



Check Point®
SOFTWARE TECHNOLOGIES LTD

SECURING THE CLOUD WITH CHECK POINT CLOUDGUARD

Richard Flanders | Head of Cloud SecurityUK

WELCOME TO THE FUTURE OF
CYBER SECURITY

POWERED BY  **CHECK POINT
INFINITY**

CLOUD • MOBILE • THREAT PREVENTION

Don't Envy the CISO



Check Point
SOFTWARE TECHNOLOGIES LTD

COMPUTERWORLD
FROM IDG

Jan 19, 2017 Attackers start wiping data from CouchDB and Hadoop databases

eSecurity Planet



Jul 12 2017 Cloud Security Failure: Millions of Wrestling Fans' Personal Data Exposed



Jun 1 2017 Booz Allen Hamilton leaves 60,000 unsecured DOD files on AWS server

Forbes

Dec 19, 2017 120 Million American Households Exposed In 'Massive' ConsumerView Database Leak

DARK
Reading

Feb 16 2017 The Era of Data-Jacking is Here. Are You Ready?

threat **post**

Jul 12 2017 Misconfigured Amazon Storage Exposes 14 Million Verizon Customer Records



siliconANGLE

Apr 3 2018 37M Panera Bread customer records found to be exposed to all and sundry in the cloud

THE
HILL

Jul 17 2017 Dow Jones customer data exposed in cloud error

The diagram illustrates a VPC architecture for a Kubernetes cluster. It is divided into two main subnets:

- External subnet: 10.0.0.0/24**
 - Default route: Internet GW
 - Gateway Cluster**
 - `eth0`
 - Private IP : 10.0.0.20
 - Secondary IP (Cluster IP) : 10.0.0.10
 - Secondary IP (Web) : 10.0.0.40
- Internal & sync subnet: 10.0.1.0/24**
 - Default route: Member A /eth1
 - Cluster Member A Active**
 - `eth1`
 - Private IP : 10.0.1.20
 - Secondary IP (Cluster IP) : 10.0.1.10

Instances are represented by orange squares in the internal subnet. Client Apps connect to the Gateway Cluster via an Internet Gateway. The architecture also shows a CI/CD pipeline using Azure Pipelines, Helm, and Docker to deploy to a Container registry.

The diagram illustrates a cloud-native architecture for a data-driven application, divided into two main sections: Front end and Back-end services.

Front end: Client Apps connect to an Azure load balancer, which routes traffic to an Ingress controller (N) within a Kubernetes cluster. The Ingress controller is part of a Namespace.

Back-end services: The Ingress controller routes traffic to Back-end services, which are deployed as Pods. These Pods interact with an External data store (SQL) and an External data source (RDS instance). The Pods are managed by a Pod autoscaling mechanism.

CI/CD and DevOps: CI/CD (Azure Pipelines) manages the deployment of the application. It uses Helm for Kubernetes deployments and Docker for container management. The process involves pushing Docker images to a Container registry and pulling them back for updates. DevOps (represented by a person icon) manages the overall system.

Data Processing Pipeline: Source data is processed through a Data staging layer (AWS Lambda) to an Input validation / conversion layer (AWS Lambda), and finally to an Input tracking layer (AWS Lambda). The data is then stored in an External data store (SQL) and an External data source (RDS instance).

The diagram illustrates a data pipeline architecture for Amazon Redshift. It starts with 'Source data' (Department / Franchise) being loaded into a 'Data staging layer' (S3 bucket). The data then flows through an 'Input validation / conversion layer' (AWS Lambda), another 'Data staging layer' (S3 bucket), an 'Input tracking layer' (AWS Lambda), an 'Aggr Job Submission Layer' (AWS Lambda), and an 'Aggr job monitoring layer' (AWS Lambda). The pipeline then uses an 'EMR cluster with Spark' for 'Aggregation and load', finally loading data into 'Amazon Redshift'. An 'RDS db instance' is connected to the 'Aggr job monitoring layer'. The entire pipeline is managed by 'Identity and Access Management (IAM)' and 'Monitoring and logging (CloudWatch)'.

