Check Point
SOFTWARE TECHNOLOGIES LTD

THE EU GENERAL DATA PROTECTION REGULATION

CHECK POINT FOR EFFICIENT AND EFFECTIVE COMPLIANCE

WELCOME TO THE FUTURE OF CYBER SECURITY

EXECUTIVE SUMMARY

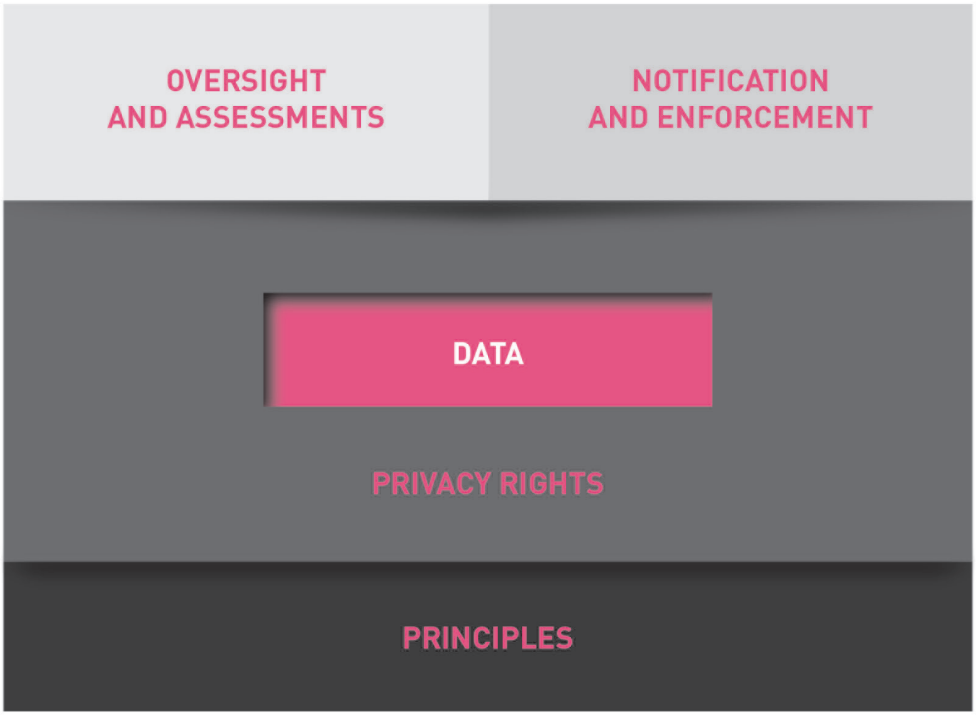
The European Union's General Data Protection Regulation ("GDPR") is a game changer for data protection. Its broad scope applies to any organization worldwide that handles any EU citizen's private information. It imposes an extensive list of protections on that data, limitations on how it is used, and customer notifications and consent in a wide range of situations. Crucially, GDPR mandates significant penalties for non-compliance. GDPR takes effect in mid-2018, which means organizations need to start planning their strategy for compliance now. Check Point solutions enable organizations to take immediate steps towards compliance with minimal impact to applications and operations. The following white paper presents an overview of the regulation, followed by a description of how Check Point can help organizations take immediate steps towards achieving compliance.

> "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."
>
> *— GDPR, Article 5*

BACKGROUND:
THE EU GENERAL DATA PROTECTION REGULATION

The European Union's new General Data Protection Regulation (EU 2016/679, commonly known as "GDPR") will have far reaching consequences for many organizations worldwide. By establishing data protection as a fundamental right (and not just a consumer right), GDPR places significant policy and technical responsibilities on any organization that handles EU citizens' personal data, whether or not that organization physically operates in the EU. The regulation takes effect in May 2018, strongly suggesting that organizations need to start working on compliance now.

A key reason GDPR is so potentially impactful is the magnitude of the penalties for non-compliance. Fines for non-compliance can range up to 4% of a business's worldwide revenue. Also, breach notification within a very short time window (72 hours) may be required when control over personal data is compromised. This notification can include both government compliance bodies and the impacted citizens themselves. Regardless of the fines, it should be clear that the main intent of this regulation is that the privacy rights shall be enacted while preserving the possibility of "free flow" of personal data. GDPR in its highest scope should not be considered as not preventive – but an enabler! It gives rules under which the processing of data and personal information is permitted.



