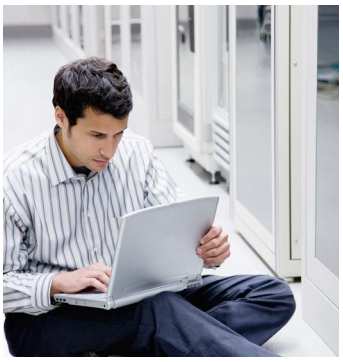
McAfee Firewall Enterprise (Sidewinder®)



Sicherheitsfunktionen von McAfee Firewall Enterprise

Firewall
- Paket-, zustands- und vollständig anwendungsbezogene Filterung
- Mehrer Ausbringungsoptionen, einschließlich Multi-Firewall-Appliances (bei denen eine Appliance bis zu 32 virtuelle Firewalls verwalten kann) sowie eine virtuelle Firewall-Appliance
- NAT (Network Address Translation)

Authentifizierung
- Lokal
- Active Directory
- LDAP (iPlanet, Open LDAP, Custom LDAP)
- RADIUS
- Windows-Domänenauthentifizierung
- Windows NTLM-Authentifizierung
- Passport (Single Sign-On)
- Starke Authentifizierung (SafeWord, SecurID)

Hohe Verfügbarkeit (HA - High Availability)
- Aktiv/aktiv
- Aktiv/passiv
- Zustandsbezogenes Sitzungs-Failover
- IP-Remote-Überwachung

Globale Bedrohungsanalyse
- Weltweiter TrustedSource-Bewertungsservice
- Geolocation-Filterung

Verschlüsselte Anwendungsfilterung
- SSH
- SFTP
- SCP
- SSL/HTTPS*

* Nicht im Lieferumfang enthalten.

Die heutigen Herausforderungen für Firewalls erfordern ein neues Sicherheitsmodell

Firewalls sind die erste Verteidigungslinie von Unternehmen gegen Sicherheitsbedrohungen. Sie sind daher für die Sicherheitsstrategie jedes Unternehmensnetzwerks von entscheidender Bedeutung. Aber die Bedrohungen für Unternehmen – mit neuen Angriffen gegen Anwendungs-Layer und Web 2.0-Sicherheitslücken sowie mit Signaturen umgehender Malware – werden täglich gefährlicher und unvorhersehbarer. Die Sicherheitsvorfälle nehmen zu. Dies liegt zum Teil auch an den veralteten Schutzmechanismen der Firewalls, die gegen diese neuen Bedrohungen nichts ausrichten können. Gleichzeitig mühen sich Administratoren der Firewalls bei ständig steigenden Management-Kosten mit der Verwaltung und der Fehlerbeseitigung bei alten Firewall-Richtlinien ab.

Explodierende Management-Kosten

Die Verwaltung mehrerer veralteter Firewalls ist gelinde gesagt eine zeit- und ressourcen-intensive Aufgabe. Unkoordinierte Veränderungen von Anwendungen und Netzwerken bringen Betriebsausfälle mit sich, deren Ursachen häufig erst nach Stunden oder sogar Tagen festgestellt und beseitigt werden können. Den Administratoren fehlt der Einblick in das Anwenderverhalten und reiben sich in ihren Bemühungen auf, effizient auf die sich verändernden Geschäftsanforderungen ihres Unternehmens zu reagieren. Dabei sind die ihnen immer häufiger gestellten Anforderungen zur Darstellung der Compliance mit Audit- und gesetzlichen Anforderungen noch gar nicht berücksichtigt. Eine weitere mühevolle Aufgabe, die um so teurer und arbeitsintensiv ist, wenn die geeigneten Berichtstools nicht zur Verfügung stehen.

Damit Sie sich präventiv vor der ständig sich verändernden Bedrohungslandschaft schützen können, müssen Sie in der Lage sein, zuverlässig und mit einfachen Mitteln genau die Veränderungen an Ihrer Firewall vorzunehmen, die in Ihrem Unternehmen gefordert sind. Sie brauchen also eine neue Firewall-Lösung: McAfee® Firewall Enterprise (*Sidewinder®*).

