TRITON® AP-WEB

UMFASSENDER ECHTZEITSCHUTZ VOR FORTGESCHRITTENEN BEDROHUNGEN UND DATENDIEBSTAHL

FORCEPOINT
POWERED BY Raytheon

TRITON® AP-WEB

UMFASSENDER ECHTZEITSCHUTZ VOR FORTGESCHRITTENEN BEDROHUNGEN UND DATENDIEBSTAHL

Ihr Unternehmen und Ihre Daten werden ständig angegriffen. Herkömmliche Sicherheitslösungen bieten keinen ausreichenden Schutz mehr. Im Gegenteil: sie können Sie der Gefahr eines Datenverlusts und damit verbundenen Gerichtsverfahren aussetzen. Damit Ihr Unternehmen in einer expandierenden und zunehmend riskanten digitalen Welt überleben kann, müssen Sie Ihr Netzwerk und Ihre Daten unbedingt vor fortgeschrittenen Bedrohungen, Spear-Phishing und Exploit Kits schützen.

Individuell anpassbar und bei Bedarf erweiterbar

Unternehmen benötigen maßgeschneiderte Lösungen, die genau auf ihre Anforderungen und Budgets eingehen, um sich im Ernstfall vor diesen Bedrohungen schützen zu können. TRITON® AP-WEB bietet Echtzeitschutz vor fortgeschrittenen Bedrohungen und Datendiebstahl. Dank zahlreicher Implementierungsoptionen und Module können Sie das Leistungspaket für Ihren Schutz im Web genau an Ihre individuellen Bedürfnisse anpassen.

Ganz gleich, ob Sie Schutz für Ihre Benutzer vor Ort oder Ihre Mitarbeiter außer Haus benötigen, oder ob Sie nach integrierten Maßnahmen zur Verhinderung von Datendiebstahl oder einer Lösung für mobile Benutzer suchen - TRITON AP-WEB bietet genau die Abdeckung und den Schutz, den Sie benötigen. Nicht mehr, aber auch nicht weniger.

Herausforderungen im Bereich der Web-Sicherheit

Die meisten heutzutage eingesetzten Sicherheitslösungen können fortgeschrittene Bedrohungen während eines laufenden Angriffs nicht unterbinden. TRITON AP-WEB bietet erweiterten Echtzeitschutz vor Bedrohungen.

REDUZIERUNG VON RISIKEN

Komplexe, unkoordinierte Sicherheitslandschaften mit Produkten verschiedener Anbieter erhöhen das Sicherheitsrisiko. TRITON AP-WEB bietet einen vollkommen integrierten Schutz entlang der gesamten “Kill Chain”.

VERHINDERUNG VON DATENDIEBSTAHL

Die meisten eigenständigen DLP-Lösungen sind für eine effektive Implementierung zu komplex. TRITON AP-WEB bietet eine vollständig integrierte, leicht zu implementierende DLP mit branchenführendem Schutz.

SCHUTZ FÜR MOBILE MITARBEITER

Erweitern Sie Ihren Schutz nahtlos vom Büro auf Remote-Nutzer und mobile Mitarbeiter, ohne dabei eine andere Lösung einsetzen zu müssen.

“Wir brauchen eine Lösung, die uns vor den neuesten Bedrohungen im Web schützt, DLP-Funktionen enthält und die Produktivität unserer Mitarbeiter maximiert. Genau das erhalten wir [von Forcepoint] - und zwar sowohl vor Ort, als auch in der Cloud. Es wird einem schnell klar, warum Forcepoint ein Marktführer ist.”

—Ben Schoenecker, IT Security Specialist
AllSouth Federal Credit Union

TRITON AP-WEB

ECHTZEITANALYSEN FÜR SCHUTZ VOR FORTGESCHRITTENEN BEDROHUNGEN

TRITON AP-WEB geht weit über eine Antivirus- Lösung hinaus und nutzt im Rahmen der Forcepoint™ ACE (Advanced Classification Engine) acht Schutzbeurteilungsbereiche in einem kombinierten Scoring-Modell mit vorausschauenden Analysen. Mehrere Echtzeit- Content-Engines analysieren den gesamten Inhalt einer Website, unter anderem auch aktive Skripts, Web-Links, Kontextprofile sowie ausführbare und sonstige Dateien.

EINFACHER ZUGRIFF AUF FORENSISCHE DATEN ÜBER DAS DASHBOARD

Das erweiterte Bedrohungs-Dashboard in TRITON AP-WEB liefert forensische Berichte darüber, wer angegriffen wurde, welche Daten gestohlen werden sollten, wohin sie beinahe übertragen worden wären und wie der Angriff ausgeführt wurde. Die Sicherheitsvorfälle beinhalten, wenn möglich, eine Erfassung von Datendiebstahl. Verteidigungssysteme analysieren die ein- und abgehende Kommunikation.

