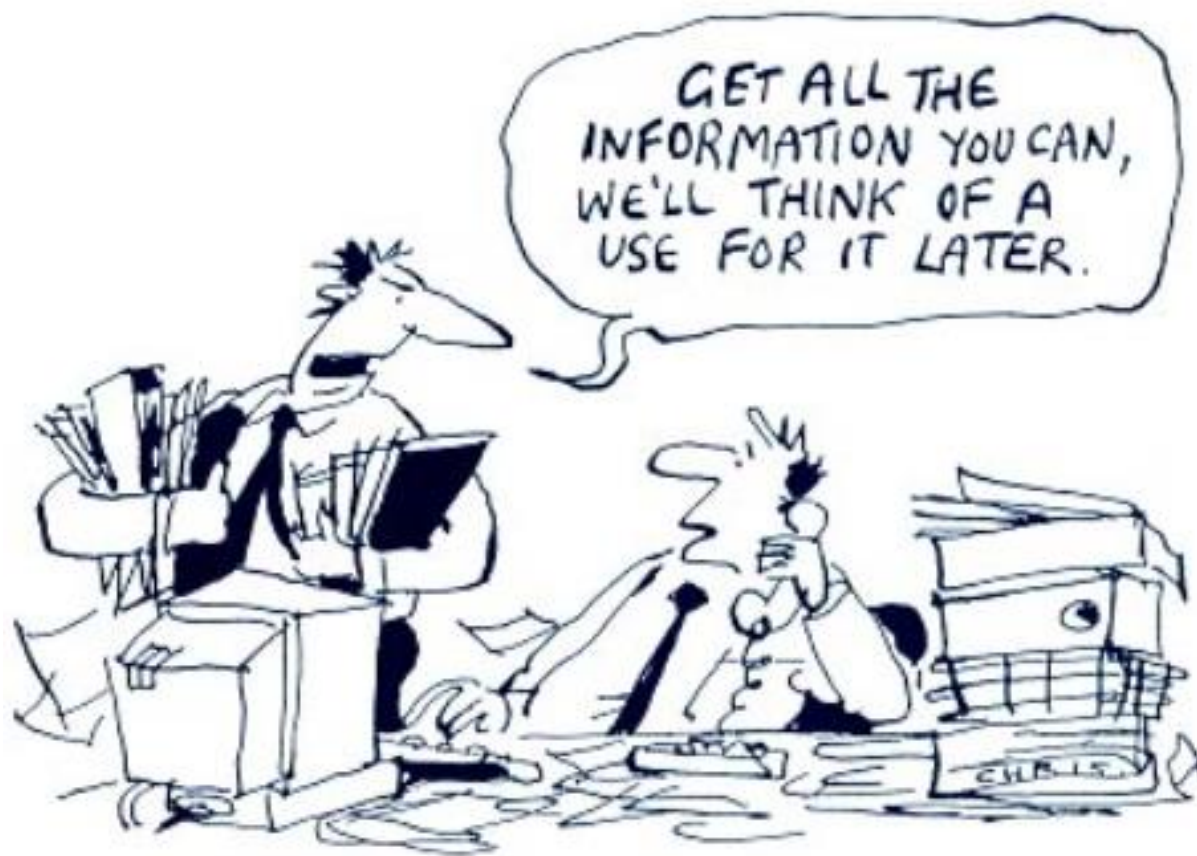


A GDPR AWARE NETWORK

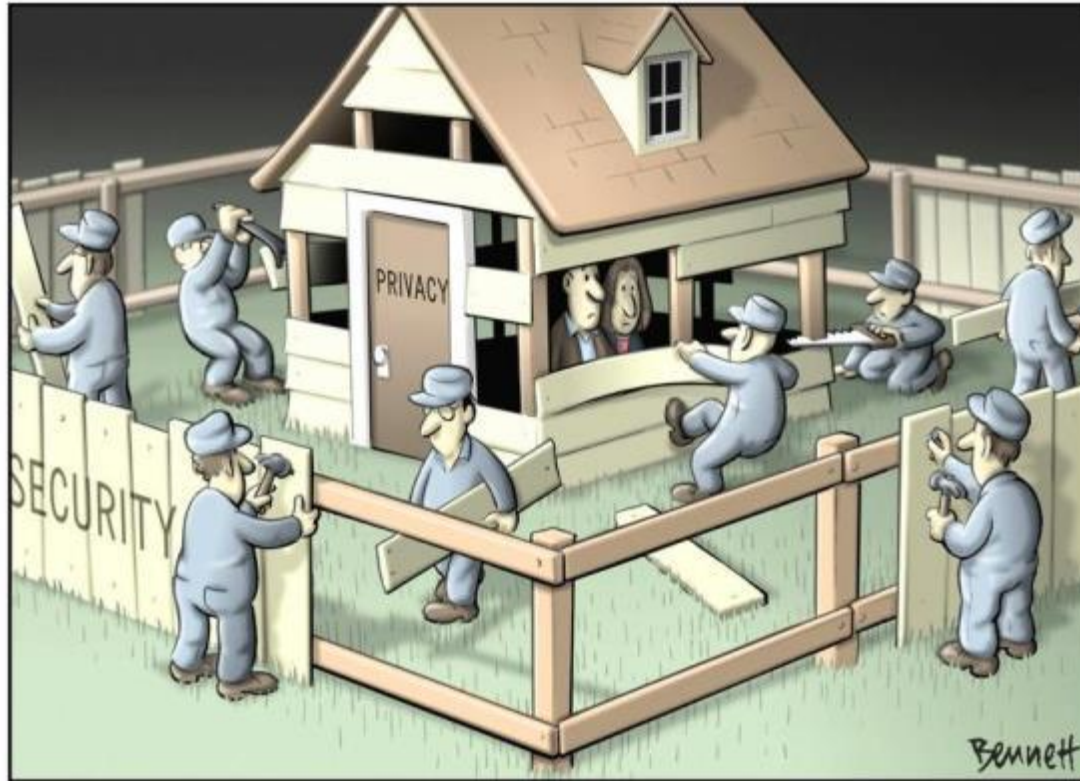
A Proactive Security Approach for GDPR

Sunny Gill, Security Expert Europe

Check Point Software Technologies Ltd



Is GDPR a Privacy or a Security Regulation?





Is GDPR a Privacy or a Security Regulation?

- Personal data should be processed in a manner that ensures **appropriate security**...preventing **unauthorised access** to or use of personal data. (Introduction, Clause 39)
- Ensuring network and information security...include **preventing unauthorised access** to electronic communications networks and malicious code distribution... (Introduction, Clause 49)
- In order to maintain security...evaluate the risks... **implement measures to mitigate those risks**, such as encryption. (Introduction, Clause 83)
- Personal data shall be processed in a manner that **ensures appropriate security of the personal data**, including **protection against unauthorised or unlawful processing and against accidental loss**, destruction or damage, using appropriate technical or organisational measures. (Chapter 2, Article 5, Clause 1f)
- **Implement appropriate technical and organisational measures** to ensure a level of security appropriate to the risk. (Chapter 4, Section 2, Article 32-1)



Malware attack on UVA Health gave hacker access for 19 months

The Charlottesville-based provider discovered the breach in December 2017 and has been working with the FBI on its investigation.

By [Jessica Davis](#) | February 22, 2018 | 12:39 PM



Breach Data



Physician devices



Medical records



1,882 patients



19 months

GDPR Core Principles for Organizations



Check Point
SOFTWARE TECHNOLOGIES LTD

1 Data transparency

2 Ad hoc data collection

3 Reasoning & Logic

4 Data accuracy

5 Prevention of unauthorized use or accidental loss of the data

6 Data protection “by design and by default”

Check Point



GDPR: Five Step Attack Plan

State of the art (SOTA, Articles 25 and 32). This principle is "future proofing" GDPR, as IT technologies are developing faster than the regulator can respond. Therefore, the burden is on the individual organization to prove that it has a view on what SOTA is, in order to justify why it did or did not implement certain technologies, based on an assessment of SOTA on the context of cost, risk, and context. This understanding needs to be reviewed on a regular basis, to keep up with technology