Veraltete Schutzmechanismen versagen bei den aktuellen Bedrohungen

Die herkömmlichen Verfahren mit Regeln und Signaturen reichen nicht mehr aus. Neue Bedrohungen werden zu komplexen Angriffen kombiniert, die mehrere Sicherheitslücken auf einmal ausnutzen. Schlimmer noch, sie kommen sowohl von außerhalb als auch von innerhalb des Netzwerks, ja sogar über verschlüsselte Protokolle. Dieser Bedrohungsumgebung Herr zu werden war noch nie so schwierig, da Netzwerke und die Möglichkeiten eine Verbindung herzustellen immer umfangreicher und die Bedrohungen im Schnellfeuertempo zunehmen. Ohne einen Einblick in diese neu auftretenden Bedrohungen benötigen die Administratoren zu viel Zeit und Arbeit, um mit der Entwicklung Schritt halten zu können.

Übersicht über McAfee Firewall Enterprise

Mit McAfee Firewall Enterprise und den zugehörigen Produkten können Administratoren sofort damit beginnen, Firewall-Regeln in einen richtigen unternehmerischen Kontext zu setzen und die Vorteile eines zentralisierten Firewall-Managements, entsprechender Berichte und anwenderfreundlicher Funktionen zur Regelerstellung zu nutzen. Darüber hinaus bietet Firewall Enterprise ein bisher unerreichtes Level an Schutz vor aktuellen Bedrohungen. Erweiterte Funktionen, wie die reputationsbasierte globale Bedrohungsanalyse, der konfigurierbare Schutz auf Anwendungsebene, die Prüfung verschlüsselter Daten, Virenschutz, Inhaltsfilterung und Intrusion Prevention, blockieren Angriffe, bevor sie das Netzwerk erreichen.

Optimierung des Firewall-Managements und der Einhaltung gesetzlicher Bestimmungen bei höherer Flexibilität Ihres Unternehmens

McAfee Firewall Profiler, eine eigene Appliance der Firewall Enterprise-Produktlinie, unterstützt Administratoren bei einer der zeitraubendsten Aufgaben im derzeitigen Firewall-Management - nämlich der Suche und Beseitigung von Firewall-Ausfällen. Durch die Zuweisung der Firewall-Regeln zu Anwendern und Anwendungen

Sicherheitsfunktionen von McAfee Firewall Enterprise (Forts.)

Intrusion Prevention System (IPS)*
- Über 10.000 Signaturen
- Automatische Signatur-Updates
- Anwenderspezifische Signaturen
- Vorkonfigurierte Signatur-Gruppen

Viren- und Spyware-Schutz*
- Schützt vor Spyware, Trojanern und Würmern
- Heuristik
- Automatische Signatur-Updates

Web-Filtering*
- McAfee SmartFilter®
- Blockiert Java, Active-X, JavaScript und SOAP

Spam-Schutz
- Weltweiter TrustedSource-Bewertungsservice

SVPN
- ICSA IPsec-zertifiziert
- IKEv1 und IKEv2
- DES-, 3DES-, AES-128- und AES-256-Verschlüsselung
- SHA-1- und MD5-Authentifizierung
- Diffie-Hellmann-Gruppen 1, 2 und 5
- Richtlinieneingeschränkte Tunnel
- NAT-T
- Xauth

Anwendungstransparenz und -steuerung
- VoIP (SIP)
- SQL (Oracle, MS-SQL)
- Multimedia (H.323)
- SSH
- SMTP
- Citrix
- FTP
- HTTP
- HTTPS*
- IM/P2P
- Andere

McAfee SecureOS®-Betriebssystem
- McAfee Type Enforcement®-Technologie
- Vorkonfigurierte BS-Sicherheitsrichtlinie
- BS-Abschottung
- Netzwerk-Stack-Trennung

* Nicht im Lieferumfang enthalten.

in Echtzeit, ermöglicht Firewall Profiler Administratoren den Einblick in die Auswirkungen neu erstellter oder geänderter Firewall-Regelsätze. Die stunden- oder tagelange mühevolle Arbeit mit der Erstellung und der Korrektur von Regeln ist nun eine Frage von wenigen Mausklicks. Dadurch sinken die Betriebskosten und die Firewall-Administratoren können nun neue Anwendungen schneller implementieren und kurzfristiger auf unternehmerische Anforderungen reagieren.