CORE ELEMENTS OF GDPR

PRIVACY RIGHTS GRANTED BY THE GDPR

At the heart of GDPR is the goal of defining data protection rights afforded to all EU citizens. The focus of the regulation is on mandating those rights, no matter what organization is processing a citizen's personal data, or where it is taking place. Therefore core elements of the GDPR detail a number of "Rights of EU Citizens" with respect to how their personal data are used. The list is extensive, and will require significant changes to applications, policies and procedures to attain compliance. For example:

- Organizations must obtain consent from the citizen to process his or her data, and this consent must be obtained in a way that is clear to the citizen (no pages of legal text with an "Accept" checkbox at the bottom).
- They must make available to all citizens information on exactly what data is being gathered, what purpose it is being used for, where it is being processed, and with what other organizations the data might be shared.
- They must provide an explanation of the logic involved in any automated processing that is being performed on a person's data.
- There is a "right to be forgotten", that is, the right to request that all data about an individual be deleted, as well as a right to easily transfer one's data from one organization to another.

The rather extensive set of rights will place a significant burden on any organization that handles EU citizen data.

> "...the controller and the processor shall implement appropriate... measures to ensure a level of security appropriate to the risk, including...the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services"
>
> *— GDPR, Article 32*

GDPR PRINCIPLES

Beyond the rights of citizens, GDPR defines a set of "principles" that govern all processing of personal data. The idea is to define the conditions on which data processing is permitted. If an organization can't show they are operating within those conditions, then their activities may be considered unlawful under the GDPR.

A key principle is that data can only be collected "for specified, explicit and legitimate purposes", which means it won't be acceptable to collect data first and figure out how it could be used later. Furthermore only the minimum amount of data necessary to perform these tasks may be collected. And organizations cannot hold onto the data in a format that allows easy identification of the people involved after it is no longer needed for the original purpose.

Most relevant for security professionals, the GDPR states that data must be processed in a manner that ensures "data security, integrity and confidentiality". However what the GDPR does not do is include a detailed list of technical controls to be implemented to meet these requirements. Unlike for example PCI DSS, GDPR maximizes flexibility, and instead provides only a basic set of guidelines. These guidelines are included in Article 32 of the GDPR text and specify that controllers and processors of data should implement controls that ensure:

1
THE PSEUDONYMISATION AND ENCRYPTION OF PERSONAL DATA

2
THE ONGOING CONFIDENTIALITY, INTEGRITY, AVAILABILITY AND RESILIENCE OF PROCESSING SYSTEMS AND SERVICES

3
THE ABILITY TO RESTORE THE AVAILABILITY AND ACCESS TO PERSONAL DATA IN A TIMELY MANNER IN THE EVENT OF A PHYSICAL OR TECHNICAL INCIDENT

4
A PROCESS FOR REGULARLY TESTING, ASSESSING AND EVALUATING THE EFFECTIVENESS OF TECHNICAL AND ORGANISATIONAL MEASURES FOR ENSURING THE SECURITY OF THE PROCESSING

The GDPR aligns these controls to a risk-based approach and notes that controls should be "baked into" systems and applications when they are designed, rather than added after the fact.

Consistent with security best practices, GDPR also mandates ensuring the availability of data. The text of the framework requires that data processors provide: "...the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident." Therefore, to be compliant with GDPR, organizations must implement sufficient systems and processes to maintain high availability of personal data. They must also regularly test and evaluate the security measures implemented to protect that data.

> "...the controller shall, both *at the time of the determination of the means for processing* and at the time of the processing itself, implement appropriate technical and organisational measures...which are designed to implement data-protection principles...in an effective manner and to integrate the necessary safeguards into the processing..."
>
> *— GDPR, Article 25 (italics added)*

PREPARING FOR GDPR

Preparing for GDPR is challenging for two reasons:

1. The regulation is new, and there is no experience from previous audits that an organization can draw upon.
2. Many aspects of GDPR are still a "work in progress." For example, GDPR introduces the concept of Codes of Conduct: industry specific policies and controls that could be adopted to demonstrate compliance. However, no Codes of Conduct currently exist. As another example, GDPR establishes a European Data Protection Board (EDPB) to "take an active role in enforcing EU data protection law." However, the formalization of the EDPB is still in process and the specifics are yet to be determined.*

