Security Solution Architecture for VDI

A reference implementation of VMware View

BENEFITS

- Validated solution architecture provides unprecedented end-to-end security dashboard for virtual desktop infrastructure (VDI)
- Integrated and tested VMware and Technology Alliance Partner solution based on security and compliance
- Highlighted real-time compliance monitoring and considerations for auditing
- Introduction of security zoning allows VDI to support multiple compartments at same security level
- VMware services and partnerships make it easy to implement the security solution template

Desktop Security: An Architectural Approach

The importance of desktop security is magnified in today's increasingly connected, mobile, multi-device business environment. High-profile security breaches such as stolen laptops and compromised desktops only underscore what IT professionals already know: protecting sensitive data is an increasingly urgent priority.

The move to virtual desktop infrastructure (VDI) using VMware View is gaining momentum because it solves some of the most pressing security concerns: all sensitive data is housed in the data center rather than the desktop; application software is isolated from the operating system; PC software images are consolidated and access can be controlled more tightly.

However, VDI and VMware View alone cannot resolve all desktop security issues. This brief provides an overview of the desktop security vulnerabilities which exist in both virtual and physical environments that must be addressed throughout the typical connection sequence, along with the VMware and third-party products that remediate the issues. Together, these products and technologies comprise a security solution architecture for VDI—an architecture that goes beyond the viruses, worms, and phishing attacks mostly commonly addressed in desktop security technology to include data loss, system management, and compliance monitoring.

The purpose of this brief is not to provide detailed information about any of the point products mentioned, but rather to highlight the potential problems and the solutions available, so that VMware View customers can take the appropriate actions to fully secure their environment and achieve compliance.

Threats and Vulnerabilities

Desktop security is not simply about securing the desktop device. An effective desktop security architecture must address security vulnerabilities at the user level, the endpoint device level, the application level, data center level, the network level, and the management level. The diagram below presents the typical connection sequence in a VMware View environment; the next sections of this brief describe the specific security vulnerabilities at each phase of the connection flow and the VMware and third-party products that remediate the issue.

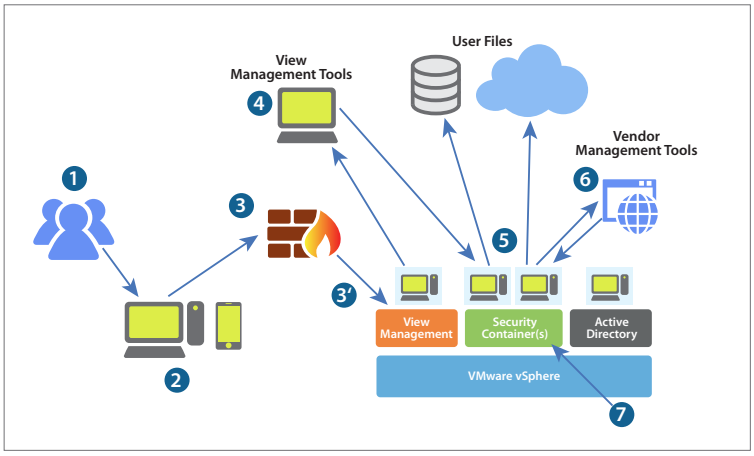

Figure 1: View Connection Sequence

The connection flow for VMware View can be simply described by the following steps:

1. A VMware View user using View Client connects to the View Security Server and authenticates

2. When a PCoIP desktop is selected, the PCoIP protocol goes to the View Security Server
3. If the PCoIP session is on behalf of an authenticated user, it is then forwarded to the correct desktop
4. VMware View management tools are used to provision desktops and set user access, entitlement and permission policies
5. User data is stored within the data center using the company's privacy policies and selected encryption technologies
6. Vendor management tools are used for aggregate desktop configuration, reporting, and compliance management

Figure 1 illustrates the logical steps of how the connection interacts with Active Directory and management tools during desktop access.

The security practices should address user mobility, since the data is centrally located and users can access the same data from many different network nodes. The architecture implementation should also cover major updates and patches that are applied to every single desktop and pushed to the entire VDI deployment.

