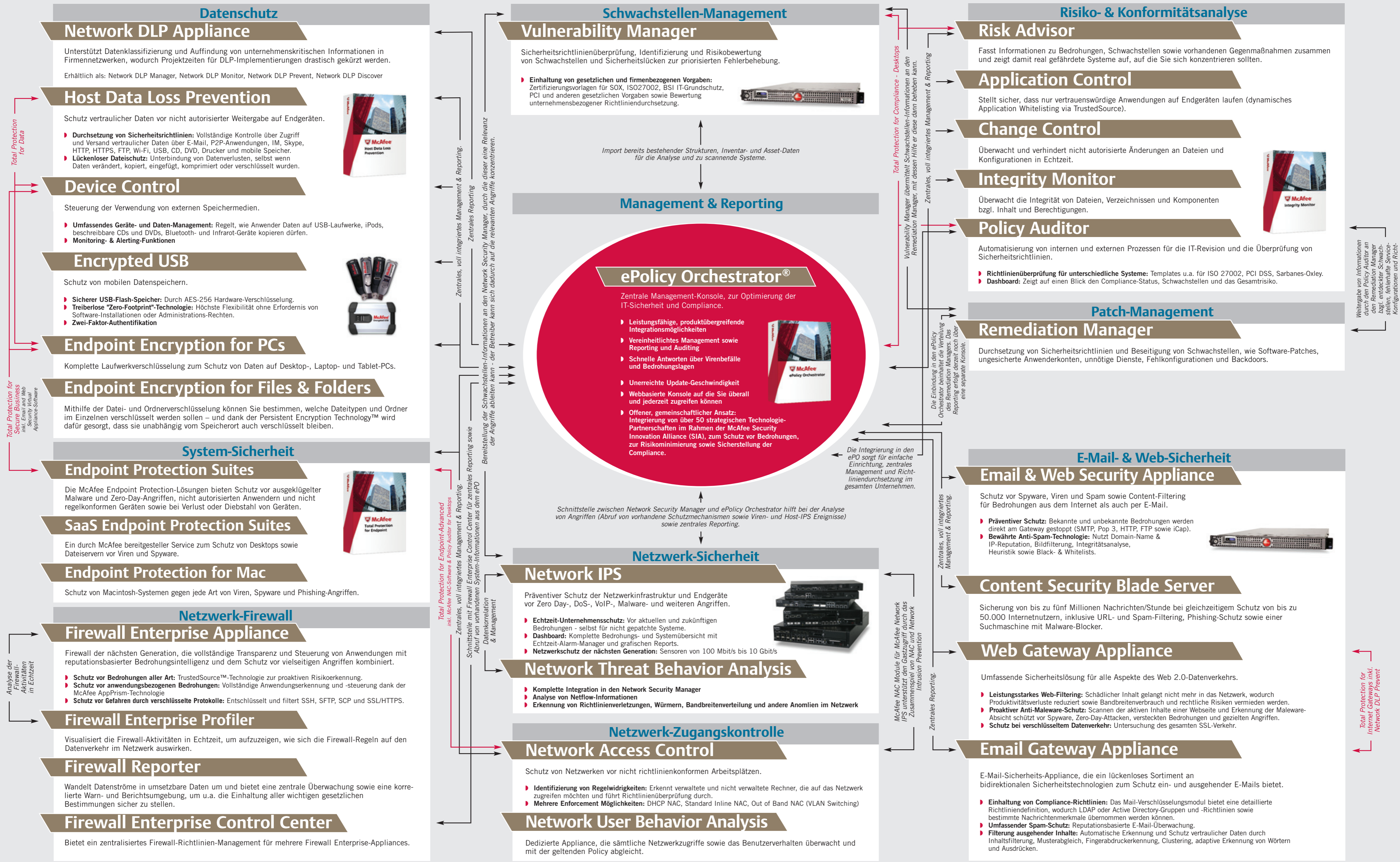


# SRM: Die McAfee Sicherheits-Risikomanagement-Strategie



### Datenschutz

#### Network DLP Appliance

Unterstützt Datenklassifizierung und Auffindung von unternehmenskritischen Informationen in Firmennetzwerken, wodurch Projektzeiten für DLP-Implementierungen drastisch gekürzt werden.  
Erhältlich als: Network DLP Manager, Network DLP Monitor, Network DLP Prevent, Network DLP Discover