Server-less

Public Cloud Further Changes the Game

- Cloud-native: Everything as a service
 - Load balancers, Data and DBs, File systems, Storage, Identity, etc.
- Elastic & Ephemeral Infrastructure
 - Auto Scaling models with Short-lived Entities
- Multi-Cloud makes it even more Complex

Watch “The Perimeter is Dead. Long Live the Perimeters!”

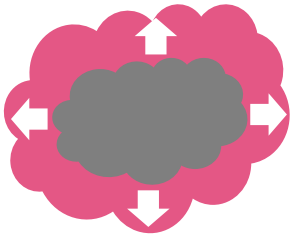
<https://www.youtube.com/watch?v=nvVI3azDmOQ>

Cloud Security Key Challenges



Check Point[®]
SOFTWARE TECHNOLOGIES LTD

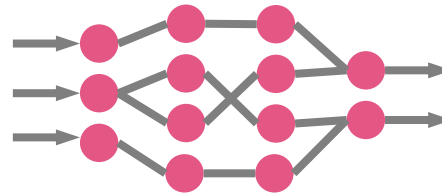
Cloud environments are dynamic



Cloud Security Should....

Prevent fatal misconfigurations, enforce strict security posture

Cloud applications have evolved



Cloud Security Should....

Actively protect workloads and cloud services from modern attacks

Security should not slow down cloud innovation



Cloud Security Should....

Enable the cloud to stay agile and elastic



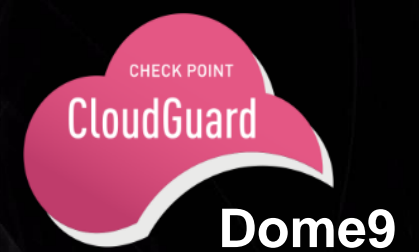
Check Point CloudGuard IaaS

Protection for private and public cloud networks

- Advanced threat prevention
- Next Gen Firewall (NGFW)
- Application and data security
- Forensic analysis
- Dynamic policies
- Comprehensive Networking



