



ACHIEVING CLOUD SECURITY WITH CONFIDENCE ACROSS CLOUDS

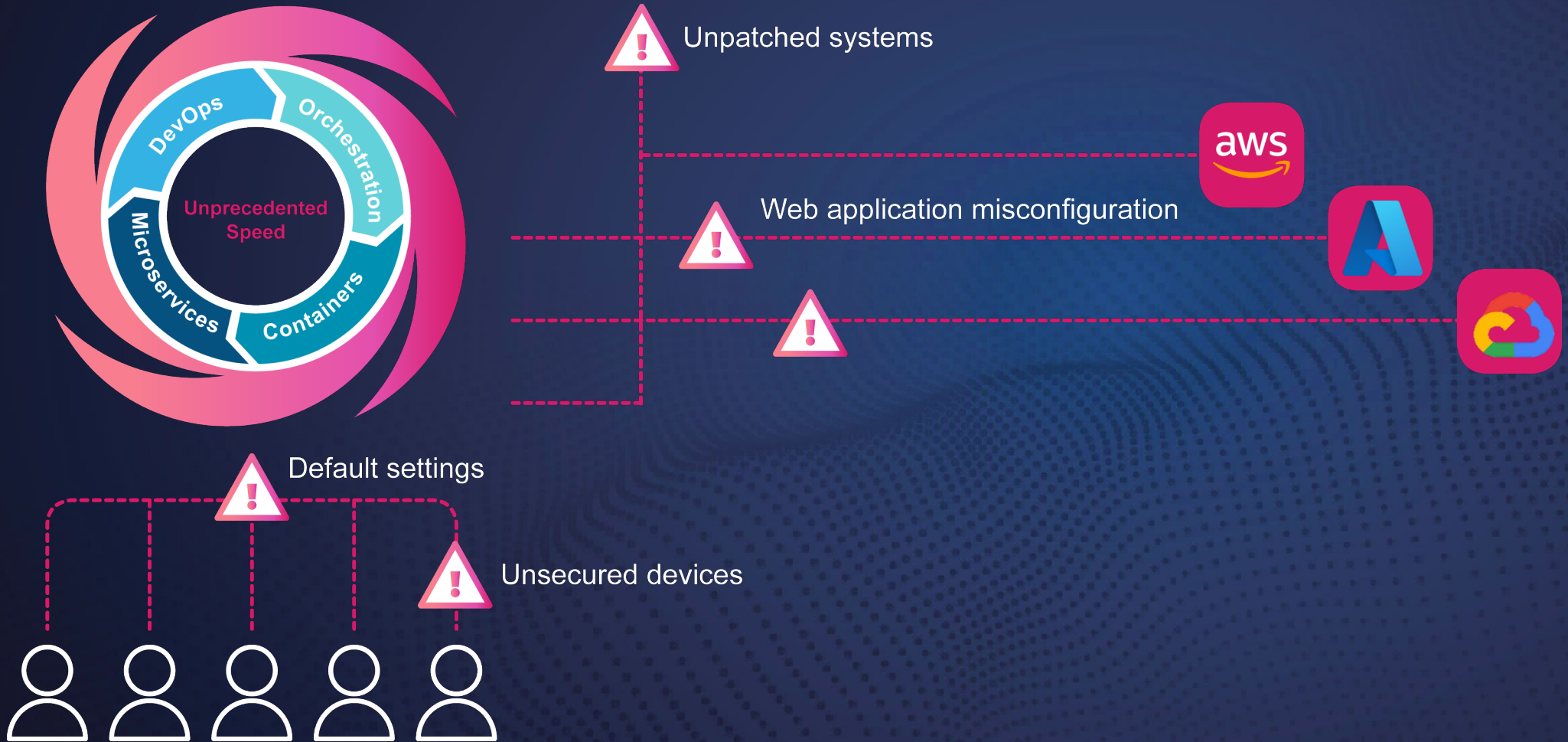
Balder Borup
Security Engineer





Check Point[®]
SOFTWARE TECHNOLOGIES LTD

Migrating applications to the Cloud



Mistakes create misconfigurations

EXCESSIVE PERMISSIONS

Thousands of IAM permissions to maintain

UNATTENDED SECURITY ISSUES

Due to insufficient time and resources

LACK OF VISIBILITY, SECURITY GAPS

Multi-cloud = multi-complexity



Misconfigurations generate risk

An internal code repo used by New York State's IT office was exposed online

Zack Whittaker @zackwhittaker / 11:00 AM PDT • June 24, 2021

Featured Article

Peloton's leaky API let anyone grab riders' private account data

But the company won't say if it has evidence of malicious exploitation

Zack Whittaker @zackwhittaker / 4:00 AM PDT • May 5, 2021

The Register®



BlueBleed: Microsoft customer data leak claimed to be 'one of the largest' in years

SOCRadar says sensitive info from 150,000 orgs was exposed, Redmond disputes findings

[Jeff Burt](#)

Thu 20 Oct 2022 // 15:00 UTC

WHAT IS BLUEBLEED?

SOCRadar detected sensitive information of 150 000 companies leaked by 6 large public storage buckets

LEVEL OF DATA

