RSACONFERENCE2013

Locking Down the Cloud – Security is Not a Myth

Kurt Hagerman

Director of Information Security - FireHost

Security in knowledge

Session ID: SPO2-R35

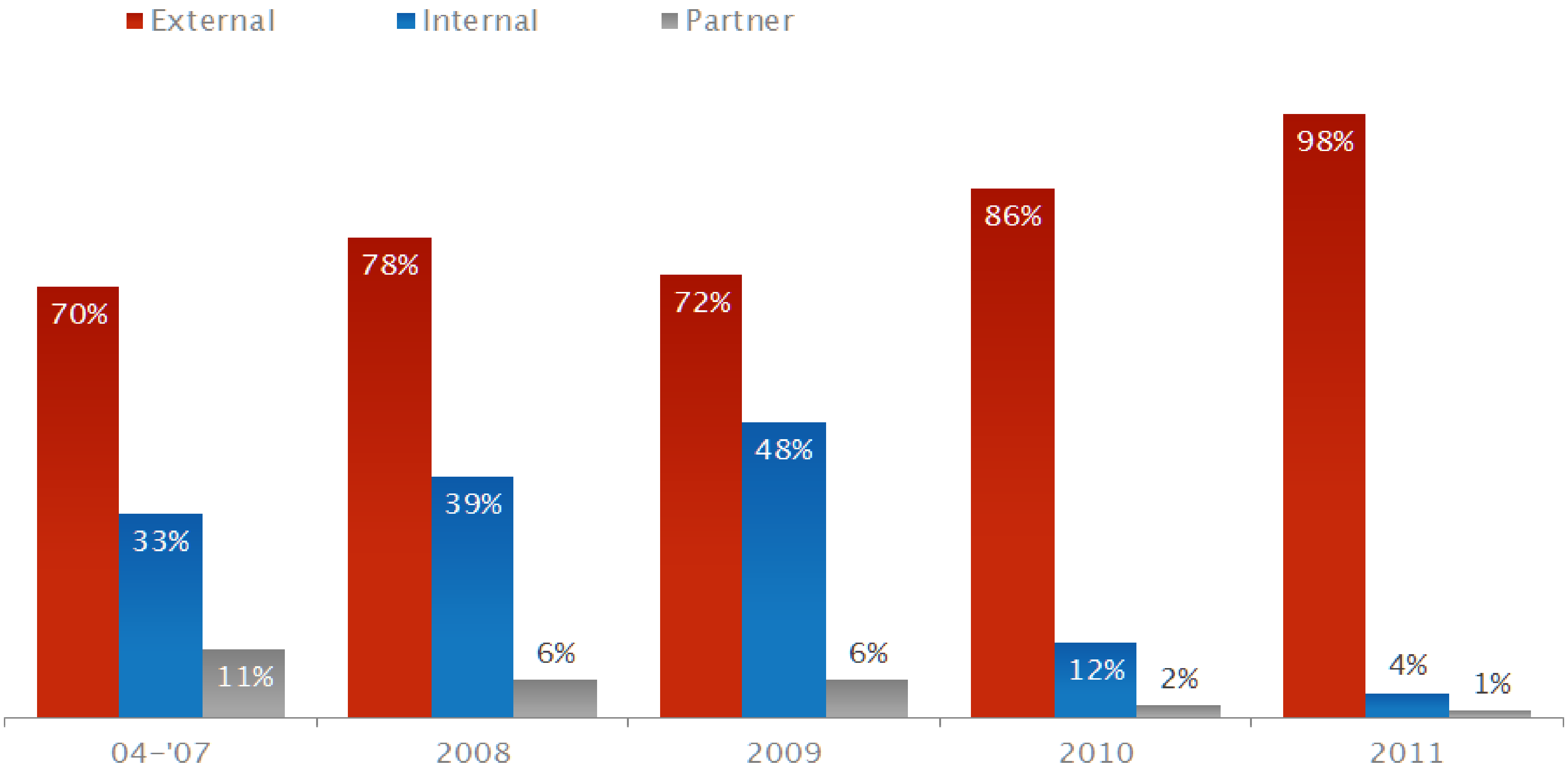
Session Classification: Intermediate

Agenda

- Background
- The Secure Cloud is Not a Myth
  - Perimeter Security
  - Host Security
  - Supporting Security Services
  - Secure Administrative Access
- Your Security Program and Compliance
  - Challenges and Solutions