INTEGRIERTE MASSNAHMEN ZUR VERHINDERUNG VON DATENDIEBSTAHL

Branchenführende (optionale) integrierte Maßnahmen zur Verhinderung von Datenraub erkennen und unterbinden Datendiebstahlsversuche und gewährleisten die Einhaltung behördlicher Vorschriften zur Verhinderung von Datenverlust (Data Loss Prevention, DLP). Zu diesen Funktionen zählen beispielsweise die Erkennung von benutzerdefiniert verschlüsselten Uploads, eines Diebstahls von Passwortdaten und langsamer Datenlecks (Drip-DLP), eine optische Zeichenerkennung (OCR) für Text innerhalb von Grafikdateien sowie die Ermittlung geografischer Standorte.

INTEGRIERTES SANDBOXING

Erfahren Sie, wie Sie Ihr Unternehmen besser schützen können, indem Sie das Verhalten von Malware automatisch anhand des integrierten optionalen Sandbox-Dienstes analysieren.

Module für erhöhten Schutz

WEB-CLOUD- ODER WEB-HYBRID-MODUL	**Erweitern Sie den Web-Schutz und die Durchsetzung von Richtlinien auf Remote-Nutzer.** Implementieren Sie TRITON AP-WEB komplett vor Ort mit unserer skalierbaren Appliance, wählen Sie eine zu 100 % cloudbasierte Implementierung, oder setzen Sie auf ein Hybrid-Netzwerk. Die Wahl liegt ganz bei Ihnen und hängt einzig und allein von Ihren Netzwerkanforderungen ab.
WEB-DLP-MODUL	**Fügen Sie eine leistungsstarke kontextsensitive DLP-Engine hinzu, um sich vor Datendiebstahl von innen zu schützen.** Das Web-DLP-Modul bietet Eindämmungsmaßnahmen gegen Datendiebstahl und ermöglicht mit mehr als 1.700 vordefinierten Richtlinien und Vorlagen die Einhaltung sämtlicher behördlicher Anforderungen. Es umfasst weiterhin branchenführende Schutzmaßnahmen wie z.B. Drip-DLP gegen langsame Datenlecks, optische Zeichenerkennung (OCR) gegen den Diebstahl von Daten in Bilddateien, sowie eine Erkennung individueller Verschlüsselungen, anhand derer sich kriminell verschlüsselte Dateien aufspüren lassen.
WEB-SANDBOX-MODUL	**Integrieren Sie verhaltensorientiertes Sandboxing für eine automatische und manuelle Analyse von Malware-Dateien.** Analysieren Sie verdächtige Dateien in einer virtuellen Umgebung und untersuchen Sie deutlich mehr als nur eine einfache Dateiausführung, um einen höchstmöglichen Schutz vor fortgeschrittener Malware zu bieten. Sobald schädliche Dateien erkannt werden, erhalten Sie automatisch einen detaillierten forensischen Bericht.
TRITON® AP-MOBILE	**Erweitern Sie Richtlinien und Schutz auf iOS- und Android-Nutzer.** Ermöglichen Sie den Einsatz von Mobilgeräten an Ihrem Arbeitsplatz, indem Sie Ihre bestehenden Sicherheitsrichtlinien auf mobile Endgeräte ausweiten, um diese vor fortgeschrittenen Bedrohungen, mobiler Malware, Phishing-Angriffen, Spoofing, etc. zu schützen.
TRITON® APX	**Die von Forcepoint empfohlene Lösung für erweiterten Schutz.** Erweitern Sie Ihren Schutz von TRITON AP-WEB auf TRITON AP-EMAIL, TRITON AP-DATA oder TRITON AP-ENDPOINT, um einen leistungsstarken, integrierten Schutz über sämtliche Angriffskanäle hinweg zu erhalten.

Sonstige Funktionen

SCHUTZ VON REMOTE-BENUTZERN
Verwalten Sie Benutzer in der Unternehmenszentrale, in Zweigniederlassungen oder unterwegs anhand der Web Cloud- oder Hybrid-Module über eine einzige Konsole und eine einzige Richtlinie.

SCHUTZ MOBILER BENUTZER
Erweitern Sie Richtlinien und Sicherheitseinstellungen auf Android- oder iOS-Geräte, indem Sie diese über die TRITON AP-MOBILE-Lösung integrieren.