Introducing Check Point CloudGuard Dome9



Security for the Public Cloud Native Controls
Delivered as a Service

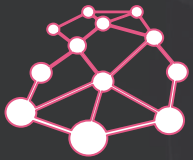


Microsoft
Azure



Google Cloud Platform

Introducing Check Point CloudGuard Dome9



Network
Security



Continuous
Compliance



Privileged
Identity
Protection



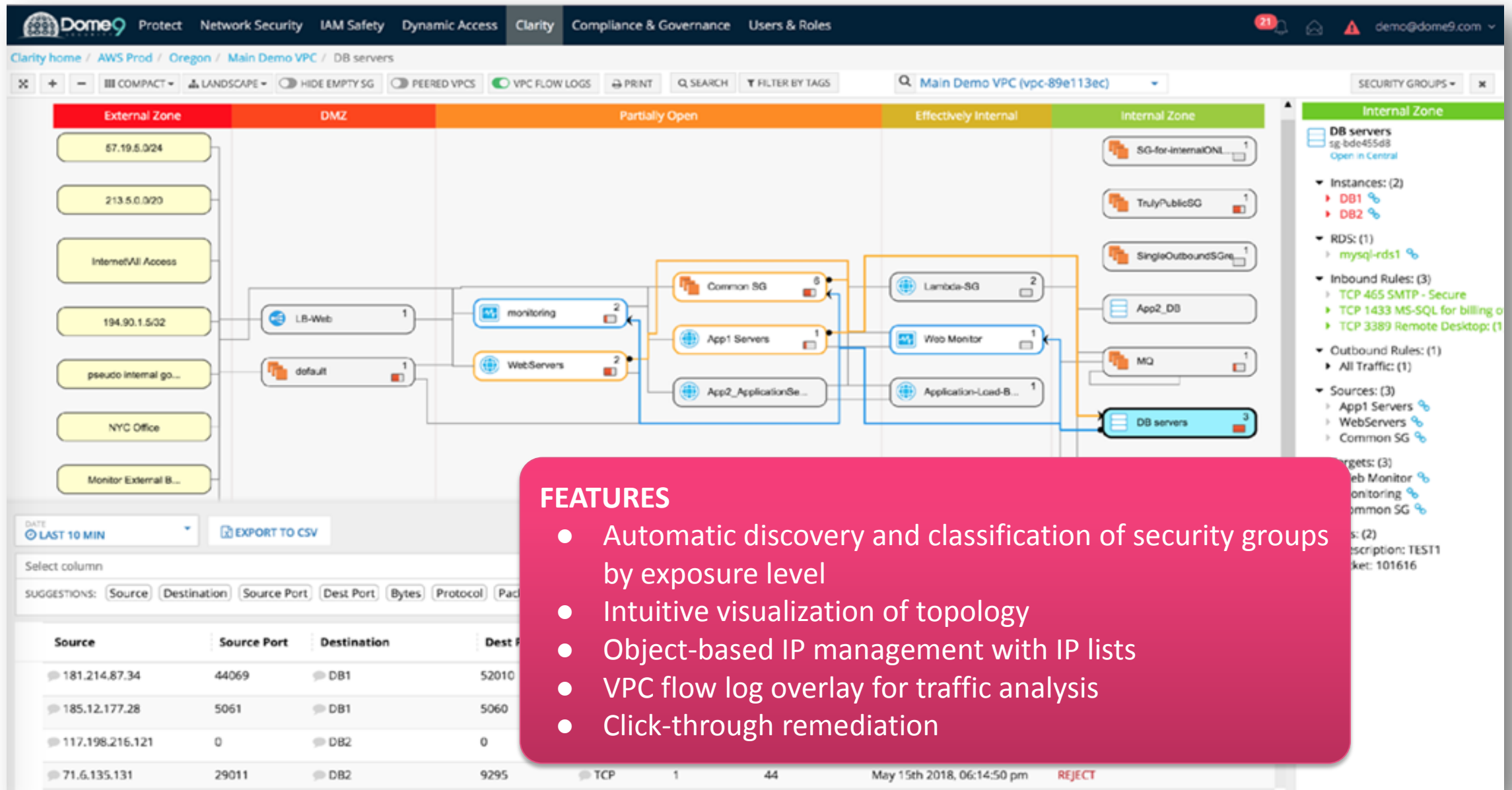
Cloud Threat
Intelligence

Protecting your Cloud workloads and services is no longer complex. Get full security visibility & control with continuous compliance

