Barracuda

Barracuda Advanced Threat Protection

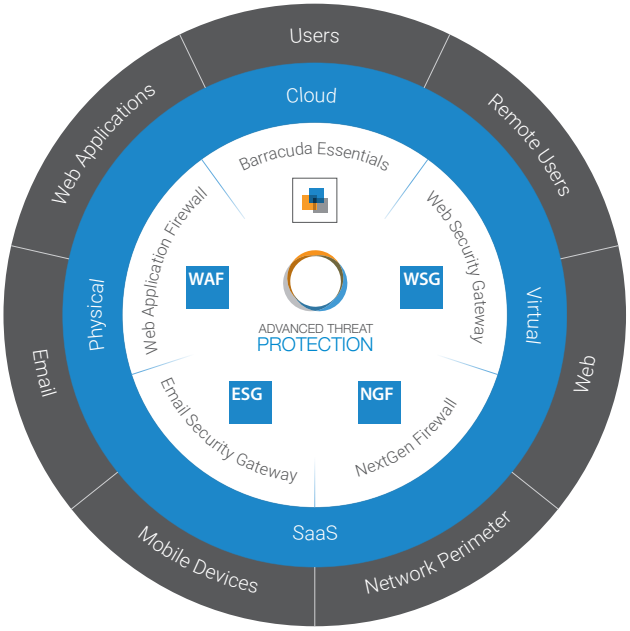
White Paper

Moderne Bedrohungen erfordern einen mehrstufigen Schutz

Aufgrund des polymorphen Designs moderner Cyberbedrohungen erweisen sich herkömmliche signaturbasierte Abwehrmechanismen als unzureichend. Andererseits sind tiefgreifende Abwehrtechniken wie Sandboxing teuer und benötigen zusätzliche Leistung. Umfassender zuverlässiger Schutz vor Angriffen durch Ransomware und APTs (Advanced Persistent Threats) erfordert einen mehrstufigen Ansatz mit zunehmend ausgefeilteren Abwehrtechniken, die ein Gleichgewicht zwischen sorgfältiger Bedrohungserkennung und schnellen Reaktionszeiten schaffen. Darüber hinaus sollte die Architektur Schutz vor ***allen*** Bedrohungen über ***alle*** Bedrohungsvektoren und die unterschiedlichen Angriffsflächen wie physische und virtuelle Infrastrukturen, SaaS-Services und Public Cloud-Plattformen hinweg bieten.

Die 6 häufigsten Internet-Bedrohungsvektoren

Barracuda Advanced Threat Protection (BATP) ist ein Cloud-basierter Dienst, der tiefgreifenden Schutz vor Ransomware, Malware und ausgeklügelten Cyberangriffen bietet. Er besteht aus einer mehrstufigen Erkennung – einschließlich Signatur-, statischer und Verhaltensanalyse bis hin zu umfassendem Sandboxing für eine sorgfältige Erkennung vieler verschiedener polymorpher Angriffe. Dieser Cloud-basierte Dienst ist in alle Sicherheitslösungen von Barracuda integriert und schützt somit Bedrohungsvektoren wie Internet, Benutzer, Netzwerk, E-Mails und Anwendungen über alle Bereitstellungsoberflächen hinweg. BATP ist automatisch mit einem globalen Threat Intelligence-Netzwerk verbunden, das Bedrohungsdaten von unterschiedlichen Quellen weltweit erfasst und dadurch Echtzeit-Schutz für alle Bedrohungsvektoren bietet.



Barracuda Advanced Threat Protection (BATP)

Moderne Bedrohungen umgehen herkömmliche Erkennungstechniken

Das Volumen und die Komplexität moderner Angriffe nehmen rasant zu. Neue Malware-Varianten wie Ransomware sind so gestaltet, dass sie herkömmliche Erkennungstechniken umgehen, und werden häufig durch gezielte Zero-Hour-Angriffe verbreitet.

