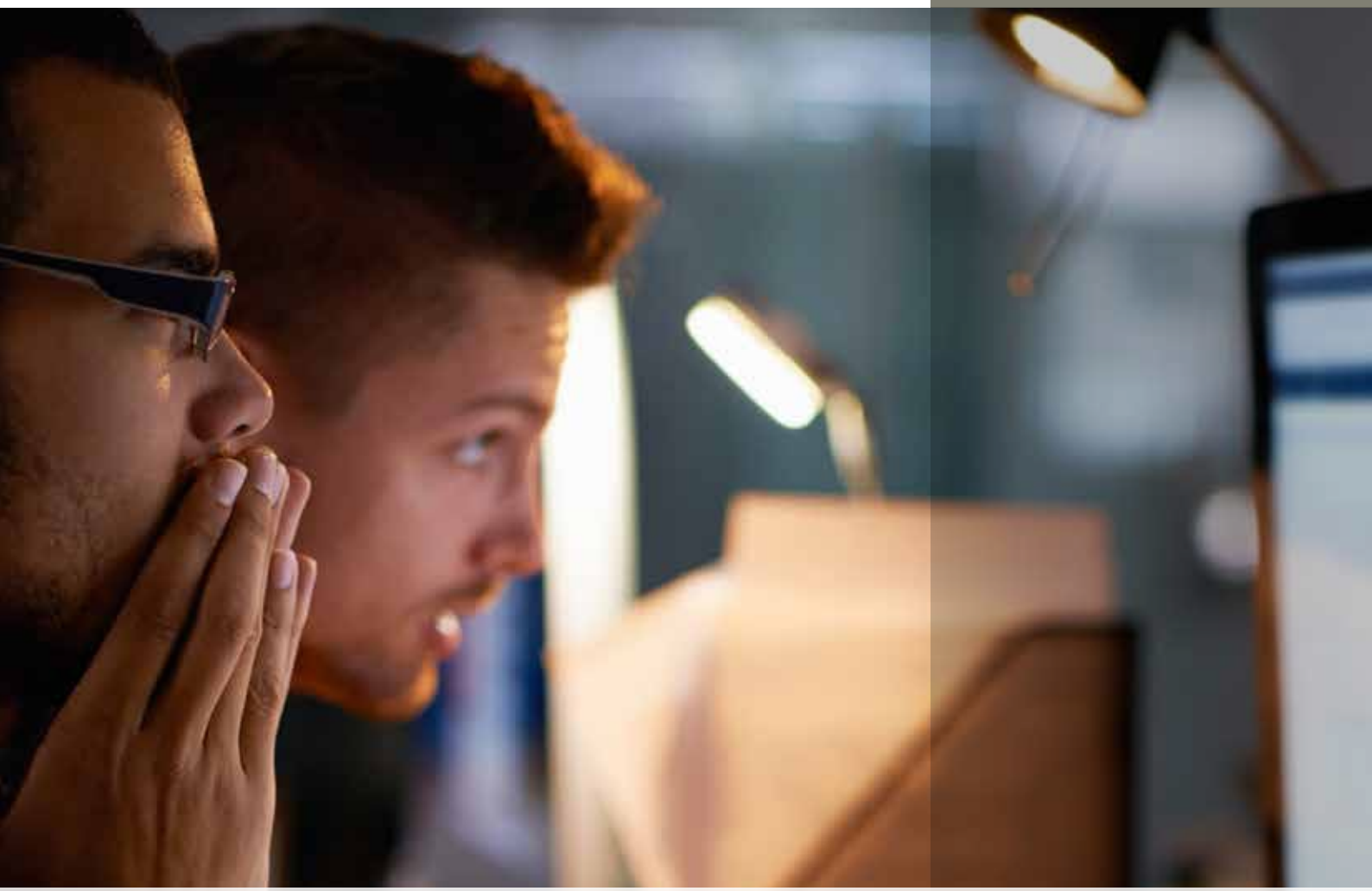
FORTINET

WHITE PAPER



# Das Fortinet Advanced Threat Protection-Framework

## Ein kohärenter Ansatz zum Umgang mit komplexen, gezielten Angriffen

# Das Fortinet Advanced Threat Protection-Framework

## Inhaltsverzeichnis

# Einleitung

## Ausgeklügelte Angriffe lohnen sich

In den Jahren 2013 und 2014 haben viele bekannte Marken und große Unternehmen Schlagzeilen gemacht. Der Grund dafür war jedoch weder eine beachtenswerte wirtschaftliche Leistung noch ein innovatives Produkt, sondern die Tatsache, dass sie Opfer von massivem Datenklau wurden. Durch nur einen dieser dreisten und weitreichenden Angriffe wurden die personenbezogenen und/oder Kreditkartendaten von über 100 Millionen Kunden gestohlen.