Vulnerabilities and Threats in the Connection Sequence

End User Authentication

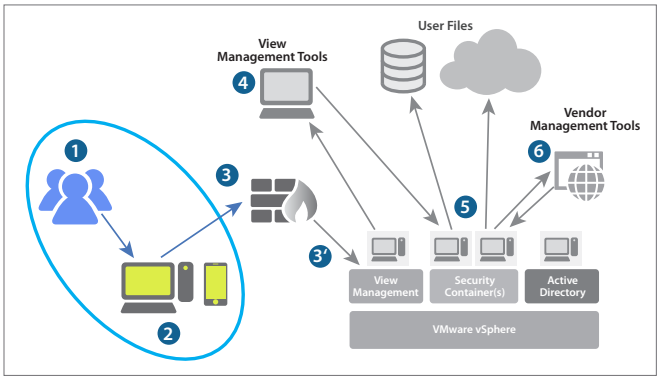

Figure 2: End User Authentication

SECURITY VULNERABILITIES

- Spoofing user identity
- External theft of credentials (two-factor authentication token)
- Hijacking user desktop session
- Unsigned certificate can potentially direct user to a compromised network
- Insecure device

REMEDIATION / SOLUTION

- System Management Software – VMware vCenter Configuration Manager (used for OS and application updates and patches)
- Endpoint Identity Access – Two-factor authentication uses smart card, eToken, biometric sensor, and one-time password token (secureID token)
- Vulnerability Monitoring and Scanning – Port scanning for the entire network and real-time vulnerability analysis on desktops and servers based on a vulnerability database maintained by ISVs
- Data Encryption – Prevention of unauthorized access and downloads of sensitive data from corporate environment

Untrusted to Trusted Connection

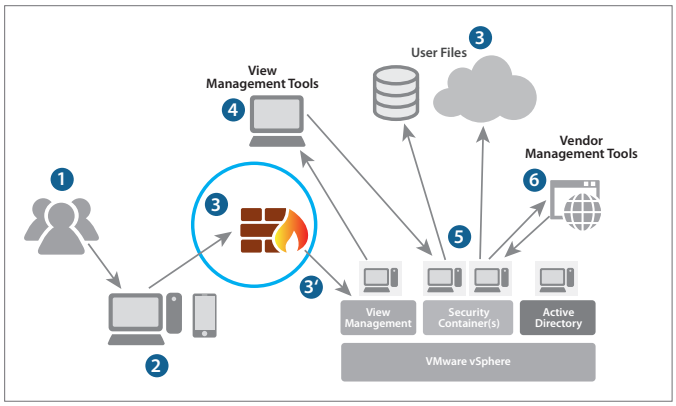

Figure 3: Untrusted to Trusted Connection

SECURITY VULNERABILITIES

- Denial of IP service (DoS) or load balancing
- Denial of user service (lockout due to too many attempts)
- Time-of-Day access for external desktop sessions
- Windows server default known vulnerabilities

REMEDIATION / SOLUTION

- Implement virtual/physical firewalls that can detect and counter against denial of service (DoS) attacks, and null route any malicious traffic that's identified as a DoS attack
- Allow access to private network from outside as a NAT device, e.g. VMware vShield Edge
- Disable account logon privilege after x failed login attempts
- Vulnerability scanning/monitoring – real-time crosscheck known vulnerabilities that affect the OS

Provisioning Desktop

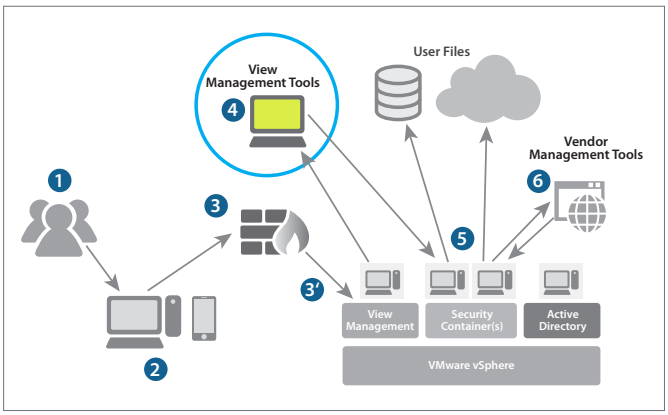

Figure 4: Provisioning Desktop

SECURITY VULNERABILITIES

- Desktops containing known viruses
- Desktops not meeting compliance standards
- Desktops containing malware/virus propagation and traversal
- Un-patched software/OS with known vulnerability
- Unmanaged or orphaned VM from pool