Customer emails, SOW contracts, product offers, invoices, signed documents and customer asset documents

BlueBleed

ONWARD, UPWARD

One bucket contained 2.4 TB of data containing sensitive information belonging to Microsoft due to an **insecure public Azure Blob Storage**

The answer of the cyber security industry

Posture
Management

Workload
Protection

Threat
Intelligence

Vulnerability
Management

CIEM

Pipeline
Security

Cloud-native Application Protection Platform (CNAPP)

More visibility != more security?

Today's Cloud Posture Management tools focus on misconfigurations



*“More alerts create more noise which generates an **alert fatigue**”*



It's time to put your cloud security in context

So how can we do better?

More Context, Better Security, Faster

NEW!

Effective Risk
Management & Auto-Remediation

Posture
Management

Workload
Protection

Threat
Intelligence

Vulnerability
Management

CIEM

Pipeline
Security

Cloud-native Application
Protection Platform (CNAPP)

Misconfigurations need context to identify risks



Security Parameters
Misconfigurations
Vulnerabilities
Malware



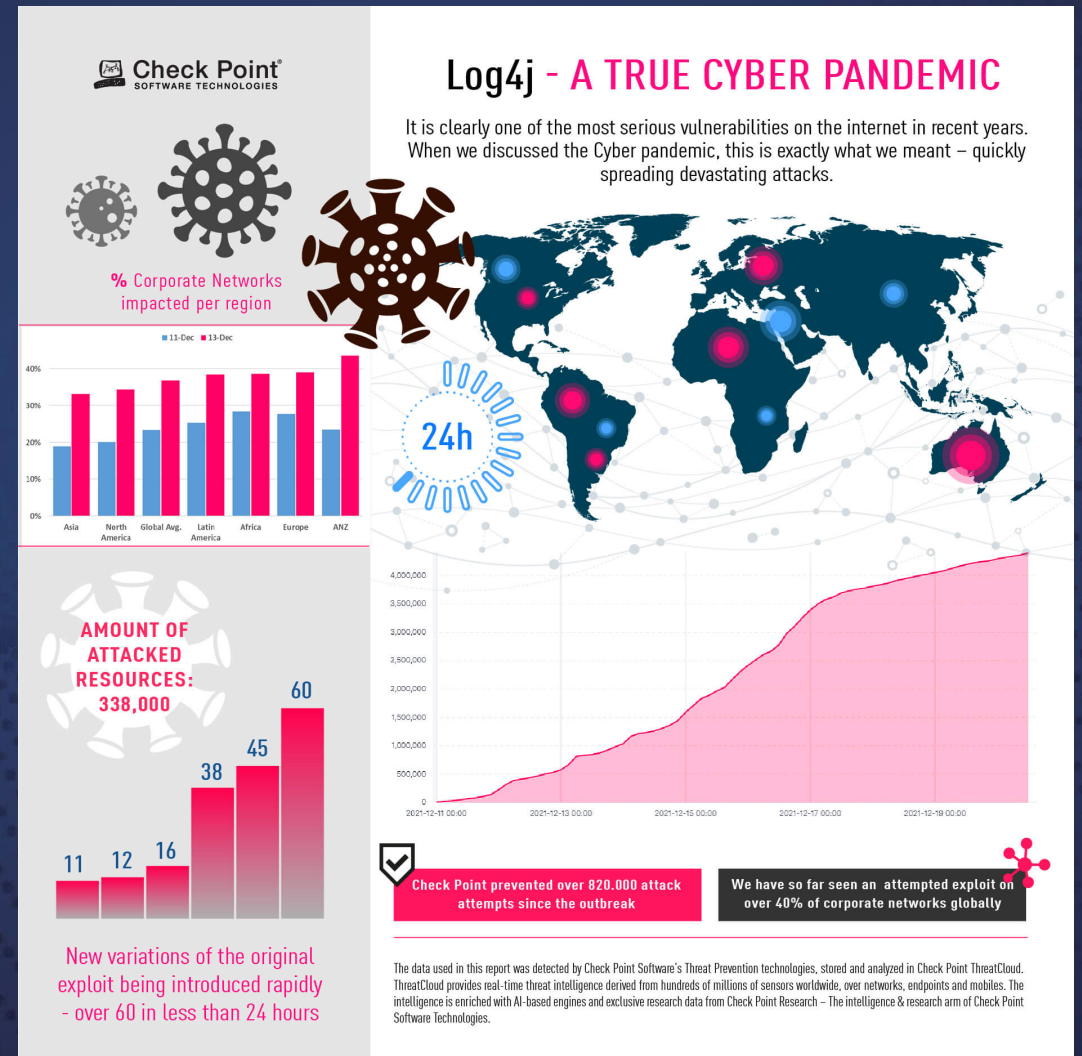
Contextual Parameters
Network Exposure
Runtime Protection Status
Entity Status