Fighting the REAL Threats

- Threats over time by percent of breaches
  - 2012 Data Breach Investigations Report – Verizon/US Secret Service



The Cloud Market is Between a Rock and a Hard Place

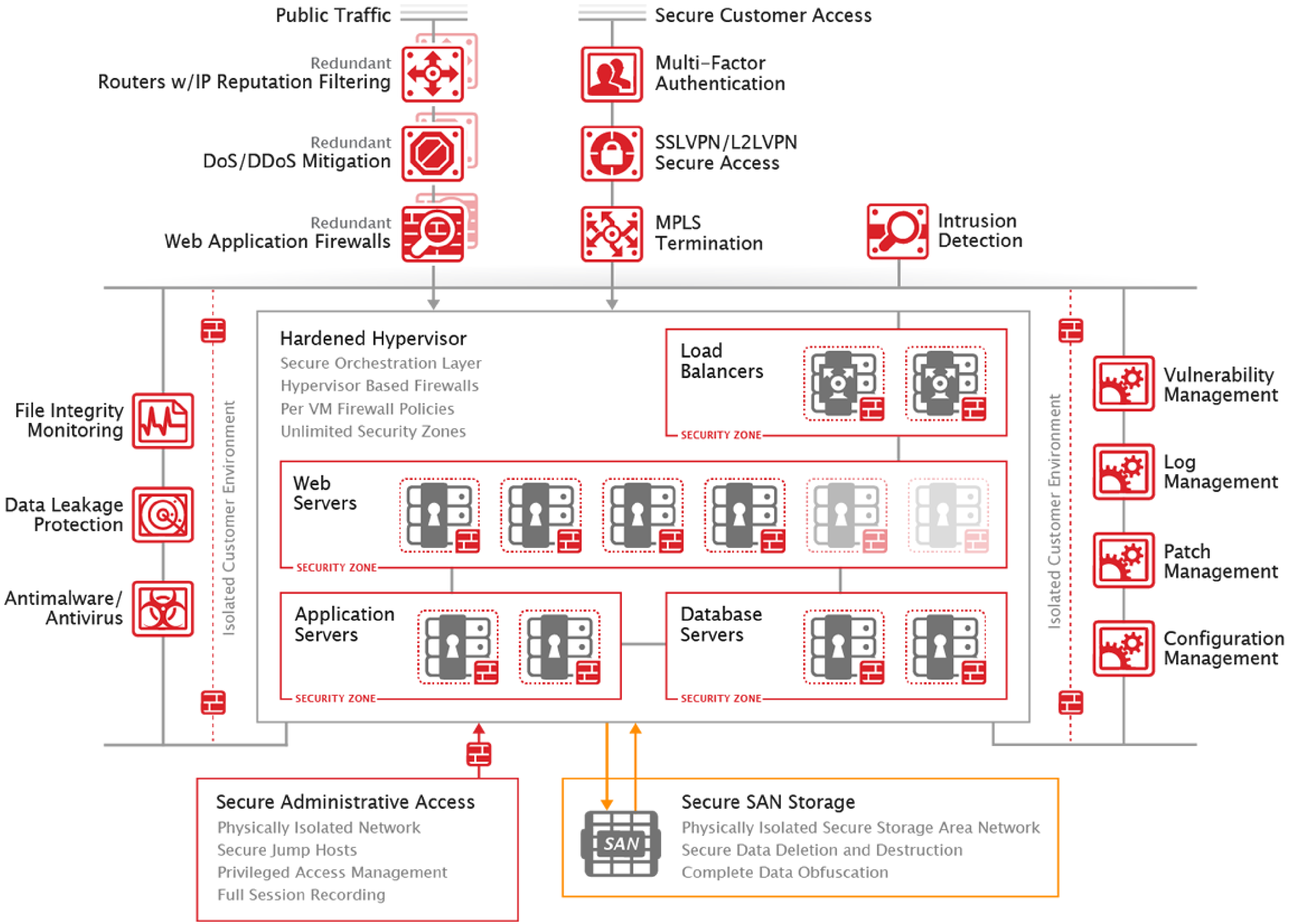
- **Rock** = Relentless Security Threats (Partial list from the month of December 2012 alone)
  - Verizon (3,000,000 accounts compromised)
  - HP (100,000 customer accounts compromised)
  - Wells Fargo, US Bank, PNC, BB&T, Citi, Bank of America (DDoS)
  - U.S. Army (36,000 machines controlled within Command Center)
  - Tumblr (8,600 blocks defaced including USA Today, Reuters and CNET)
  - Pizza Hut ("thousands" of customer records leaked)
- Security Pain Prospects Face
  - Internal security capabilities
  - External threats growing exponentially
  - Limited view of external threats