innovation. SOTA encourages organizations to implement appropriate IT solutions and develop good processes within reasonable cost, risk, and context, so that they always protect personal data in the best possible way. Investing in market-leading IT security, data protection, and analytics solutions with an innovative road map will make it easier to comply with SOTA and will also make the job of the data protection officer much easier.



DPO



Auditor



**Trusted Advisor
"Check Point"**

Personal Data – Where is it?



On the Corporate network



On our Laptops



In the Cloud



On our Devices

SK122355: GDPR Security Check Up for R80.10

Sample Report

Get background on GDPR

1

Understand your Environment

DLP

EXECUTIVE SUMMARY

SECURITY CHECKUP

private information. It requires an extensive list of protections on that data, limitations on how it is used, and customer notifications and consent in a wide range of situations.

Check Point solutions enables organizations to take immediate

6

12.5GB

2

Perform Risks Assessment

Antivirus & Threat Emulation

and to be compliant with GDPR requirements.

Malware and Attacks

287 computers infected with bots

4.6K communications with C&C* sites

* C&C - Command and Control. If proxy is deployed, there might be additional infected computers.

8 known malware downloads

10 users

21 new malware downloaded

New malware variant is a zero-day attack or malicious code with no known anti-virus signature.

14 unique software vulnerabilities were attempted to be exploited


Indicates potential attacks on computers on a network.




AntiBot

IPS

GDPR: Not A One-Bullet-Solution

EU Data Privacy



Chapter	Name	Articles
 0	Introductory Clauses (173)	
1	General Provisions	1 – 4
 2	Principles	5 – 11
3	Rights of the Data Subject	12 – 23
 4	Controller and Processor	24 – 43
5	Transfer of Personal Data to 3 rd Countries	44 – 50
6	Independent Supervisory Authorities	51 – 59
7	Cooperation and Consistency	60 – 76
8	Remedies, Liabilities and Penalties	77 – 84
9	Provisions relating to Specific Processing Situations	85 – 91
10	Delegated Acts and Implementing Acts	92 – 93
11	Final Provisions	94 - 99



Chapter 0 - Introductory Clauses, Article 49

“...this could, for example, include **preventing unauthorised access** to electronic communications networks and **malicious code distribution** and **stopping 'denial of service' attacks** and damage to computer and electronic communication systems.