Nevertheless, the limited lead time until the regulation goes into effect requires that organizations begin the process of planning their GDPR strategy now. The following table summarizes recommended focus areas and action items to begin the GDPR preparation process (the items below are not placed in chronological order):

GDPR Preparation Area	Recommended Actions
Staffing	Identify executive sponsor, technical lead, and decide whether to hire or outsource Data Protection Officer
Data Audit and Classification	Locate in-scope personal data. Map data flows and relevant systems, including third parties and backup systems
Risk Analysis	Evaluate risk based on data types, volume, and processing systems
Logging of Activity and Breach Identification	Establish robust audit trail of activity on in-scope systems, especially data access and admin activity, as well as rich logging across all protections in order to identify potential breach activity
Fundamental Controls	Specify basic control set on in-scope systems and define implementation projects

These preparation areas cover a wide scope of activities. This document will focus primarily on the fundamental controls associated with ensuring the confidentiality, integrity and availability of protected data.

* Check Point will update this document as aspects of GDPR are clarified.

FUNDAMENTAL SECURITY CONTROLS

The GDPR guidelines are based on a risk-based approach to ensuring the privacy and security of an individual's data. Specifically, GDPR proposes that relevant entities implement measures that are appropriate to the value or damage associated with the loss of personal information.

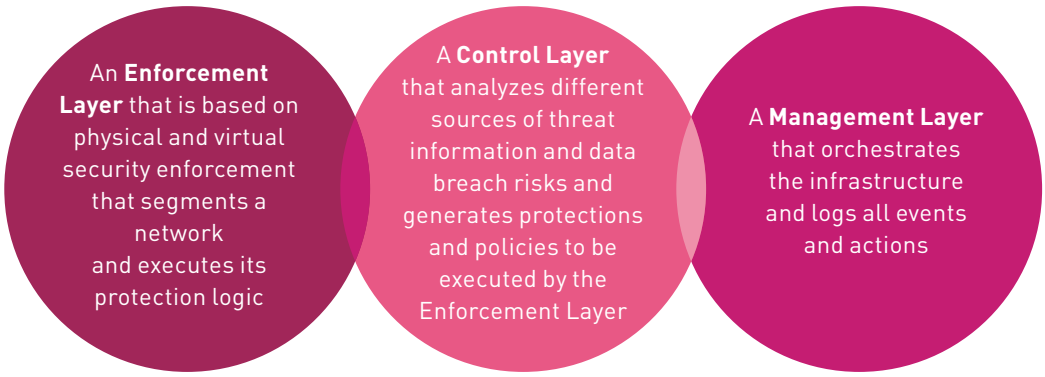
GDPR does not list the exact controls that organizations should implement to be compliant. Nevertheless, general security best practice suggests that the following would serve as a good starting point:

1 DATA CLASSIFICATION	2 CONFIGURATION CHANGE MANAGEMENT	3 ADMINISTRATOR CONTROLS AND SEPARATION OF DUTIES	4 SECURE SYSTEM CONFIGURATION
5 ACCESS CONTROL	6 NETWORK-BASED SEGMENTATION	7 ENCRYPTION AND PSEUDONYMISATION	8 DATA LEAK PREVENTION
9 DDOS PREVENTION	10 USER ACTIVITY MONITORING	11 VULNERABILITY MANAGEMENT	12 DISASTER RECOVERY

IMPLEMENTING FUNDAMENTAL SECURITY CONTROLS WITH CHECK POINT SOFTWARE DEFINED PROTECTION

Until GDPR implementation guidelines and certification standards are better established, organizations can leverage existing methodologies that are based on a risk-based approach. Check Point's Software Defined Protection (SDP) is such a model.

The SDP architecture uses a three-tiered security approach that partitions the security infrastructure into three interconnected layers:



The selection of relevant protections that are implemented in the enforcement layer is based on an understanding of the risk associated with a security event. In the case of GDPR, such an event could be the loss or modification of an individual's personal data or a network breach that would provide access to the individual's data.