Impact Parameters
IAM Risk
Business Priorities

Log4j use case – a true cyber pandemic

- Most popular java log library. over 400,000 GitHub downloads
- Used by a vast number of companies worldwide
- Easily exploited - Remote Code Execution (RCE)
- Started: December 10th 2021
- CVE severity score: 10.0 / 10.0



How to mitigate the next “cyber pandemic” in the cloud?

Find out if you are vulnerable

Vulnerability Management

- VMs
- Container images
- Serverless code

The screenshot displays the CloudGuard interface with a sidebar on the left containing navigation options: OVERVIEW, EVENTS, ASSETS (highlighted), POSTURE MANAGEMENT, NETWORK SECURITY, RISK MANAGEMENT, CIEM, WORKLOAD PROTECTION, and INTELLIGENCE. The main content area shows a 'Protected Assets' view for 'AWS EC2 Instance' type, displaying 223 of 1,968 results. A table lists assets with columns for Risk, Name, Platform, and a 'Findings' section. A circular callout provides a detailed view of the 'Findings' and 'Risks' for a specific asset, showing counts for various CVEs.

Risk	Name	Platf...	Findings	CVEs
9.8	Hong Kong Ins	AWS	0 0 0 0	13 176 203 35
9.8	Hong Kong Ins2	AWS	0 0 0 0	13 176 202 34
8.6	EMR NAT	AWS	0 0 0 0	21 50 63 2
7.8	New ins after share	AWS	0 79 0 0	0 0 0 0
7.8	daniel1-linux	AWS	0 79 0 0	0 0 0 0
6.2	Aviram	AWS	0 102 0 0	0 0 0 0
6.2	Inspector	AWS	0 102 0 0	0 0 0 0
6.2	New Agent	AWS	0 0 0 0	0 0 0 0
6.2	Public	AWS	0 102 0 0	0 102 0 0
6.2	CrossAccountTestIdan	AWS	0 102 0 0	0 102 0 0
6.2	Ireland instance	AWS	0 102 0 0	0 102 0 0
6.2	Mumbai Instance	AWS	0 102 0 0	0 102 0 0
5.3	public zone2	AWS	0 2 0 0	0 2 0 0
5.3	i-0b203a5bb63826134	AWS	0 2 0 0	0 2 0 0
5.2	Public-Instance	AWS	0 1 0 0	0 1 0 0
5.2	public-instance-1	AWS	0 1 0 0	0 1 0 0
5.2	windows-bastion	AWS	0 1 0 0	0 1 0 0
5.2	instance1	AWS	0 1 0 0	0 1 0 0
5.2	i-0db6d58fb28c6f87a	AWS	0 1 0 0	0 1 0 0
5.2	DB1	AWS	0 1 0 0	0 1 0 0

