STORMSHIELD

ANTWORT AUF UNBEKANNTE ANGRIFFE

# Breach Fighter

CLOUD-BASIERTE SANDBOX

NETWORK SECURITY | ENDPOINT SECURITY | DATA SECURITY

# Stormshield Breach Fighter

DYNAMISCHER SCHUTZ GEGEN UNBEKANNTE ANGRIFFE AUFGRUND DER KOMBINATION VON STORMSHIELD-TECHNOLOGIEN

Als Gegenmaßnahme gegen die immer komplexeren Angriffe und Schadprogramme verlieren die traditionellen Ansätze mit Signaturen, etwa bei der Antivirussoftware, zunehmend an Wirkung. Jeden Tag werden wie Unternehmen Opfer der Cyberkriminalität, obwohl sie Sicherheitssysteme eingerichtet haben. Die Breach Fighter-Lösung von Stormshield **erweitert die Kapazitäten der Stormshield Next Generation Firewalls und garantiert den Echtzeitschutz** gegen Angriffe mit einer einzigartigen Technologie, die auf der Umgebungsanalyse-Funktion von Stormshield Endpoint Security beruht.

## OPTIMALER SCHUTZ GEGEN ANGRIFFE

Breach Fighter kombiniert den Antivirusschutz auf hohem Niveau durch den Kaspersky-Motor, den Schutz durch den patentierten IPS-Motor und die Technologie von Stormshield Endpoint Security. Diese Technologie, die spezifisch als Reaktion auf hochkomplexe Bedrohungen entwickelt wurde, konnte sich bei gezielten Angriffen und Ransomware bereits bewähren. Diese Kombination aus Produkten wird durch eine Analyse der Bedrohungen durch unser Security Watch-Team ergänzt.

## SCHUTZ ÜBER MEHRERE SCHICHTEN

Breach Fighter läuft in der Cloud. Clients können sich daher auf mehrere hundert Stormshield Network Security-Appliances stützen, die auf der ganzen Welt eingerichtet sind. Diese Community ist bei einer infizierten Datei automatisch geschützt. Der Ansatz *Multi-layer Collaborative Security* von Stormshield ermöglicht es Clients, diesen Schutz ohne Zeitverzögerung in Anspruch zu nehmen.

## VERTRAUENSWÜRDIGER CLOUD-SERVICE

Im Rahmen des Cloud-Angebots von Stormshield wird Breach Fighter in europäischen vertrauenswürdigen Rechenzentren bereitgestellt, sodass alle rechtlichen Vorschriften und die zukünftige europäische Datenschutz-Grundverordnung (DSGV) eingehalten werden. Außerdem profitieren sie von den Zertifizierungen und Qualifikationen der Stormshield Network- und Endpoint Security-Produkte.

## EINFACHE INTEGRATION

Breach Fighter wird als Service angeboten und kann auf einer Stormshield-Appliance mit einem Klick aktiviert werden. Da keine zusätzlichen Geräte integriert werden müssen, hat dieser Service keine Auswirkungen auf die Infrastruktur, weil einfach nur eine neue Prüfung mit der Bezeichnung *Sandboxing* auf die zu analysierenden Datenströme angewendet wird.

