Application Develc
Application Develc
Application Develc
Application Develc
Application Develc
Business Continuit
Business Continuit
Business Continuit
Business Continuit
Business Continuit
Business Continuit
Business Continuit
Business Continuit
Business Continuit
Business Continuit
Business Continuit
Business Continuit
Category Text
Change Control &
Change Control &
Change Control &
Change Control &
Change Control &
Data Security
Data Security
Data Security
Data Security
Data Security
Data Security
Data Security
Data Security
Data Security
Data Security
Data Security
Data Security
Data Security
Data Security
Data Security
Data Security
Data Security
Data Security
Data Security
Data Security
Data Security
Data Security
Data Security
Data Security
Data Security
Data Security
Data Security

Data Security
Data Security
Data Security
Data Security
Data Security
Data Security
Data Security
Data Security
Identity & Access M
Identity & Access M
Identity & Access M
Identity & Access M
Identity & Access M
Identity & Access M
Identity & Access M
Identity & Access M
Identity & Access M
Identity & Access M
Identity & Access M
Mobile Security
Mobile Security
Mobile Security
Mobile Security
Mobile Security
Mobile Security
Network Security
Network Security
Network Security
Network Security
Network Security
Network Security
Network Security
Network Security
Network Security
Network Security
Network Security
Network Security
Network Security
Network Security
Network Security
Physical Security
Physical Security
Policy & HR
Policy & HR
Policy & HR
Policy & HR
Policy & HR
Policy & HR
Policy & HR

Policy & HR
Policy & HR
Policy & HR
Policy & HR
Policy & HR
Policy & HR
Policy & HR
Policy & HR
Policy & HR
Policy & HR
Policy & HR
Policy & HR
Policy & HR
Policy & HR
Policy & HR
Policy & HR
Policy & HR
Policy & HR
Policy & HR
Policy & HR
Policy & HR
Security Incident H
Security Incident H
Security Incident H
Security Incident H
Security Incident H
Security Incident H
Security Incident H
Security Incident H
Security Incident H
Security Incident H
Security Incident H
Security Incident H
Security Incident H
Security Incident H
Security Incident H
Security Incident H
Security Incident H
Security Incident H
Solution Overview
Solution Overview
Solution Overview
Solution Overview
Solution Overview
Solution Overview
Solution Overview
Solution Overview

Do you use industry standards (BSIMM benchmarks, Open Group ACS Framework, NIST, etc.) to
Will Check Points data be in use in the development/ test environment?
Do the production environment is physically and logically separated from development and test
Do you conduct application-layer vulnerability scans regularly as prescribed by industry best pra
Are data input and output integrity routines (i.e., reconciliation and edit checks) implemented f
Are mission critical systems redundant?
Please describe your backup methods
Are backups taken of all systems that stores Check Points data?
Are all backups encrypted?
Does Check Point can export / download its data?
Do you have more than one provider for each service you depend on?
Do you provide tenants with geographically resilient hosting options?
Do you have a Business Continuity Plan?
When it was last approved and tested?
Are the plans tested at least annually, and are the tests formally documented and approved by
Do you provide customers with ongoing visibility and reporting of your operational Service Leve
Do you offer a Service Level Agreement (SLA) for your services? If yes, what is the uptime guara
Question Text
Describe the (1) network, (2) infrastructure and (3) application change control procedures imple
Has a change management process been implemented to track and approve all changes to the
Have specific procedures been implemented to address the change management process in em
Do you have a patch management process (for network, application and databases -hardware &
Do you have controls in place to restrict and monitor the installation of unauthorized software
Where Check Point's data is retained? Is the data stored on laptops, mobile devices or removab
Do you provide tenants with documentation that describes scenarios in which data may be mov
Please attach the documents your provide your tenants
Do you allow tenants to specify which of your geographic locations their data is allowed to mov
Please specify all controls that are in place for protecting Check Points confidentiality data base
What type of environment do you have?
Are you able to logically segment customer data so that only data for a specific client may be pr
How do you prevent data leakage, and co-mingling of Check Point's data with other customers?
Explain the (1) access control management (is it role based model?) and (2) how are access to d
Is multi-factor authentication (MFA) enforced accross all internet facing, remote access and crit
What type of strong 2 factor authentication mechanisms is in place for systems processing Chec
Do you provide tenants with strong (multifactor) authentication options (digital certs, tokens, b
Do you allow tenants/customers to define password and account lockout policies for their acco
Does the application support SSO to Azur AD (based on the standard of SAML 2.0)?
Do you have mechanisms in place for unlocking accounts that have been locked out (e.g., self-s
How many users, from which type have potential access to systems that process/ store Check P
Do you monitor and log privileged access (administrator level) to information security managen
Do you manage and store the identity of all personnel who have access to the IT infrastructure,
Does any of your vendor's/ 3rd party have access to Check Points data?
Does customer or sensitive data leave the production systems under any circumstances, includi
What monitoring capabilities are implemented to identify access to Check Points data and serve
Do you restrict personnel access to all hypervisor management functions or administrative cons
Do you have a capability to detect attacks that target the virtual infrastructure directly (e.g., shi
Are encryption mechanisms are in place both for data in transit and data at rest?