REMEDIATION / SOLUTION

- Create security trust zone to segregate management network from desktops, e.g. vShield Manager Zone creation
- Use system configuration, e.g. vCenter Configuration Manager, to enforce desktop compliance and updates
- Use endpoint protection e.g. vShield Endpoint, to prevent malware and viruses at desktops

User Data

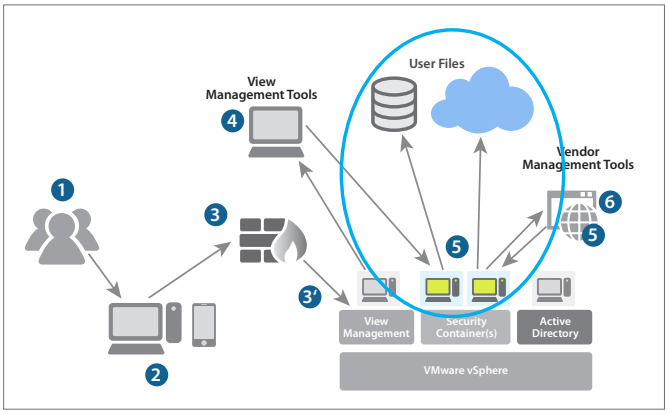

Figure 5: User Data

SECURITY VULNERABILITIES

- One user viewing another user's data
- Data leakage at rest via internal/external cloud
- Data leakage in motion with user data over network
- Data written/stored to USB removable devices

REMEDIATION / SOLUTION

- Data Encryption

Uninformed Management Tools

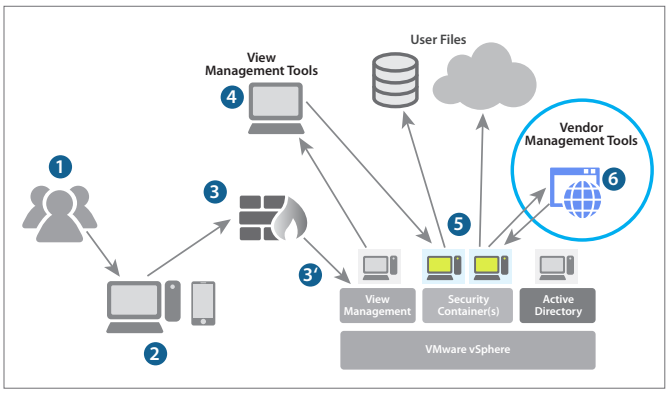

Figure 6: Uninformed Management Tools

SECURITY VULNERABILITIES

- Virtual machines enter and exit between scheduled scanning periods without knowledge of user data stored on central store
- Issues underreported by management tools

REMEDIATION / SOLUTION

- vShield Endpoint / Trend Micro Deep Security
- vCenter Configuration Manager

Desktop Configuration

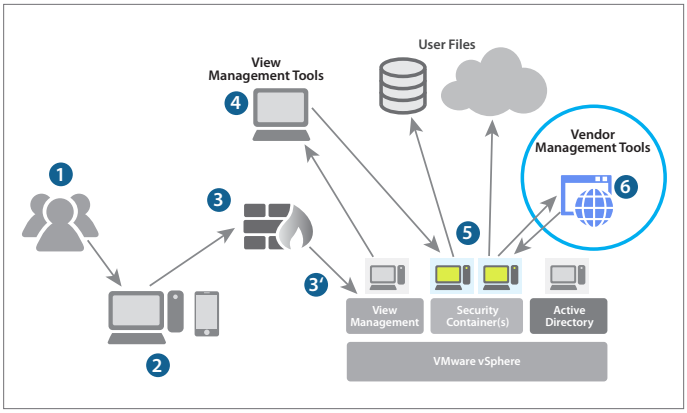

Figure 7: Desktop Configuration

SECURITY VULNERABILITIES

- Desktop host configuration has known threats due to missing patches or mis-configuration