- Article 49

R80.10 –
Business aware
Security Gateway

Gen V
Protections

DDoS Protector
Security Gateway
IPS

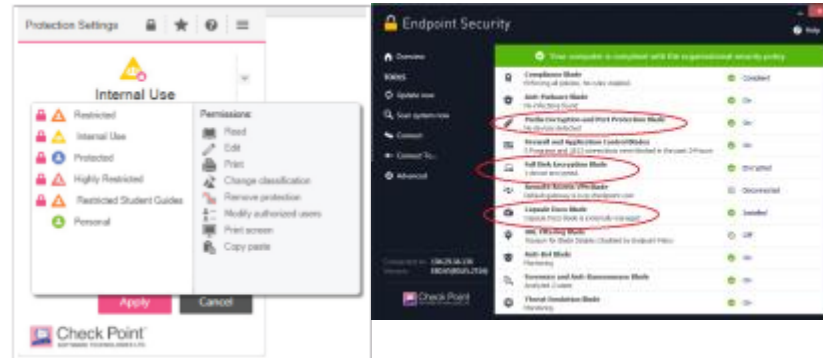
72 Hour Breach Notification to Data Subject



3. The communication to the data subject referred to in paragraph 1 shall **not** be required if any of the following conditions are met:
 - (a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data **unintelligible** to any person who is not **authorised** to access it, such as **encryption**;

Capsule Docs
Capsule Workspace
FDE
MEPP

Article 34, Paragraph 3



Security Landmarks for GDPR



DATA
CLASSIFICATION



CONFIGURATION
CHANGE
MANAGEMENT



ADMINISTRATOR
CONTROL AND
SEPARATION OF DUTIES



SECURE SYSTEM
CONFIGURATION



ACCESS CONTROL



NETWORK BASED
SEGMENTATION



ENCRYPTION AND
PSUEDINYMISATION



DATA LEAK
PREVENTION



DDOS PREVENTION



USER ACTIVITY
MONITORING

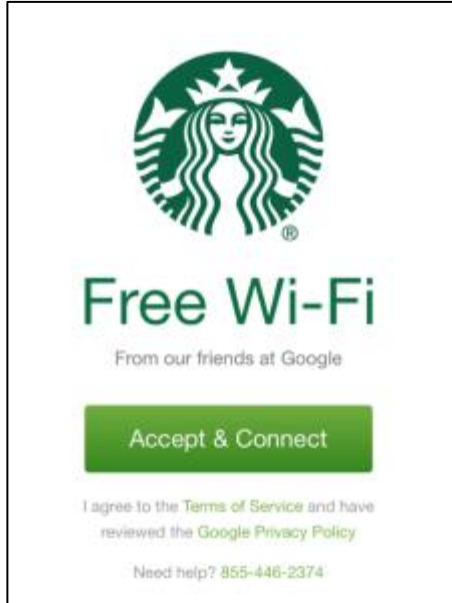


VULNERABILITY
MANAGEMENT



DISASTER
RECOVERY

Data Loss/Breach Scenarios



What does GDPR expect from us?

“...include **preventing unauthorised access** to electronic communications networks and **malicious code distribution** and **stopping 'denial of service' attacks** and damage to computer and electronic communication systems.”

