SOFTWARE-DEFINED PROTECTION
SOFTWARE-DEFINED PROTECTION
Modern security architecture powered by collaborative intelligence

Business today is driven by free-flowing information. Corporate data travels through the cloud and mobile devices and radiates through ideas and posts in social networks. BYOD, mobility and cloud computing have revolutionized static IT environments, introducing the need for dynamic networks and infrastructures.

But if our IT environment has changed quickly, the threat landscape has changed even faster. The sophistication and velocity of this evolution is growing exponentially by unleashing new attack types frequently, combining known and unknown threats, taking advantage of “zero-day” vulnerabilities, and utilizing hidden malware inside documents, websites, hosts and networks.

In a world with high-demanding IT infrastructures and networks, where perimeters are no longer well defined, and where threats grow more intelligent every day, we need to define the right way to protect enterprises in the ever changing threat landscape.

There is a wide proliferation of point security products; however these products tend to be reactive and tactical in nature rather than architecturally oriented. Today’s corporations need a single architecture that combines high performance network security devices with real-time proactive protections.

A new paradigm is needed to protect organizations proactively.

Software-defined Protection is a new, pragmatic security architecture and methodology. It offers an infrastructure that is modular, agile and most importantly, SECURE.

Such architecture must protect organizations of all sizes at any location: headquarters networks, branch offices, roaming through smartphones or mobile devices, or when using cloud environments.

Protections should automatically adapt to the threat landscape without the need for security administrators to follow up manually on thousands of advisories and recommendations. These protections must integrate seamlessly into the larger IT environment, and the architecture must provide a defensive posture that collaboratively leverages both internal and external intelligent sources.

The Software Defined Protection (SDP) architecture partitions the security infrastructure into three interconnected layers:

- An Enforcement Layer that is based on physical, virtual and host-based security enforcement points and that segments the network as well as executes the protection logic in high-demand environments.

- A Control Layer that analyzes different sources of threat information and generates protections and policies to be executed by the Enforcement Layer.

- A Management Layer that orchestrates the infrastructure and brings the highest degree of agility to the entire architecture.
By combining the high performance Enforcement Layer with the fast-evolving and dynamic software-based Control Layer, the SDP architecture provides not only operational resilience, but also proactive incident prevention for an ever-changing threat landscape.

Designed to be forward-looking, the SDP architecture supports traditional network security and access control policies requirements as well as the threat prevention needed by modern enterprises that embrace new technologies such as mobile computing and Software-defined Networks (SDN).

**ENFORCEMENT LAYER**

The SDP architecture Enforcement Layer is designed to be reliable, fast and simple. It consists of both network security gateways and host-based software that function as the enterprise network enforcement points. These enforcement points can be implemented as either physical, virtual or as endpoint host components in the enterprise network or in the cloud.

The main principle behind the Enforcement Layer is segmentation. Segmentation is critical for the survival of an organization under attack because each attack that targets a single component of the network should not be able to undermine the entire enterprise security infrastructure. The role of segmentation in the SDP architecture is to prevent an attack from proliferating within the network, as well as to allow only authorized traffic to flow, according to the enterprise business processes.
Implementing segmentation starts with defining the “atomic” segments in the network. An atomic segment contains elements that share the same policy and the same protection characteristics. Enforcement points are introduced at the boundaries of each atomic segment to enforce defined protection logic. Atomic segments can be grouped to allow for modular protection. In addition, trusted channels are established to protect interactions and data flow between various network segments.

Below are the four key steps of the segmentation methodology:

1. **Atomic Segments**
   - Elements that share the same policy and protection characteristics

2. **Segment Grouping**
   - Grouping of atomic segments to allow modular protection

3. **Consolidation**
   - Of physical and virtual components, as network security gateways or as host-based software

4. **Trusted Channels**
   - Protect interactions and data flow between segments

**CONTROL LAYER**

The role of the Control Layer is to generate protections and deploy them for execution at the enforcement points. This layer consists of threat prevention, access control and data protection.

The threat prevention policy is simple: “Block the bad guys!!!” This policy requires little customization and is rather generic. Threat prevention protections block attackers and deny exploitation of vulnerabilities and delivery of malicious payloads. They also prevent malware and bots from connecting to Command and Control (C&C) servers.

In order to define the correct enforcement decision, the threat prevention component of the Control Layer correlates findings of multiple engines — signatures, reputation, behavior, malware emulation and human validation — to generate the right security protection.

For threat prevention controls to be effective, they need to be fed by extensive and reliable threat intelligence. Organizations should expect a steady stream of threat intelligence to pour into their security environment without manual intervention.