The application infrastructure cannot utilize any "homegrown" cryptography any symmetric, as
Which version of TLS/SSL are you using?
How long will Check Points data be retained? What options exist to destroy/ purge sensitive dat
Do you regularly perform penetration tests to protect the confidentiality , integrity and availabi
Have you undergone a vulnerability assessment or penetration test of the environment process
Do you follow secure data destruction processes for confidential data and IT equipment/media
Does your data security framework support Bring Your Own Key (BYOK) for encryption and key
could you provide details on how tenants can bring and manage their own encryption keys with
Describe your password policy for systems that will be hosting Check Points data, or will allow a
Are all passwords encrypted using an industry best practice standard encryption algorithm?
Do you have a policy on the use of cryptographic controls? Is consideration made to internatior
Provide a detailed description of the user management processes and operations; this includes
Do connections to systems utilize the internet protected using any of the following cryptograph
Explain how least privileges and need to know concepts are implemented. How will you protect
Explain periodically processes for user (internal users and Check Points users) access review anc
Do you have full audit trail and logging capabilities on user access that can be tracked to an indi
Please describe your log review policy and procedure
Do you provide tenants with documentation showing the transport route of their data between
Can tenants define how their data is transported and through which legal jurisdictions?
Do you have a centralized mobile device management solution deployed to all mobile devices t
Does your mobile device policy require the use of encryption for either the entire device or for
Does your mobile device policy prohibit the circumvention of built-in security controls on mobil
Do you have detective and preventative controls on the device or via a centralized device mana
Do you have password policies for enterprise issued mobile devices and/or BYOD mobile device
Are your password policies enforced through technical controls (i.e. MDM)?
Do you maintain a complete inventory of all of your critical assets that includes ownership of th
Do you maintain a complete inventory of all of your critical supplier relationships?
Are all platforms hardened (Both Secure Configuration and OS Hardening)?
Are network security devices, such as firewalls and IDS/ IPS are in use to protect critical systems
Are log files available for (1) security devices (2) System Host Protection System, and (3) Virtual
Are all firewalls rules being reviewed on a regular basis?
Do you have a DB firewall? (e.g. Sentrigo, Imperva , Guradium)?
Do you have a DLP system? (Data Loss Prevention)?
Describe the protocols that are allowed to traverse the firewall from the Internet
Do you have a WAF solution?
Do all the systems within your infrastructure, including laptops, desktops, servers, and cloud ser
Do you ensure that security threat detection systems using signatures, lists or behavioral patter
Do you conduct network-layer vulnerability scans regularly as prescribed by industry best practi
Do you conduct local operating system-layer vulnerability scans regularly as prescribed by indus
Will you make the results of vulnerability scans available to tenants at their request?
Are reasonable physical security and environmental controls (e.g., fences, walls, barriers, guards
Describe the physical security protections that isolate and protect Check Point's data and syster
Please attach your Information Security Policy and list of security policies that were formally ap
When were your companys security policies and standards last reviewed?
Is your company ISO 27001 Certified (or any other ISMS)?
Has the company been audited for SOC2?
Is the service or product you provide aligned with any data privacy requirements (equal or para
Does your organization comply or is certified for any additional standards or frameworks.
Does the scope of your companys security policies and standards cover the type of services Che