- **GDPR, Article 49**

Security Controls Implemented

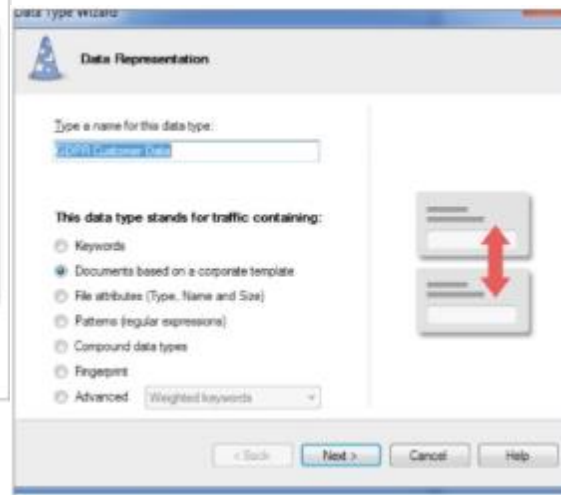




Data Classification with Capsule Docs & DLP



Check Point Capsule Docs



Check Point DLP



Configuration Change Management with R80.10 Security Management



Check Point
SOFTWARE TECHNOLOGIES LTD



Logs | General Overview | New Tab | Intrusion Prevention System (IPS) |

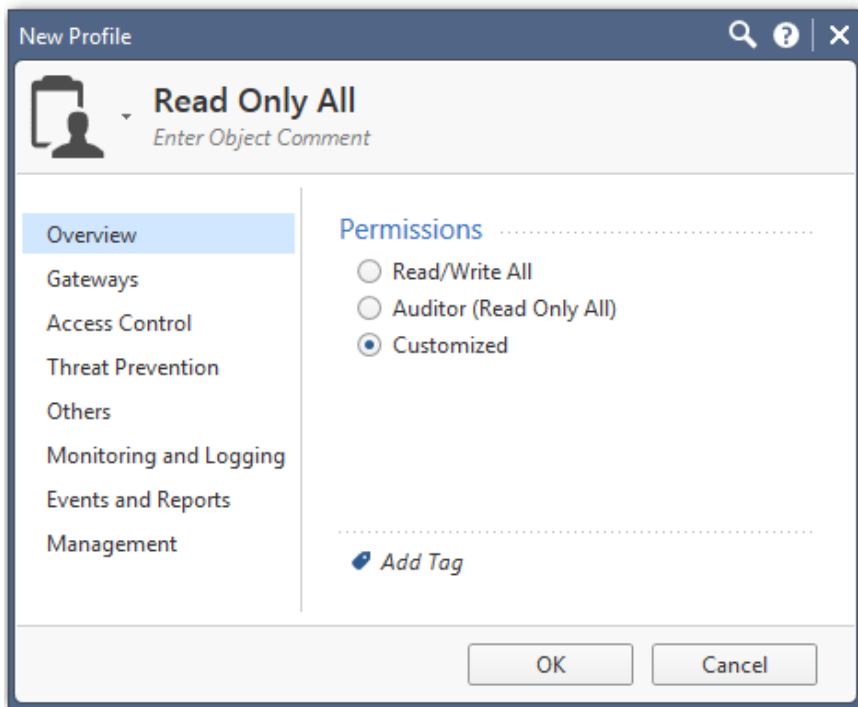
Queries | Last 7 Days | Enter search query (Ctrl+F)

Showing first 50 results (632 ms) out of at least 1,188 results

Time	Origin	Source	Source User...	Destination	Service	Ac...	Access Rule N...	Policy...	Description
Today, 11:23:12 PM	HQgw	198.54.86.174	Saul	198.51.100.193	http (TCP/80)	5	Block specific U...	Branch_...	http Traffic Dropped from 198.54.86.174 to Blocked URLs(198.5
Today, 11:23:12 PM	HQgw	198.54.86.174	Saul	198.51.100.193	http (TCP/80)	5	Block specific U...	Branch_...	http Traffic Dropped from 198.54.86.174 to Blocked URLs(198.5
Today, 11:19:50 PM	HQgw	198.51.100.15	Walter	ERP Server (198....	ftp (TCP/21)	3	ERP server bein...	Corpora...	ftp Traffic Accepted from 198.51.100.15 to 198.51.100.10
Today, 11:19:50 PM	HQgw	198.51.100.15	Walter	ERP Server (198....	ftp (TCP/21)	3	ERP server bein...	Corpora...	ftp Traffic Accepted from 198.51.100.15 to 198.51.100.10
Today, 11:18:08 PM	HQgw	198.51.100.193	Saul	198.51.100.193	http (TCP/80)	11	Clean up	Corpora...	http Traffic Dropped from 198.51.100.193 to 198.51.100.193
Today, 11:18:08 PM	HQgw	198.51.100.193	Saul	198.51.100.193	http (TCP/80)	11	Clean up	Corpora...	http Traffic Dropped from 198.51.100.193 to 198.51.100.193
Today, 10:50:48 PM	HQgw	198.51.100.193	Walter	198.51.100.193	http (TCP/80)	5	Block abuse/ hi...	Corpora...	http Traffic Dropped from 198.51.100.193 to www.bit.com(198.
Today, 10:50:48 PM	HQgw	198.51.100.193	Walter	198.51.100.193	http (TCP/80)	5	Block abuse/ hi...	Corpora...	http Traffic Dropped from 198.51.100.193 to www.bit.com(198.
Today, 10:40:53 PM	HQgw	198.51.100.193	Saul	BranchOffice (1...	http (TCP/80)	2	DHCP Server for...	Branch_...	http Traffic Accepted from 198.51.100.193 to 198.51.100.0
Today, 10:40:53 PM	HQgw	198.51.100.193	Saul	BranchOffice (1...	http (TCP/80)	2	DHCP Server for...	Branch_...	http Traffic Accepted from 198.51.100.193 to 198.51.100.0
Today, 10:31:01 PM	HQgw	198.51.100.193	Saul	198.51.100.193	http (TCP/80)	5	HR can access t...	Corpora...	http Traffic Informed from 198.51.100.193 to LinkedIn(198.51.1
Today, 10:31:01 PM	HQgw	198.51.100.193	Saul	198.51.100.193	http (TCP/80)	5	HR can access t...	Corpora...	http Traffic Informed from 198.51.100.193 to LinkedIn(198.51.1
Today, 10:22:29 PM	HQgw	198.51.100.193	Jesse	FTP_Int (198.51....	ftp (TCP/21)	1	Mobile Access f...	Corpora...	ftp Traffic Accepted from 198.51.100.193 to 198.51.100.12
Today, 10:22:29 PM	HQgw	198.51.100.193	Jesse	FTP_Int (198.51....	ftp (TCP/21)	1	Mobile Access f...	Corpora...	ftp Traffic Accepted from 198.51.100.193 to 198.51.100.12
Today, 9:28:38 PM	HQgw	198.51.100.193	Jesse	198.51.100.193	http (TCP/80)	5	Block specific ca...	Corpora...	http Traffic Dropped from 198.51.100.193 to Adobe Flash(198.5
Today, 9:28:38 PM	HQgw	198.51.100.193	Jesse	198.51.100.193	http (TCP/80)	5	Block specific ca...	Corpora...	http Traffic Dropped from 198.51.100.193 to Adobe Flash(198.5
Today, 9:24:55 PM	HQgw	198.51.100.193	Walter	198.51.100.19	http (TCP/80)	9	Policy for access...	Corpora...	http Traffic Accepted from 198.51.100.193 to Report Portal(198
Today, 9:24:55 PM	HQgw	198.51.100.193	Walter	198.51.100.19	http (TCP/80)	9	Policy for access...	Corpora...	http Traffic Accepted from 198.51.100.193 to Report Portal(198
10 Apr 17, 4:49:03 AM	HQgw	198.51.100.193	Jesse	198.51.100.193	http (TCP/80)	3	HR can access t...	Branch_...	http Traffic Informed from 198.51.100.193 to Twitter(198.51.100
Today, 9:10:30 PM	HQgw	198.51.100.193	Jesse	FTP Ext (2.3.2...	ftp (TCP/21)	8	Customers to ft...	Corpora...	ftp Traffic Accepted from 198.51.100.193 to 2.3.2.2