Complete Network & Security Visibility



Check Point
SOFTWARE TECHNOLOGIES LTD



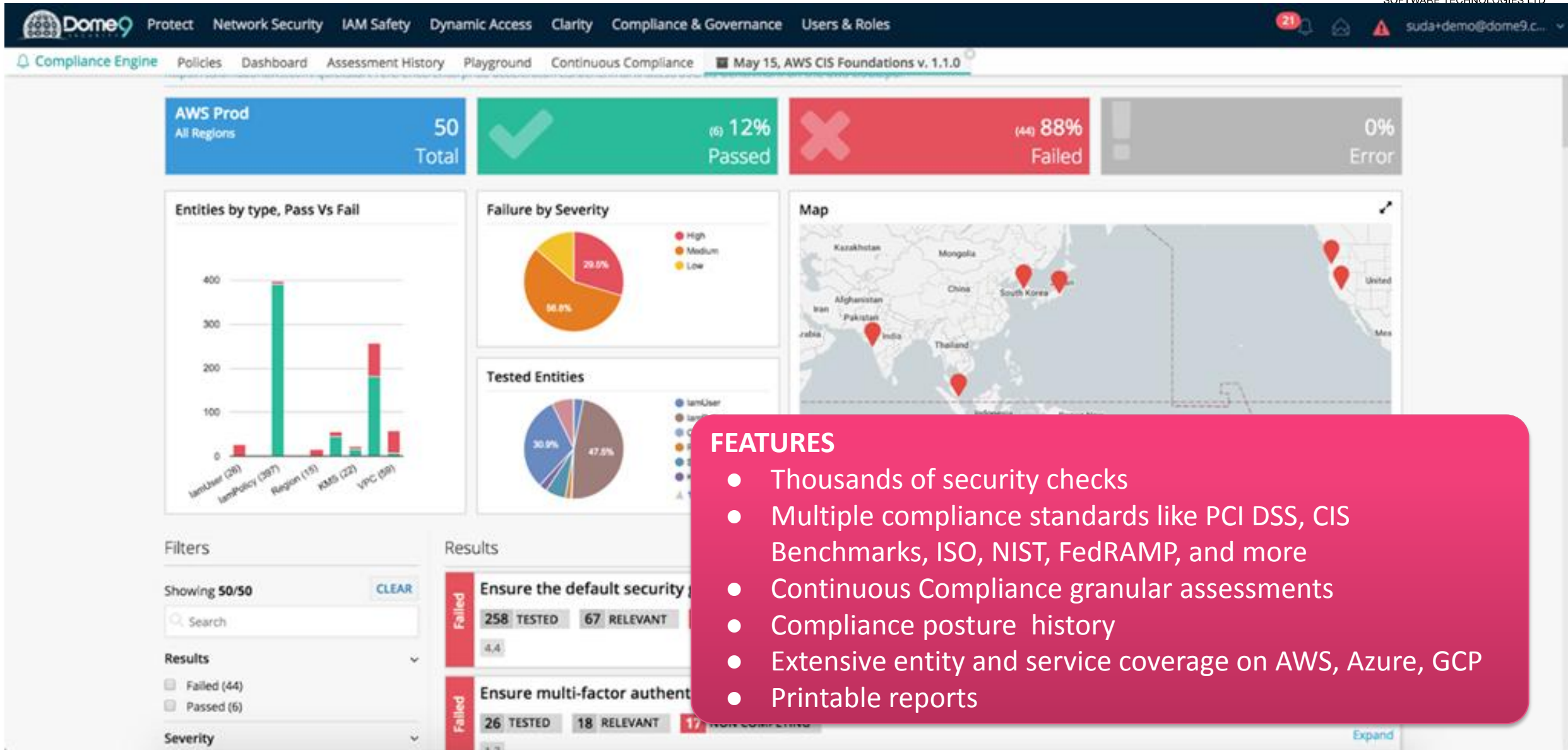
FEATURES

- Automatic discovery and classification of security groups by exposure level
- Intuitive visualization of topology
- Object-based IP management with IP lists
- VPC flow log overlay for traffic analysis
- Click-through remediation

