Preface

Rapid technological changes and evolving business requirements continually challenge organizations to protect their assets. While constant change in the business landscape drives the adoption of new technologies in IT networks, organizations find it increasingly difficult to address new and more sophisticated attacks that threaten corporate assets and disrupt business operations.

Localized security policies and devices at network perimeters can no longer safeguard corporate assets nor ensure operational continuity. Today, secure corporate networks require multiple layers of protection and implementation of a unified, system-wide, security strategy. The current Internet security landscape emphasizes the need for end-to-end security architectures, along with design and implementation guidelines for building secure and resilient network infrastructures.

In particular, data centers need secure infrastructures. In any organization, a typical data center houses the most critical and valuable assets. This guide describes an architectural data center security framework, based on Cisco's Virtual Multiservice Data Center (VMDC) 2.3 architecture, specifically designed to work with the rest of organizations' network security infrastructures.

This guide is written for network and security engineers to help them to design, implement, and operate secure network infrastructures that address today's challenging business environments.

Cisco VMDC Cloud Security Release 1.0 is a reference architecture providing design and implementation guidance for cloud deployments. Numerous service providers and enterprises have implemented multiple VMDC versions in private, public, and hybrid cloud deployments. VMDC Cloud Security 1.0 provides an end-to-end validated system that integrates a variety of Cisco and third-party products. Figure 1 shows the VMDC layers and major components.

Figure 1 VMDC Layers and Major Components