FLEXIBLE UNTERSUCHUNG VON SSLDATENVERKEHR
Anhand detaillierter Funktionen zur Untersuchung von SSL-Datenverkehr können Sie HTTPSDatenverkehr überwachen, ohne gegen Datenschutzbestimmungen oder behördliche Vorschriften zu verstoßen.

DETAILLIERTE KONTROLLE SOZIALER MEDIEN
Kontrollen für soziale Medien bieten erstklassige Flexibilität. Videokontrollen beschränken oder verhindern das Aufrufen von viralen Clips oder Unterhaltungs- und Überwachungsvideos, erlauben gleichzeitig jedoch Zugriff auf YouTube- Schulungsvideos.

KONTROLLE ÜBER ANWENDUNGEN UND PROTOKOLLE
Der Network Agent bietet eine detaillierte Kontrolle von hunderten Protokollen und Anwendungen, um Ihre Sicherheitsposition zu stärken.

FLEXIBLES BERICHTSWESEN
Vier individuell anpassbare Dashboards sowie mehr als 60 vordefinierte und anpassbare Berichte bieten leicht verständliche geschäftliche und technische Informationen sowie wertvolle Einblicke in Bedrohungsniveaus und mehr.

MEHRERE VERSCHIEDENE IMPLEMENTIERUNGSOPTIONEN
Wählen Sie zwischen einer Vor-Ort-Implementierung über eine Appliance, einer Hybrid- Implementierung zum Schutz von Remote-Nutzern oder einer vollständig cloud-basierten Lösung.

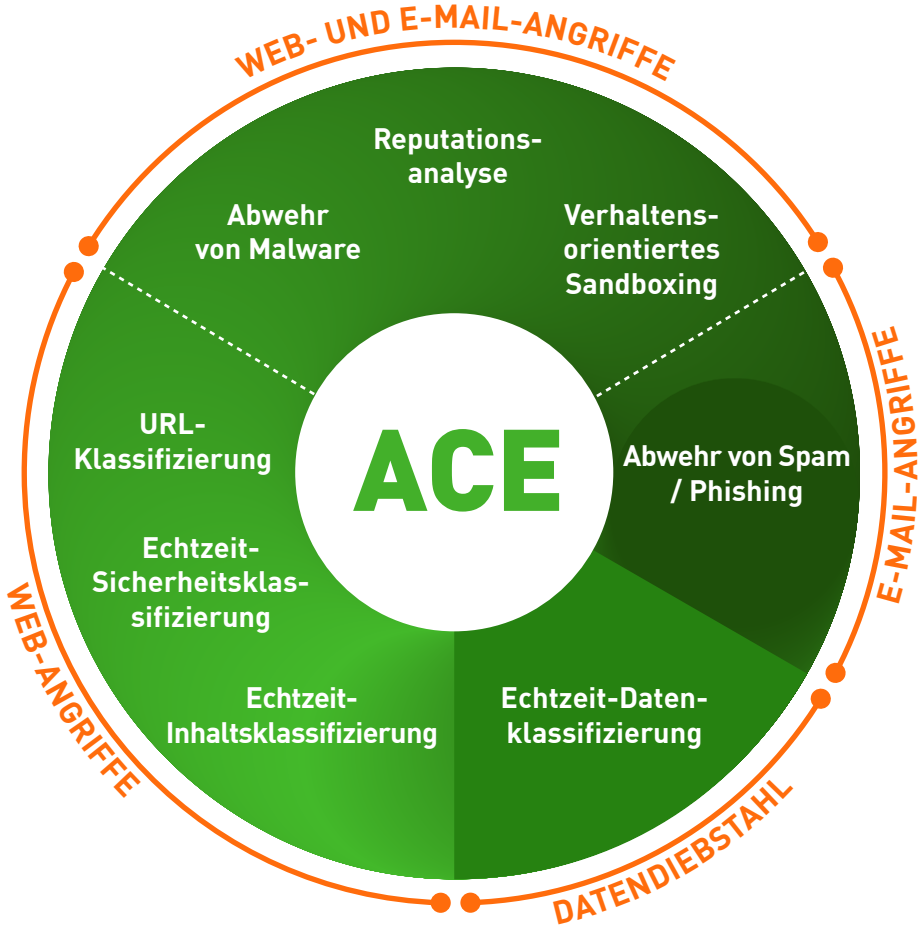
Die treibende Kraft hinter den TRITON Lösungen

ACE (Advanced Classification Engine)