Understand the context

Get answers to the questions

- Is it running?
- Publicly exposed?
- Runtime Protection enabled?
- Protected by the WAF?

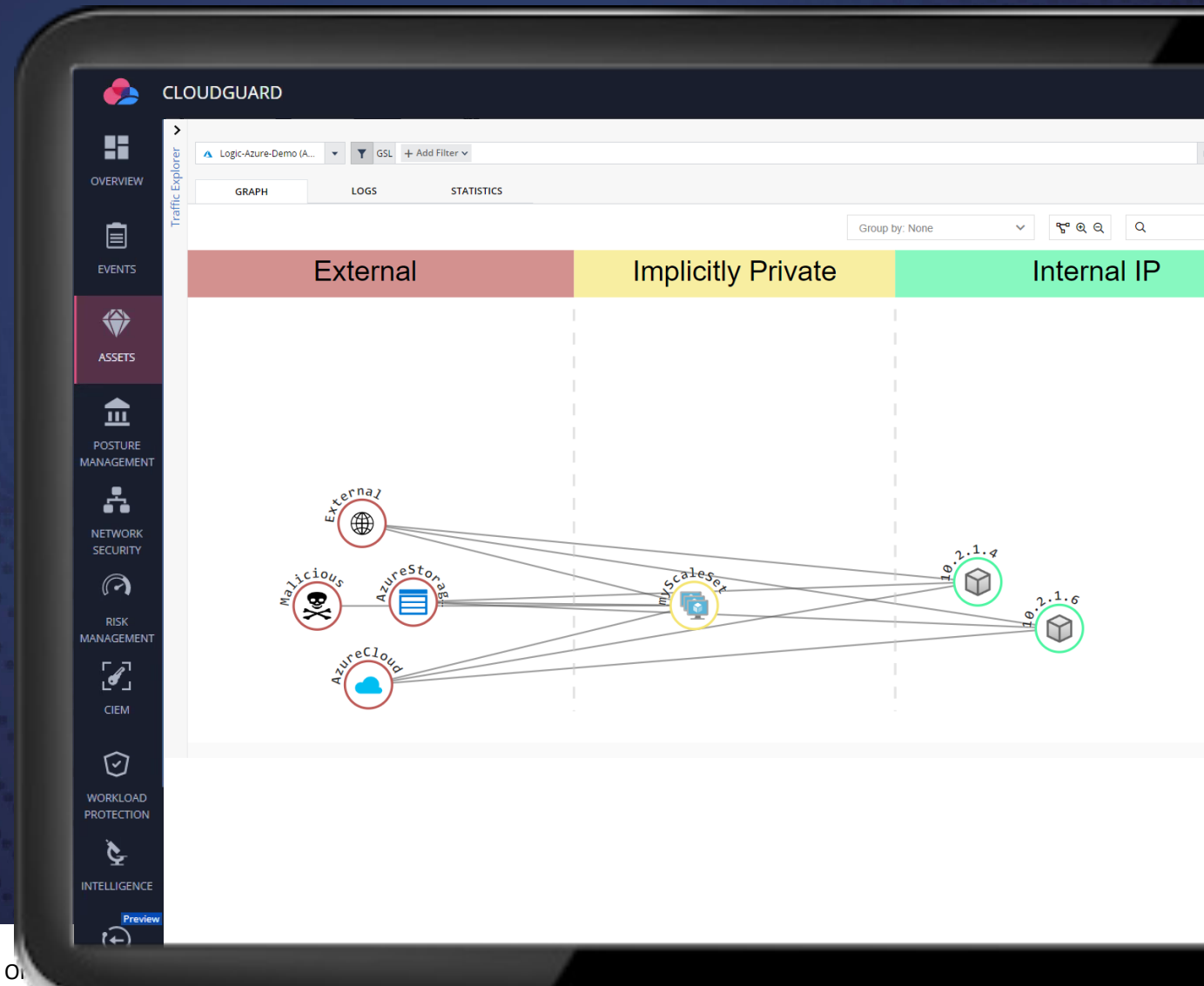
The screenshot displays the CloudGuard interface with a table of Protected Assets. The table has the following columns: Risk, Entity, Is Running, Network Exposure, and Type. A circular callout highlights a row with the following data:

Risk	Entity	Is Running	Network Exposure	Type
9.1	i-0db6d58fb28c6f87a	●	Public	AWS EC2 Instance
9.1	stanislavz-consec-ci-d	●	Public	AWS EC2 Instance
9.1	stanislavz-consec-ci-de8a5f4	●	Public	AWS EC2 Instance
9.1	stanislavz-consec-ci-den5f4	●	Public	AWS EC2 Instance
9.1	TVtest-20210422 (i-01dbc7	●	Public	AWS EC2 Instance
9.1	i-002f26409fa1e9c5d	●	Public	AWS EC2 Instance
9.1	123 (i-0144c62dc29cb751f)	●	Public	AWS EC2 Instance
9.0	Web4 (i-0174a5ae1f1082f08)	●	Public	AWS EC2 Instance
9.0	Web3 (i-02706bfd0844feb98)	●	Public	AWS EC2 Instance
9.0	Web1 (i-04deb2dbec27e5167)	●	Public	AWS EC2 Instance
9.0	Web2 (i-07ab8d65ef9d99754)	●	Public	AWS EC2 Instance
9.0	instance1 (i-0f0cca14b82d962eb)	●	Public	AWS EC2 Instance
9.0	DB1 (i-c94ed8c4)	●	Public	AWS EC2 Instance
9.0	RabbitMQ1 (i-cb4ed8c6)	●	Public	AWS EC2 Instance
9.0	WebServer2 (i-cc4ed8c1)	●	Public	AWS EC2 Instance

Understand the impact

Use CIEM and Intelligence to analyze

- Who has access to what?
- Excessive permissions?
- Any suspicious behavior?



