Intel® Security Controller

Enable software-defined security for software-defined infrastructure

Intel® Security Controller is the industry's first security controller to enable automated and dynamic security provisioning, policy synchronization, protection, and remediation for software-defined infrastructure (SDI) built on VMware NSX. It is designed to seamlessly broker between cloud orchestrators, software-defined networking (SDN) controllers, Security Connected solutions from McAfee, and the applications that manage them.

Key Advantages

- Security function virtualization (SFV) using a new, controller-based approach.
- Cost effective, easy to deploy, and simple to manage.
- Supports VMware NSX with micro-segmentation for agile, automated, distributed provisioning, policy synchronization, protection, and remediation.
- Scalable, accessible, and extensible architecture
- Industry-leading protection within the Security Connected framework, starting with the next-generation intrusion prevention system (IPS), McAfee® Network Security Platform.

Security: The Barrier to SDI Adoption

Data centers are in a state of constant transition as IT teams accelerate the move to virtualization and SDI so that their organizations may realize its benefits: increased agility, high performance, improved security, and significant cost reductions.

But as they make this transition and evolve from server and storage virtualization to embrace SDN and orchestration for their private and hybrid clouds, they quickly discover that yesterday's security solutions can't effectively secure tomorrow's data centers.

This is because traditional application and hardware-based security solutions (or virtual versions of them) depend on static configurations of the network and network traffic. They are configured using information gained from the network to secure predefined routes. And these solutions are generally perimeter-centric and purpose-built to deliver high-performance scanning, analysis, and remediation to secure and control known endpoints, servers, services, and the access to them.

Why Legacy Solutions Don't Work

While perimeter and access security is still important, these solutions cannot protect the virtual infrastructure because they do not have visibility into its dynamic creation of new endpoints, workloads, and traffic flows. They are unaware of and cannot adapt to context-based flows determined by the orchestrators and SDN controllers—and the dynamic changes they make to the network.

This lack of visibility results in:

- Critical east-west traffic left exposed and unprotected.
- Architectures that fail to meet compliance requirements.
- Networks that are inefficiently designed with traffic "hairpins" and unnecessary or redundant inspections.

As security teams try to keep pace with infrastructure automation through one-off manual deployments and reconfigurations, they find that they lose the agility, performance, and cost reductions promised by SDI.

Why Point Product Integrations Don't Work

Alternatively, some IT teams attempt to use point products with single integrations into SDN solutions. Unfortunately, this approach results in significant protection gaps, a lack of holistic security intelligence, and increased complexity for both security and infrastructure teams. The new tools may not align with organizational processes or best practices for duty and role separation. Worse, these point solutions often cannot span security policies across data centers, orchestration solutions, or even between physical and virtual deployments to maintain security investments, failing to address the reality of today's changing data centers.

A New Approach with Intel® Security Controller

Intel Security Controller introduces a new way to secure the virtual infrastructure, and enable "software-defined security." This application is deployed as a virtual machine within the virtual infrastructure and runs transparently to users and administrators. Using bi-directional, notification-based application programming interfaces (APIs) for communication, it continuously and dynamically connects and brokers between security solutions and the virtual infrastructure.

Comparable to the European Telecommunications Standards Institute (ETSI) model for SDN and network function virtualization (NFV), Intel Security Controller uses a controller-based approach, providing abstraction for the security infrastructure within SDI. It enables SFV by virtualizing and abstracting common security functions,[1] such as antivirus, IPS, sandboxing, firewall, web filtering, and data loss prevention. As a result of Intel Security Controller' s enablement and use of SFV, not only is the infrastructure secured, but security itself also becomes more adaptive, cost effective, software defined, and ubiquitous.

By enabling software-defined security, Intel Security Controller helps IT organizations safely transition their data centers with:

- Cost-effective, easy deployment, and simplified management.
- Agile, automated, distributed security function provisioning, policy synchronization, protection, and remediation.
- Scalable, accessible, and extensible architecture.
- Industry-leading protection that is hardware-enhanced for virtual infrastructures[1] through the Security Connected portfolio from McAfee.

Cost Effective, Easy to Deploy, Simple to Manage

Intel Security Controller works with current business processes, recognizes the need for duty separation, and protects infrastructure investments:

- It installs in four easy steps, configured through a simple web interface.
- Administrators use current virtual infrastructure and security management tools to centrally define and manage security policy across physical and virtual infrastructures.[1]
- It runs as a background service, requiring minimal maintenance and resources.

Agile and Automated Security

The Intel Security Controller's security function catalog contains deployable images of security services, such as next-generation IPS from the industry-leading, McAfee Network Security Platform. Through the security controller's APIs, the solution can:

- Dynamically protect the infrastructure by provisioning security services as a new concept called "distributed appliances." These services are injected into workflows where and when needed, according to context-aware policies defined by the SDN controllers and orchestrators.[1]
- Automatically and bi-directionally synchronize security policies as defined by the virtual infrastructure and security management applications.
- Provide immediate remediation within the virtual infrastructure based on action-on-alert policies and a security response API tuned to the Security Connected solution portfolio from McAfee.

Scalable, Accessible, and Extensible Architecture

Designed to require minimal resources and provide an abstraction layer, Intel Security Controller has an extensible architecture that can support:

- Simultaneous, essentially unlimited connections to any number of data centers, and supported types of SDN controllers and orchestrators.
- Simultaneous, essentially unlimited connections to any number of supported security managers.
- Immediate and unlimited deployment of security services, according to their availability and licensing models.
- A roadmap for security functions to be added to its security function catalog.
- Access to Intel® Security Controller management via a web browser or a representational state transfer (REST)-based API.