Admin Controls & Separation of Duties with R80.10 Security Management





Secure System Configuration with Check Point Compliance Blade

EU Data Privacy

Grouping: --No Grouping-- Generate Report

ID	Status	Name
001	Medium	Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including for preventing unauthorized access to
002	Good	The processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security. This could, for example,
003	Compliant	In order to maintain security and to prevent processing in infringement of this Regulation, the controller or processor should evaluate the risks inherent in the processing a
004	Medium	Personal data shall be (f) processed in a manner that ensures appropriate security of the personal data, including protection agai

EU Data Privacy Regulation Requirement 001

Regulatory Requirements Details

Description: Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including for preventing unauthorized access to or use of personal data and the equipment used for the processing. (Introductory)

Relevant Security Best Practices: 3 out of 6 items are secure

ID	Name	Blade	Status
PW001	Check that 'Clean Up Rule' is defined in Firewall Rule Base	Firewall	Secure
PW005	Check that each Firewall rule has defined Track settings	Firewall	Secure
PW130	Check that 'Stealth Rule' is Defined in Firewall Rule Base	Firewall	Poor
PW146	Check that an 'Any Any Accept' rule is not defined in the Firewall Rule...	Firewall	Secure
DLP002	Check that the DLP policy restricts the sending of General Personal D...	Data Loss Prevention	Medium
DLP129	Check that data is restricted according to the EU Data Protection Dire...	Data Loss Prevention	Medium



Go The Extra Mile TODAY! –



Check Point
SOFTWARE TECHNOLOGIES LTD

1. **GDPR Whitepaper >>>>>>>>>>>>>>**
2. **GDPR Security CheckUp**





If there is time (bonus content)

[otherwise skip 12 times!]

Using Check Point Security Products for GDPR

1
DATA
CLASSIFICATION

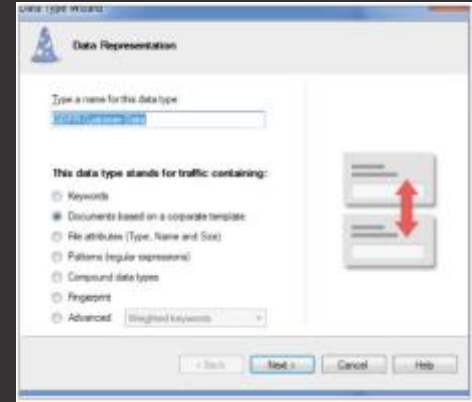
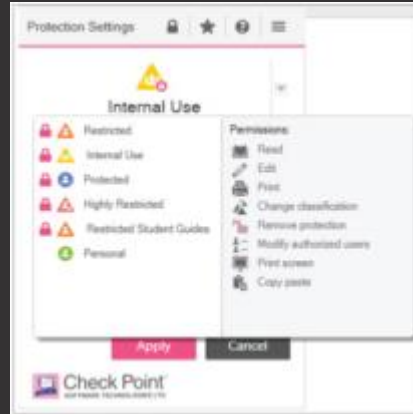
2
CONFIGURATION
CHANGE
MANAGEMENT

3
ADMINISTRATOR
CONTROLS AND
SEPARATION OF DUTIES

4
SECURE
SYSTEM
CONFIGURATION

- **Integrated DLP** - provides awareness of personal data flowing, monitoring of content, and blocking of unauthorized data transmission
- **Check Point Capsule Docs** - tools for content classification