REMEDIATION / SOLUTION

- Define bad traffic flow/user random attempts
- Desktop image compliance, e.g. vCenter Configuration Manager

Security Practices and Considerations

Security and compliance requirements can slow down the adoption of a virtual infrastructure. A lack of understanding of the requirements for business continuity, integrity, and data protection in a virtualized data center may result in a partial or a complete failure of the virtual desktop deployment or migration project.

VMware vShield provides a firewall-zoning policy. The addition of ISV partner security products can be integrated with vShield API to ensure policy enforcement.

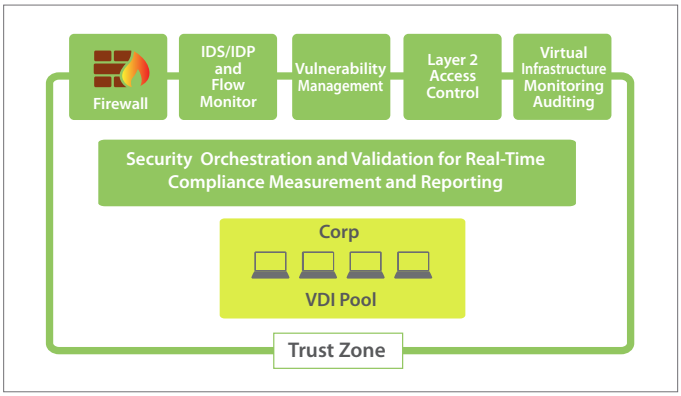

Figure 8: Real-Time Compliance Metrics and Reporting with Multi-Functional Policy Enforcement

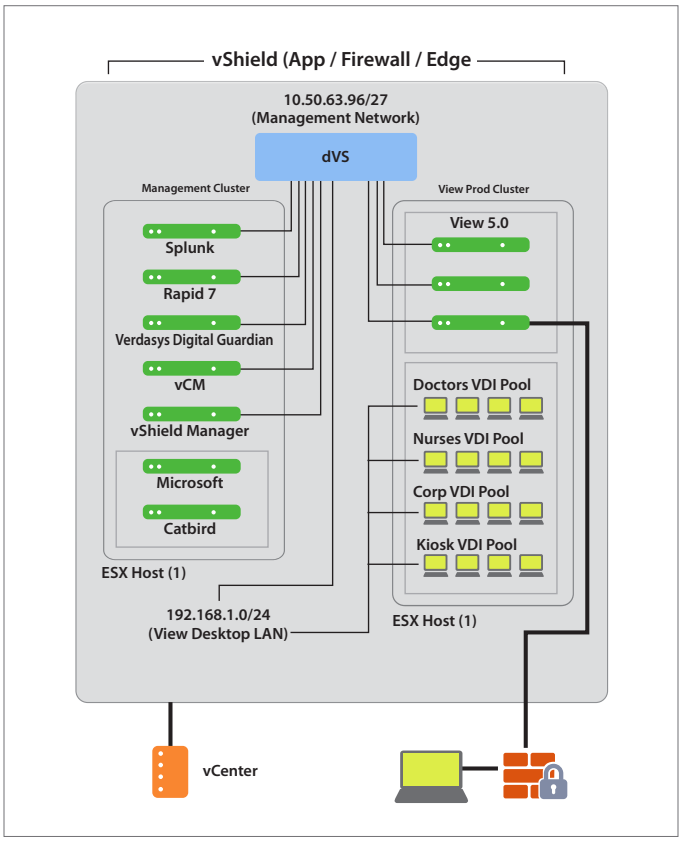

Figure 9: Solution Lab Setup for Simplified VDI Security Architecture

VMware vSphere 5 environments are built for VMware and ISV management components as well as for desktop pools including floating and persistent. Inter-network connectivity is managed using a VMware vSphere Distributed Switch (vDS). The VMware vShield firewall enforces network access control and vShield Edge provides security connectivity with the corporate home network.