Check Point's SDP fully supports the best practice controls previously noted. A further discussion of control implementation can be found in the Appendix, and includes the following:

Control	Check Point Support
Data Classification	Integrated DLP at gateway provides awareness of personal data flowing across the network, monitoring of content, and blocking of unauthorized data transmission. In addition, Check Point Capsule Docs ERM offers tools for content classification.
Configuration Change Management	SmartWorkflow and SmartLog blades establish change approval controls, full logging of configuration changes, and production of audit-quality reports automatically.
Administrator Controls and Separation of Duties	Security management supports fine-grained permissions and logging based on role, to facilitate separation of duties without impact to operational efficiency.
Secure System Configuration	Compliance Blade ensures that security definitions within an organization's architecture are consistent with GDPR.
Network-Based Segmentation	Next Generation Firewall based network segmentation isolates in-scope data, drastically reducing risk and cost of compliance. Segmentation can be defined by application or data parameters, making it simple to segment according to data protection guidelines.

Control	Check Point Support
Encryption and Pseudonymisation	Check Point's Endpoint solution extends data protection across the organization. Its Full Disk Encryption (FDE) software blade encrypts employee computer hard drives, and Media Encryption and Port Protection (MEPP) encrypts and controls connections to removable storage. The solution also protects documents with its ERM technology, Capsule Docs. Security Appliance based remote access and site-to-site encrypted VPNs protect data in motion.
Data Loss Prevention	DLP policy-based solution to monitor content and log activity based on standardized or custom rules. Real-time feedback educates users on privacy guidelines, with optional blocking of actions that would violate GDPR controls.
DDOS Prevention	Dedicated DDoS Protectors, firewall and IPS prevent volumetric and application-based attacks in real-time.
User Activity Monitoring	UserCheck agent provides real-time notification to users when they interact with sensitive applications or content, or behave in ways that contradict policy. Identity and group-based logging.
Vulnerability Management	IPS can be leveraged to block exploits to known vulnerabilities during the patch process. SandBlast advanced threat prevention identifies and prevents advanced, unknown attacks on cloud, network, endpoint and mobile.
Disaster Recovery	Virtual and physical high availability options to prevent single points of failure, including ClusterXL and support for dynamic routing and fail-over protocols to transfer traffic to systems with the fastest response times.

SUMMARY

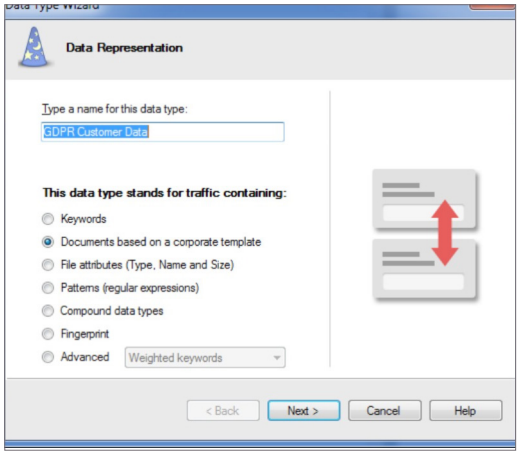
The European Union's new General Data Protection Regulation (GDPR) will have far reaching consequences for many organizations worldwide. GDPR is an emerging regulation, and what constitutes acceptable compliance with the law is not yet fully understood. However the intention of the regulation with respect to data protection is clear, and therefore it is possible to start planning for compliance now. Strategies should be researched and developed as soon as possible in areas such as data classification and scope definition, data usage policies, notifications and audit trails. Check Point solutions have long been used by organizations of all sizes and types to implement compliance controls for regulations similar to GDPR. Therefore, the combination of these solutions with a risk-based approach to GDPR enables organizations to aggressively move toward compliance in a proven yet operationally efficient manner.

APPENDIX:
CHECK POINT SOLUTIONS FOR GDPR CONTROLS

Check Point offers a range of solutions that can help companies implement security architectures that address the themes of the GDPR. The technologies operate within the three layers of the SDP architecture.

Data Classification

Check Point provides solutions, such as the Data Security (DLP) blade, that organizations can use to implement data classification guidelines quickly.



Organizations can upload corporate templates directly into the solution's management tools. Such templates can include confidentiality levels tied to data elements and can include watermarks, icons and terminology to help users understand the rules to which file types apply. The solution identifies the extent to which files flowing across the network match these templates and then allows or blocks their transmission in real-time.