Understand the impact

Correlate with business priorities

Categorize assets based on

- Tags
- Cloud account
- Asset name

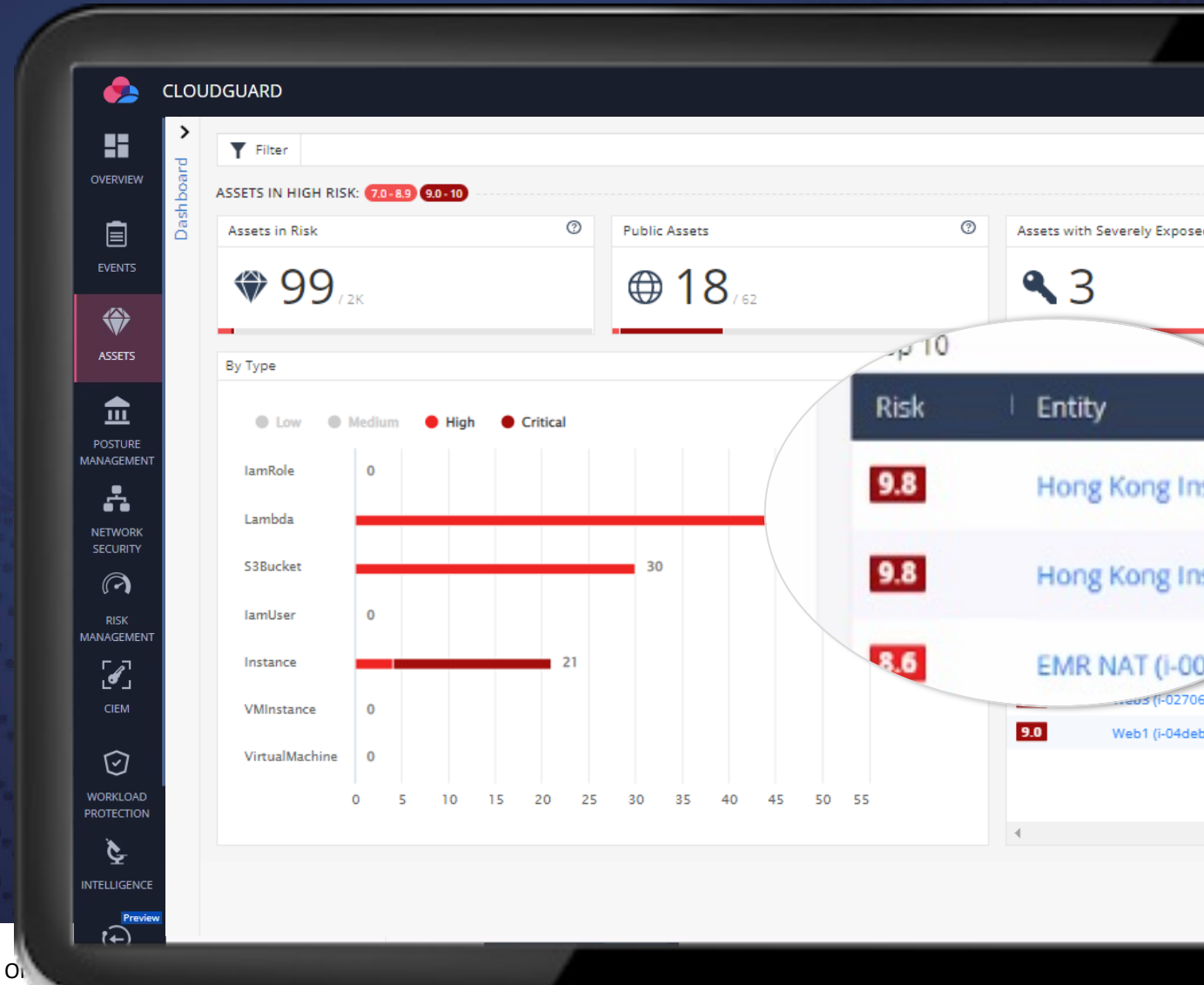
The screenshot displays the CloudGuard interface for 'Protected Assets'. A filter for 'Platform: Azure' is applied, showing 76 of 2,471 results. A table of assets is shown, with a magnified view of the first five rows. The table columns are Risk, Business Priority, Entity, Type, and Environment.

Risk	Business Priority	Entity	Type	Environment
6.9	Crown Jewel	moshi-public-vm	Azure Virtual Machine	Azure prod (4aa7abc8-...)
6.4	High Importance	noNSGtest	Azure Virtual Machine	Azure prod (4aa7abc8-...)
6.3	High Importance	galit-test-linux	Azure Virtual Machine	Azure prod (4aa7abc8-...)
6.3	High Importance	vm-canada-east-test	Azure Virtual Machine	Azure prod (4aa7abc8-...)
6.3	High Importance	TVtestVM01	Azure Virtual Machine	Azure prod (4aa7abc8-...)

Final scoring to prioritize risk

Focus on the 1% of risks that matter

- Apply contextual AI and risk scoring
- Reduce attack surface with focus on the highest priority risks
- Auto-Remediate using the “minimal effective dose” principle