Security policy definitions are created based on:

- Enforcing unauthorized connectivity (e.g. network flow) among VDI pools
- Enforcing network segmentation
- Allowing VDI pools with distinct connectivity to share enterprise-level connectivity
- Geographic and network boundaries
- Allowing access to shared resources
- Reducing operations and management costs
- Enforcing security isolation between zones
- Assigning security policy per zone
- Supporting multiple compartments at the same security level

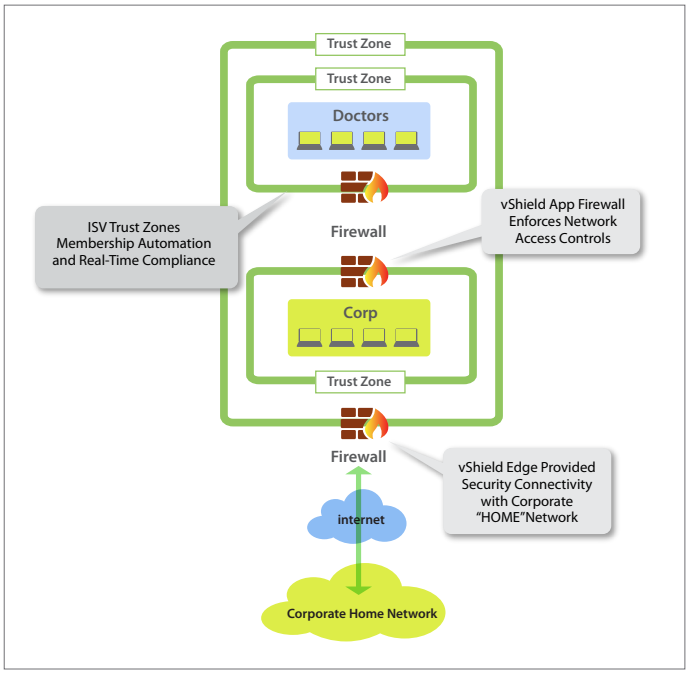

Figure 10: Using vShield App and Edge to Define the Geo and Network Boundaries

Compliance Monitoring Dashboard

The integrated dashboard is designed to provide IDS/IDP, Vulnerability Management, L2 access control, and compliance monitoring and auditing. Through an event-driven risk and compliance dashboard, enterprises can aggregate instant audit reports and ensure continuous compliance.

Integrated Splunk Dashboard

The dashboard displays the View events at SQL database and the Rapid7 Nexpose syslog events being pulled and populated into Splunk via simple expression commands. This integrated monitoring provides a true an end-to-end VDI security dashboard. The metrics include Most Recent Logins by IP (Success/Failed), Logins by Users, Desktop Uptime, Success/ Failed Login Origination, USB Policy, and Configuration Compliance.