#### Host Data Loss Prevention

Schutz vertraulicher Daten vor nicht autorisierter Weitergabe auf Endgeräten.

- Durchsetzung von Sicherheitsrichtlinien:** Vollständige Kontrolle über Zugriff und Versand vertraulicher Daten über E-Mail, P2P-Anwendungen, IM, Skype, HTTP, HTTPS, FTP, Wi-Fi, USB, CD, DVD, Drucker und mobile Speicher.
- Lückenloser Dateischutz:** Unterbindung von Datenverlusten, selbst wenn Daten verändert, kopiert, eingefügt, komprimiert oder verschlüsselt wurden.

#### Device Control

Steuerung der Verwendung von externen Speichermedien.

- Umfassendes Geräte- und Daten-Management:** Regelt, wie Anwender Daten auf USB-Laufwerke, iPods, beschreibbare CDs und DVDs, Bluetooth- und Infrarot-Geräte kopieren dürfen.
- Monitoring- & Alerting-Funktionen**

#### Encrypted USB

Schutz von mobilen Datenspeichern.

- Sicherer USB-Flash-Speicher:** Durch AES-256 Hardware-Verschlüsselung.
- Treiberlose "Zero-Footer"-Technologie:** Höchste Flexibilität ohne Erfordernis von Software-Installationen oder Administrations-Rechten.
- Zwei-Faktor-Authentifikation**

#### Endpoint Encryption for PCs

Komplette Laufwerkverschlüsselung zum Schutz von Daten auf Desktop-, Laptop- und Tablet-PCs.

#### Endpoint Encryption for Files & Folders

Mithilfe der Datei- und Ordnerschlüsselung können Sie bestimmen, welche Dateitypen und Ordner im Einzelnen verschlüsselt werden sollen – und dank der Persistent Encryption Technology™ wird dafür gesorgt, dass sie unabhängig vom Speicherort auch verschlüsselt bleiben.

### System-Sicherheit

#### Endpoint Protection Suites

Die McAfee Endpoint Protection-Lösungen bieten Schutz vor ausgeklügelter Malware und Zero-Day-Angriffen, nicht autorisierten Anwendern und nicht regelkonformen Geräten sowie bei Verlust oder Diebstahl von Geräten.

#### SaaS Endpoint Protection Suites

Ein durch McAfee bereitgestellter Service zum Schutz von Desktops sowie Dateiservern vor Viren und Spyware.

#### Endpoint Protection for Mac

Schutz von Macintosh-Systemen gegen jede Art von Viren, Spyware und Phishing-Angriffen.

### Netzwerk-Firewall

#### Firewall Enterprise Appliance

Firewall der nächsten Generation, die vollständige Transparenz und Steuerung von Anwendungen mit reputationsbasierter Bedrohungsentelligenz und dem Schutz vor vielseitigen Angriffen kombiniert.

- Schutz vor Bedrohungen aller Art:** TrustedSource™-Technologie zur proaktiven Risikoerkennung.
- Schutz vor anwendungsbezogenen Bedrohungen:** Vollständige Anwendungserkennung und -steuerung dank der McAfee AppPrism-Technologie
- Schutz vor Gefahren durch verschlüsselte Protokolle:** Entschlüsselt und filtert SSH, SFTP, SCP und SSL/HTTPS.

#### Firewall Enterprise Profiler

Visualisiert die Firewall-Aktivitäten in Echtzeit, um aufzuzeigen, wie sich die Firewall-Regeln auf den Datenverkehr im Netzwerk auswirken.