Die McAfee Firewall Enterprise Admin-Konsole vereinfacht die Erstellung neuer Richtlinien

Zuverlässige Sicherheit muss auch leicht zu konfigurieren sein. Bei der Admin-Konsole von Firewall Enterprise handelt es sich um eine anwenderfreundliche Oberfläche, die es Administratoren ermöglicht, mit nur einem Bildschirm Regeln zu erstellen und selektiv Verteidigungsmechanismen bereitzustellen, wie Anwendungsfilter, IPS-Signaturen und URL-Filterung. Neue Funktions-Updates der Software werden automatisch über das Internet ausgebracht, was den Wartungsaufwand verringert. Sie brauchen nur mit einem Mausklick den Zeitplan festzulegen. Darüber hinaus kann sich Firewall Enterprise einer unerreichten CERT-Historie rühmen. Sie werden nicht von Notsicherheits-Patches unterbrochen und Ihre Mitarbeiter können sich auf strategisch wichtigere Projekte konzentrieren.

Die Firewall Enterprise-Produktlinie enthält weitere Tools zur Vereinfachung des Managements: McAfee Firewall Reporter und McAfee Firewall Enterprise Control Center (*CommandCenter*™).

McAfee Firewall Reporter

Firewall Reporter ist im Lieferumfang von Firewall Enterprise enthalten und wandelt Auditdatenströme in umsetzbare Daten um. Dieses mehrfach ausgezeichnete Sicherheitsereignis-Management (SEM)-Tool bietet eine zentrale Überwachung sowie eine korrelierte Warn- und Berichtsumgebung. Sie können Ihre Netzwerkdaten völlig problemlos mithilfe von über 800 grafischen Berichten darstellen und zur Einhaltung aller wichtigen gesetzlichen Bestimmungen beitragen, einschließlich:

- Sarbanes-Oxley-Gesetz (SOX)
- Bestimmungen des PCI (Payment Card Industry) Security Standards Council
- Gramm-Leach-Bliley Act (GLBA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Federal Information Security Management Act (FISMA)

McAfee Firewall Enterprise Control Center

Firewall Enterprise Control Center ist als zusätzliches Tool erhältlich und bietet ein zentralisiertes Firewall-Richtlinien-Management für mehrere Firewall Enterprise-Appliances. Dies ermöglicht Ihnen, die betriebliche Effizienz zu maximieren, die Richtlinienkontrolle zu vereinfachen, die Regeln und Software-Updates zu optimieren, und die Einhaltung gesetzlicher Bestimmungen nachzuweisen. Sie können sogar die Richtlinien-konfigurationen aller mit Control Center verwalteten Geräte vergleichen, um die Konsistenz im gesamten Netzwerk sicherzustellen. Leistungsfähige Funktionen für das Konfigurations-Management ermöglichen die zentrale Auffindung, Verfolgung und Validierung aller Richtlinienänderungen. Darüber hinaus kann Control Center jetzt auch in McAfee ePolicy Orchestrator® (ePO™) integriert werden, wodurch ePO eine Transparenz der Firewall-Statusdaten und -Berichte erhält.

Bereitstellung globaler Bedrohungsinformationen in Echtzeit zur Vermeidung unerwünschter Daten

Firewall Enterprise beseitigt praktisch die Anfälligkeiten für unbekannte Angreifer durch zwei besondere Verfahren: McAfee TrustedSource™, das branchenweit erste globale Bewertungssystem für Absender im Internet sowie die Geolocation-Filterung, die eine geografische Transparenz und das Richtlinien-Management auf Grundlage des Ursprungslands der Daten ermöglicht.

Globale Bedrohungsanalyse

McAfee TrustedSource hat im Bereich der präventiven Erkennung neue Standards gesetzt. Mit der Unterstützung der Avert Labs, der weltweit größten Organisation für Bedrohungsanalyse, schlüsselt dieser im Internet gehostete Dienst die Daten statt anhand von Signaturen über das bisherige Verhalten von internetbasierten Hosts und Geräten auf. TrustedSource weist Verbindungen von bekanntermaßen negativen Absendern, infizierten Webseiten, komplexen Bedrohungen und Host-Computern, die in Malware verbreitende Zombies umgewandelt wurden, zurück und blockiert diese Angriffe auf diese Weise effizient am Netzwerkperimeter.

Durch die Blockierung dieser Angriffe stoppt TrustedSource auch über 70 Prozent der unerwünschten Daten am Netzwerkrand. Dadurch werden Datenströme auf nachgeschalteten Netzwerk-Servern verringert, was Bandbreite und Verarbeitungszeit spart.