Führenden Branchenanalysten zufolge können wir bis zum Jahr 2023 pro Quartal mit mehr als 200 neuen Ransomware-Varianten rechnen.[1] Für Angreifer ist dies eine riesige Geschäftsmöglichkeit und für sie ist es erst der Anfang: Allein durch Ransomware erwirtschaften Kriminelle im Jahr 2017 einen Umsatz von über 1 Milliarde US-Dollar. Dies sind zwar großartige Neuigkeiten für Kriminelle, aber alle anderen suchen nach der besten Möglichkeit, sich vor diesen neuen Arten von Angriffen zu schützen.

Bedrohungen wie Ransomware nutzen verschiedene Bedrohungsvektoren

Mehr denn je setzen Kriminelle heute mehrere Bedrohungsvektoren für moderne Malware-Exploits ein, um so höchste Effizienz und Wirksamkeit zu erzielen. Am Beliebtesten ist dabei Einschleusen per E-Mail, insbesondere für Phishing- und Spear Phishing-Angriffe. IDC geht in der Tat von Folgendem aus: „Mehr als 90 % von Ransomware-Infektionen erfolgen bekanntermaßen über schädliche E-Mail-Anhänge."[2]

Benutzer können durch Social Engineering-Methoden, Spoofing, gehackte Websites, manipulierte URLs und andere Techniken zudem zum Download von Schadsoftware verleitet werden. Außerdem reicht eine Gateway-Firewall alleine bei so vielen mobilen Mitarbeitern und immer verteilteren Netzwerken wahrscheinlich nicht aus.

Denken Sie daran: Eine umfassende Sicherheitsstrategie sollte ***alle*** Bedrohungen über ***alle*** Bedrohungsvektoren hinweg abdecken. Darüber hinaus sollte ein effektives Framework zum Bedrohungsschutz unterschiedliche Threat Intelligence-Daten, die über alle Vektoren hinweg erfasst wurden, neu kombinieren.

Sandboxing allein ist nicht effizient

Sandboxing ist die Methode der Wahl für die Erkennung von Zero-Hour-Angriffen. Dabei werden Dateianhänge in einer virtuellen Sandbox geöffnet, die für Angriffe anfällige Endpunkte emuliert.

Sandboxing kann zwar effektiv sein (aufgrund der hohen Verarbeitungsanforderungen), es kann aber beim Einsatz für jeden Anhangtyp auch sehr zeitaufwändig sein. Um große Verzögerungen bei der Content-Bereitstellung zu verhindern, benötigen Unternehmen sehr umfangreiche und kostspielige Sandboxing-Anwendungen. Andernfalls riskieren sie einen Angriff, indem sie die Zustellung von Anhängen vor ihrer vollständigen Untersuchung zulassen. Einige moderne Bedrohungen sind so konzipiert, dass sie Sandboxing-Umgebungen, die rein auf virtuellen Maschinen basieren, erkennen. Um die Sandbox zu umgehen, verschleiern diese Bedrohungen dann die schädliche Aktivitäten und machen die Sandbox somit wirkungslos.

Außerdem werden On-Premise Sandboxing-Lösungen in der Regel am Hauptsitz des Unternehmens bereitgestellt und Remotestandorte bzw. Filialen müssen Anhänge zurück zur Sandbox leiten. Lokale Sandbox-Lösungen skalieren auch nicht mit, wenn Unternehmen weiteren Datenverkehr, Standorte und Benutzer hinzufügen. Weiter verkompliziert wird die Angelegenheit, da Unternehmen ihre Infrastruktur in die Cloud verschieben. Deshalb müssen sie ihren Sicherheitsstatus auf die Cloud ausweiten, was noch mehr Aufwand für die standortbasierte Sandbox mit sich bringt.

[1] *Analyst, Michael Osterman 2016*

[2] *IDC ANALYST CONNECTION: Why SaaS-Based Productivity Tools Require Additional Threat Protection - 2017*

Tiefgreifender Schutz mit Barracuda Advanced Threat Protection

Um diese Herausforderungen anzugehen, hat Barracuda mithilfe seiner jahrzehntelangen Erfahrung mit moderner Malware eine Cloud-basierte Plattform konstruiert, die umfangreichen Schutz vor allen Arten von Malware bietet, ohne dabei Abstriche hinsichtlich Leistung, Abdeckung, Genauigkeit oder Sicherheit zu machen.