The Check Point solution set also includes tools that allow administrators to quickly define repositories and network segments where data security controls should be implemented. The Capsule Docs (ERM) offering integrates directly into Microsoft Office and Adobe Acrobat to embed data classification at the time of document creation

Configuration Change Management

Data security programs require a combination of process and technology controls. Within the process area, organizations need to validate if changes were made to the systems that are involved in processing data as well as those that protect the data elements themselves. Check Point's management system includes functions, such as SmartLog, that track administrator changes to rules as well as specific data security-related events at both network and endpoint levels. These can be configured to automatically categorize relevant changes into reports that auditors and data privacy officers can review to ensure that identified changes follow or conflict with relevant data privacy guidelines. In addition, solutions such as SmartWorkflow can introduce change management steps such that attempts to modify configuration settings would require an approval process prior to implementation.

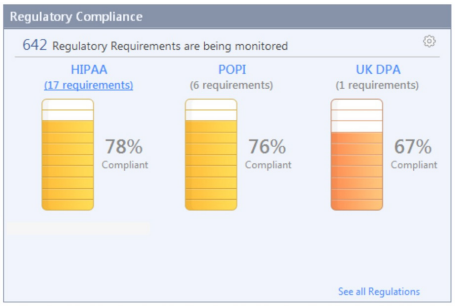
Administrator Controls and Separation of Duties

One of the primary tenants of all security frameworks is separation of duties. This principle is intended to ensure that only individuals who need to access certain information and systems can do so. The definition and modification of security policies is an area to which this guideline clearly applies.

Practitioners with responsibility for access control rules should be delineated from those who oversee threat prevention or data security so that one person cannot modify an organization's entire security architecture. Check Point's management solutions embrace this principle and allow administrators to define rules that are assigned to individual users or types of users. This applies to different classes of security controls as well as specific rules within the organization's security policy.

Secure System Configuration

The Check Point Compliance Blade offers an automated method to assess if the configuration of security definitions within an organization's architecture are consistent with government regulations.



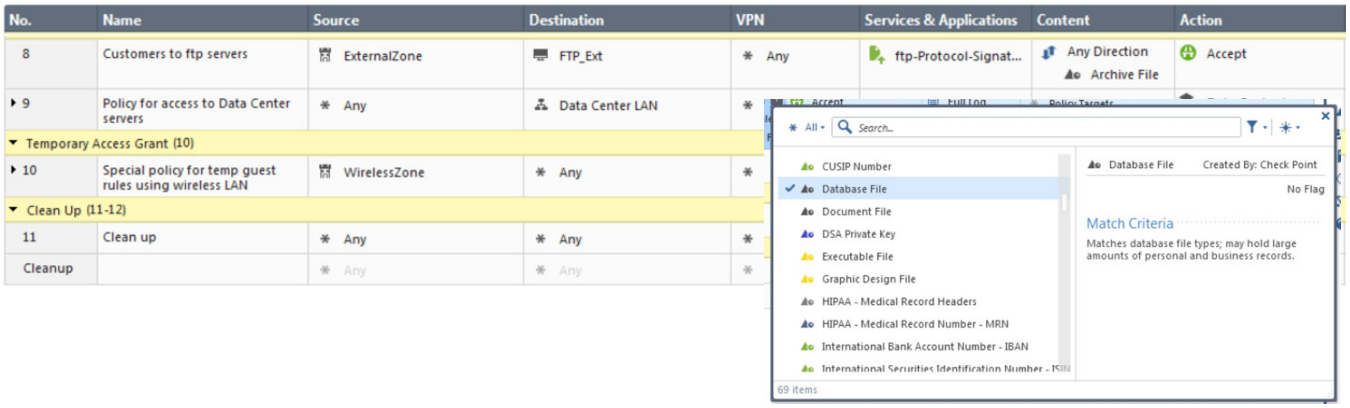
The solution reviews device and rule-base settings in real-time and compares them with the specific controls of the various regulations. It then calculates the extent to which configuration and rule-base definitions are compliant with the relevant regulatory framework.

Administrators can leverage this information to speed their GDPR preparations. The solution includes an array of European and other country-specific regulatory frameworks, including an initial set of GDPR controls.