Threat intelligence is obtained using external and internal sources of threat data. These sources should ideally include public security intelligence, such as Computer Emergency Readiness Teams (CERTs) and Computer Security Incident Response Teams (CSIRTs), various security analysts, security product vendors and other organizations within the security community. In addition to such external sources, threat intelligence is generated within the enterprise through malware research, sandboxing techniques and data analysis of security events collected from enforcement points.
Threat intelligence describes threat agents, campaigns, and Tactics, Techniques and Procedures (TTPs) and provides real-time threat indicators.

The threat prevention controls using threat intelligence translate the security Big Data into actionable intelligence in the form of indicators and attack descriptions. Those indicators are the logic from which the enforcement layers execute their enforcement decisions.

Unlike threat prevention, both access and data controls are much more specific to individual enterprises.

Access control and data protection enable business processes by defining the interactions between users and data within the corporate network. They apply the minimum level required to support the business and enforces the security principle of “Least Privilege.”

These protective controls depend on repositories that describe enterprise-specific business rules, assets, users, roles and applications and define security policies for the set of authorized interactions between these same assets, users and applications.

The analysis and control of traffic are done in an adaptive way based on context. For example, in the case of Internet traffic, the control layer may consult with a cloud database for the latest applications and protocols, while in the case of internal traffic, it may use the definition of a propriety application or protocol used by the organization. In addition, the Control Layer is aware of network changes and definitions implemented in other IT systems. Examples may be: user repositories changes, automatically applying security to a new Virtual Machine, or allowing access to a new host defined in a Domain Name Server (DNS).

Threat Intelligence

- Security Analysts
- CERTs
- Security Community

External Sources

- Malware Research
- Sandboxing
- Security Events Analysis

Internal Sources

Big Data Analysis

Threat Indicators

Context and Metadata

Security Protections

External Sources

- Security Analysts
- CERTs
- Security Community

Internal Sources

- Malware Research
- Sandboxing
- Security Events Analysis

Big Data Analysis

Threat Indicators

Context and Metadata

Security Protections
The Management Layer makes the Software-defined Protection architecture come alive. By enabling each component of the architecture, this layer acts as the interface between the security administrators and the other two SDP layers.

The SDP management layer should be open, modular and allow visibility into the enterprise security posture.

Enterprise configurations evolve rapidly, with networks, applications, hosts, users and roles adapting dynamically to a changing business environment. This is especially true in virtualized environments using server virtualization and SDN, where protections must follow rapid changes in server and network identities and locations. Open management infrastructure allows orchestration and automation capabilities to synchronize the Control Layer security policy with enterprise dynamic environments including cloud directors, configuration databases, asset inventory systems and identity management infrastructures.

Modular SDP management enables the definition of access and data control policies and the activation of threat prevention separately. The threat prevention policies can then be applied automatically to traffic allowed by the access and data controls policies but could also be managed by separate people or even outsourced.

Modularity also supports policy layers and sub-layers associated with various network segments, while providing the ability to delegate their management to specific administrators who can work on all of them simultaneously.

Visibility is needed for two reasons: situation awareness — understanding what is happening in the network; and incident response — doing something about it.

The Management Layer collects, consolidates and correlates events from enforcement points deployed in the network. Incident responders are provided with real-time visualization of the chain of events, which allows identification of initial attack vectors as well as subsequently subverted hosts and compromised data. Event investigation can generate new threat indicators for malware, threat behavior and network addresses associated with each identified attack. These indicators are then fed automatically to the Control Layer and distributed from there to the Enforcement Layer in order to protect the organization.

SUMMARY

Today’s security challenges require a fresh perspective on protection architecture. They mandate an architecture that adapts quickly and keeps pace with fast-evolving threats and the ever-changing requirements of advanced enterprise information systems.

The Software-defined Protection architecture is a new paradigm — a practical approach to implementing a modular and dynamic security infrastructure. It combines a solid, reliable Enforcement Layer and a fast-adapting intelligence-based Control Layer to deliver real-time proactive protections to corporate networks, while its Management Layer provides overall orchestration and agility.

With this modern architecture that integrates collaborative threat intelligence, attacks are repelled and external threats that could subvert internal resources are detected, contained and removed.
CHECK POINT
SOFTWARE-DEFINED PROTECTION
CHECK POINT
SOFTWARE-DEFINED PROTECTION

Software-defined Protection (SDP) is a pragmatic security architecture presented by Check Point to its customers and the community at large. Check Point SDP offers a security infrastructure that is modular, agile and most importantly SECURE.

In this paper we will explain how to build the SDP Architecture using Check Point products and security services across networks, hosts and mobile and cloud environments.