Classification with
Capsule Docs



Classification of Data
with Check Point DLP

Using Check Point Security Products for GDPR



Check Point
SOFTWARE TECHNOLOGIES LTD

1
DATA
CLASSIFICATION

2
CONFIGURATION
CHANGE
MANAGEMENT

3
ADMINISTRATOR
CONTROLS AND
SEPARATION OF DUTIES

4
SECURE
SYSTEM
CONFIGURATION

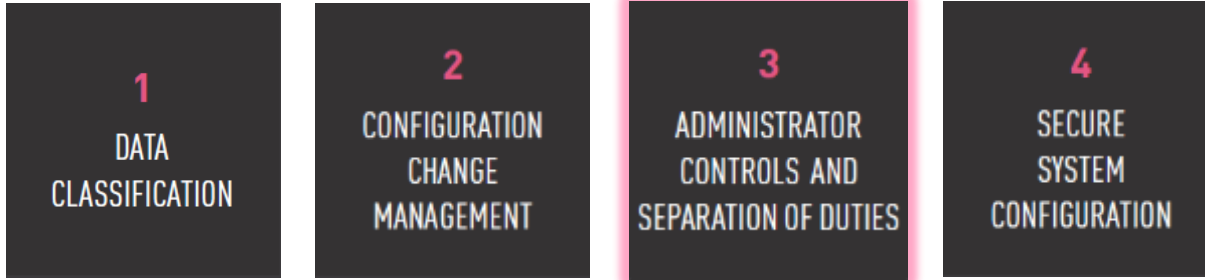
Check Point R80's SmartLog

- Smart Workflow
- SmartLog

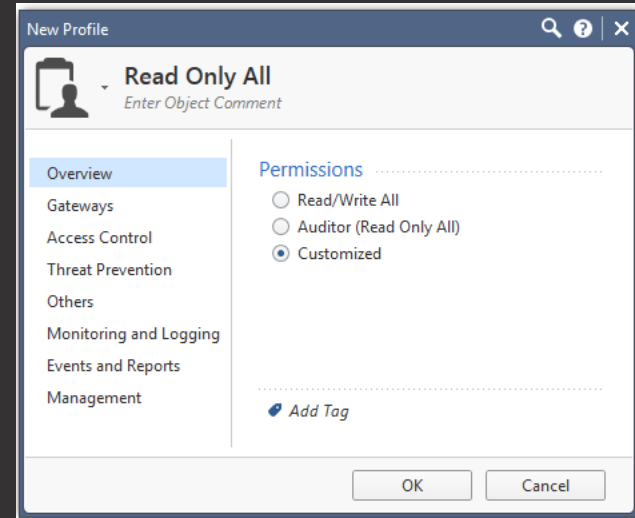
Change approval controls,
full logging of
configuration,
production
of audit-quality automatic
reports

Time	Origin	Source	Source User	Destination	Service	Ac...	Access Rule N...	Policy...	Description
Today, 11:23:12 PM	HQgw	198.54.86.174	Saul	198.51.100.193	http (TCP/80)	5	Block specific U...	Branch...	http Traffic Dropped from 198.54.86.174 to Blocked URL[198.51.100.193]
Today, 11:23:12 PM	HQgw	198.54.86.174	Saul	198.51.100.193	http (TCP/80)	5	Block specific U...	Branch...	http Traffic Dropped from 198.54.86.174 to Blocked URL[198.51.100.193]
Today, 11:19:50 PM	HQgw	198.51.100.15	Walter	ERP Server (198...	ftp (TCP/21)	3	ERP server bein...	Corpora...	ftp Traffic Accepted from 198.51.100.15 to 198.51.100.10
Today, 11:19:50 PM	HQgw	198.51.100.15	Walter	ERP Server (198...	ftp (TCP/21)	3	ERP server bein...	Corpora...	ftp Traffic Accepted from 198.51.100.15 to 198.51.100.10
Today, 11:18:08 PM	HQgw	198.51.100.193	Saul	198.51.100.193	http (TCP/80)	11	Clean up	Corpora...	http Traffic Dropped from 198.51.100.193 to 198.51.100.193
Today, 11:18:08 PM	HQgw	198.51.100.193	Saul	198.51.100.193	http (TCP/80)	11	Clean up	Corpora...	http Traffic Dropped from 198.51.100.193 to 198.51.100.193
Today, 10:50:48 PM	HQgw	198.51.100.193	Walter	198.51.100.193	http (TCP/80)	5	Block abuse/ hl...	Corpora...	http Traffic Dropped from 198.51.100.193 to www.bit.com[198.51.100.193]
Today, 10:50:48 PM	HQgw	198.51.100.193	Walter	198.51.100.193	http (TCP/80)	5	Block abuse/ hl...	Corpora...	http Traffic Dropped from 198.51.100.193 to www.bit.com[198.51.100.193]
Today, 10:40:53 PM	HQgw	198.51.100.193	Saul	BranchOffice (1...	http (TCP/80)	2	DHCP Server for...	Branch...	http Traffic Accepted from 198.51.100.193 to 198.51.100.0
Today, 10:40:53 PM	HQgw	198.51.100.193	Saul	BranchOffice (1...	http (TCP/80)	2	DHCP Server for...	Branch...	http Traffic Accepted from 198.51.100.193 to 198.51.100.0
Today, 10:31:01 PM	HQgw	198.51.100.193	Saul	198.51.100.193	http (TCP/80)	5	HR can access t...	Corpora...	http Traffic Informed from 198.51.100.193 to LinkedIn[198.51.100.193]
Today, 10:31:01 PM	HQgw	198.51.100.193	Saul	198.51.100.193	http (TCP/80)	5	HR can access t...	Corpora...	http Traffic Informed from 198.51.100.193 to LinkedIn[198.51.100.193]
Today, 10:22:29 PM	HQgw	198.51.100.193	Jesse	FTP_Int (198.51...	ftp (TCP/21)	1	Mobile Access f...	Corpora...	ftp Traffic Accepted from 198.51.100.193 to 198.51.100.12
Today, 10:22:29 PM	HQgw	198.51.100.193	Jesse	FTP_Int (198.51...	ftp (TCP/21)	1	Mobile Access f...	Corpora...	ftp Traffic Accepted from 198.51.100.193 to 198.51.100.12
Today, 9:28:38 PM	HQgw	198.51.100.193	Jesse	198.51.100.193	http (TCP/80)	5	Block specific ca...	Corpora...	http Traffic Dropped from 198.51.100.193 to Adobe Flash[198.51.100.193]
Today, 9:28:38 PM	HQgw	198.51.100.193	Jesse	198.51.100.193	http (TCP/80)	5	Block specific ca...	Corpora...	http Traffic Dropped from 198.51.100.193 to Adobe Flash[198.51.100.193]
Today, 9:24:55 PM	HQgw	198.51.100.193	Walter	198.51.100.19	http (TCP/80)	9	Policy for access...	Corpora...	http Traffic Accepted from 198.51.100.193 to Report Portal[198.51.100.193]
Today, 9:24:55 PM	HQgw	198.51.100.193	Walter	198.51.100.19	http (TCP/80)	9	Policy for access...	Corpora...	http Traffic Accepted from 198.51.100.193 to Report Portal[198.51.100.193]
10 Apr 17, 4:49:03 AM	HQgw	198.51.100.193	Jesse	198.51.100.193	http (TCP/80)	3	HR can access t...	Branch...	http Traffic Informed from 198.51.100.193 to Twitter[198.51.100.193]
Today, 9:10:20 PM	HQgw	198.51.100.193	Jesse	FTP_Est (2.3.2...	ftp (TCP/21)	8	Customers to ft...	Corpora...	ftp Traffic Accepted from 198.51.100.193 to 2.3.2.2