Figure 11: Integrated Security Dashboard

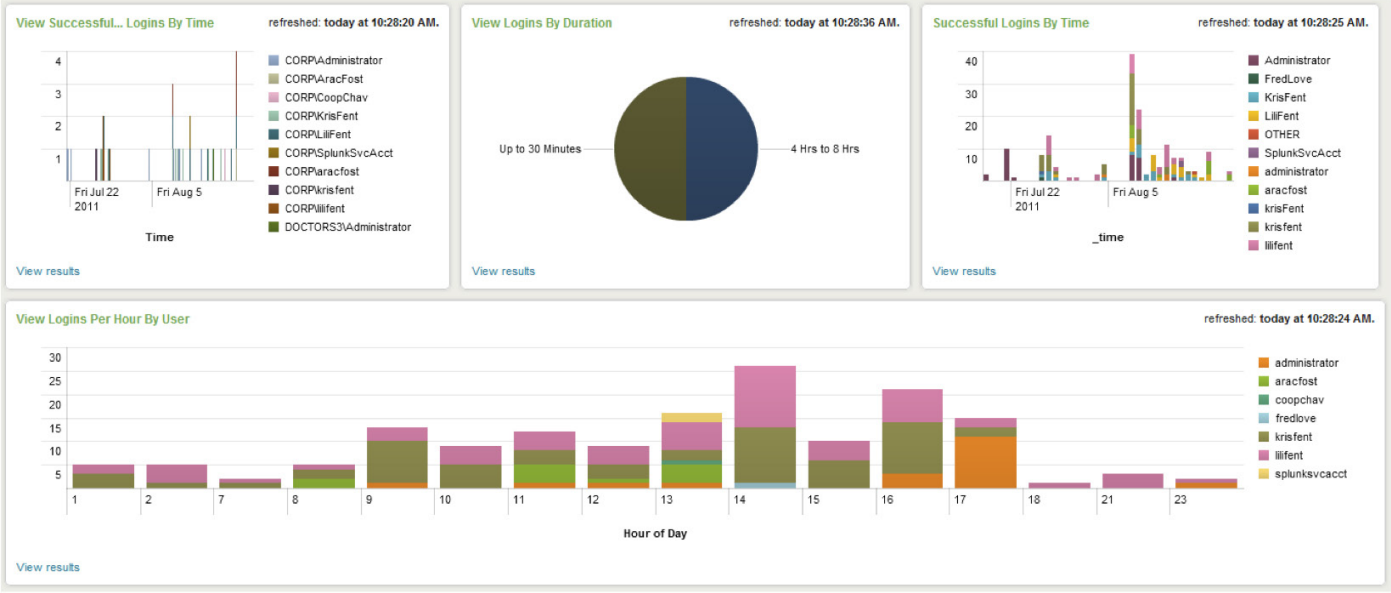

Figure 12: View Event Manager Default Log

Compliance Template (HIPAA, SOX, FISMA, PCI, DIACAP, and COBIT)

Compliance requires collection and correlation of data from multiple technical controls. Every mandate contains different sets of technical controls. In-depth controls for VDI include the following:

- Inter-network segmentation
- Intra-network and inter-VM segmentation
- Layer 2/3/4 controls
- Application layers (5-7) controls
- Deep packet controls for most applications
- Botnet command and control server (C&C) controls
- Malware site controls
- Anti-phishing/anti-pharming controls
- Integration with VM configuration
- Zone-based policy controls
- Network change control process
- Block metasploit attack
- Automated workflow

Together, VMware and partners such as Catbird offer an integrated compliance dashboard (illustrated below in figures 13 and 14) that provides security templates allowing for real-time monitoring of the certification process on VDI designs. For example, the Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) ensures that risk management is applied on information systems. With the compliance dashboard, VDI customers can analyze and visualize multiple aspects of DIACAP compliance, including boundary defense, remote access for privileged functions, remote access for user functions, access for computing facilities, and so on.