Industry-Leading Protection with Security Connected from McAfee

Security functions[1] contained within the Intel Security Controller security function catalog are virtualized translations of products from the Security Connected portfolio, offering IT organizations the most comprehensive and advanced set of security solutions available today. Unlike stand-alone, ported versions of these products, when delivered from the Intel Security Controller's security function catalog, they are:

- Optimized as part of the virtual infrastructure (for example, as a VMware ESX agent), they transform separate, security product platforms into adaptive, intelligent engines.
- Hardware-enhanced and optimized for Intel architecture to increase security processing and network performance.
- Integrated as part of the Security Connected framework from McAfee. Security functions[1] operate in conjunction with security management and intelligence solutions such as ePolicy Orchestrator® software, McAfee Enterprise Security Manager, McAfee Global Threat Intelligence, and McAfee Threat Intelligence Exchange.

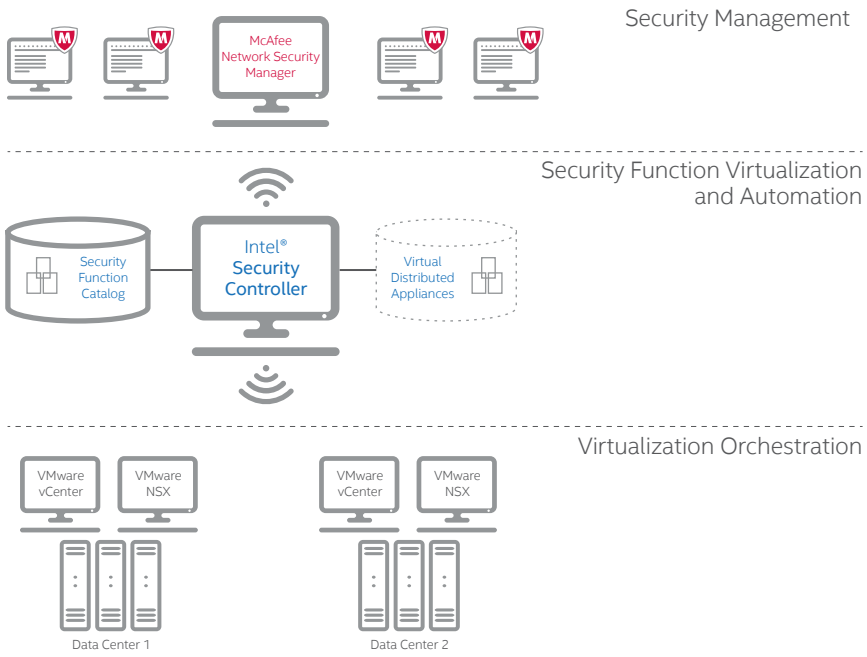

Figure 1. Software-defined security with Intel Security Controller.

Use Case—Securing VMware NSX Environments with Next-Generation IPS

Intel® Security Controller secures VMware NSX environments with scalable, next-generation IPS protection from McAfee Network Security Platform, a Gartner Magic Quadrant Leader and NSS Labs "Recommend" for IPS. Integrated capabilities include:

- Native-like integration with VMware vCenter with support for micro-segmentation, security profiles, policies, and groups.
- Network IPS protection dynamically and automatically provisioned to protect intra-VM traffic within the VMware NSX data center. Network traffic is secured, protecting business-critical assets and supporting compliance requirements.
- Dramatic reduction in management costs by eliminating manual configuration and reconfiguration steps required when using physical or traditional virtual appliances.
- Scales across one or more VMware NSX data centers and across essentially unlimited instances of McAfee Virtual Network Security Platform sensors and Network Security Managers.
- Consistent policy enforcement and investment protection as McAfee Network Security Manager manages across both physical and virtual appliances and virtual instances as part of an integrated Intel Security Controller.
- High-performance IPS protection with the McAfee Virtual Network Security Platform, the first next-generation IPS optimized for Intel architecture using Intel® Xeon™ technology for Intel® HyperScan, and Intel® Data Plane Development Kit (Intel DPDK).

The table below provides specifications for Intel® Security Controller, which are available to customers of the McAfee Virtual Network Security Platform.

Learn More

For more information about the Intel Security Controller, Intel Security Group solutions for Software-Defined Security, or to request participation in our evaluation program, visit **www.intelsecurity.com/sdi**.

Table 1. Intel Security Controller Specifications

Requirements and Compatibility	Specifications
Console	• Web browsers: Microsoft Internet Explorer, Google Chrome, Mozilla Firefox, Apple Safari
Host: Platform, hypervisor, and network	• Cores: 4 • Memory: 8 GB • Disk: 50 GB • VMware ESXi v5.5 • IPv4 environments only
Virtualization management	• VMware vCenter Server v.5 • VMware vSphere Web Client v.5.5 or above (VMware vSphere Client does not fully support VMware NSX)
Orchestration management	• VMware NSX Manager v.6.1
Security functions	• McAfee Virtual Network Security Platform (sensor) 8.1
Security managers	• McAfee Network Security Manager 8.2

1. Please review Table 1 for specifications and compatibility for version 1.0.

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com