Using Check Point Security Products for GDPR



- **Security Management** - separation of duties without impact to operational efficiency



Check Point
R80



Using Check Point Security Products for GDPR

1
DATA
CLASSIFICATION

2
CONFIGURATION
CHANGE
MANAGEMENT

3
ADMINISTRATOR
CONTROLS AND
SEPARATION OF DUTIES

4
SECURE
SYSTEM
CONFIGURATION

- Check Point Compliance Blade – security definitions consistent with GDPR



Using Check Point Security Products for GDPR

5
ACCESS
CONTROL

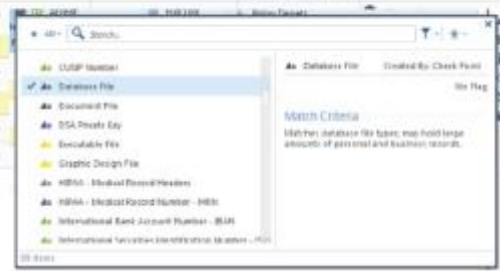
6
NETWORK-
BASED
SEGMENTATION

7
ENCRYPTION
AND
PSEUDONYMISATION

8
DATA
LEAK
PREVENTION

- **Next Generation Firewall** – isolates in-scope data, drastically reducing risk and cost of compliance

No.	Name	Source	Destination	VPN	Services & Applications	Content	Action
8	Customers to ftp servers	ExternalZone	FTP_Est	Any	ftp-protocol-Signat...	Any Direction Archive File	Accept
9	Policy for access to Data Center servers	Any	Data Center LAN				
Temporary Access Grant (20)							
10	Special policy for temp guest rules using wireless LAN	WirelessZone	Any				
Clean Up (11-12)							
11	Clean up	Any	Any				
Cleanup		Any	Any				