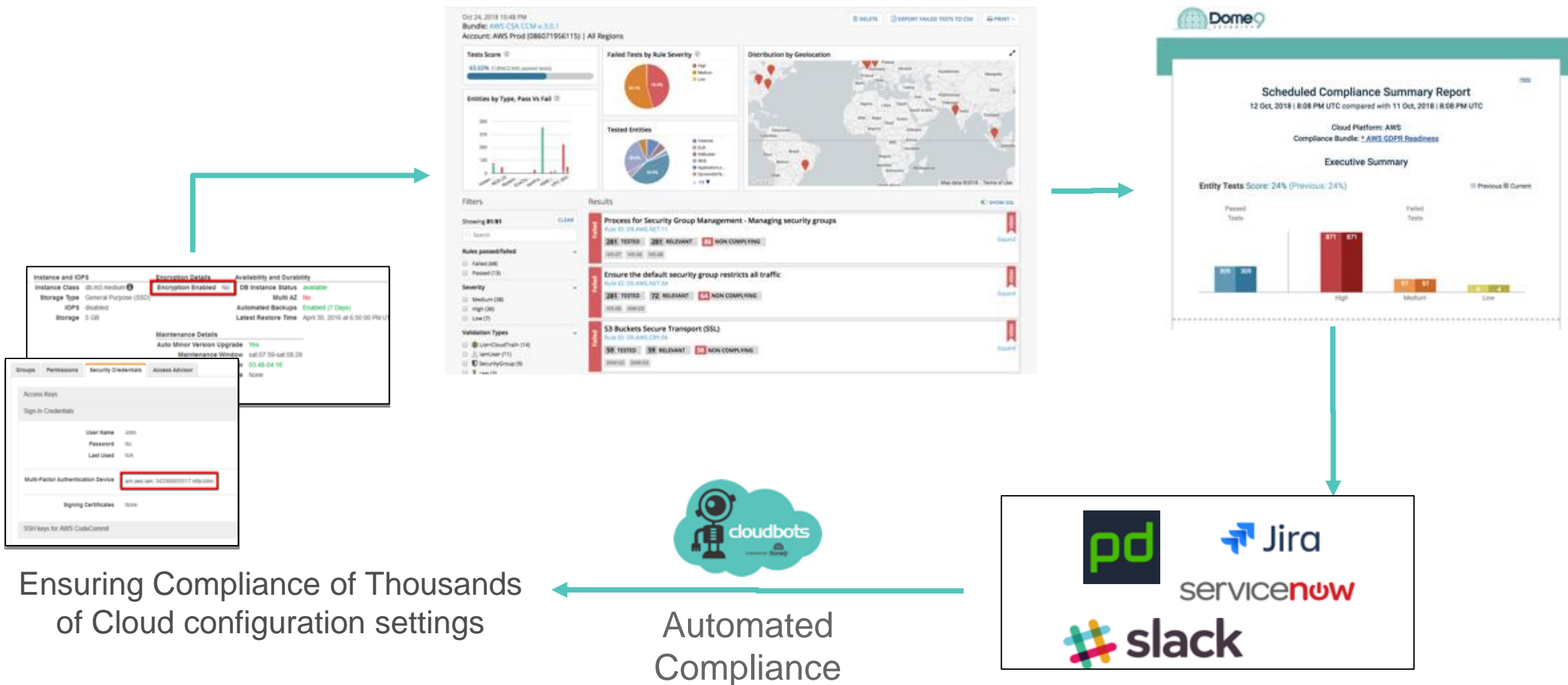
Cloud Compliance and Best Practices



Check Point
SOFTWARE TECHNOLOGIES LTD.



Automate Compliance with Continues Compliance and CloudBots Remediation



Ensuring Compliance of Thousands of Cloud configuration settings

Automated Compliance

Governance and Compliance Knowledge Base



Check Point
SOFTWARE TECHNOLOGIES LTD

GSL KNOWLEDGE BASE

Dome9 Governance Specification Language (GSL) allows Dome9 users to create Compliance and Security rules written in a concise, common language that is easy to understand. With an online visual editor, a hundred lines of code can be reduced to a short human readable GSL statement.

This Knowledge Base provides Dome9 GSL Best Practices for AWS, Azure and GCP environments. We constantly update this Knowledge Base, so please check this page for new updates!

<https://gsl.dome9.com/>

Showing 119 from 119

Clear all

Search

Risk Level

- ☐ High
- ☐ Medium
- ☐ Low

Domain

- ☐ Network Security
- ☐ Encryption and Key Management
- ☐ Logging
- ☐ Network Ports Security

Entity

- ☐ Security Group
- ☐ Storage Bucket
- ☐ VPC Network
- ☐ Virtual Machine Instances