Diese Angriffe ziehen die Aufmerksamkeit von Verbrauchern, Juristen und Medien auf sich, weil es Hackern gelingt, in sehr große Unternehmen mit eigenen Sicherheitsteams und einer umfangreichen Infrastruktur, die genau das verhindern sollen, einzudringen. Niemand ist gefeit. Auch kleinere Unternehmen werden zum Ziel, entweder als Teil eines größeren koordinierten Angriffs oder durch verschiedenste verteilte Malware.

Die Konsequenz? Es ist höchste Zeit für einen gründlichere und umfassender Auseinandersetzung mit dem Thema Cybersecurity.

*„Alle Unternehmen müssen jetzt davon ausgehen, dass sie kontinuierlich gefährdet sind.“*

– Gartner

*„18 % der Unternehmen gaben in einer im Jahr 2014 durchgeführten Umfrage an, dass es einen erfolgreichen Angriff von außen auf ihr Netzwerk gab.“*

*– PwC*

*„44 % der befragten Unternehmen gaben an, dass eine Datenpanne in jüngster Vergangenheit die Anschaffung einer NGFW maßgeblich vorangetrieben hat.“*

*– Forrester/Fortinet*

## Täuschung – das gefährlichste Instrument im Arsenal von Hackern

Angespornt durch die erfolgreichen Angriffe auf renommierte Ziele erwarten wir einen Innovationsschub in der Hackerszene, der sich noch stärker auf die Täuschung und Umgehung bestehender Sicherheitslösungen konzentriert. Kriminelle Hacker haben versucht, Malware durch verschiedene Dateitypen und Komprimierungsmuster zu tarnen, um Schwachstellen in den gängigen Maßnahmen zum Schutz von Netzwerken auszunutzen. Des weiteren kommen immer mehr ausgeklügelte Malware-Plattformen in Umlauf, die für gezielte Angriffe angepasst werden können.

Einmal in ein Netzwerk eingeschleust verändert sich die Malware, entweder eigenständig oder von außen gesteuert, passt ich an, bewegt sich möglichst lange unentdeckt durch das Netz und durchsucht es nach den unterschiedlichsten Informationen, von Kundendaten und geistigem Eigentum über Geräteprofile bis hin zu Anmeldedaten von Mitarbeitern. **Wenn die Sicherheitssysteme die Malware oder ihre Kommunikationsverbindungen in dieser Phase nicht aufspüren, ist es nur eine Frage der Zeit, bis die gesammelten Daten en bloc abgeschöpft, d. h. an den Angreifer übertragen, werden.**

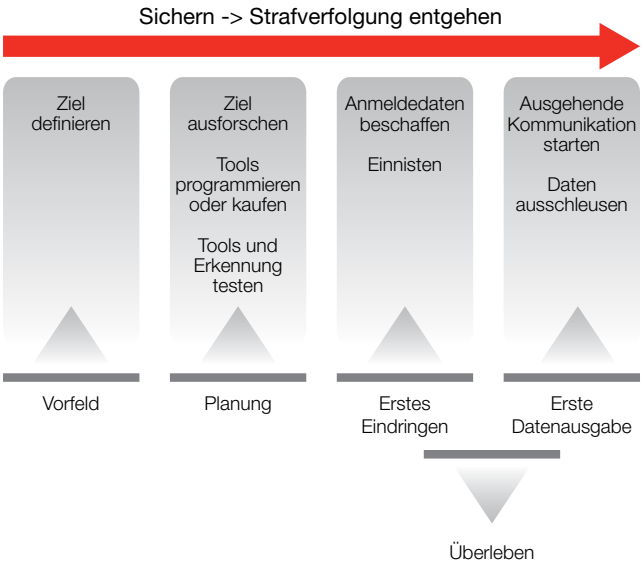



ABBILDUNG 1: ANATOMIE EINER KOMPLEXEN BEDROHUNG

## Gegen komplexe Bedrohungen hilft nur entsprechender Schutz

Gegen die oben beschriebenen, komplexen, gezielten Angriffe gibt es keine „Wunderwaffe“. Ständige Neuentwicklungen an der Malware-Front, häufige Zero-Day-Angriffe und neue Verschleierungstechniken können jeden eindimensionalen Ansatz, maßgeschneiderte Angriffe zu verhindern, zunichte machen.