COMMON CRITERIA EAL4+ CERTIFIED

ICSA labs CERTIFIED

McAfee®

Das Betriebssystem McAfee SecureOS gewährleistet die beste Absicherung der Appliance

Im Kern der Appliance wird McAfee Firewall Enterprise auf dem hochsicheren Hochgeschwindigkeits-Betriebssystem McAfee SecureOS ausgeführt. Es beinhaltet die patentierte McAfee Type Enforcement-Technologie, die eine unerreichte Stufe der Plattformsicherheit gewährleistet. SecureOS weist eine unerreichte CERT-Historie auf und wird in den weltweit anspruchsvollsten Netzwerken eingesetzt.

Optionen für Management und Administration

- Grafische Windows-Oberfläche
- Lokale Konsole
- Vollständige Befehlszeile
- Sicherung und Wiederherstellung der USB-DR-Konfiguration
- Schnelle Problembeseitigung und Auswirkungsanalyse für Firewall-Regeln mithilfe von McAfee Firewall Profiler (nicht im Lieferumfang enthalten)

Protokollierung, Überwachung und Berichterstellung

- On-Box-Protokollierung
- Geplante Protokollarchivierung und -exportierung
- Firewall Enterprise-Protokoll im Software Extract-Format (SEF)
- Mehrere Exportformate (XML, SEF, W3C, WebTrends)
- Syslog
- SNMP Version 1, 2c und 3
- McAfee Firewall Reporter SEM enthalten

Netzwerk- und Routing-Funktionen

- Dynamisches Routing (RIP Version 1 und 2, OSPF, BGP und PIM-SM)
- Statische Routes
- 802.1Q VLAN-Tagging
- DHCP-Client
- Standardrouten-Failover
- QoS

Sichere Server

- Secure DNS (einzeln oder gesplittet)
- Secure Sendmail (einzeln oder gesplittet)

Appliances und Hardware

- Upgrade-Gewährleistung mit bis zu 4-Stunden-Reaktion für die meisten Modelle
- Virtualisierungslösungen und Rugged Appliance-Optionen erhältlich
- Einfache sowie Dual-Core- und Quad-Core-Prozessoren
- ASIC-basierte Beschleunigung
- RAID HDD-Konfigurationen
- Redundante Netzteile

* Nicht im Lieferumfang enthalten.

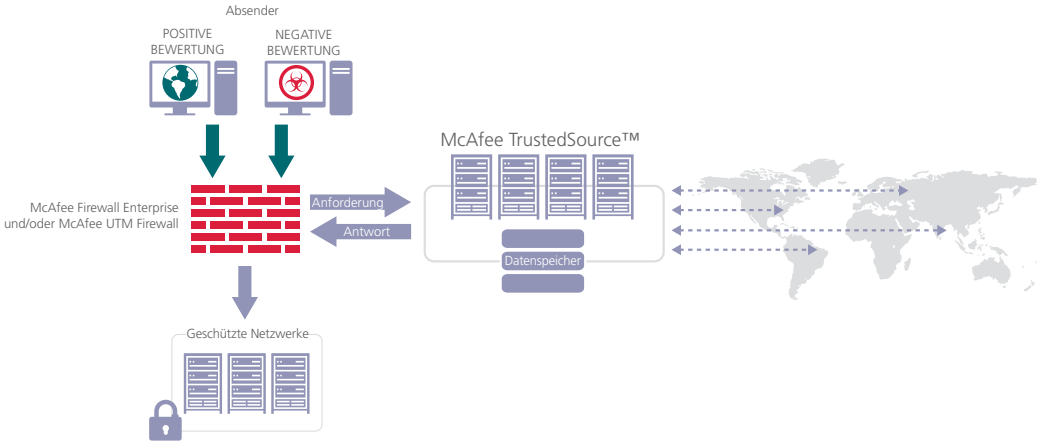
McAfee bietet mehrfach ausgezeichneten technischen Support

- Technischer Telefon-Support rund um die Uhr
- Technischer Support mit internetbasiertem Ticketing und Knowledgebase rund um die Uhr

McAfee®

Geolocation-Filterung

Die Geolocation-Funktion von Firewall Enterprise schränkt die globalen Bedrohungen dadurch noch weiter ein, dass Daten anhand eines Ländercodes gefiltert werden. Zahlreiche Unternehmen verbrauchen Bandbreite und System-Ressourcen für Datenströme aus Ländern und ganzen Kontinenten, mit denen sie in keiner Geschäftsbeziehung stehen und setzen sich dabei auch noch unnötigen Risiken aus. Mithilfe von Geolocation sorgen Sie dafür, dass nur die Daten zugelassen werden, die sich auf Ihre Geschäftsvorgänge beziehen.