Explain how Information Security Policy is communicated to staff
at what frequency (months) Information Security Policy is communicated to staff?
Is there an Information Security Group/Steering Committee?
Describe audit processes that your company complies with
Please specify your privacy policy, is it aligned with industry standards?
Is the service or product you provide aligned with any data privacy requirements (equal or para
Are systems in place to monitor for privacy breaches and notify tenants expeditiously if a privac
Pursuant to local laws, regulations, ethics and contractual constraints, are all employment cand
Are all personnel required to sign NDA or Confidentiality Agreements as a condition of employn
Is annual security awareness training is in place to all employees?
Do you specifically train your employees regarding their specific role and the information securi
Is successful and timed completion of the training program considered a prerequisite for acquir
Are documented policies, procedures and guidelines in place to govern change in employment a
Please specify your disciplinary process and actions taken agains employees who have violated
Do the above procedures and guidelines account for timely revocation of access and return of a
Are policies and procedures established and measures implemented to strictly limit access to yo
Do you provide tenants with a role definition document clarifying your administrative responsib
Do you provide documentation regarding how you may or access tenant data and metadata?
Do you collect or create metadata about tenant data usage through inspection technologies (se
Do you allow tenants to opt out of having their data/metadata accessed via inspection technolo
Do you provide a formal, role-based, security awareness training program for cloud-related acc
Are administrators and data stewards properly educated on their legal responsibilities with rega
Do you have a documented security incident response plan?
Describe your security incident response. Please include forensic capabilities and policies and pr
What notification and escalation processes exist in case of security incident?
Is there a process to notify Check Point about incidents that affect Check Points business or dat
Do you integrate customized tenant requirements into your security incident response plans?
Does your logging and monitoring framework allow isolation of an incident to specific tenants?
Are you capable of supporting litigation holds (freeze of data from a specific point in time) for a
Do you enforce and attest to tenant data separation when producing data in response to legal s
Will you share statistical information for security incident data with your tenants upon request?
Do you publish a roles and responsibilities document specifying what you vs. your tenants are r
Have you tested your security incident response plans in the last year?
Does your security information and event management (SIEM) system merge data sources (app
Do you have a SOC center?
Please describe your detection process for DDoS attack
Please describe your prevention process for DDoS attack
Do you have D/DOS protection?
Have you suffered a security breach in the last 3 years?
Please attach all relevant network diagrams, data-flow charts and integration points with Check
Please select all data transfer and integration points that apply to our engagement.
Please describe how data is transferred between Check Point and your platform, what configura
Is part of the integration requires from Check Point to create inbound rules in its firewall?
Please specify which Check Point data (including employees , customers or partners details) will
Please describe Who is the hosting provider?
Please select all applicable territories in which data or systems will be accessed from, processed
Please provide a comma separated list of your company domain names (e.g. checkpoint.com).