The Cloud Market is Between a Rock and a Hard Place

- **Hard Place** = Demanding Compliance Requirements (Partial list)
  - PCI DSS 2.0 (Payment Card Industry Data Security Standard)
  - HIPAA (Health Insurance Portability and Accountability Act)
  - HITRUST CSF (HIPAA, NIST, ISO, PCI, FTC and COBIT)
  - ISO 27001:2005 (International Organization of Standardization)
  - SSAE16 SOC 1 Type II, SOC 2 Type II, SOC 3 (Service Organization Control)
- Compliance Pain Prospects Face
  - Zero to little internal capabilities
  - 3rd party audit required so no dead bodies allowed
  - Mixed internal IT environments = complex compliance scope
  - Compliance requirements continue to evolve
  - Compliance is the bare minimum requirement for security

The Secure Cloud is Not a Myth

- Build for security and compliance
- Follow security best practices vs. chasing compliance guidelines
- Deploy multiple security countermeasures using a layered approach
- Perimeter, Host, Supporting, Admin Access
  - Physical Security
  - DDoS/DoS Mitigation
  - IP Reputation Filtering
  - Web Application Firewalls
  - Intrusion Detection/Prevention
  - Isolated Security Zones
  - Hypervisor-based Firewalls
  - Secure Remote Access
  - Multi-Factor Authentication
  - Vulnerability Monitoring
  - Logging and log review
  - Anti-Virus
  - Patching
  - Encryption



Public Traffic

Redundant Routers w/IP Reputation Filtering

Redundant DoS/DDoS Mitigation

Redundant Web Application Firewalls

Secure Customer Access

Multi-Factor Authentication

SSLVPN/L2LVPN Secure Access

MPLS Termination

Intrusion Detection

File Integrity Monitoring

Data Leakage Protection

Antimalware/ Antivirus

Isolated Customer Environment

Hardened Hypervisor

- Secure Orchestration Layer
- Hypervisor Based Firewalls
- Per VM Firewall Policies
- Unlimited Security Zones