Kontrolle und Steuerung von Anwendungen

Je organisierter und nachhaltiger Computerkriminelle zu Werke gehen, desto wachsamer müssen Netzwerksicherheits-Administratoren beim Schutz der unternehmenskritischen Netzwerke, Anwendungen und Daten sein. Hacker greifen insbesondere die Anwendungen an: Mindestens 80 Prozent aller neuen Angriffe konzentrieren sich auf die Sicherheitslücken von Anwendungen. Mit herkömmlichen Firewalls oder Systemen, die entweder nur zustandsbezogene Analysen oder tiefgehende Prüfungen durchführen, können Sie Ihr Unternehmen nicht mehr ausreichend schützen.

Firewall Enterprise verwendet sowohl zustandsbezogene Analysen als auch tiefgehende Prüfungen, lässt als echte Firewall auf Anwendungsebene aber auch, wo immer diese benötigt werden, erweiterte Schutzfunktionen zu, ohne dass hierbei Leistungseinbußen auftreten.

Steuerungen auf Anwendungsebene stehen für viele der heute verwendeten Protokolle zur Verfügung, wie zum Beispiel:

- E-Mail (SMTP)
- Internet (HTTP und HTTPS)
- Multimedia (H.323)
- Oracle und MS-SQL
- Citrix
- Voice over IP / Session Initiation Protocol (VoIP/SIP)
- Secure Shell (SSH)
- File Transfer Protocol (FTP)

Einhaltung von PCI DSS-Anforderungen

Der Datensicherheitsstandard der Zahlkartenindustrie (PCI DSS) fordert von den Kreditkarten ausgebenden Unternehmen die Ausbringung einer Anwendungs-Firewall. Firewall Enterprise unterstützt Sie bei der Einhaltung dieser Anforderungen und dem präventiven Schutz der Kontendaten Ihrer Kunden.

Beseitigung von Sicherheitslücken verschlüsselter Anwendungen

Die meisten heutigen Unternehmen verschlüsseln zumindest einen Teil ihrer Internetdaten, die sie für die Kommunikation mit Geschäftspartnern oder Kunden bzw. für die Systemkommunikation zwischen Clients und Servern verwenden. Dabei stellt die Verschlüsselung zwar einen wertvollen Schutz von übermittelten Daten dar, sie ist aber auch eine Gelegenheit für Computerkriminelle. Die meisten älteren Firewalls prüfen nämlich keine verschlüsselten Daten und können daher auch keine Malware- oder Intrusion Prevention-Signaturen in verschlüsselten Daten erkennen. Dies öffnet der Ausnutzung von Servern und Anwendungen durch Hacker Tür und Tor.

Firewall Enterprise beseitigt diese Sicherheitslücke durch die Entschlüsselung, Filterung und Steuerung von Secure Shell (SSH)-, Secure FTP (SFTP)-, Secure Channel Protocol (SCP)- und Secure Socket Layer (SSL)- bzw. HTTPS-Daten. Dadurch werden Überraschungsangriffe auf Ihre Internet- und Anwendungs-Server ausgeschlossen und die Integrität und Authentizität der verschlüsselten Nachrichten dennoch geschützt.

Produktlinie von McAfee Firewall Enterprise

Die Firewall Enterprise-Produktlinie enthält Appliances für Unternehmen jeder Größe sowie begleitende Produkte wie McAfee Firewall Profiler, McAfee Firewall Enterprise Control Center und McAfee Firewall Reporter für die Optimierung der Verwaltungsvorgänge und die Reduzierung der Betriebskosten. Flexible Hybrid-Delivery-Optionen mit physischen Appliances, Multi-Firewall-Appliances, virtuellen Appliances und Appliances wie McAfee Firewall Enterprise RM700 für hochzuverlässige Umgebungen. Weitere Informationen finden Sie in den Datenblättern der einzelnen Produkte.

