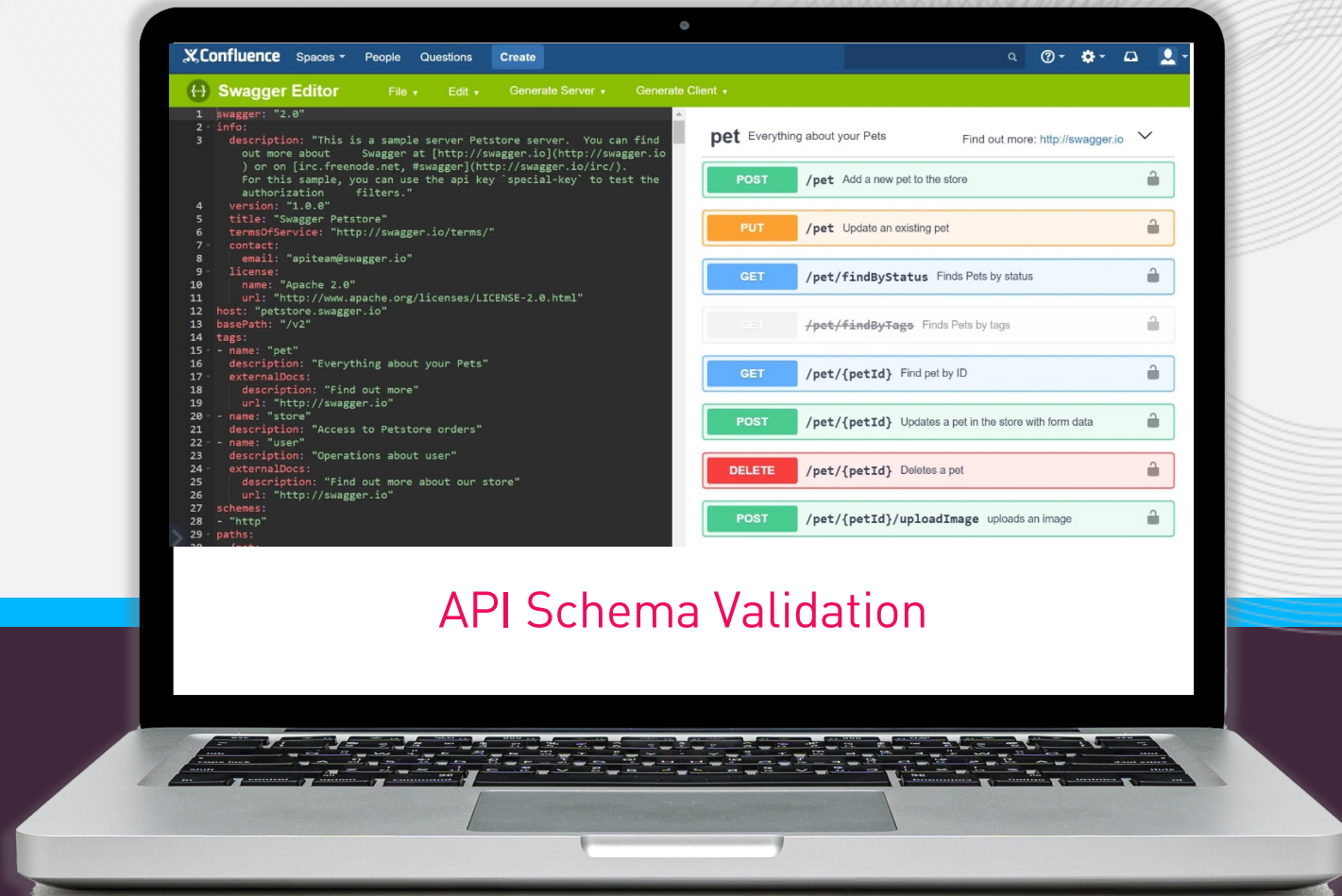
CloudGuard WAF

COMING
SOON

WAF as a Service



API Discovery



API Schema Validation

CloudGuard CNAPP with Prevention

Block Your Most Critical Attack Paths Based on Context

RELEASED
IN 2023

NEW

Uncover Exposures



Exposed
Secrets



Over permissive
identities



Vulnerabilities



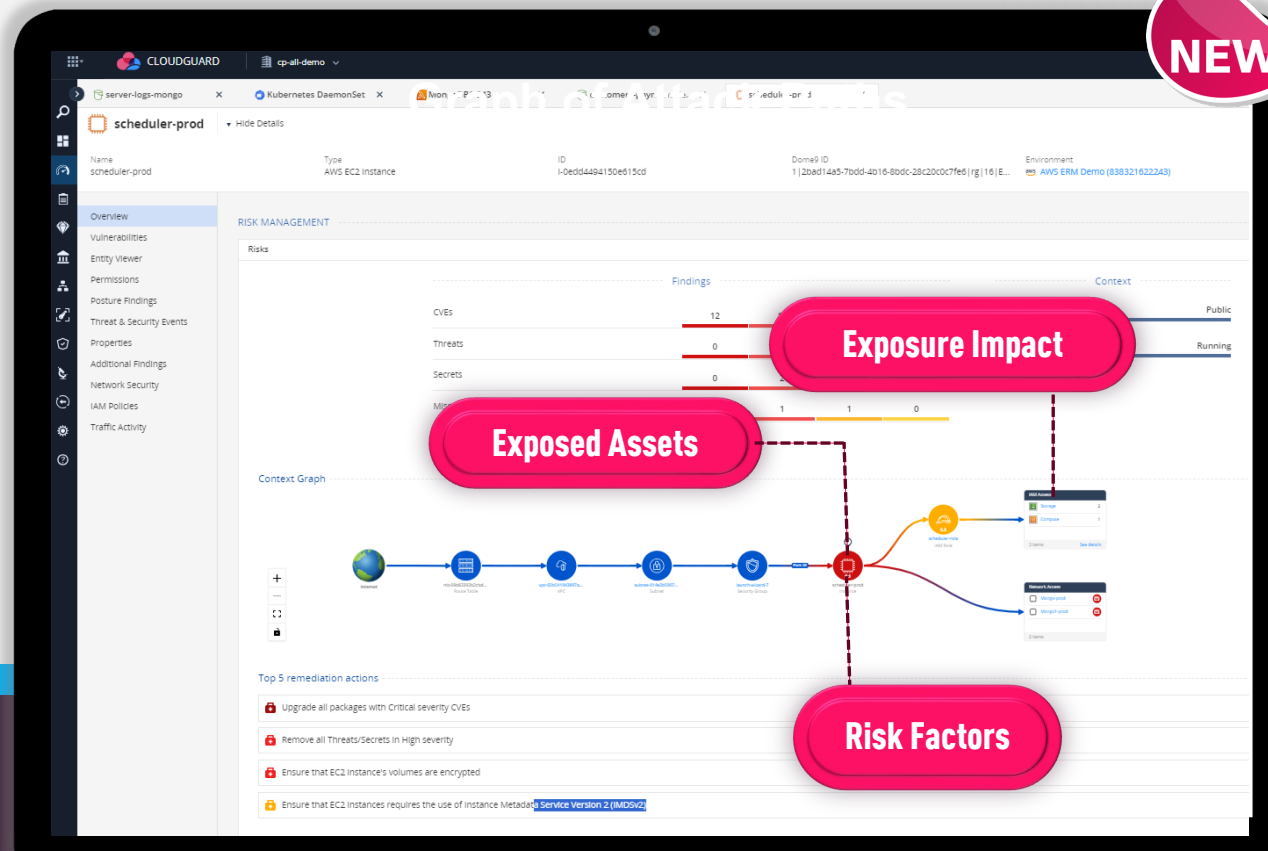
Sensitive
Data



Exposed
Assets



Misconfiguration



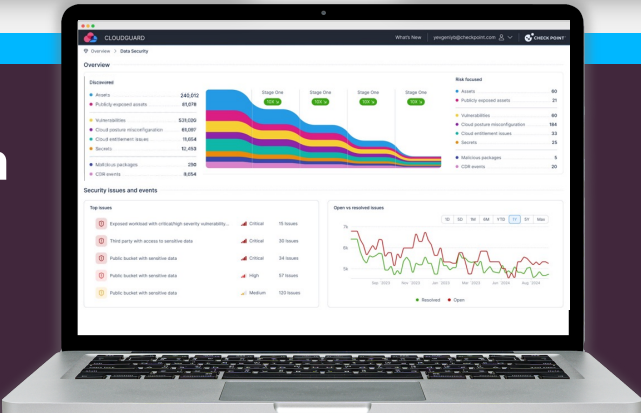
Connecting CNAPP with Network and WAF Prevention

COMING
IN 2024

Discovered	
● Assets	240,012
● Publicly exposed assets	81,078
<hr/>	
● Vulnerabilities	531,020
● Cloud posture misconfiguration	61,097
● Cloud entitlement issues	11,654
● Secrets	12,453
<hr/>	
● Malicious packages	250
● CDR events	8,654

Risk focused	
● Assets	60
● Publicly exposed assets	21
<hr/>	
● Vulnerabilities	60
● Cloud posture misconfiguration	184
● Cloud entitlement issues	33
● Secrets	25
<hr/>	
● Malicious packages	5
● CDR events	20

CNAPP Without Prevention
Thousands of Risk Alerts



CNAPP With Prevention
Reduces 70% of the Critical Risks

Network Security and WAF



Network Security

- ▶ Azure - Virtual WAN - Direct Ingress, TF / ARM Template support
- ▶ Self updateable Controller
- ▶ AWS - Cloud WAN Service Integration
- ▶ GCP - GCP Packet Intercept