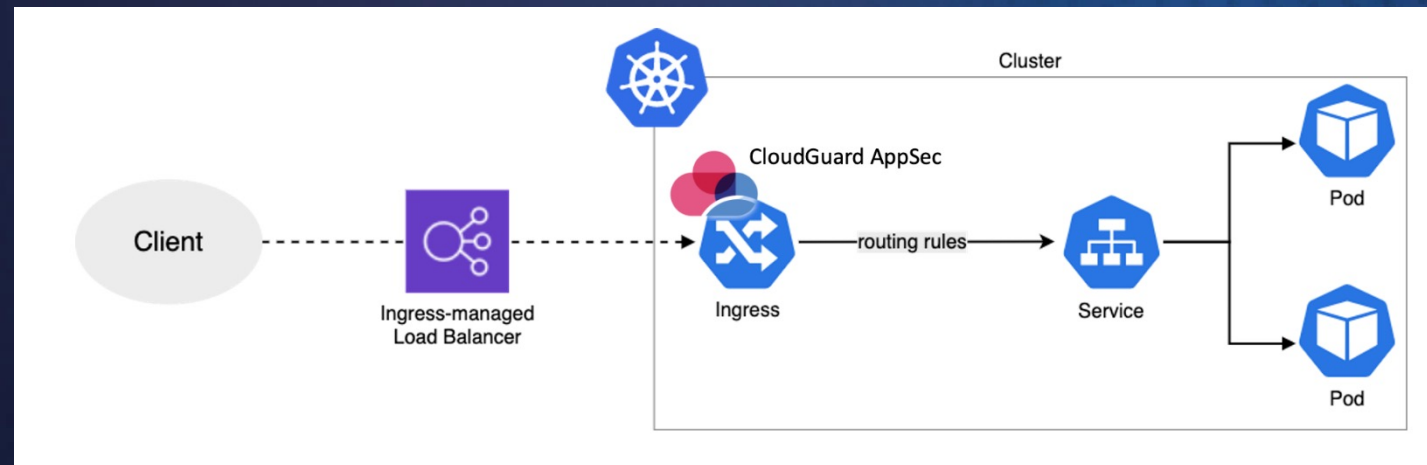
What other preventive measures can I take?

❖ Use runtime protection for containers and serverless

<input type="checkbox"/>	Entity	Environment	Type ↑	Runtime Protection	Protection Mode
<input type="checkbox"/>	azurefunctiontest-chris	Christopher Dome9 demo 01 (d039a90b-ebd4-4439-b548-ecac32978)	⚡ Azure Function App		
<input type="checkbox"/>	MyNewLambda-Elimo	Logic-Azure-Demo (cc9f6b3f-a7b2-45a5-b259-be9a765aed96)	⚡ Azure Function App		
<input type="checkbox"/>	WinPrinter	Logic-Azure-Demo (cc9f6b3f-a7b2-45a5-b259-be9a765aed96)	⚡ Azure Function App		
<input type="checkbox"/>	ServerlessSlackChatBot	SevelessDemo (bf449c98-693c-4316-9da6-079f0851c458)	⚡ Azure Function App	🛡 Protected	🛡 Prevent
<input type="checkbox"/>	CovidStatsDemo	SevelessDemo (bf449c98-693c-4316-9da6-079f0851c458)	⚡ Azure Function App	🛡 Protected	👁 Detect
<input type="checkbox"/>	CloudguardServerlessDemo	SevelessDemo (bf449c98-693c-4316-9da6-079f0851c458)	⚡ Azure Function App	🛡 Protected	🛡 Prevent
<input type="checkbox"/>	CloudguardScanScheduler	SevelessDemo (bf449c98-693c-4316-9da6-079f0851c458)	⚡ Azure Function App		
<input type="checkbox"/>	ItayFunctionApp	SevelessDemo (bf449c98-693c-4316-9da6-079f0851c458)	⚡ Azure Function App	🛡 Protected	👁 Detect

What other preventive measures can I take?

- ❖ Apply WebApp & API security with pre-emptive protection against zero-days













What other preventive measures can I take?

- ❖ Implement security at the build phase (shift security left)

Code

Protect your CI/CD pipelines

Monitor private & public repositories in your CI

 GitLab CI/CD	 GitHub Action	 Travis	 Jenkins	 CircleCI
 AWS CodeBuild	 Azure DevOps Pipeline	 Bitbucket Pipeline	 Google Cloud Build	 Other CI Systems

Concluding thoughts

Use context to identify risks

Integrated platform approach provides complete visibility for more context



Focus on the 1% risks that matter

Prioritize based on business critical risk



Real-time prevention where you can

Implement technologies that prevent attacks



CloudGuard



Thank you!