Network-Based Segmentation

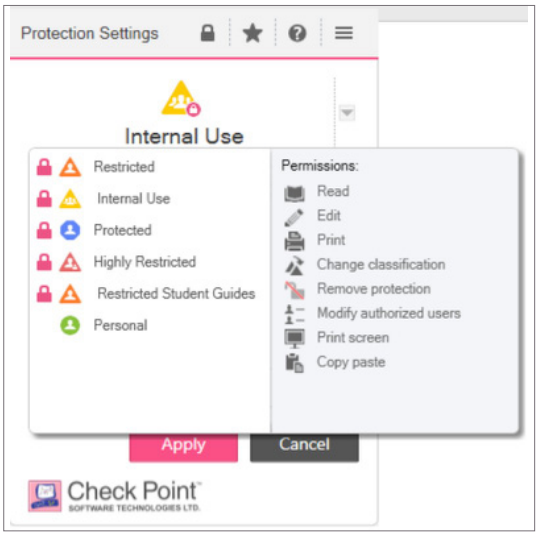
The GDPR framework emphasizes that data security should be built-in to an organization's processes and not bolted-on after the fact. Check Point helps companies build security architectures that are consistent with this built-in approach.

Network segmentation can be defined according to network, application and data parameters within the same rule. This content awareness makes it much easier to segment networks according to data security guidelines.



Encryption and Pseudonymisation

Pseudonymisation and/or encryption should be implemented across all systems where individual data records are processed and stored. Key to this recommendation is the binding of data encryption to the creation of files that might include personal information.



The Check Point Capsule Docs offering integrates into productivity tools, such as Microsoft Office, and can be configured so that all content created by users is encrypted and therefore inaccessible to unauthorized parties. These protections integrate into email clients, such as Outlook, to prevent users from accidentally sending files to the wrong recipients. This function applies to the computers, mobile devices and cloud-based systems with which users interact.

The Check Point Endpoint solution offers a wide variety of encryption technologies, including:

- IPSec and SSL encryption of data in transit through remote access VPN tunneling
- Disk and removable media encryption
- Port protection to control the use of physical ports on end user devices.

Data Loss Prevention

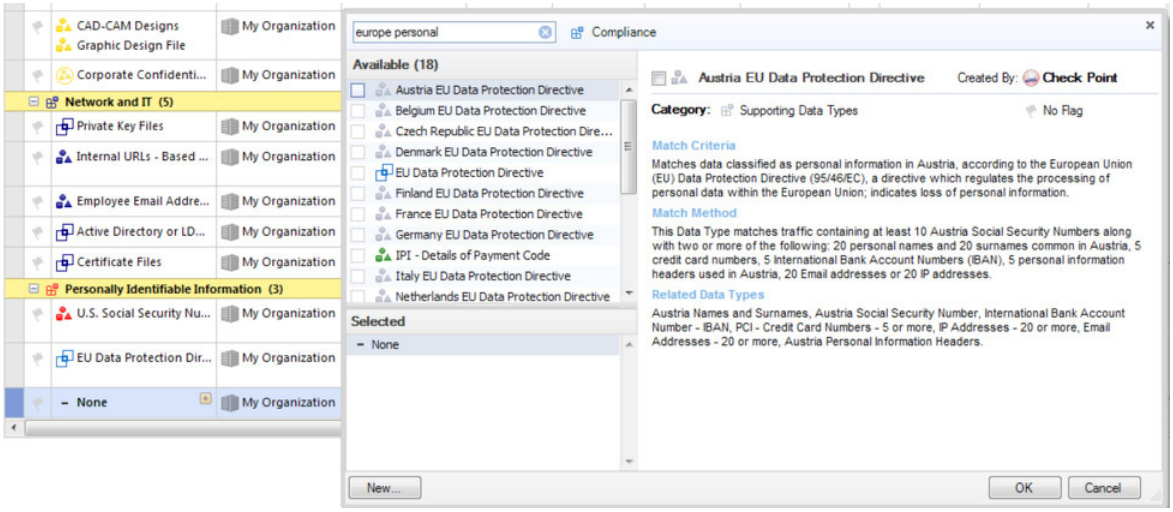
Incidents of data breach take place either as a result of human error or malicious intent. Implementing controls that address both scenarios can be complex and time consuming. Check Point simplifies the data security process by providing administrators with a database of common file types. This especially true for personally identifiable information (PII). Check Point's DLP capabilities can filter traffic for multiple PII formats automatically. The solution will also inspect content based on the rules associated with different regulatory frameworks.