Amazon Web Services



Microsoft Azure



Google Cloud Platform

Network Security

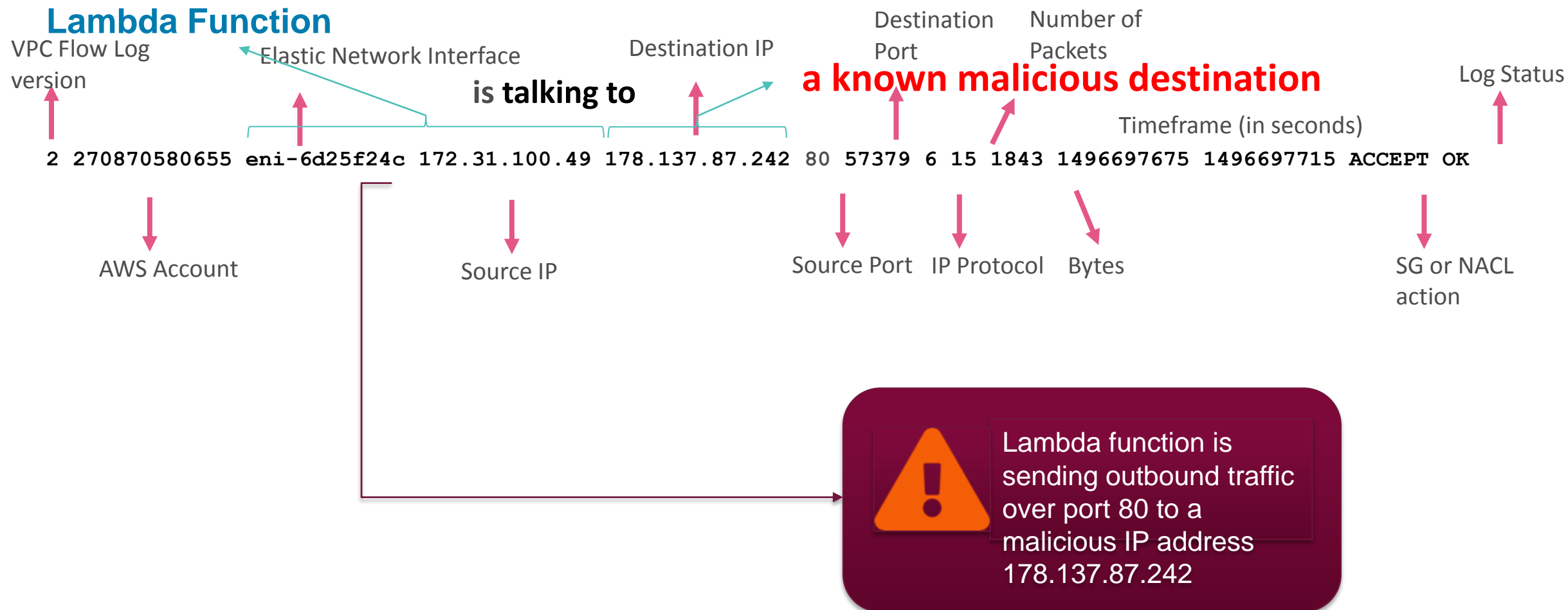
- Unused firewall rules _____ GCP Security Group
- Global Firewall rule that allows all traffic _____ GCP Security Group
- Ensure that Cloud Storage bucket is not anonymously and/or publicly accessible _____ Storage Bucket
- Ensure that there are no publicly accessible objects in storage buckets _____ Storage Bucket
- Ensure the default network does not exist in a project _____ GCP VPC Network
- Asset is not labeled _____ Virtual Machine Instances
- Asset does not contain a security tag _____ Virtual Machine Instances
- Google Instance with public IP _____ Virtual Machine Instances
- Disable IP forwarding while creating instances _____ Virtual Machine Instances

Encryption and Key Management

- Ensure VM disks are encrypted with Customer-Supplied Encryption Keys (CSEK) _____ Virtual Machine Instances