Forcepoint ACE bietet integrierte, kontextbezogene Echtzeit-Verteidigungsmaßnahmen für Web-, E-Mail-, Daten- und mobile Sicherheit. Das System nutzt eine kombinierte Risikobeurteilung sowie vorausschauende Analysen, um eine maximal effektive Sicherheit zu gewährleisten. Zudem ermöglicht es eine Eindämmung potenzieller Schäden durch eine Analyse ein- und abgehenden Datenverkehrs über datensensitive Maßnahmen, die branchenführenden Schutz vor Datendiebstahl bieten. Klassifizierungen für Echtzeitsicherheit sowie Datenund Inhaltsanalysen, die aus vielen Jahren der Forschung und Entwicklung hervorgegangen sind, versetzen ACE in die Lage, jeden Tag mehr Bedrohungen zu erkennen als herkömmliche Antivirus-Programme (der Nachweis hierzu wird täglich unter http://securitylabs.forcepoint.com aktualisiert). ACE ist die primäre Schutzstruktur, auf der alle Forcepoint TRITON-Lösungen aufbauen. Sie wird durch die Forcepoint ThreatSeeker® Intelligence Cloud unterstützt.

INTEGRIERTER SATZ VON SCHUTZBEURTEILUNGSFUNKTIONEN MIT ACHT KERNBEREICHEN.

- 10.000 verfügbare Analyseformen zur Unterstützung tiefgreifender Untersuchungen.
- Vorausschauende Sicherheits-Engines, die immer schon ein paar Schritte voraus sind.
- Durch die Inline- Einbindung werden Bedrohungen nicht nur überwacht, sondern auch **blockiert.**



ThreatSeeker® Intelligence Cloud

Die von den Forcepoint Security Labs™ verwaltete ThreatSeeker Intelligence Cloud liefert die zentralen kollektiven Sicherheitsdaten für alle von Forcepoint angebotenen Sicherheitsprodukte. Sie führt mehr als 900 Millionen Endpunkte zusammen, unter anderem auch Informationen von Facebook, und analysiert gemeinsam mit den Schutzmaßnahmen der Forcepoint ACE bis zu 5 Milliarden Anfragen pro Tag. Durch dieses umfangreiche Wissen über Sicherheitsbedrohungen ist die ThreatSeeker Intelligence Cloud in der Lage, Echtzeit-Sicherheits-Updates zu liefern, die fortgeschrittene Bedrohungen, Malware, Phishing-Angriffe, Köder und Betrugsversuche blockieren und die neuesten Web-Ratings bieten. Im Hinblick auf ihren Umfang und den Einsatz der von der ACE gelieferten Echtzeit-Schutzmaßnahmen zur Analyse kollektiver Inputs ist die ThreatSeeker Intelligence Cloud einzigartig. (Bei einem Upgrade auf Web Security hilft die ThreatSeeker Intelligence Cloud, Ihre Exponierung gegenüber Bedrohungen aus dem Web und Datendiebstahl zu reduzieren.)

TRITON-Architektur

Dank seiner erstklassigen Sicherheit bietet die integrierte Forcepoint TRITONArchitektur Point-of-Click-Schutz mit Inline-Schutzmaßnahmen in Echtzeit über die Forcepoint ACE. Die beispiellosen Echtzeit-Schutzmaßnahmen der ACE werden durch die Forcepoint ThreatSeeker Intelligence Cloud und die Expertise der Analysten der Forcepoint Security Labs unterstützt. Das leistungsstarke Ergebnis ist eine einzige, integrierte Architektur mit einer einzigen, integrierten Benutzeroberfläche und integrierten Sicherheitsdaten.

TRITON APX

TRITON APX bietet Unternehmen, die einen bestmöglichen Schutz vor fortgeschrittenen Bedrohungen entlang der 7-stufigen "Kill Chain" wünschen, zahlreiche wesentliche Vorteile. Diese lassen sich in den folgenden drei Aussagen zusammenfassen:

- **Sicherheit die dazulernt** - Anwendung von adaptiven Sicherheitslösungen für sich schnell verändernde Technologien und Bedrohungsszenarien.
- **Überall geschützt** - Schutz Ihrer Unternehmensdaten gegen Cyberkriminalität in der Cloud, On-Premise und auf mobilen Endgeräten.
- **Sicherheitsintelligenz erhöhen** - Verbesserung des Schutzes durch Bereitstellung vorausschauender und direkt verwertbarer Informationen in allen Phasen einer Bedrohung.

CONTACT
www.forcepoint.com/contact

[BROCHURE_TRITON_AP_WEB_DE] 400002DE.011416

FORCEPOINT
POWERED BY Raytheon