SingleChoice	YesNoN/A	TRUE
SingleChoice	YesNoN/A	TRUE
SingleChoice	YesNoN/A	TRUE
SingleChoice	YesNoN/A	TRUE
SingleChoice	YesNoN/A	FALSE
SingleChoice	YesNoN/A	TRUE
FreeText		TRUE
SingleChoice	YesNoN/A	TRUE
SingleChoice	YesNoN/A	TRUE
SingleChoice	YesNoN/A	TRUE
SingleChoice	YesNoN/A	TRUE
SingleChoice	YesNoN/A	TRUE
SingleChoice	YesNoN/A	TRUE
SingleChoice	0-33-66-1212+Nev	TRUE
SingleChoice	YesNoN/A	FALSE
SingleChoice	YesNoN/A	FALSE
FreeText		FALSE
Question Type	Possible Answers	Mandatory
FreeText		FALSE
SingleChoice	YesNoN/A	FALSE
SingleChoice	YesNoN/A	FALSE
SingleChoice	YesNoN/A	TRUE
SingleChoice	YesNoN/A	FALSE
MultiChoice	LaptopsMobile de	FALSE
SingleChoice	YesNoN/A	FALSE
File		FALSE
SingleChoice	YesNoN/A	TRUE
FreeText		FALSE
SingleChoice	Shared environme	TRUE
SingleChoice	YesNoN/A	TRUE
FreeText		FALSE
FreeText		FALSE
SingleChoice	YesNoN/A	TRUE
MultiChoice	Hardware tokenM	FALSE
SingleChoice	YesNoN/A	FALSE
SingleChoice	YesNoN/A	FALSE
SingleChoice	YesNoN/A	TRUE
SingleChoice	YesNoN/A	FALSE
FreeText		FALSE
SingleChoice	YesNoN/A	TRUE
SingleChoice	YesNoN/A	FALSE
SingleChoice	YesNoN/A	TRUE
SingleChoice	NoYesN/A	TRUE
FreeText		FALSE
SingleChoice	YesNoN/A	FALSE
SingleChoice	YesNoN/A	FALSE
SingleChoice	YesNoN/A	TRUE

FreeText		FALSE
MultiChoice	SSL 2.0SSL 3.0TLS 1	TRUE
FreeText		FALSE
SingleChoice	YesNoN/A	TRUE
SingleChoice	YesNoN/A	TRUE
SingleChoice	YesNoN/A	FALSE
SingleChoice	YesNoN/A	TRUE
FreeText		TRUE
FreeText		TRUE
SingleChoice	YesNoN/A	FALSE
FreeText		FALSE
FreeText		FALSE
MultiChoice	IPSecSSLSSH/SCPP	FALSE
FreeText		TRUE
FreeText		FALSE
SingleChoice	YesNoN/A	TRUE
FreeText		FALSE
SingleChoice	YesNoN/A	FALSE
SingleChoice	YesNoN/A	FALSE
SingleChoice	YesNoN/A	FALSE
SingleChoice	YesNoN/A	FALSE
SingleChoice	YesNoN/A	FALSE
SingleChoice	YesNoN/A	FALSE
SingleChoice	YesNoN/A	FALSE
SingleChoice	YesNoN/A	FALSE
SingleChoice	YesNoN/A	TRUE
SingleChoice	YesNoN/A	TRUE
SingleChoice	YesNoN/A	TRUE
SingleChoice	YesNoN/A	TRUE
SingleChoice	YesNoN/A	FALSE
SingleChoice	YesNoN/A	TRUE
SingleChoice	YesNoN/A	TRUE
SingleChoice	YesNoN/A	FALSE
FreeText		FALSE
SingleChoice	YesNoN/A	TRUE
SingleChoice	YesNoN/A	TRUE
SingleChoice	YesNoN/A	FALSE
SingleChoice	YesNoN/A	TRUE
SingleChoice	YesNoN/A	FALSE
SingleChoice	YesNoN/A	FALSE
SingleChoice	YesNoN/A	TRUE
FreeText		FALSE
File		TRUE
SingleChoice	Last month3 mont	TRUE
SingleChoice	YesNo	TRUE
SingleChoice	YesNo	TRUE
SingleChoice	YesNoN/A	TRUE
MultiChoice	ITARCSAHIPAAPCI/	TRUE
FreeText		TRUE