- ▶ Azure - S2S VPN, SD-WAN
- ▶ AWS - IPv6 for GWLB

WAF

- ▶ WAF as a Service EA
- ▶ API Discovery
- ▶ WAF as a Service GA
- ▶ Auto Rate Limit (self learning)
- ▶ User Challenge on suspicious activities



Q1 2024
(Delivered)



Q2 2024



H2 2024

ERM

- ▶ Toxic Combinations (Delivered)
- ▶ WAF-aware Residual Risk
- ▶ CGNS-aware Residual Risk
- ▶ Extending Toxic Combinations

Platform and CSPM

- ▶ Executive Reporting (Delivered – Preview)
- ▶ Org Onboarding and Automated Account Discovery
- ▶ Copilot Integration



H1 2024



H2 2024

DSPM

- ▶ Purview integration (Delivered)
- ▶ DSPM dashboard
- ▶ Sentra DSPM integration

CDR

- ▶ MITRE ATT&CK event mapping and event visualization (Preview – Delivered)

CIEM

- ▶ Azure – support additional permission types and service accounts for Least privilege suggestion
- ▶ Azure – Identify inactive users/roles
- ▶ XDR Integration: threat hunting, investigation, incident response, copilot



H1 2024



H2 2024

Code Security and Code-to-Cloud

- CVE Explorer (Delivered)
- SBOM Explorer
- Drift detection
- Ownership resolution

Workload Protection

- Windows VM Agentless Scanning (Delivered)
- K8S Windows Image Scanning
- File Integrity Monitoring (Agentless)
- CIS Benchmark for VMs (Agentless VM Hardening Verification)



H1 2024

H2 2024