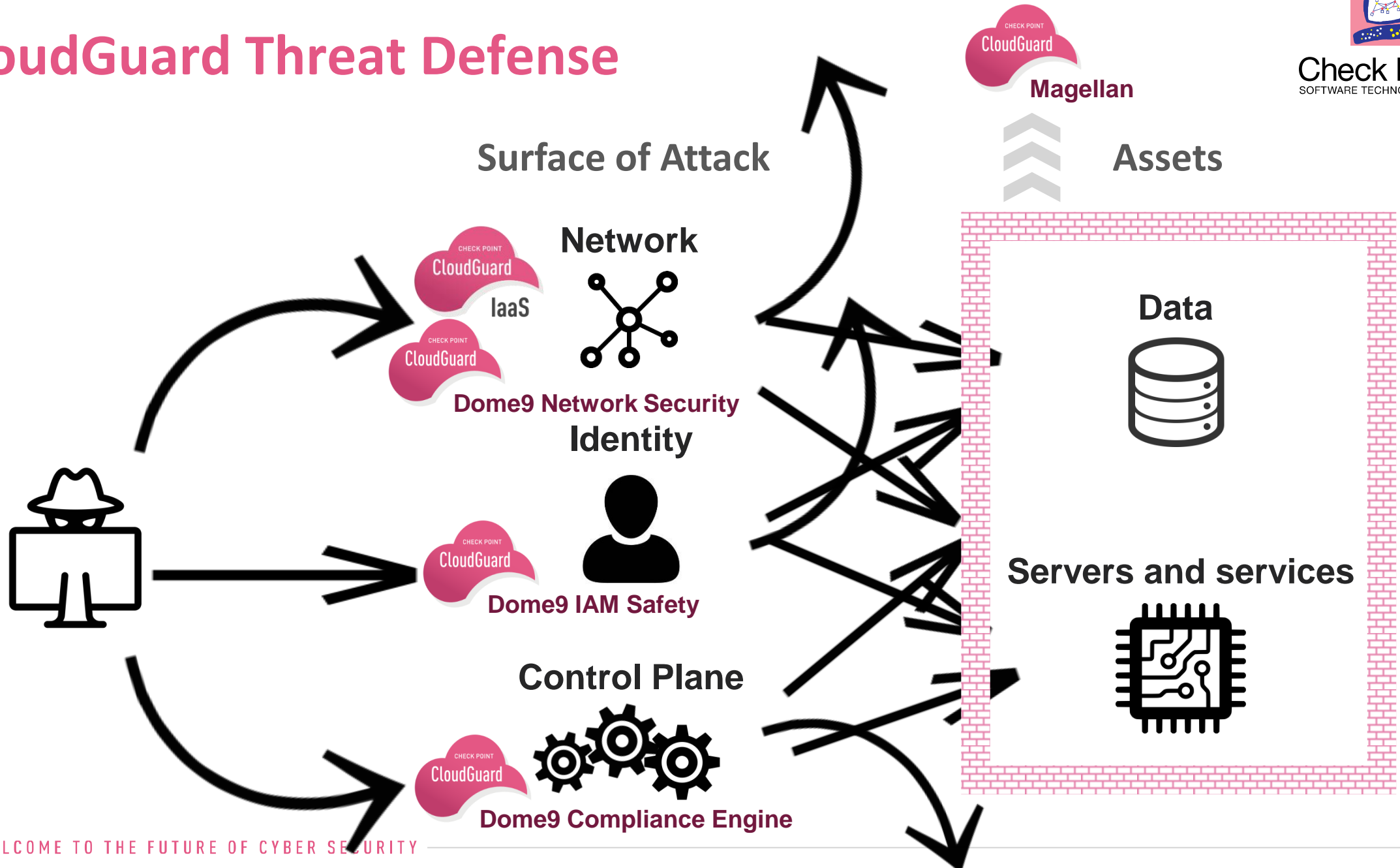
Analyzing Cloud Traffic Is Hard



CloudGuard Threat Defense



Check Point
SOFTWARE TECHNOLOGIES LTD



CloudGuard: Comprehensive Multi-Cloud Security



- Market-leading threat prevention – anti-bots, IPS, anti-malware, AV and more
- Securely connect your hybrid cloud
- Adaptive policy for macro-segmentation

- Full security visibility and control
- Cloud services and applications are never exposed
- Continuous compliance for cloud native services
- Auto-remediation of security misconfigurations
- Active protection against identity theft and data loss

Proven Success with Over 300 Enterprise Customers



Check Point
SOFTWARE TECHNOLOGIES LTD

Financial Services and Insurance



Technology



Manufacturing



Telecommunications



Brands



2019 Cloud Offering



Check Point®
SOFTWARE TECHNOLOGIES LTD



Protecting enterprise data by preventing targeted attacks on SaaS applications and cloud-based email



Protecting public & private cloud networks with advanced threat prevention, network segmentations and policies that span across multiple clouds and hybrid environments

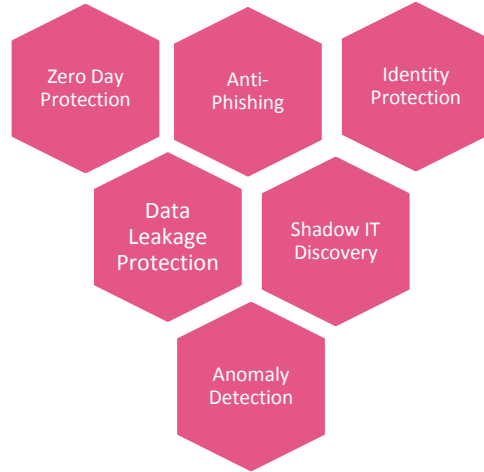


Protecting against cloud configuration mistakes, identity theft and data loss. Delivers full visibility and control of network security posture, and best in class governance and compliance