Für eine möglichst effektive Verteidigung ist stattdessen eine kohärente und erweiterbare Sicherheitsarchitektur erforderlich. Dieses Framework umfasst aktuelle Sicherheitslösungen, neuen Technologien und einen angepassten Lernmechanismus, der neu entdeckte Bedrohungen in verwertbare Sicherheitsdaten übersetzt. Letzteres ist unbestritten die wichtigste Komponente, um im Wettlauf gegen die Bedrohungen die Nase vorn zu behalten.

## Ein einfaches Framework gegen komplexe Bedrohungen

Das Fortinet Advanced Threat Protection-Framework besteht aus drei Stufen:

- **Vorbeugen:** Auf Grundlage bekannter Bedrohungen und Daten Vorkehrungen treffen
- **Erkennen:** Bisher unbekannte Bedrohungen identifizieren
- **Abwehren:** Auf potenzielle Vorfälle reagieren

Das Konzept des Framework ist einfach. Es umfasst ein breites Spektrum hoch entwickelter und klassischer Tools zum Schutz von Netzwerken, Anwendungen und Endgeräten sowie zur Erkennung und Abwehr von Bedrohungen. Diese Tools werden durch intensive Forschung und Verarbeitung von Bedrohungsanalysen flankiert, die Daten aus vielen Quellen in anwendbare Schutzmechanismen umwandeln. Die Stufen des Framework (und auch einzelne enthaltene Technologien) können voneinander isoliert betrieben werden. Einen weitaus besseren Schutz erreichen Unternehmen jedoch, wenn sie sie im Rahmen einer ganzheitlichen Sicherheitsstrategie gemeinsam einsetzen.

## Stufe 1 – Vorbeugen Auf Grundlage bekannter Bedrohungen und Daten Vorkehrungen treffen

Bekannte Bedrohungen werden mithilfe von Next-Generation Firewalls, sicheren E-Mail-Gateways, Endgerätesicherheit und ähnlichen Lösungen, die hochpräzise Sicherheitstechnologien nutzen, sofort blockiert (Stufe 1 des Fortinet Advanced Protection-Framewroks). Beispiele für diese Lösungen sind u. a. Anti-Malware, Webfilter, Intrusion Prevention usw. **Das ist die effektivste Methode, um ohne größere Auswirkungen auf die Netzwerkleistung eine Vielzahl an Bedrohungen auszusieben.**

So kann Anti-Malware beispielsweise Viren, Botnets und sogar vorausgesagte Varianten von Malware durch Einsatz von Technologien, wie der patentierten Compact Pattern Recognition Language (CPRL) von Fortinet, innerhalb kürzester Zeit erkennen und blockieren.

Eine weitere Maßnahme zur Abwehr von Angriffen ist die Verkleinerung der Angriffsfläche. Je weniger Angriffspunkte bzw. potenzielle Bedrohungsvektoren Sie Cyberkriminellen bieten, umso besser. Das heißt, auch eine sorgfältige Zugangskontrolle und der Einsatz von VPNs sind ein wichtiger Aspekt dieser ersten Stufe und Teil der vordersten Verteidigungslinie gegen gezielte Angriffe.

Datenverkehr, der in dieser Phase nicht schnell verarbeitet werden kann, wird an Stufe 2 übergeben...

## Stufe 2 – Erkennen
## Bisher unbekannte Bedrohungen erkennen

Bedrohungen bereits in Stufe 1 zu erkennen, hat offensichtliche Vorteile. Je mehr Bedrohungen in die Kategorie „bekannt" fallen, desto besser. Unbekannte „Zero-Day"-Bedrohungen und ausgeklügelte Angriffe, die sich klassischen Gegenmaßnahmen entziehen, werden ebenfalls täglich eingesetzt, um lukrative Ziele zu infiltrieren. **In Stufe 2 des Frameworks kommen hoch entwickelte Technologien zur Bedrohungserkennung zum Einsatz, die das Verhalten von Netzwerkverkehr, Nutzern und Inhalten genauer überprüfen, um neue Angriffe aufzudecken.**

Mithilfe einer Reihe neuer Ansätze können bisher unbekannte Bedrohungen automatisch erkannt und in verwertbare Bedrohungsdaten umgemünzt werden. Besonders das Sandboxing ist eine Möglichkeit, potenzielle Schadsoftware in eine isolierte Umgebung umzulenken, um ihr gesamtes Verhalten ohne Auswirkungen auf die produktiven Netzwerke direkt zu beobachten. Zusätzlich markiert die Botnet-Erkennung Kommunikationsmuster, die auf Botnet-Aktivitäten hinweisen. Ebenso verfahren Client-Reputationsservices auf Basis von Kontextprofilen mit potenziell infizierten Endgeräten.