Check Point software-defined protections provide the flexibility needed to cope with new threats and embrace new technologies. Our solutions generate new and updated protections for known and unknown threats and proactively distribute this knowledge through the cloud. Implementing Check Point security solutions based on sound architectural security design empowers enterprises to embrace leading-edge information system solutions with confidence.

Software-defined Protection describes enterprise security architecture in the context of three inter-connected architectural layers that work together to provide adaptive, centrally managed high-performance security.
CHECK POINT SDP ENFORCEMENT LAYER

As the borders of the perimeter continue to blur and expand, organizations need to segment their IT environments including both their internal network and their cloud and mobile environments.

To secure the boundaries of each segment, Check Point offers a wide range of enforcement points. These include high-performance network security appliances, virtual gateways, and endpoint host software and mobile device applications. Check Point provides enterprises with all the building blocks needed to engineer segmented, consolidated and secure systems and networks.

Figure 2A - Check Point SDP Enforcement Layer
Network Enforcement Gateways

Check Point offers network enforcement gateways in the shape of appliances and software that can run on open platforms, allowing customers to choose their own flavor of enforcement points.

Check Point security appliances feature 19 different models that can fit organizations of all sizes. The Check Point appliance product line starts with the 600 and 1100 appliances to protect small and branch offices, and goes up to the 61000 security gateway, the fastest security gateway in the industry that offers unparalleled performance and scalability for high-end enterprise and data centers.

Powered by GAiA—Check Point secure, robust and manageable appliance security operating system—the Check Point appliances combine high performance multi-core capabilities with fast networking technologies to provide the highest level of network security.

All Check Point security gateways can also provision and host virtual gateways. These virtual gateways help organizations further optimize and simplify their security by consolidating a virtual network of many routers, switches, and virtualized security gateways into a single hardware platform.

On-host Enforcement Points for Endpoints and Mobile

To efficiently secure the network, segment boundaries should be complemented with host-based software agents that can enforce security policy at the host level.

Check Point Endpoint Security for Windows and Mac OS operating systems provides on-host security enforcement point for workstations and mobile devices.

The Check Point Mobile application for iOS and Android provides an encrypted container that allows authenticated users to access a secure environment containing corporate emails and calendars, while providing separation from other personal data and applications that might exist in a BYOD environment.

Finally, the Mobile Access Blade from Check Point complements endpoint and mobile enforcement points by providing trusted channels using VPN access from mobile devices to the Internet and to internal enterprise assets.
Private and Public Cloud

Cloud computing is increasingly used to achieve economies of scale and to leverage corporate computing, storage and networking resources.

For private cloud environments, the Check Point Virtual Edition (VE) offers both hypervisor-level and VM-level enforcement, allowing customers to segment inter-VM traffic. VE enforcement points are provisioned automatically by the Management Layer, securing new VMs as they are created and moved between physical hosts.

Check Point Amazon Security Gateway allows enterprises to enforce segmentation and firewall policies on systems within the Amazon Web Services (AWS) public cloud environment.

Check Point Gateway in the Cloud

For mobile users that roam outside the protected corporate environment, Check Point offers enforcement gateways in the cloud that allow organizations to extend their security policies to the cloud. All roaming user traffic is tunneled through an enforcement point in the cloud supporting Check Point threat prevention, access control and data protection.

CHECK POINT SDP CONTROL LAYER

The Control Layer is the core of the SDP Architecture. Its role is to generate protections and to deploy them for execution at the appropriate enforcement points. It is also the area where for the past twenty years, Check Point has been providing customers with innovative and industry leading protections.

Figure 3A - Check Point SDP Control Layer
Check Point Software Blade Architecture

Check Point SDP control layer is based on Check Point Software Blade Architecture that provides customers with flexible and effective security solutions to match their exact needs. With a choice of over 20 Software Blades, the modular nature of the Software Blade Architecture allows customers to build a relevant security solution per enforcement point and to expand their security infrastructure over time.

Next Generation Threat Prevention

Check Point efficiently delivers controls to counter many of the known and unknown threats. The Check Point Threat prevention solution includes the following components:

- **Integrated Intrusion Prevention System (IPS)**, blocking the exploit of known and often unpatched vulnerabilities
- **Network based Anti-Virus**, blocking signature-based threats such as malware, viruses, and Trojans from entering and infecting a network as well as preventing access to malicious web sites.
- **Threat Emulation**, preventing infections from undiscovered exploits and zero-day and targeted attacks by inspecting and running files in a virtual sandbox to discover malicious behavior.
- **Anti-Bot**, a post-infection solution that detects infected machines and prevents further damages by blocking bot communications to their C&C centers.

It is critical that threat prevention controls are fed with up-to-date threat intelligence. To that effect, Check Point built a unique cloud-based threat intelligence big data and protection generator, Check Point ThreatCloud™.