DIACAP Analysis: Virtual Infrastructure

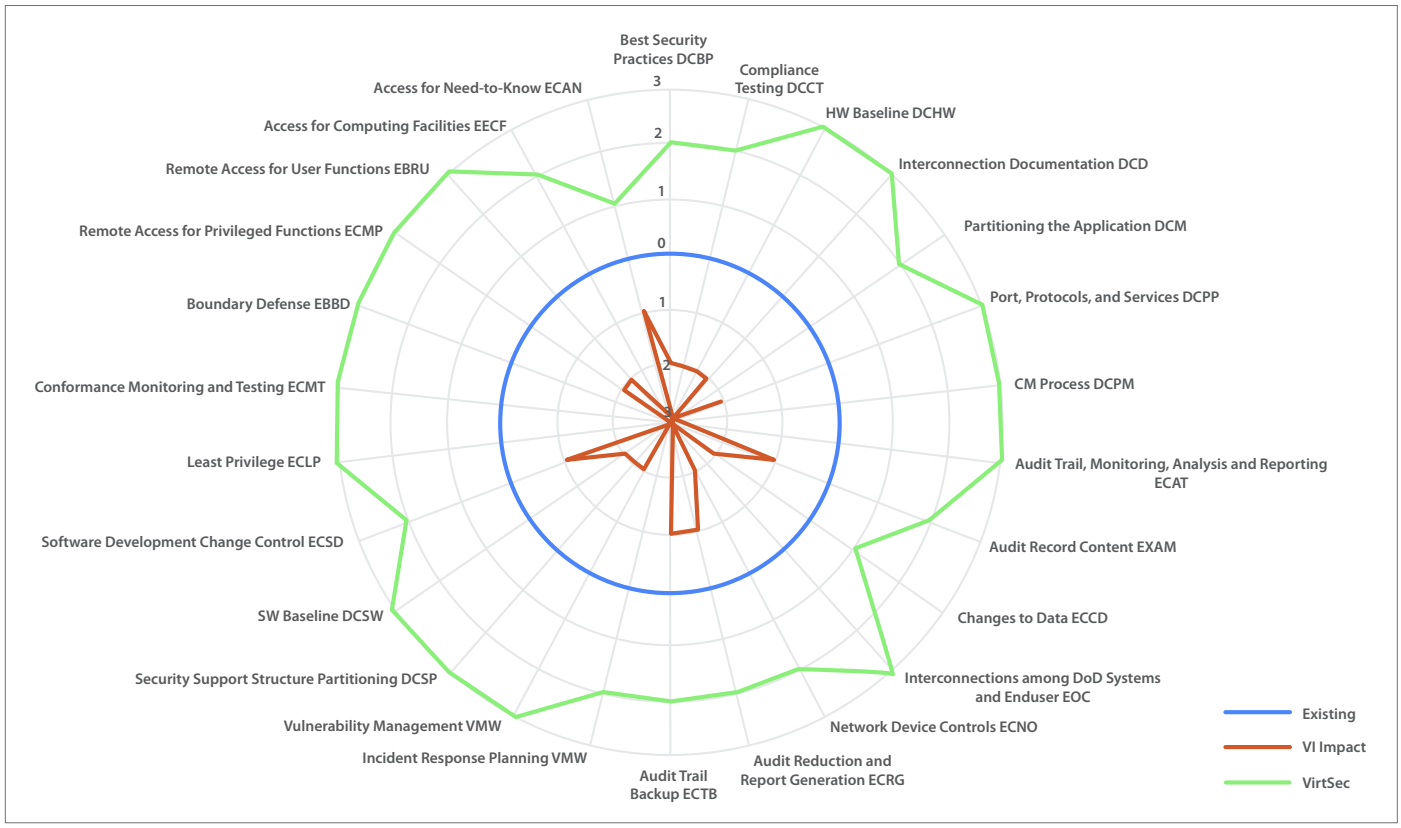

Figure 13: Technical Controls Used for DIACAP in a Virtual Infrastructure by Catbird