Load Balancers

SECURITY ZONE

Web Servers

SECURITY ZONE

Application Servers

SECURITY ZONE

Database Servers

SECURITY ZONE

Isolated Customer Environment

Vulnerability Management

Log Management

Patch Management

Configuration Management

Secure Administrative Access

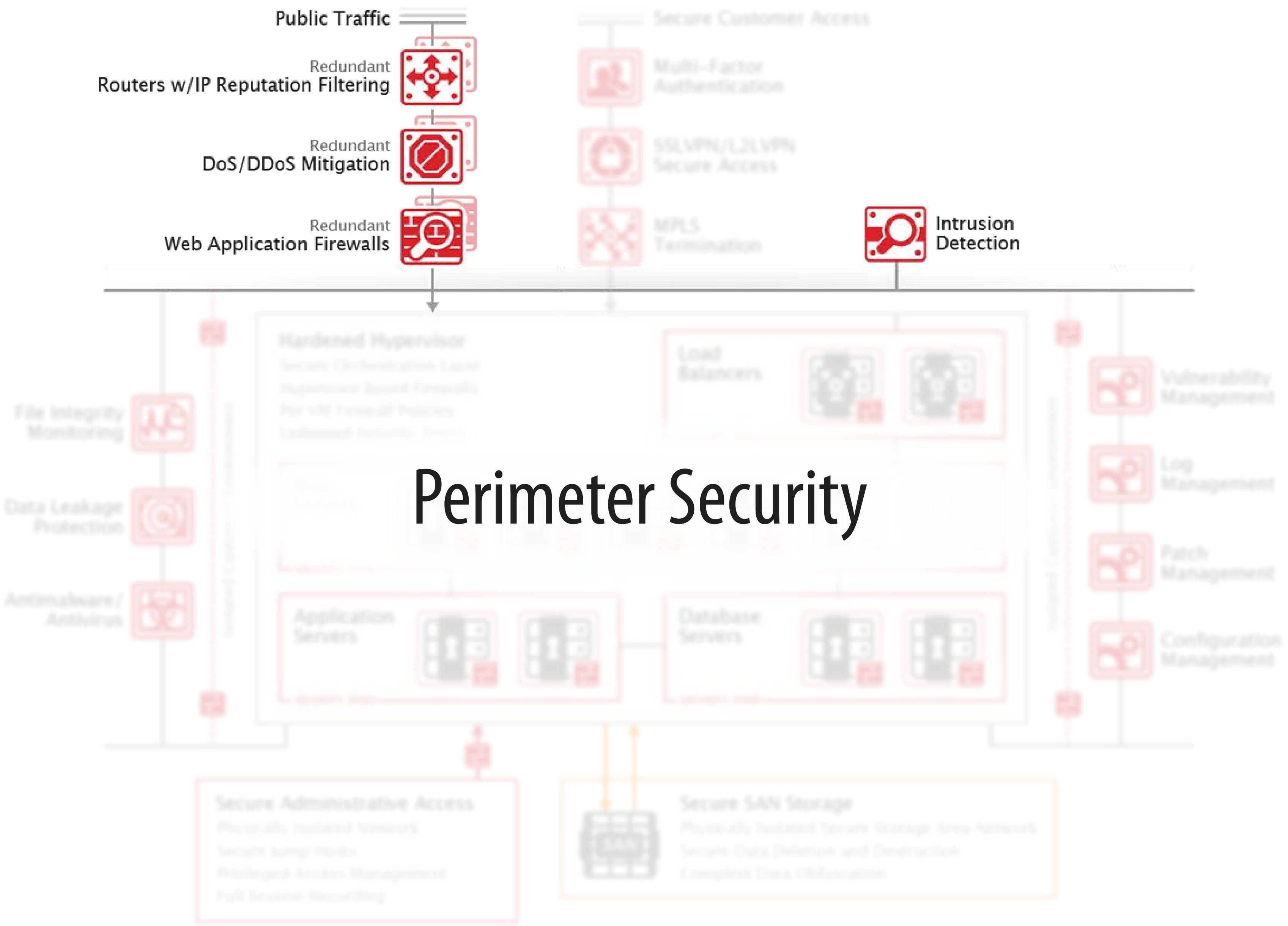
- Physically Isolated Network
- Secure Jump Hosts
- Privileged Access Management
- Full Session Recording