Mehrstufiger Schutz

Bei Barracuda Advanced Threat Protection (BATP) handelt es sich um einen integrierten Cloud-basierten Dienst, der aus einer mehrstufigen Bedrohungserkennung in Kombination mit Technologien des maschinellen Lernen besteht. Jede Erkennungsschicht soll zunehmend Bedrohungen mit unterschiedlichen Sicherheits- und Komplexitätsstufen eliminieren. Durch eine Vorfilterung der Bedrohungen in den verschiedenen Schichten kann BATP sehr schnell auf jede Art von Angriff reagieren – und zwar mit nur minimalen Verzögerungen im Datenpfad und ohne Kompromisse bei den Sicherheitsrichtlinien. Darüber hinaus tauschen die verschiedenen Schichten der Bedrohungserkennung die Ergebnisse automatisch miteinander aus. So kann der Dienst insgesamt besser und schneller auf neue Bedrohungen reagieren, da mehr Daten verarbeitet werden. Dadurch wird sichergestellt, dass wiederholt auftretende Bedrohungen schnell in einer niedrigeren Schicht erfasst werden können, während die ressourcenintensiveren Schichten wie Sandboxing explizit für neu entstehende Bedrohungen verfügbar sind.

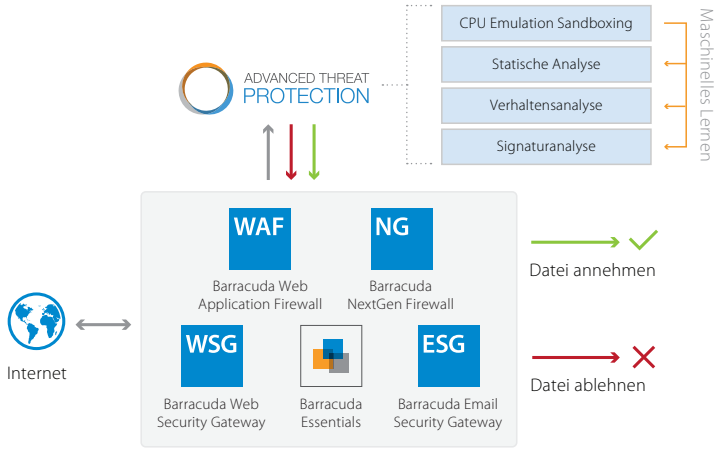
Zu den Sicherheitsschichten gehören folgende:

1. **Erweiterte Bedrohungssignaturen:** Barracuda erfasst Bedrohungssignaturen von über als 250.000 Barracuda-Endpunkten (Appliances und Services im Internet) sowie Informationen von Honeypots, Crawlern, Downloads, Viren, Malware, Spyware, E-Mail-Anhängen, Netzwerk- und Anwendungsdaten. Daraus entsteht eine riesige Threat Intelligence-Signaturdatenbank, die sicherstellt, dass alle neuen Bedrohungen im Barracuda-Wirkungsbereich sofort an alle Sicherheitsprodukte und Subscriber in Echtzeit weitergegeben werden.

2. **Verhaltens- und Heuristikanalyse:** Bei der Verhaltens- und Heuristikanalyse handelt es sich um einen Prozess, bei dem die Ausführung bestimmter Programmierbefehle eines fragwürdigen Codes oder Skripts in einer kontrollierten Umgebung erfolgt. Das daraus resultierende Verhalten wird auf gängige Virenaktivitäten wie Replikation, Dateiüberschreibungen und Verschleierungsversuche der verdächtigen Datei hin analysiert. Zu sonstigen verdächtigen Aktivitäten gehören extrem lange Timer, tagelange Programmierschleifen oder Codes, die versuchen, auf die Registrierung oder Speicherfunktionen zuzugreifen.

3. **Statische Codeanalyse:** Bei der statischen Analyse werden Teile einer ausführbaren Datei ohne tatsächliche Ausführung untersucht. Schadcodeschreiber versuchen, den schädlichen Code zu verschleiern, um Schadcodedetektoren wie Virenschutzsoftware auszuschalten. Die Schicht der statischen Analyse analysiert und deckt fragwürdige Codekonstrukte auf. Diese Schicht stellt eine äußerst effektive und schnelle Methode für die Vorfilterung von Malware vor dem Versand fragwürdiger Dateien an die Sandboxing-Schicht dar.