360° Cloud Security



Check Point®
SOFTWARE TECHNOLOGIES LTD



THREATCLOUD

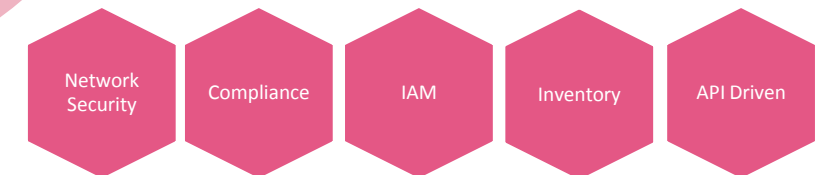
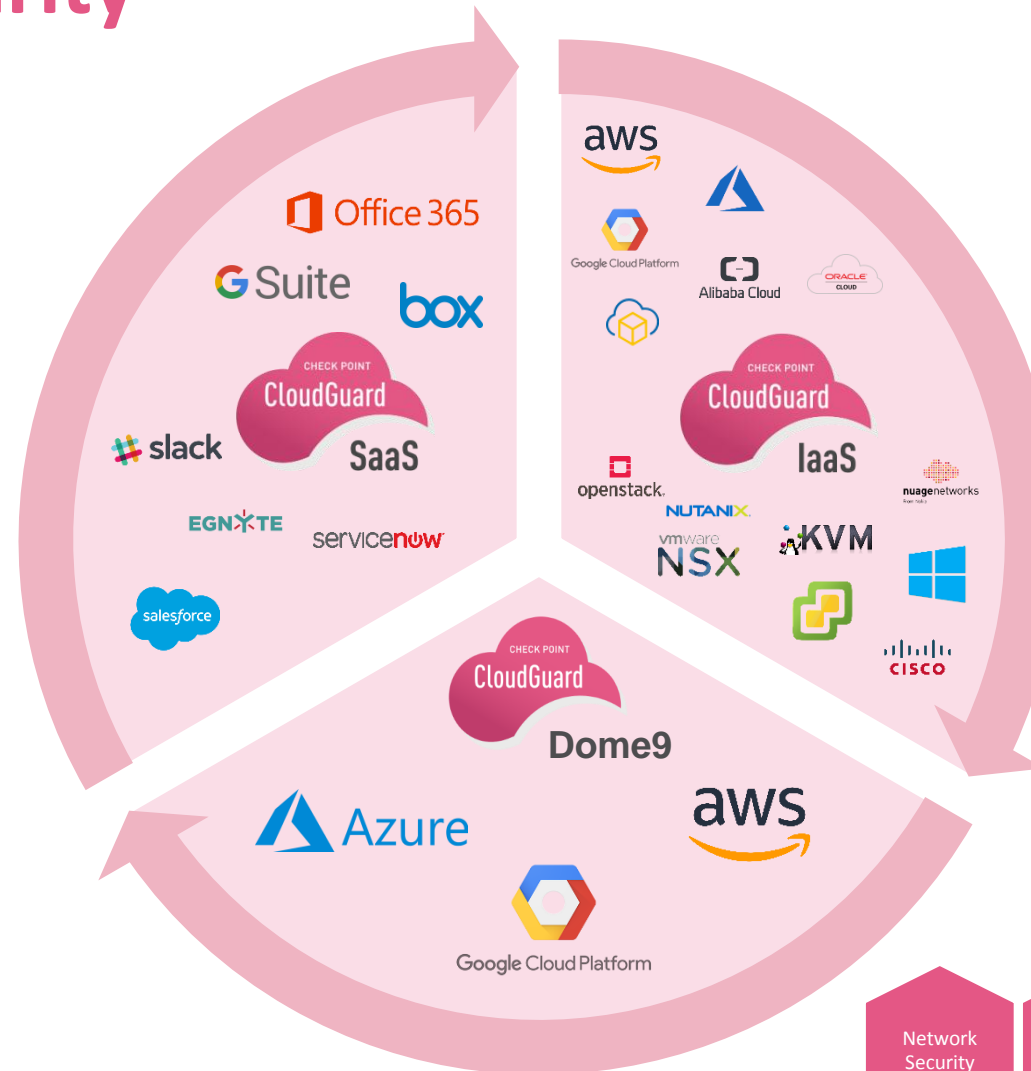
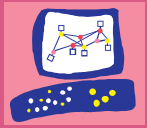


Chart source information goes here

WELCOME TO THE FUTURE OF CYBER SECURITY

©2018 Check Point Software Technologies Ltd.



Check Point®
SOFTWARE TECHNOLOGIES LTD

THANK YOU!

Securing the Cloud with Check Point CloudGuard

Richard Flanders | Head of Cloud UK

WELCOME TO THE FUTURE OF
CYBER SECURITY

POWERED BY  **CHECK POINT
INFINITY**

CLOUD • MOBILE • THREAT PREVENTION