SAN

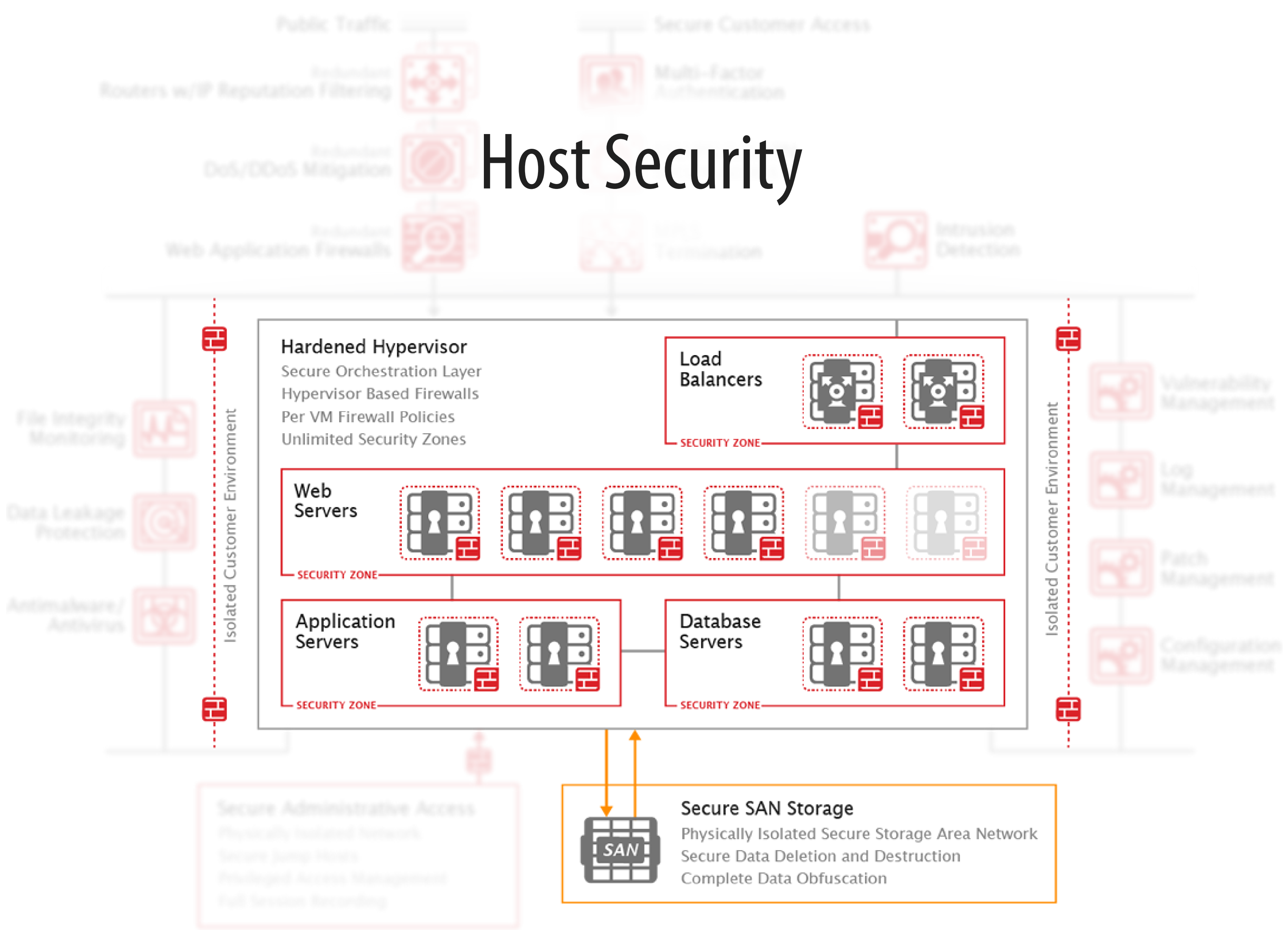
Secure SAN Storage

- Physically Isolated Secure Storage Area Network
- Secure Data Deletion and Destruction
- Complete Data Obfuscation

Perimeter Security



Host Security



Public Traffic

Redundant Routers w/IP Reputation Filtering

Redundant DoS/DDoS Mitigation

Redundant Web Application Firewalls

Secure Customer Access

Multi-Factor Authentication

SSL Termination

Intrusion Detection

File Integrity Monitoring

Data Leakage Protection

Antimalware/ Antivirus

Vulnerability Management

Log Management

Patch Management

Configuration Management

Hardened Hypervisor

- Secure Orchestration Layer
- Hypervisor Based Firewalls
- Per VM Firewall Policies
- Unlimited Security Zones