FreeText		TRUE
SingleChoice	0-33-66-1212+	TRUE
SingleChoice	YesNoN/A	TRUE
FreeText		TRUE
MultiChoice	ISO/IEC 27018Non	FALSE
SingleChoice	YesNoN/A	TRUE
SingleChoice	YesNoN/A	FALSE
SingleChoice	YesNoN/A	FALSE
SingleChoice	YesNoN/A	FALSE
SingleChoice	YesNoN/A	FALSE
SingleChoice	YesNoN/A	FALSE
SingleChoice	YesNoN/A	FALSE
SingleChoice	YesNoN/A	FALSE
FreeText		FALSE
SingleChoice	YesNoN/A	FALSE
SingleChoice	YesNoN/A	FALSE
SingleChoice	YesNoN/A	FALSE
SingleChoice	YesNoN/A	FALSE
SingleChoice	YesNoN/A	TRUE
SingleChoice	YesNoN/A	FALSE
SingleChoice	YesNoN/A	FALSE
SingleChoice	YesNoN/A	FALSE
SingleChoice	YesNoN/A	TRUE
FreeText		TRUE
FreeText		TRUE
SingleChoice	YesNoN/A	TRUE
SingleChoice	YesNoN/A	TRUE
SingleChoice	YesNoN/A	TRUE
SingleChoice	YesNoN/A	TRUE
SingleChoice	YesNoN/A	TRUE
SingleChoice	YesNoN/A	TRUE
SingleChoice	YesNoN/A	TRUE
SingleChoice	YesNoN/A	TRUE
SingleChoice	YesNoN/A	TRUE
SingleChoice	YesNoN/A	TRUE
FreeText		TRUE
FreeText		TRUE
SingleChoice	YesNoN/A	FALSE
SingleChoice	NoYes	TRUE
File		FALSE
MultiChoice	Web applicationSc	TRUE
FreeText		FALSE
SingleChoice	YesNoN/A	TRUE
FreeText		TRUE
FreeText		TRUE
MultiChoice	EuropeNorth Ame	TRUE
FreeText		FALSE

Yes
No
Yes
Yes
Yes
Yes
Coralogix employs robust backup methods as part of its Business Continuity Plan. Data is backed up to AWS S3
Yes
Yes
Yes
No
Yes
Yes
6-12
Yes
Yes
Yes, Coralogix offers a Service Level Agreement (SLA) with an uptime guarantee of 99.9%. If the availability dro
Answers
Coralogix has a comprehensive change control process for network, infrastructure, and application changes. T
Yes
Yes
Yes
Yes
Data is stored only within datacenters. Coralogix uses AWS cloud storage for data retention and does not stor
Yes, Coralogix provides tenants with documentation as part of its Business Continuity Plan (BCP) and Disaster
Will be attached
Yes, Coralogix offers flexibility for customers to choose where their data is stored, and it can comply with geog
Our business focuses on processing customer logs, treating this data
Shared environment
Yes, Coralogix provides multi-tenancy with strict logical segregation at the index and URL level. This ensures th
Coralogix prevents data leakage and co-mingling of Check Point's data with other customers through logical se
Coralogix employs a role-based access control (RBAC) model to manage access control. Access to system comp
Yes
Hardware token, Mobile Authenticator Apps
Yes
Yes
Yes
Yes
<p class="MsoNormal" style="margin: 0cm; font-size: 12pt; font-family: Aptos, sans-serif; color: rgb(0, 0, 0);">
Yes, Coralogix monitors and logs privileged access to its information security management systems. This includ
Yes, all personnel access is managed and stored. Access levels are documented and regularly reviewed, ensuri
Yes, only our authorized sub-processors for example AWS which is our infra .
No
Coralogix implements comprehensive monitoring capabilities to identify access to Check Point data and server
Yes.
Yes, Coralogix employs various technical controls, including firewalls, network segmentation, intrusion detecti
Yes, encryption mechanisms are in place for both data in transit and data at rest. Data at rest is encrypted usir