Diese Art der Bedrohungserkennung ist zwar äußerst leistungsstark aber auch ressourcenintensiv. Daher ist sie Bedrohungen vorbehalten, die durch effizientere, herkömmliche Methoden nicht identifiziert werden konnten. Aber auch die Erkennung ist nur eine Stufe des ATP-Framework. Die nächste Stufe befasst sich explizit mit diesen neuartigen Bedrohungen.

## Stufe 3 – Abwehr
## Auf potenzielle Vorfälle reagieren

Wenn potenzielle Vorfälle und neue Bedrohungen in Stufe 2 erkannt werden, müssen Unternehmen die Bedrohung umgehend bewerten und den Schaden möglichst gering halten. Nutzer, Geräte und/oder Inhalte müssen mithilfe vorhandener, automatischer und manueller Systeme isoliert werden, um die Sicherheit von Netzwerkressourcen und Unternehmensdaten zu gewährleisten.

Gleichzeitig stoßen erkannte Bedrohungen einen weiteren wichtigen Datenfluss an. Sie melden die gewonnenen Daten an die Forschungs- und Entwicklungsabteilungen zurück. So können taktische Schutzmaßnahmen installiert werden. **Bisher unbekannte Bedrohungen können hier gründlich untersucht werden. Dadurch können Korrekturen vorgenommen werden, die alle Sicherheitsebenen berücksichtigen und für jede einzelne Ebene die richtige Mischung an aktuellem Schutz bereitstellen.** In dieser Phase liegt der Schlüssel zur Bereitstellung einer extrem leistungsfähigen Sicherheitslösung darin, Redundanzen zu eliminieren und Synergien zwischen verschiedenen Sicherheitstechnologien zu schaffen. Das Unbekannte kommt ans Licht.

Selbstverständlich schließt sich der Kreis erst, wenn verwertbare Bedrohungsdaten bei den relevanten Stellen verfügbar sind und global freigegeben werden, damit Stufe 1 bei der Bekämpfung der jetzt bekannten Bedrohung gestärkt wird. So profitiert nicht nur ein Unternehmen von der neuen Waffe gegen die Cyberkriminellen, sondern alle Unternehmen weltweit.

**Effizienz bei der Erkennung und Vorbeugung (durch Kombination der Stufen 1, 2 und 3) ist entscheidend, um eine hohe Netzwerkleistung zu gewährleisten und den Schutz zu optimieren.**

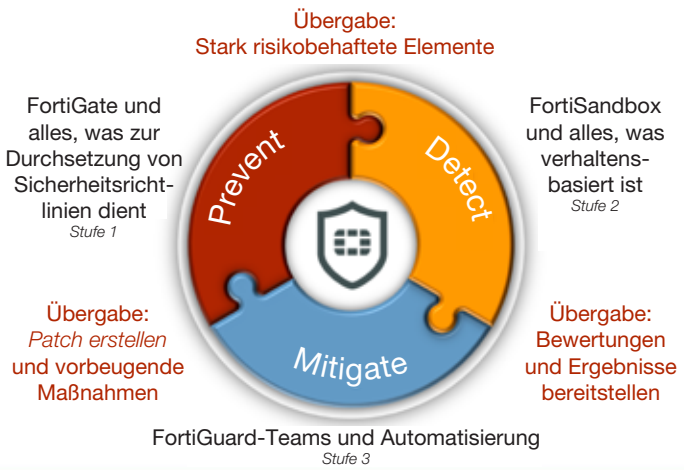



ABBILDUNG 2: DAS FORTINET ADVANCED THREAT PROTECTION-FRAMEWORK

## Informationsfluss – das fehlende Glied

Das vielleicht wichtigste Feature des ATP-Frameworks, welches in den Sicherheitsinfrastrukturen vieler Unternehmen fehlt, ist weniger als spezielle Technologien oder Komponenten die Idee des Informationsflusses. Der Schutz vor komplexen Bedrohungen (Advanced Threat Protection, ATP) besteht aus mehreren Sicherheitstechnologien, Produkten und Forschung. Jede Komponente spielt dabei ihre eigene Rolle. Ihre volle Effektivität erreichen diese Komponenten jedoch erst, wenn sie fortwährend miteinander kommunizieren und Daten untereinander austauschen.