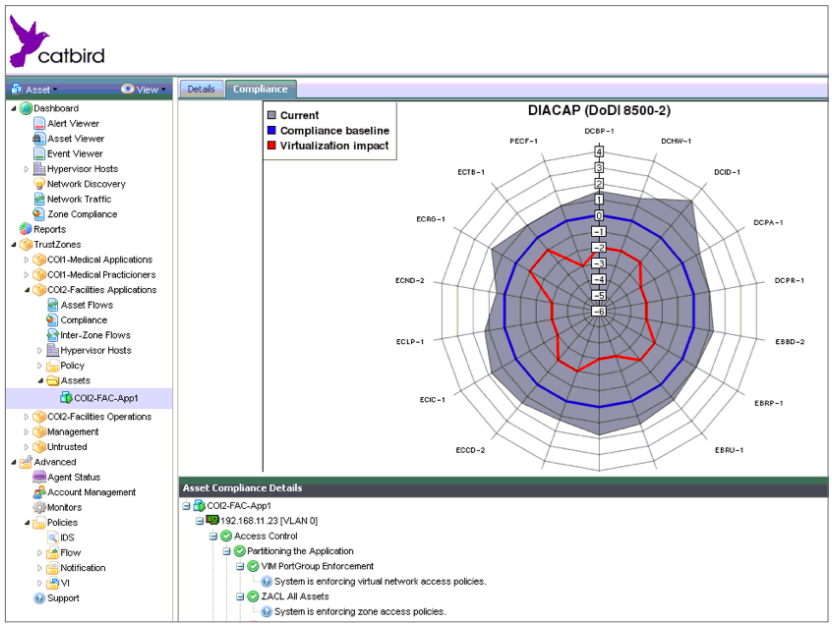

Figure 14: VDI-DIACAP-Catbird Compliance Dashboard

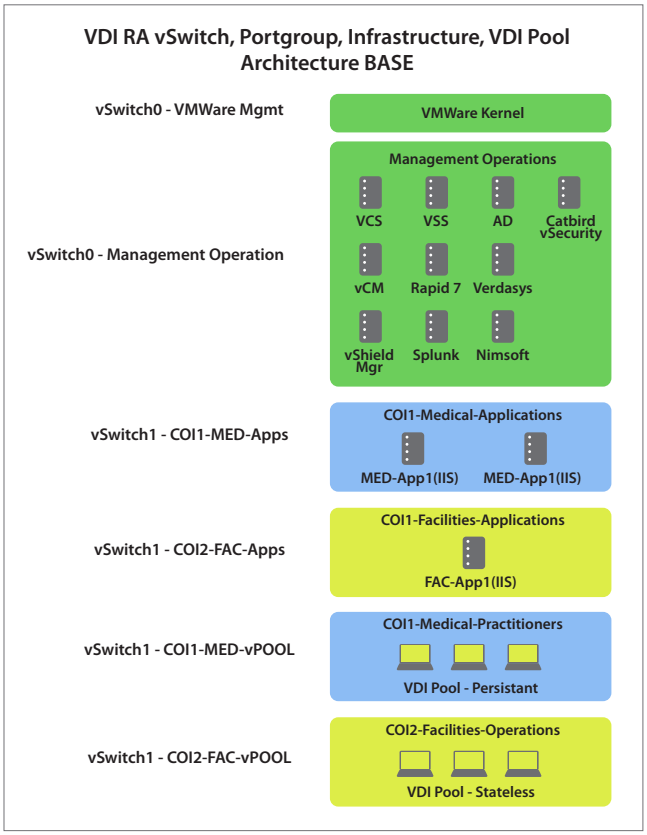

Figure 15: Community of Interest Zone Design for Desktops and Applications

Summary

Security vendors realize that the enterprise perimeter and desktop security vulnerabilities have changed. Firewalls with basic allow/deny rule sets, based on IP addresses and application ports, are not flexible enough for the dynamic type of connectivity enterprises required with outside partners, part-time contractors and guests, as well as an increasingly mobile work force. Perimeter security access technology now adapts to become more aware of applications, virtual desktop use cases, end-user identity, and enterprise policy.

VMware partner products and solutions integrated with the VMware security framework meet these updated security requirements. A security solution architecture dashboard easily showcases multiple security aspects and considerations for an end-to-end VDI practice. The solution architecture presents one of the many security options you can consider, not *the* only option.

Authors

This brief was prepared by the Solution Management Team in the VMware End User Computing business unit. The Solution Management Team is responsible for architecting and validating both horizontal and vertical solutions that feature VMware View along with requisite partner products. For this paper, integration efforts were provided by security architects from VMware and teams at our partner organizations, including Catbird, Splunk, Verdasys, and Rapid7.

A summary of the VMware and partner products used in the security architecture for VDI is provided in the chart below.

Security Architecture for VDI: VMware and Partner Products

PARTNER PRODUCTS	USE CASES IN SECURITY DASHBOARD
VMware View	• Compose and recompose desktop images • Profile redirection • Application SSO • USB redirection • Access from mobile or stationary endpoints • Task worker stateless desktop secure access • Instant user entitlement
Catbird	• Real-time compliance monitoring and trust zone policy enforcement www.catbird.com
Splunk	• Comprehensive dashboard of the results from various products and data points www.splunk.com
Rapid7 Nexpose	• Vulnerability scanning https://community.rapid7.com/docs/DOC-1164
Verdasys Digital Guardian	• Protection from data loss to USB devices http://www.verdasys.com/ • File level monitoring with visibility • File encryption • Network upload monitoring and control • Clipboard, print, printscreen monitoring and controls • Data classification by the content of documents • Data classification by the context of documents • Data Discovery

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com