Coralogix uses AES-256 for encryption at rest on index. Customers can also choose to store their logs on their
TLS 1.3 with fallback to TLS 1.2
Check Point's data is retained on index for the duration specified in the contract with each customer. At the er
Yes
Yes
Yes.
No, not on our index. If you use your own S3 then you can utilize BYOK.
Coralogix does not support BYOK for index. Instead, Coralogix uses AWS Key Management Service (KMS) for m
Coralogix enforces a comprehensive password policy for systems hosting or accessing Check Points data. The p
Yes
Coralogix has a policy on the use of cryptographic controls to ensure the protection of information. This policy
Coralogix implements a formal user access provisioning process to assign or revoke access rights for all user ty
No.
Access to customers' accounts
User access reviews are conducted quarterly by the Coralogix CISO to ensure that access privileges are approp
Yes
Coralogix has a comprehensive log review policy and procedure in place. Event logs recording user activities, e
Yes
Yes
N/A
N/A
N/A
N/A
N/A
N/A
Yes, Coralogix maintains an inventory of all hardware and software. All hardware is tracked using asset manag
Yes, Coralogix maintains a complete inventory of all critical supplier relationships as part of our Supplier Secur
Yes.
Yes. AWS Security Groups, Cloud Flare, STA.
Yes
Yes
Yes
No.
Coralogix allows specific protocols to traverse the firewall from the Internet, which are controlled and monito
Yes
Yes
Yes
Yes
Yes
Yes, results of vulnerability scans can be shared with tenants upon request, under an NDA.
Yes
Coralogix offices have multiple layers of physical security, including 24/7 guards, gates to control elevator acce
Please see attached.
Last month
Yes
Yes
Yes
SOC2, ISO-27001, ISO-27701, 27017, 27018 PCI-DSS, HIPAA, gdpr, FedRAMP Ready
Yes, Coralogix's security policies and standards cover a wide range of areas relevant to the services Check Poir

The Information Security Policy is communicated to all employees through multiple methods. Upon hiring, em
6-12
Yes
SOC 2 Type 2, ISO's 27001, 27701, 27017, 27018, FedRAMP Ready, PCI-DSS
ISO/IEC 27018
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
There is a formal and communicated disciplinary process in place to take action against employees who have
Yes
N/A
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Coralogix has a comprehensive security incident response plan that is activated in the event of a suspected or
In the event of a security incident, Coralogix has established notification and escalation processes. Security bre
Yes
No
Yes
Yes
Yes
Yes
Yes,
Yes
Yes
Yes
Coralogix employs a multi-layered approach to detect DDoS attacks. This includes the use of firewalls and intru
Coralogix employs multiple layers of defense to prevent DDoS attacks. We utilize CloudFlare for DDoS protecti
Yes.
No
Please refer to the attached diagrams: 'diagram 1.pdf' and 'diagram 2.pdf' for network diagrams, data-flow ch
Web application, Software / Application, API, VPN / Remote access
Data is transferred between Check Point and Coralogix primarily through secure methods such as APIs. All dat
Since you push your logs to the Coralogix platform, you don't need to create inbound rules.
Coralogix's business is the processing of your selected system logs; the data stored depends on what custome
The hosting provider for Coralogix is Amazon Web Services (AWS). We offer 5 distinct AWS regions to host you
Europe, North America, Asia, Middle East. Depends on where you choose to store your data. Our R&D ce
coralogix.com

	TRUE
	TRUE
	TRUE
	TRUE
	TRUE
	TRUE
	TRUE
	TRUE
	TRUE
	TRUE
	TRUE
	TRUE
	TRUE
	TRUE
Conditional	Allow Additional Info
	TRUE
	TRUE
	TRUE
	TRUE
	TRUE
	TRUE
1:Yes	FALSE
	TRUE
	TRUE
	TRUE
	TRUE
	TRUE
	TRUE
	TRUE
	TRUE
	TRUE
	TRUE
	TRUE
	TRUE
	TRUE
	TRUE
	TRUE
	TRUE

TRUE

TRUE
TRUE
TRUE
TRUE

TRUE

TRUE

TRUE

TRUE
TRUE
TRUE
TRUE
TRUE
TRUE
TRUE
TRUE
TRUE
TRUE
TRUE
TRUE
TRUE
TRUE

TRUE
TRUE
TRUE
TRUE
TRUE
TRUE
TRUE

FALSE
TRUE
TRUE
TRUE
TRUE
TRUE

TRUE
TRUE

TRUE
TRUE
TRUE
TRUE
TRUE
TRUE
TRUE
TRUE
TRUE

TRUE
TRUE
TRUE
TRUE
TRUE
TRUE
TRUE
TRUE
TRUE
TRUE

TRUE
TRUE
TRUE
TRUE
TRUE
TRUE
TRUE
TRUE
TRUE
TRUE

TRUE
TRUE

TRUE

TRUE

TRUE