Load Balancers

Web Servers

Application Servers

Database Servers

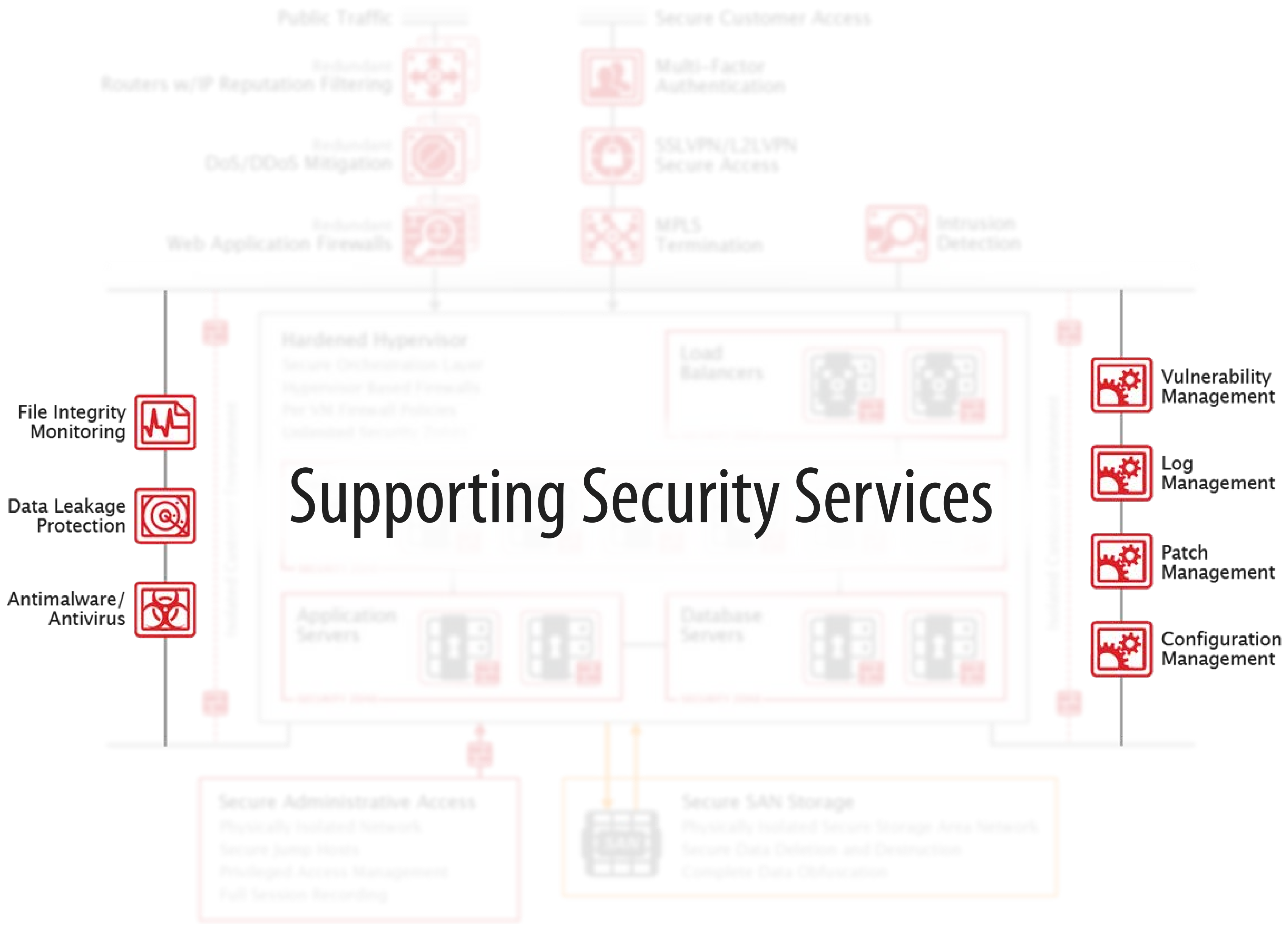
Secure SAN Storage

- Physically Isolated Secure Storage Area Network
- Secure Data Deletion and Destruction
- Complete Data Obfuscation

Secure Administrative Access

- Physically Isolated Network
- Secure Jump Hosts
- Privileged Access Management
- Full Session Recording

