



# CHECK POINT SECURITY MANAGEMENT

## CHECK POINT SECURITY MANAGEMENT

The future of security management

### Product Benefits

- Keep pace with dynamic network changes
- Reduce operational overhead
- Better align security with business goals
- Anticipate & prevent the next attack

### Product Features

- Single console for all aspects of security
- Unified policy for managing entire infrastructure
- Unparalleled policy granularity & segmentation
- R80 API enables security self-service and automated workflows
- Concurrent administration & segregation of duties
- Integrated threat management
- Scalable, extensible architecture

## INSIGHTS

Today, managing security can be a complex endeavor. The growing complexity of networks, business innovation requirements, and rapid delivery of services and applications require a new approach to managing security. Traditional security management approaches of multiple point products, manual change processes, monolithic policies and data siloes no longer work. Security needs to be agile, efficient and anticipate the latest threats.

## SOLUTION

Check Point R80 Security Management sets the standard for reliability and ease-of-use in security management. From policies and operations to people and technology, its future-proof design anticipates your security needs. It consolidates all aspects of your security environment seamlessly so you can deploy the strongest protections across your organization effectively and efficiently – without impeding business innovation.

## BUILT UPON A SCALABLE, EXTENSIBLE ARCHITECTURE



Next Generation  
Policy



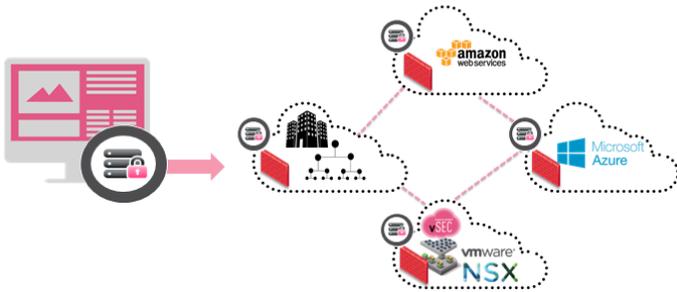
Efficient, Automated  
Operations



Integrated Threat  
Management

## UNIFIED CONSOLE, UNIFIED POLICY

With R80, access control and threat prevention management for all enforcement points are fully unified under the same console, removing the need to move between multiple interfaces. Unified management for both physical and virtual networks, on-premise or cloud enforcement points, ensures security consistency and full visibility into traffic across the network.



**Figure 1: One single policy for your entire infrastructure**

A single policy for users, data, applications and networks allows unparalleled granularity control, speeds administration and reduces policy change backlogs.

No.	Name	Source	Destination	Services & Applications	Data	Action	Install On
1	Outbound access	production_net	Internet	Any	Any	AccessSubLayer	Policy Targets
1.1	Social media for marketing	marketing_role	Internet	Twitter, LinkedIn, Instagram	Any	Accept	SG13000
1.2	Developers upload	developer_role	Internet	Dropbox, Box	Any	Accept	SG13000
2	Access Sensitive Servers	Any	Any	Any	SensitiveServers	Accept	Solid Targets
2.1	Mobile Access	Mobile Devices	MailUS	MailServer	Any	Accept	Mobile
2.2	Access to Web Server	Any	WebServer	https	Any	Accept	AWS, VMware



**Figure 2: Unified policy with unparalleled granularity**

## NEXT GENERATION POLICY

Today's virtual cloud environments enable extreme agility where applications, services and servers are automatically provisioned without human interaction. Security installed on the perimeter simply cannot keep up. Check Point's next generation policy makes it extremely easy to segment policy into manageable sections. These sub-policies can be aligned to your network or business function. Each sub-policy can be delegated, automated or deployed independently. Workload can be distributed across teams, freeing key security personnel for strategic tasks.

## EFFICIENT OPERATIONS

With too much work and too little staff, security teams need to work smarter. Automation and granular delegation are key to helping alleviate operational overhead. With the R80 API, security teams can automate any task or create web portals for security self-service.

Other efficiency elements include features built into the management interface to anticipate the daily needs of an administrator, providing him security intelligence to make better policy decisions. Concurrent administration now allows multiple administrators to work simultaneously on the same policy without conflict.

## FULLY INTEGRATED THREAT MANAGEMENT

With R80, Threat Management is fully integrated, with logging, monitoring, event correlation and reporting in one place. A visual dashboard provides full visibility into security across the network, helping you monitor the status of your enforcement points and stay alert to potential threats.



**Figure 3: Visual, comprehensive view of your environment**

This fully customizable dashboard allows you to focus only on what matters to you. You get a comprehensive view of your security posture, and can quickly drill down into incident or log details with a few clicks. Reports are easily tailored to for your stakeholders and accessible from any web browser.

## SCALABILITY AND EXTENSIBILITY

The R80 platform was built to scale to the most complex and dynamic environments. With our R80 API, it is easy to connect security to IT processes and systems across your network, paving the way for you to automate security change control and provisioning across your infrastructure.

## SECURITY MANAGEMENT SUITE

The Check Point Security Management suite consists of the following modules:

POLICY MANAGEMENT	
Policy Management	Unified network policy management for Check Point gateways and software blades.
Multi-Domain Management	Central management of many distinct security policies across multiple domains, allowing administrators to consolidate hardware.
Management Portal	Browser-based security management access for groups, such as technical support teams or auditors, to view policies, gateway status and user administration.
OPERATIONS MANAGEMENT	
Compliance	Validates policy and configuration changes in real-time, against a library of 300+ security best practices and industry standards.
Provisioning	Centralizes Check Point device provisioning. Using profiles, security administrators can automate device configuration and easily roll out changes to multiple, geographically distributed devices via a central console. Also enables quick deployment of new devices.
Workflow	Automates policy change management to centrally manage editing, review, approval and auditing of policy changes.
User Directory	Centralizes user management, enabling gateways to use LDAP-based information stores, eliminating risks associated with manually maintaining and synchronizing redundant data stores.
THREAT MANAGEMENT	
SmartEvent and Reporter	Centralizes security event correlation for Check Point enforcement points. Minimizes time spent analyzing data, isolating and prioritizing the real security threats. Centralizes reporting on network, security and user activity and consolidates data into concise pre-defined or custom-built reports.
Monitoring	Centrally monitors Check Point devices. Alerts security team to changes in gateway, end point, remote user and security activity. Presents a complete picture of network and security performance, enabling fast responses to changes in traffic patterns or security events.

R80 Upgrade Path	Versions
Security Management servers supported	R75.47, R76, R77, R77.10, R77.20, R77.30

### CONTACT US

**Worldwide Headquarters** | 5 Ha'Soleim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com  
**U.S. Headquarters** | 959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233 | www.checkpoint.com