Using Check Point Security Products for GDPR

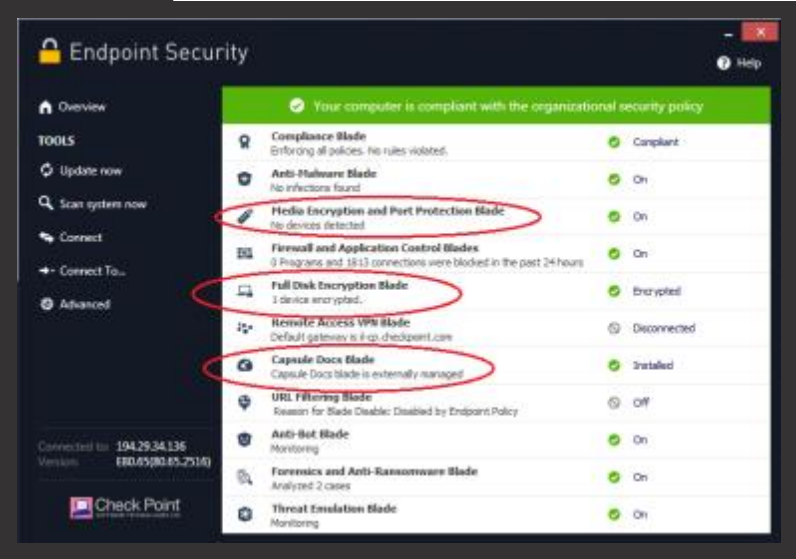
5
ACCESS
CONTROL

6
NETWORK-
BASED
SEGMENTATION

7
ENCRYPTION
AND
PSEUDONYMISATION

8
DATA
LEAK
PREVENTION

- **Endpoint Solution** – extends data protection across organizations
- **Full Disk Encryption (FDE)**
- **Media Encryption and Port Protection (MEPP)**
- **Capsule Docs**
- **Security Appliance, encrypted VPNs**



The screenshot displays the 'Endpoint Security' dashboard. At the top, a green banner indicates 'Your computer is compliant with the organizational security policy'. Below this, a list of security blades is shown with their status:

Blade Name	Status
Compliance Blade	Compliant
Anti-Malware Blade	On
Media Encryption and Port Protection Blade	On
Firewall and Application Control Blades	On
Full Disk Encryption Blade	Encrypted
Rewrite Access VPN Blade	Disconnected
Capsule Docs Blade	Installed
URL Filtering Blade	Off
Anti-Bot Blade	On
Forensics and Anti-Ransomware Blade	On
Threat Emulation Blade	On

Red circles highlight the 'Media Encryption and Port Protection Blade', 'Full Disk Encryption Blade', and 'Capsule Docs Blade' in the original image.

Using Check Point Security Products for GDPR

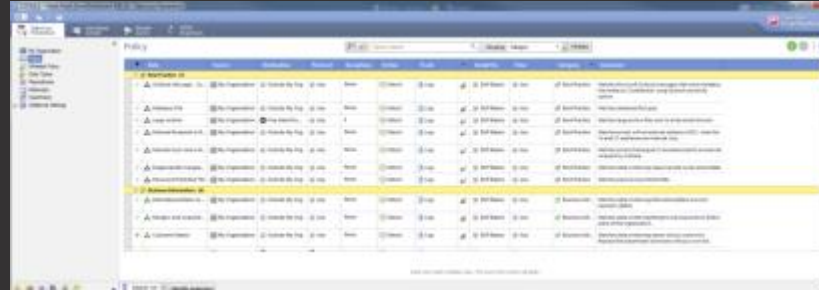
5
ACCESS
CONTROL

6
NETWORK-
BASED
SEGMENTATION

7
ENCRYPTION
AND
PSEUDONYMISATION

8
DATA
LEAK
PREVENTION

Check Point DLP –
policy-based to
monitor content and
log activity



Using Check Point Security Products for GDPR

9
DDOS
PREVENTION

10
USER
ACTIVITY
MONITORING

11
VULNERABILITY
MANAGEMENT

12
DISASTER
RECOVERY

- DDoS Protectors
- Firewall
- IPS

Real-time prevention of volumetric and application-based attacks

Using Check Point Security Products for GDPR

9
DDOS
PREVENTION

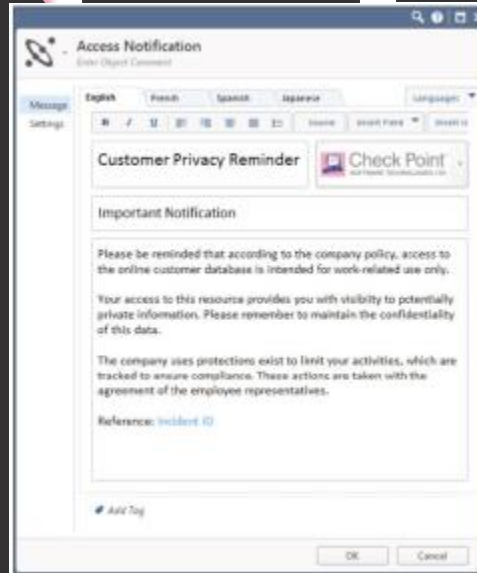
10
USER
ACTIVITY
MONITORING

11
VULNERABILITY
MANAGEMENT

12
DISASTER
RECOVERY

- UserCheck Agent

Real-time notifications on contradictions of policy



Using Check Point Security Products for GDPR

9
DDOS
PREVENTION

10
USER
ACTIVITY
MONITORING

11
VULNERABILITY
MANAGEMENT

12
DISASTER
RECOVERY

- **Check Point IPS** – blocks known vulnerabilities
- **Check Point SandBlast** – prevents advanced, unknown attacks on cloud, network, endpoint and mobile

Using Check Point Security Products for GDPR

9

DDOS
PREVENTION

10

USER
ACTIVITY
MONITORING

11

VULNERABILITY
MANAGEMENT

12

DISASTER
RECOVERY

Virtual and physical high availability options to prevent single points of failure

THANK YOU