Supporting Security Services



File Integrity Monitoring

Data Leakage Protection

Antimalware/ Antivirus

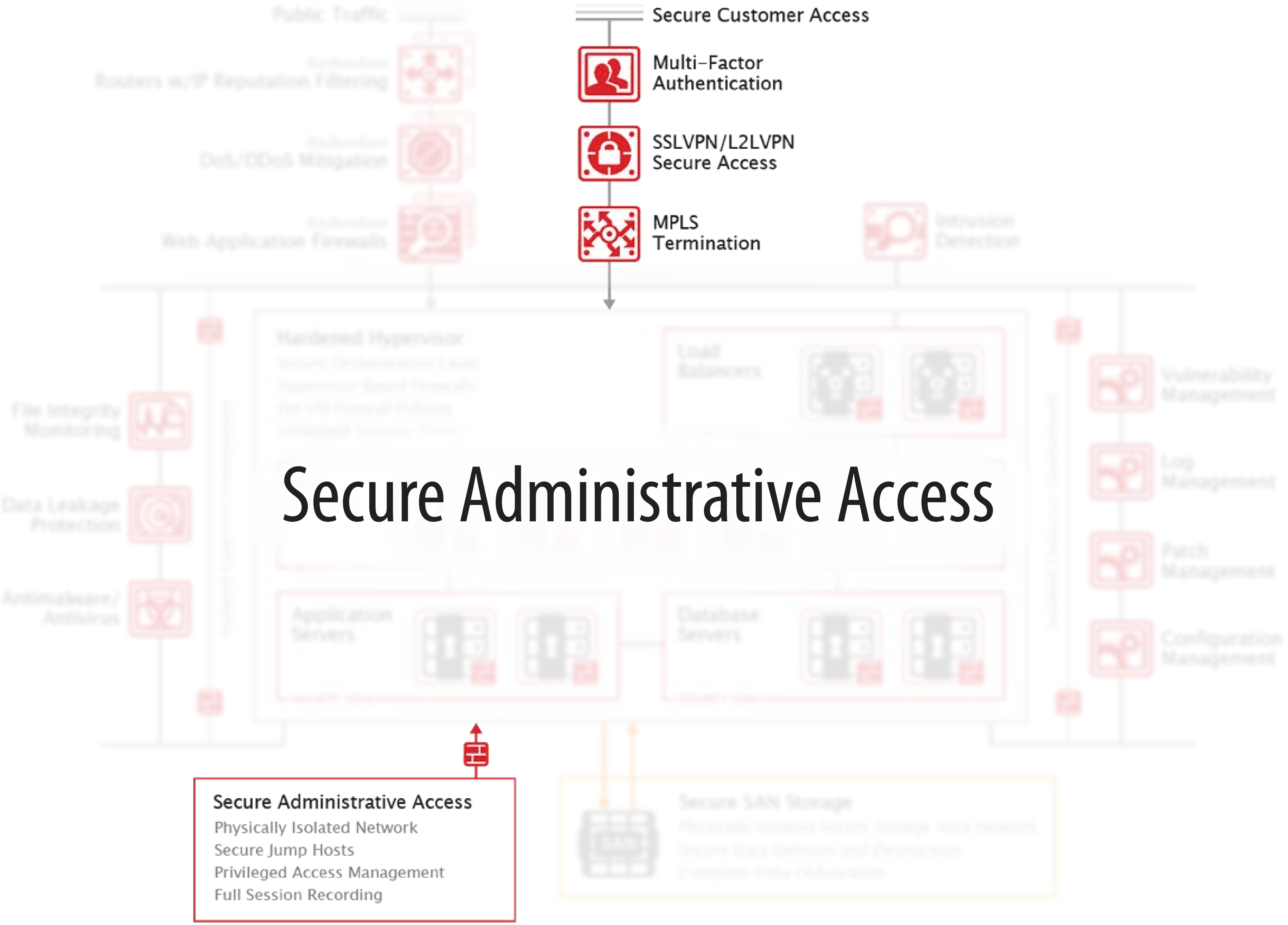
Vulnerability Management

Log Management

Patch Management

Configuration Management

Secure Administrative Access



Secure Customer Access

Multi-Factor Authentication

SSLVPN/L2LVPN Secure Access

MPLS Termination

Secure Administrative Access

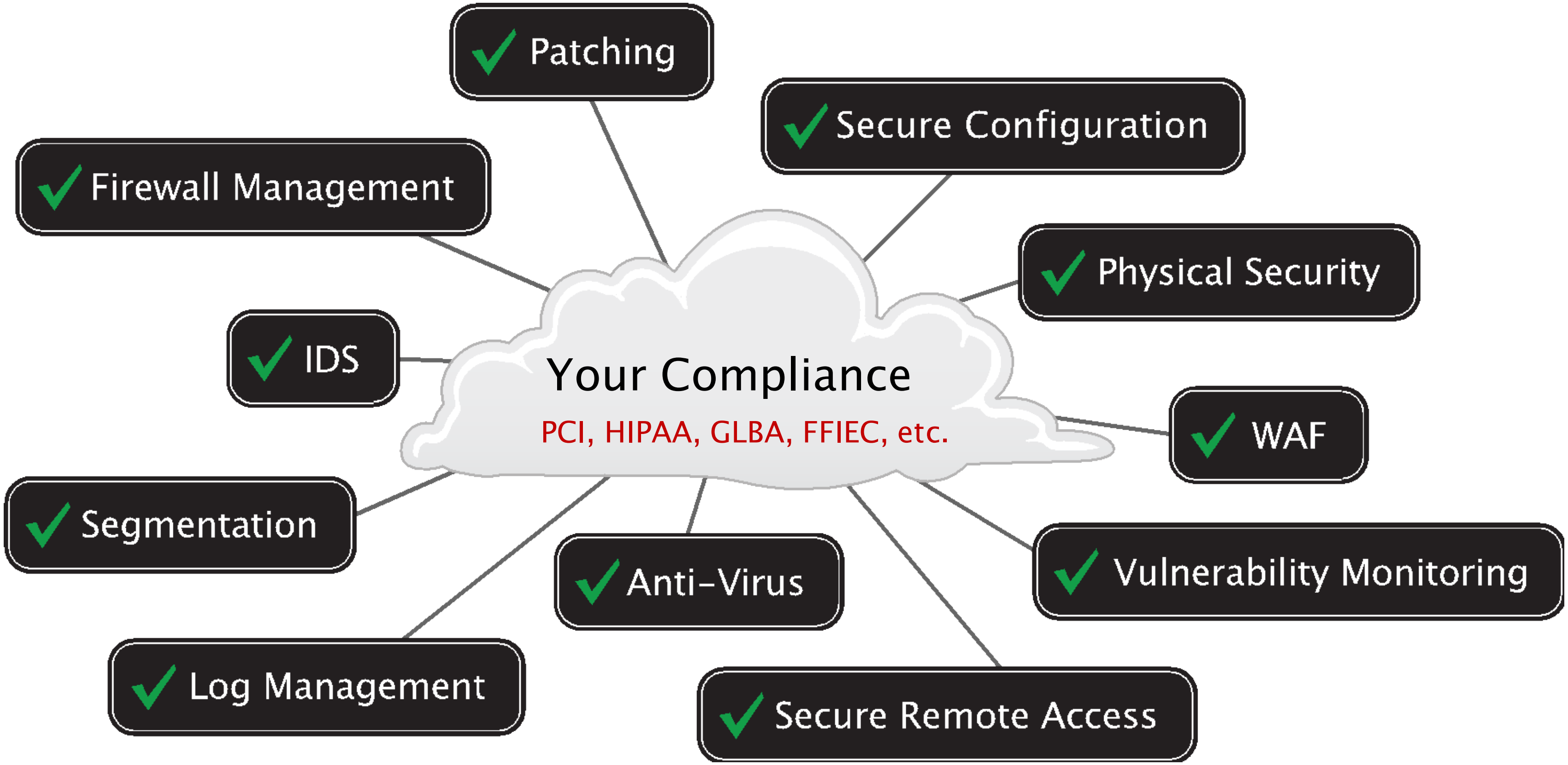
- Physically Isolated Network
- Secure Jump Hosts
- Privileged Access Management
- Full Session Recording

firehost™
SECURE CLOUD HOSTING

Compliance Challenges for Cloud

- Multiple compliance framework and regulatory requirements to meet
- Diverse data types being handled (Credit card, health, financial, PII, etc.)
- Communication of compliance assistance to customers
- Tracking changes in compliance requirements
- Questions around data sovereignty
- Continuous requests for audit support

Compliance Requirements = Common Controls



Data Sovereignty & Privacy | Business Continuity | Contracting & SLAs

Compliance Challenge Solutions

- Treat all data as sensitive (after all, it’s all 1’s and 0’s to the systems)
- Develop a Common Security Framework (CSF) of controls based on industry standard frameworks; enabling efficient compliance adoption and validation reporting
- Provide clear responsibility matrices to customers
- Future proof compliance iterations via your CSF
- Guarantee data sovereignty
- Be auditor friendly - Be organized and transparent - implement a continuous audit program

Summary

- Security threats and compliance requirements are challenges for Cloud
- Use a layered approach to secure the cloud
- Ensure isolation between customer and management environments
- Implement a physically isolated secure storage area network for better security and performance
- Develop a Common Security Framework for your security program
- Continuously monitor and audit

Thanks for your participation

Kurt Hagerman

Director of Information Security

FireHost

kurt.hagerman@firehost.com

877.262.3473 x8073