Check Point ThreatCloud enables a collaborative way to fight cybercrime, delivering real-time security threat intelligence converted into security indicators to the control layer.
At last count, ThreatCloud contained over 11 million malware signatures, 2.7 million malware-infested sites and over 5,500 different botnet communication patterns.

ThreatCloud is constantly updated with new threat information from a worldwide network of sensors, third party feeds, Check Point security researchers, security research organizations and Check Point gateways. Check Point enforcement points get updated with real time security indicators from ThreatCloud. In this collaborative process, if one company is attacked with malware, the relevant attack information is instantly shared with ThreatCloud. A signature of the attack is added to the massive database, and is leveraged instantaneously by all other customers.

Next Generation Firewall and Data Protection

Access control and data protection are critical to secure desired business processes by defining the interactions between users and data within the network.

Check Point access control is based on our next generation firewall combined with multiple software blades and enables a unified context-based security policy. It includes the following capabilities:

- **Next Generation Firewall and VPN** – Check Point patented Stateful Inspection provides a flexible infrastructure for layering security protections by providing an engine for network inspection at all network, application and data layers.

- **User identity Awareness** – supports advanced security policies based on the user’s identity. Check Point security gateways and endpoint hosts share user identity and endpoint status information, providing a cooperative enforcement capability across the enterprise.

- **Application Control** – offers protection with the industry’s largest web application library, supporting over 5,000 applications and 300,000 widgets. Application traffic is monitored, selectively blocked and/or rate-limited to enforce any enterprise security policy. Tightly integrated with URL Filtering, Application Control also supports reputation and categorization-based protections for enforcing dynamic enterprise security policies.

- **Data and Content Awareness** – is based on Check Point DLP software blade and features a large set of automatic classifications technologies available to determine the specific importance of each document.

Next Generation Data Protection

Check Point Next Generation Data Protection adds data awareness. It includes our Data Loss Prevention (DLP) software blade which performs content inspection and matches file contents with files stored in enterprise repositories. Check Point DLP supports content inspection for more than 800 file types and includes over 650 pre-defined content types. This makes it one of the most comprehensive and efficient Data Loss solutions on the market.

In addition, Check Point provides Data Protection for data at rest and in storage with encryption technologies. These technologies can be implemented on all enforcement points protecting sensitive documents and confidential data from being accessed or transferred to removable media or by unauthorized users.
The Management Layer makes the Software-defined Protection architecture come alive. By enabling each component of the architecture, this layer acts as the interface between the security administrators and the other two SDP layers.

Check Point Modular / Layered Policy Management

All Check Point protections and enforcement points are managed from a single unified security management console. Check Point security management is highly scalable, providing the ability to manage tens of millions of objects while maintaining super-fast user interface response times.

The SDP Architecture requires the Management to support the enterprise segmentation, allowing administrators to define security policy for each segment while enforcing segregation of duties. Each administrator should be provided with a simple view of the security policies under his responsibility for threat prevention, access control or data protection.

Check Point Security Management fulfills these SDP requirements with a new concept called Layers and Sub Layers. Policies can be defined for each segment. Access control policies can be defined using separate layers, which can be assigned to different administrators. Multiple administrators can then work on the same policy simultaneously.

Automation and Orchestration

As defined by the SDP Architecture, access control and data protection policies are organization-specific and change constantly based on new users, applications and new business processes.

In order to support these business process changes, Check Point Security Management provides CLIs and Web Services APIs that allow organizations to integrate with other systems such as network management, CRM, trouble ticketing, identity management and cloud orchestrators.

Open interfaces to external systems enable the Management Layer to understand the changes to the environment and to coordinate security policies with these changes. For example, a new virtual machine would be automatically protected by the appropriate segment policy, based on the machine’s classification.
Visibility with Check Point SmartEvent

Security visibility is an integral part of the resilient security posture. The Management Layer is required to provide both situation awareness and incident response capability.

Check Point SmartEvent performs big data analysis and real-time security event correlation. It offers the ability to provide a consolidated and correlated view of an incident based on multiple sources of information. An accurate event view is provided and helps incident responders identify the necessary actions to be taken in order to defend the network.

Security event analysis creates actionable intelligence in the form of threat indicators that can be distributed via ThreatCloud to block threats in real-time. Automated response mechanisms can provide threat containment, allowing responders to take necessary actions before resuming operations.

SUMMARY

In order to protect against fast-evolving changes, enterprises must adopt an architecture that can handle fast growing network traffic but also that is dynamic and up to date with real-time protections.

Software-defined Protection is the right architecture for today’s and tomorrow’s security challenges.

Check Point provides all the right components needed to implement a complete SDP architecture with the best management and the best security.