Hardware-Daten

	410	510	1100	2100	2150	2150VX	4150
Formfaktor	1U für kleine Unternehmen	1U für kleine Unternehmen	1U für große Unternehmen	2U für große Unternehmen	2U für große Unternehmen	2U für große Unternehmen	5U für große Unternehmen
Unbegrenzte Anwenderlizenzen	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Empfohlene Anwenderzahl	300	600	Mittelgroß	Mittelgroß	Groß	Groß	Große Unternehmen
RAID	Nicht zutreffend	Nicht zutreffend	RAID 1	RAID 1	RAID 5	RAID 5	RAID 5
Netzteil	Einfach	Einfach	Redundant	Redundant	Redundant	Redundant	Redundant
Kupfer-Schnittstellen (grundl./max.)	8 GB	8 GB	8/14 GB	8/20 GB	8/20 GB	20 GB	14/24 GB
Option für Glasfaser-Schnittstellen (max.)	Nicht zutreffend	Nicht zutreffend	4	6	6	Nicht zutreffend	6
Option für 10 GB-Schnittstelle (max.)	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend	2	2	2	2
SSL/HTTPS-Entschlüsselung und -Filterung	Nicht zutreffend	Nicht zutreffend	Ja	Ja	Ja	Ja	Ja
Einhaltung gesetzlicher Bestimmungen	FCC (nur in den USA) Klasse B, ICES (Kanada) Klasse B, CE Mark (EN 55022 Klasse B, EN55024, EN61000-3-2, EN61000-3-3), VCC (Japan) Klasse B, BSMI (Taiwan) Klasse A, C-Tick (Australien/Neuseeland) Klasse B, SABS (Südafrika) Klasse B, CCC (China) Klasse B, MIC (Korea) Klasse B, UL 60950, CAN/CSA C22.2 Nr. 60950, IEC 60950						
Zertifizierungen	ICSA Labs IPSec VPN, Common Criteria EAL4+ mit Anwendungsschutzprofil (einzige Firewall mit dieser EAL4+-Zertifizierung), FIPS 140-2, Stufe 2						
Leistung							
Durchsatz Paketfilterung (TCP)	275 Mb/s	650 Mb/s	1,9 Gb/s	1,9 Gb/s	3,1 Gb/s	3,1 Gb/s	3,8 Gb/s
Zustandsbezogener Durchsatz	250 Mb/s	600 Mb/s	1,8 Gb/s	1,8 Gb/s	2,9 Gb/s	2,9 Gb/s	3,6 Gb/s
Gleichzeitige Verbindungen	100.000	500.000	1.000.000	1.000.000	1.600.000	1.600.000	2.000.000
Durchsatz der Anwendungsfilterung	230 Mb/s	250 Mb/s	1,4 Gb/s	1,4 Gb/s	2,2 Gb/s	2,2 Gb/s	2,7 Gb/s
IPSec VPN-Durchsatz	160 Mb/s	160 Mb/s	240 Mb/s	240 Mb/s	350 Mb/s	350 Mb/s	400 Mb/s
Abmessungen, Gewicht, Umgebungen							
Breite	54,6 cm	54,6 cm	42,6 cm	44,43 cm	44,43 cm	44,43 cm	44,27 cm
Tiefe	42,54 cm	57,6 cm	77,2 cm	74,4 cm	74,4 cm	74,4 cm	67,43 cm
Höhe	4,2 cm	4,2 cm	4,26 cm	8,64 cm	8,64 cm	8,64 cm	21,77 cm
Gewicht	11,8 kg	11,8 kg	16,3 kg	23 kg	28,85 kg	28,85 kg	45,36 kg
Stromversorgung	345 W 110/220 V	345 W 110/220 V	Redundant 670 W 110/220 V	Redundant 750 W 110/220 V	Redundant 750 W 110/220 V	Redundant 750 W 110/220 V	Redundant 930 W 110/220 V
Betriebstemperatur	10 °C - 35 °C	10 °C - 35 °C	10 °C - 35 °C	10 °C - 35 °C	10 °C - 35 °C	10 °C - 35 °C	10 °C - 35 °C

McAfee®
McAfee GmbH
Ohmstr. 1
85716 Unterschleißheim
Deutschland
Telefon: +49 (0)89 3707 0
www.mcafee.com/de

5495brf_fire_0109_fnl