#### Firewall Reporter

Wandelt Datenströme in umsetzbare Daten um und bietet eine zentrale Überwachung sowie eine korrelierte Warn- und Berichtsumgebung, um u.a. die Einhaltung aller wichtigen gesetzlichen Bestimmungen sicher zu stellen.

#### Firewall Enterprise Control Center

Bietet ein zentralisiertes Firewall-Richtlinien-Management für mehrere Firewall Enterprise-Appliances.

### Schwachstellen-Management

#### Vulnerability Manager

Sicherheitsrichtlinienüberprüfung, Identifizierung und Risikobewertung von Schwachstellen und Sicherheitslücken zur priorisierten Fehlerbehebung.

- Einhaltung von gesetzlichen und firmenbezogenen Vorgaben:** Zertifizierungsvorlagen für SOX, ISO27002, BSI IT-Grundschutz, PCI und anderen gesetzlichen Vorgaben sowie Bewertung unternehmensbezogener Richtlinien durchsetzung.

Import bereits bestehender Strukturen, Inventar- und Asset-Daten für die Analyse und zu scannende Systeme.

### Management & Reporting

#### ePolicy Orchestrator®

Zentrale Management-Konsole, zur Optimierung der IT-Sicherheit und Compliance.

- Leistungsfähige, produktübergreifende Integrationsmöglichkeiten
- Vereinheitlichtes Management sowie Reporting und Auditing
- Schnelle Antworten über Virenbefälle und Bedrohungslagen
- Unerreichte Update-Geschwindigkeit
- Webbasierte Konsole auf die Sie überall und jederzeit zugreifen können
- Offener, gemeinschaftlicher Ansatz: Integration von über 50 strategischen Technologie-Partnerschaften im Rahmen der McAfee Security Innovation Alliance (SIA), zum Schutz vor Bedrohungen, zur Risikominimierung sowie Sicherstellung der Compliance.

Schnittstelle zwischen Network Security Manager und ePolicy Orchestrator hilft bei der Analyse von Angriffen (Abruf von vorhandene Schutzmechanismen sowie Viren- und Host-IPS Ereignisse) sowie zentrales Reporting.

### Netzwerk-Sicherheit

#### Network IPS

Präventiver Schutz der Netzwerkinfrastruktur und Endgeräte vor Zero Day-, DoS-, VoIP-, Malware- und weiteren Angriffen.

- Echtzeit-Unternehmensschutz:** Vor aktuellen und zukünftigen Bedrohungen - selbst für nicht gepatchte Systeme.
- Dashboard:** Komplette Bedrohungs- und Systemübersicht mit Echtzeit-Alarm-Manager und grafischen Reports.
- Netzwerkschutz der nächsten Generation:** Sensoren von 100 Mbit/s bis 10 Gbit/s

#### Network Threat Behavior Analysis

- Komplette Integration in den Network Security Manager
- Analyse von Netflow-Informationen
- Erkennung von Richtlinienverletzungen, Wurmern, Bandbreitenverteilung und andere Anomalien im Netzwerk

### Netzwerk-Zugangskontrolle

#### Network Access Control

Schutz von Netzwerken vor nicht richtlinienkonformen Arbeitsplätzen.

- Identifizierung von Regelwidrigkeiten:** Erkennt verwaltete und nicht verwaltete Rechner, die auf das Netzwerk zugreifen möchten und führt Richtlinienüberprüfung durch.
- Mehrere Enforcement Möglichkeiten:** DHCP Inline NAC, Standard Inline NAC, Out of Band NAC (VLAN Switching)

#### Network User Behavior Analysis

Dedizierte Appliance, die sämtliche Netzwerkzugriffe sowie das Benutzerverhalten überwacht und mit der geltenden Policy abgleicht.