The Check Point DLP Policies can be defined so that users are notified in real-time if their behavior contradicts with organizational guidelines. This helps reinforce security awareness programs, which are often key components of information and data security regulatory frameworks.

DDOS Prevention

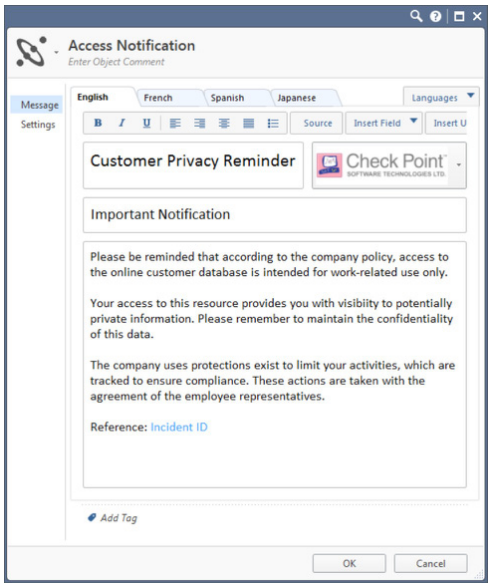
GDPR suggests that organizations ensure an individual's access to their information at all times. Considering the near continuous flow of denial service attacks on the Internet, it can be difficult for organizations to abide by this recommendation and ensure that online services are consistently available.

Check Point provides a range of capabilities to simplify this effort. Dedicated DDoS Protectors prevent volumetric and application-based attacks in real-time. Check Point IPS and firewall features can also be used to throttle connections and block malformed packets associated with DDoS behavior.



User Activity Monitoring

Users represent the weakest link in any data security program. Their mistakes and malicious behavior open the door to attacks and lead to data leakage.



To address this challenge, organizations can leverage a combination of functions within the Check Point solution set:

1. Identity Awareness defines rules according to the attributes and identities of specific employees and employee groups.
2. UserCheck provides real-time notification to users when they interact with sensitive applications, content or behave in ways that contradict policy.
3. Logging functions highlight security events, such as data loss, and include the names and identifiers of the individuals associated with the events.

Of particular value in user activity monitoring is the ability to capture evidence from user computers. The Check Point Endpoint security solution includes a forensic function that records incidents of data exfiltration caused by either intentional behavior or malware activity.

Vulnerability Management

Standard security practice recommends that organizations perform regular vulnerability management to identify if their applications and network components are vulnerable to attack. This is an important step in limiting the options that attackers have at their disposal to breach systems and steal sensitive personal data.

Challenges arise with patching these systems to remediate vulnerabilities identified during the assessment process. It can take time to update operating systems and applications across the enterprise. Check Point's IPS technologies can be leveraged to block exploits to known vulnerabilities immediately, prior to the completion of the patch process.

With the rise of zero day attacks, organizations need to also consider ways to block exploits based on unknown vulnerabilities. These would not be identified during standard vulnerability management processes. Check Point's SandBlast solutions help identify and prevent advanced, unknown attacks. SandBlast operates on the network, cloud and endpoint. The technology emulates files within virtualized OS instances to trigger attack processes, and the SandBlast solutions also strip active content on the fly in order to clean any malicious or active content from files.

Disaster Recovery

The GDPR recommendations associated with disaster recovery are intended to ensure that individuals can gain access to their data at all times. Complying with these recommendations requires multiple layers of redundancy. Network and application components need to be configured in high-availability (HA) clusters so that the potential loss of an individual system does not cause service disruption. Check Point's solutions provide multiple HA options to prevent single points of failure, from native clustering technologies such as ClusterXL, to support for dynamic routing and fail-over protocols that leverage the network or hypervisor fabric to transfer traffic to systems with the fastest response times.

Check Point also offers multiple virtual gateway options. These enable organizations to apply their security architectures within virtualization platforms, public and private, and thereby develop disaster recovery sites quickly and with their full set of data and network security controls.

CONTACT US

Worldwide Headquarters

5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 |
Email: info@checkpoint.com

U.S. Headquarters

959 Skyway Roaad, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233 |
www.checkpoint.com