Wie in Abbildung 2 dargestellt, übergibt Stufe 1 (Vorbeugung) hochriskante Elemente an Stufe 2 (Erkennung). Darüber hinaus werden bisher unbekannte Bedrohungen zur weiterführenden Analyse oder Abwehr an Stufe 3 weitergeleitet. Und schließlich werden Bedrohungsdaten und aktualisierte Schutzmaßnahmen von Stufe 3 wieder an die in Stufe 1 und 2 verwendeten Produkte übergeben. **Durch diesen konstanten Kreislauf wird die Abwehr und Erkennung immer raffinierterer Angriffe effizient verbessert.**

## Fortinet – der Bedrohungen immer einen Schritt voraus

### FortiGuard Labs Synergie und Forschung

Eine der größten Stärken von Fortinet ist die Synergie zwischen seiner selbst entwickelten Software, Hochleistungs-Appliances und, am allerwichtigsten, den FortiGuard Labs-Teams zur Erforschung von Bedrohungen. Die Forschungsgruppen von FortiGuard Labs sind die zentrale Schaltstelle für Daten und stellen sicher, dass alle drei Stufen nahtlos ineinandergreifen. Sie untersuchen bisher unbekannte Bedrohungen, entwickeln umfassende Gegenstrategien von Anfang an mit Blick auf ihre Leistungsfähigkeit und effizienten Schutz und stellen Sicherheitsdaten bereit, die die Vorbeugung und Erkennung im Laufe der Zeit kontinuierlich stärken.

**Umfassende Sicherheit**: FortiGuard Labs nutzt Echtzeitdaten zur Bedrohungslandschaft, um umfassende Sicherheits-Updates für die gesamte Palette der Fortinet-Lösungen und Kerntechnologien für einen synergetischen Schutz bereitzustellen.

**Vorausschauende Bedrohungsabwehr:** Sowie neue Bedrohungen auf den Plan treten, aktualisiert FortiGuard Labs Global Operations 365 Tage im Jahr rund um die Uhr in Echtzeit die Sicherheitsdaten in Fortinet-Lösungen und schützt somit umgehend gegen neue und aufkommende Bedrohungen.

**Leistungsstarke Lösungen:** Fortinets Portfolio integrierter Sicherheitsdienstleistungen ist von Anfang an darauf ausgelegt, den Schutz zu maximieren und die Leistung über alle Fortinet-Sicherheitslösungen (physisch und virtuell) hinweg zu optimieren.

Der Datenkreislauf zum Schutz vor komplexen Bedrohungen von Stufe 3 zurück an Stufen 1 und 2 schließt sich, wenn die umfassenden Daten zur Bedrohung, die von FortiGuard Labs entwickelt wurden, über das globale Verteilungsnetzwerk von Fortinet an alle Nutzer unserer Lösungen übermittelt werden. Darüber hinaus macht Fortinet, als Mitglied der Cyber Threat Alliance und ähnlicher Initiativen, Daten zu Bedrohungen einer größeren Gruppe von Forschern zugänglich. Dadurch erweitert es die Reichweite seiner Arbeit und intern im Rahmen dieses Framework gewonnener Bedrohungsdaten über die Grenzen des Unternehmens hinaus.

## Gemeinsam liefern Fortinet-Lösungen einen besseren Schutz

Mehrere einzelne Sicherheitsprodukte, so leistungsstark sie auch sein mögen, können keine optimale Sicherheit garantieren, wenn sie isoliert agieren. Die einzelnen Komponenten der Lösung müssen ineinandergreifen, um optimalen Schutz zu bieten. Fortinet integriert die von FortiGuard Labs gewonnenen Daten in FortiGate Next-Generation Firewalls, sichere FortiMail E-Mail-Gateways, FortiClient Endgerätesicherheit, hoch entwickelte FortiSandbox Bedrohungserkennung und andere Sicherheitsprodukte aus eigener Entwicklung, um das Sicherheitsniveau jedes einzelnen Unternehmens kontinuierlich zu optimieren und zu verbessern.

Weitere Informationen zu Fortinet und unserem Portfolio an Produkten zum Schutz vor komplexen Bedrohungen erhalten Sie unter www.fortinet.com/sandbox.

KONZERNSITZ
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
USA
Tel.: +1 (408) 235 7700
www.fortinet.com/sales

VERTRIEBSBÜRO EMEA
120 rue Albert Caquot
06560, Sophia Antipolis,
Frankreich
Tel.: +33 (0)4 8987 0510

VERTRIEBSBÜRO APAC
300 Beach Road 20-01
The Concourse
Singapur 199555
Tel.: +65 6513 3730

VERTRIEBSBÜRO LATEINAMERIKA
Prol. Paseo de la Reforma 115 Int. 702
Col. Lomas de Santa Fe,
C.P. 01219
Del. Alvaro Obregón
México D.F.
Tel.: +52 (55) 5524 8480