### Risiko- & Konformitätsanalyse

#### Risk Advisor

Fasst Informationen zu Bedrohungen, Schwachstellen sowie vorhandenen Gegenmaßnahmen zusammen und zeigt damit real gefährdete Systeme auf, auf die Sie sich konzentrieren sollten.

#### Application Control

Stellt sicher, dass nur vertrauenswürdige Anwendungen auf Endgeräten laufen (dynamisches Application Whitelisting via TrustedSource).

#### Change Control

Überwacht und verhindert nicht autorisierte Änderungen an Dateien und Konfigurationen in Echtzeit.

#### Integrity Monitor

Überwacht die Integrität von Dateien, Verzeichnissen und Komponenten bzgl. Inhalt und Berechtigungen.

#### Policy Auditor

Automatisierung von internen und externen Prozessen für die IT-Revision und die Überprüfung von Sicherheitsrichtlinien.

- Richtlinienüberprüfung für unterschiedliche Systeme:** Templates u.a. für ISO 27002, PCI DSS, Sarbanes-Oxley.
- Dashboard:** Zeigt auf einen Blick den Compliance-Status, Schwachstellen und das Gesamtrisiko.

### Patch-Management

#### Remediation Manager

Durchsetzung von Sicherheitsrichtlinien und Beseitigung von Schwachstellen, wie Software-Patches, unsichere Anwenderkonten, unnötige Dienste, Fehlkonfigurationen und Backdoors.

### E-Mail- & Web-Sicherheit

#### Email & Web Security Appliance

Schutz vor Spyware, Viren und Spam sowie Content-Filtering für Bedrohungen aus dem Internet als auch per E-Mail.

- Präventiver Schutz:** Bekannte und unbekannt Bedrohungen werden direkt am Gateway gestoppt (SMTP, Pop 3, HTTP, FTP sowie iCap).
- Bewährte Anti-Spam-Technologie:** Nutzt Domain-Name & IP-Reputation, Bildfilterung, Integritätsanalyse, Heuristik sowie Black- & Whitelists.

#### Content Security Blade Server

Sicherung von bis zu fünf Millionen Nachrichten/Stunde bei gleichzeitigem Schutz von bis zu 50.000 Internetnutzern, inklusive URL- und Spam-Filtering, Phishing-Schutz sowie einer Suchmaschine mit Malware-Blocker.

#### Web Gateway Appliance

Umfassende Sicherheitslösung für alle Aspekte des Web 2.0-Datenverkehrs.

- Leistungsstarkes Web-Filtering:** Schädlicher Inhalt gelangt nicht mehr in das Netzwerk, wodurch Produktivitätsverluste reduziert sowie Bandbreitenverbrauch und rechtliche Risiken vermieden werden.
- Proaktiver Anti-Malware-Schutz:** Scannen der aktiven Inhalte einer Webseite und Erkennung der Malware-Absicht schützt vor Spyware, Zero-Day-Angriffen, versteckten Bedrohungen und gezielten Angriffen.
- Schutz bei verschlüsseltem Datenverkehr:** Untersuchung des gesamten SSL-Verkehr.

#### Email Gateway Appliance

E-Mail-Sicherheits-Appliance, die ein lückenloses Sortiment an bidirektionalen Sicherheitstechnologien zum Schutz ein- und ausgehender E-Mails bietet.

- Einhaltung von Compliance-Richtlinien:** Das Mail-Verschlüsselungsmodul bietet eine detaillierte Richtliniendefinition, wodurch LDAP oder Active Directory-Gruppen und -Richtlinien sowie bestimmte Nachrichtenmerkmale übernommen werden können.
- Umfassender Spam-Schutz:** Reputationsbasierte E-Mail-Überwachung.
- Filterung ausgehender Inhalte:** Automatische Erkennung und Schutz vertraulicher Daten durch Inhaltsfilterung, Musterabgleich, Fingerabdruckererkennung, Clustering, adaptive Erkennung von Wörtern und Ausdrücken.