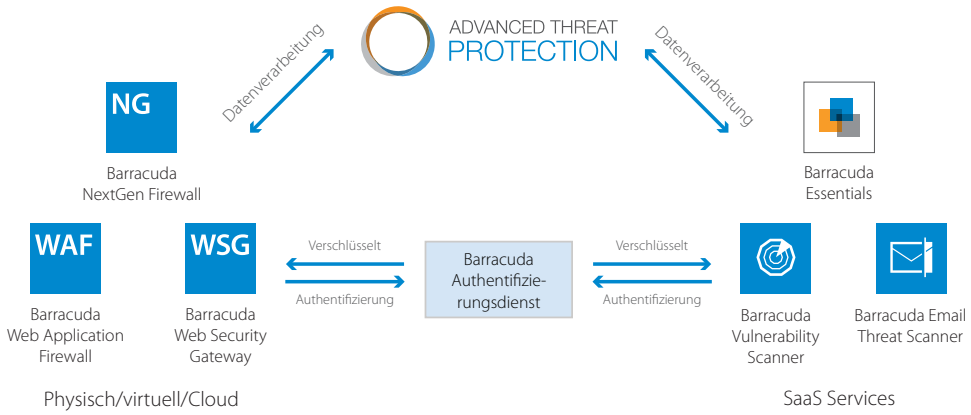
4. **Sandboxing auf CPU-Emulation-Basis:** Die letzte Abwehrmaßnahme ist eine umfassende Sandbox auf CPU-Emulation-Basis, die Anhänge, die von den vorherigen Schichten nicht eindeutig analysiert wurden, ausführlich zerlegt. Mithilfe von CPU-Emulationstechniken kann die Sandbox Bedrohungen erkennen, die so gestaltet sind, dass sie herkömmliche virtualisierungsbasierte Sandboxes umgehen. Außerdem stellt BATP mithilfe der Vorfilterung der Dateien durch die anderen Schichten sicher, dass die Sandbox wirklich komplexe Bedrohungen mit minimalen Verzögerungen verarbeiten kann.



Mehrstufiger Schutz vor Bedrohungen

Verteilter, skalierbarer Cloud-Dienst

BATP schöpft die Vorteile einer global verteilten, äußerst skalierbaren Cloud-Mikrodienstarchitektur voll aus. Diese Architektur kommt im gesamten Portfolio der Barracuda-Sicherheitsprodukte, darunter Netzwerk-, Webanwendungs-, E-Mail- und Websicherheitslösungen, zum Einsatz. Der Dienst kann hinsichtlich Leistung und Abdeckung automatisch erweitert werden, um zunehmendes Datenverkehrsvolumen von Barracuda-Kunden weltweit zu bewältigen. Dabei werden hochsichere Kommunikationskanäle zur Sicherstellung von Datenschutz und Sicherheit bei der Datenübertragung eingesetzt.