## WICHTIGSTE VORTEILE

**Schutz gegen komplexe Angriffe in Echtzeit**

**Kombination aus Vorbeugung gegen Eindringlinge und SNS mit SES-Erfahrung**

**Keine Auswirkungen auf die Infrastruktur**

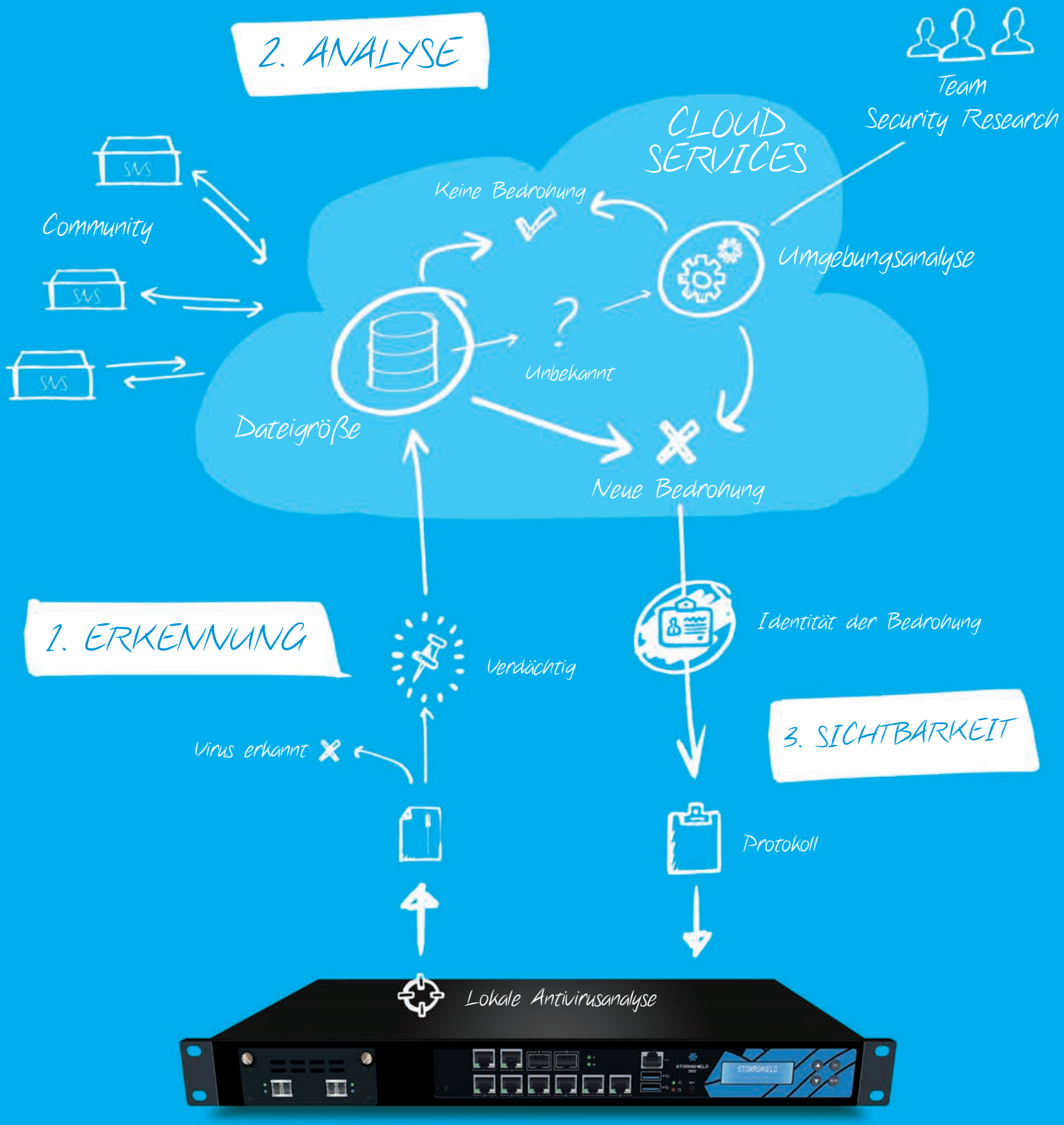
**Rechenzentren in Europa**

### Was ist die Multi-Layer Collaborative Security?

Wir entwickeln Lösungen, die entsprechend unserem Ansatz der Sicherheit für die Zusammenarbeit auf mehreren Ebenen in Echtzeit kooperieren.

Unsere Lösungen ermöglichen es Unternehmen, die den Schutz ihrer Ressourcen verstärken möchten, das Schutzniveau an den erforderlichen Stellen gezielt und dynamisch zu erweitern.

Die Stormshield-Lösungen verstärken das Sicherheitsniveau basierend auf der Korrelationsanalyse der Schadrisikoindikatoren automatisch, in Echtzeit und mit geringeren Kosten.




# Arbeitsweise von Stormshield Breach Fighter

Fall einer E-Mail mit verdächtiger Anlage

**VORAUSSETZUNGEN**

**SNS-Produkte**
ab SN500

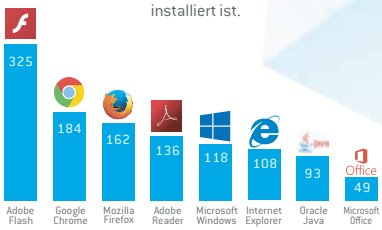
**Kaspersky-Option**
Aktiviert

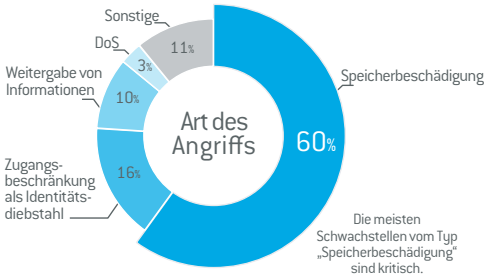
# Bewährte Technologie

Endpoint Security Monitoring Review 2015

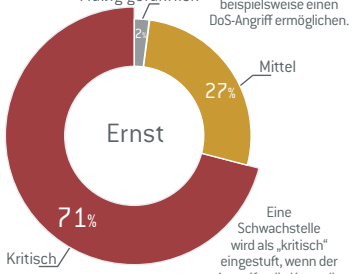
## Von Stormshield analysierte Schwachstellen


Diese Schwachstellen betreffen gängige Software, die auf den meisten Computern installiert ist.




Die meisten Schwachstellen vom Typ „Speicherbeschädigung" sind kritisch.




Die „mäßig gefährlichen" Schwachstellen können beispielsweise einen DoS-Angriff ermöglichen.

Eine Schwachstelle wird als „kritisch" eingestuft, wenn der Angreifer die Kontrolle des Computers übernehmen kann.

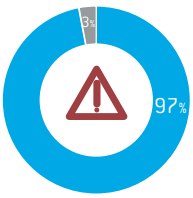
## Proaktive Blockierung durch SES

Stormshield SES kann die meisten Angriffe auf Schwachstellen proaktiv verhindern. Wenn dies nicht gelingt, wird von SES eine Meldung über notwendige Veränderung der Sicherheitsrichtlinien ausgegeben.


### Bekannte* und kritische Exploits

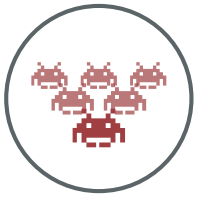
Stormshield SES hat 100 % der kritischen Angriffe mit bekannten Exploits blockiert.

*„Bekannt" = tatsächlich beobachtet




### Kritische Exploits

AUCH WENN diese Schwachstellen, nicht ausgenutzt wurden, blockiert SES 97 % der Exploits kritischer Schwachstellen. Die restlichen 3 % werden in Sicherheitsmeldungen von Stormshield erfasst.



### Malware

SES blockiert AUCH Malware, die keine Schwachstellen ausnutzt, beispielsweise Ransomware wie Locky, Dridex, CryptoLocker, CryptoWall, TeslaCrypt.

STORMSHIELD

WWW.STORMSHIELD.EU

dach@stormshield.eu