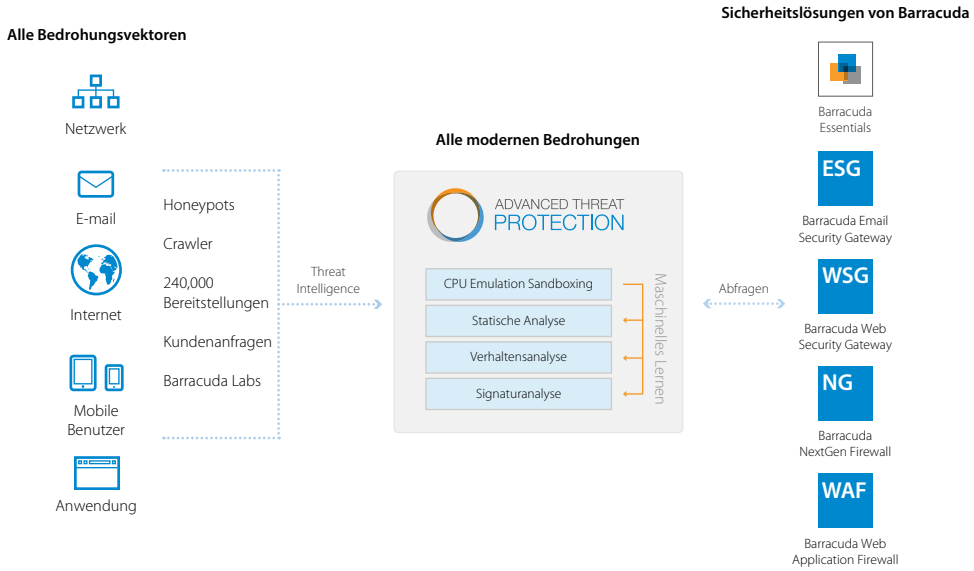
Barracuda BATP-Architektur

Globales Threat Intelligence-Netzwerk

Da unterschiedliche Bedrohungsvektoren beschützt werden müssen, nutzt BATP ein leistungsstarkes Threat Intelligence-Netzwerk, das große Mengen unterschiedlicher Bedrohungsinformationen von mehr als 50 Millionen bereitgestellten Sammelpunkten weltweit untersucht. Die ATP-Infrastruktur von Barracuda setzt eine Hardware-beschleunigte Farm für maschinelles Lernen ein, die diese Daten durch Untersuchung von über 900 Attributen pro Artefakt analysiert.

Alle Barracuda-Produkte, die durch BATP abgedeckt werden, sind Teil dieses sehr vielfältigen Netzwerks, das Threat Intelligence-Daten über alle Bedrohungsvektoren hinweg weitergibt, damit die Subscriber von Echtzeit-Schutz profitieren können. Eine Bedrohung, die zunächst per E-Mail verbreitet wird, wird beispielsweise von BATP erkannt, und der Schutz wird umgehend auf alle anderen über den Dienst abgesicherten Bedrohungsvektoren ausgeweitet. Darüber hinaus werden die Informationen nach Ermittlung der neuen Bedrohung und Erstellung

einer Signatur an Schicht 2 weitergeleitet. Somit kann diese Bedrohung beim nächsten Eindringversuch in Ihr Netzwerk blockiert werden und muss nicht erneut an die Sandbox gesendet werden. Bei einem im Jahr 2016 durchgeführten unabhängigen Test für Advanced Threat Protection-Technologie konnte Barracuda als einziger Anbieter ganz ohne falsch positive und falsch negative Ergebnisse eine 100 %ige Effizienz erzielen.



Threat Intelligence-Infrastruktur von Barracuda

Fazit

Der Aufbau eines umfassenden Sicherheitsansatzes zum Schutz vor den modernen Bedrohungen ist eine multi-dimensionale Aufgabe. Barracuda Advanced Threat Protection in Kombination mit dem Barracuda-Portfolio maßgeschneiderter Sicherheitslösungen bietet Unternehmen eine einfache, wirtschaftliche, skalierbare und leistungsstarke Möglichkeit, diese Herausforderung zu meistern.

Über Barracuda Networks, Inc.

Barracuda (NYSE: CUDA) vereinfacht die IT mit Cloud-Lösungen, mit denen Kunden ihre Netzwerke, Anwendungen und Daten unabhängig von ihrem Speicherort schützen können. Diesen leistungsstarken, benutzerfreundlichen und kostengünstigen Lösungen vertrauen mehr als 150.000 Unternehmen weltweit. Die Implementierung erfolgt in Appliance-, virtuellen Appliance-, Cloud- und Hybrid-Konfigurationen. Mit seinem kundenorientierten Geschäftsmodell konzentriert sich Barracuda auf die Bereitstellung hochwertiger, abonnementbasierter IT-Lösungen, die umfassende Netzwerksicherheit und Datenschutz bieten. Weitere Informationen erhalten Sie unter barracuda.com.

Barracuda

Barracuda Networks Inc
Brunel House, Stephenson Road, Houndmills, Basingstoke, RG21 6XR, United Kingdom

t: +44 (0) 1256 300 100
e: emeainfo@barracuda.com
w: barracuda.com