TRITON® AP-ENDPOINT

STOPPEN SIE FORTGESCHRITTENE BEDROHUNGEN UND SCHÜTZEN SIE DIE VERTRAULICHEN DATEN MOBILER NUTZER

FORCEPOINT
POWERED BY Raytheon

TRITON® AP-ENDPOINT

STOPPEN SIE FORTGESCHRITTENE BEDROHUNGEN UND SCHÜTZEN SIE DIE VERTRAULICHEN DATEN MOBILER NUTZER

Von einer Schädigung des Rufs bis hin zu behördlich auferlegten Bußgeldern und Strafen – eine Datenpanne kann verheerende Auswirkungen haben. Außerhalb des Unternehmens tätige Mitarbeiter vor Bedrohungen und Datendiebstahl zu schützen stellt für die IT nach wie vor eine erhebliche Herausforderung dar. Mit einer einfach zu verwendenden Lösung schützt TRITON® AP-ENDPOINT mobile Nutzer innerhalb und außerhalb des Netzwerks vor fortgeschrittenen Bedrohungen und Datendiebstahl. Ausgereifte Technologien helfen Ihnen, vertrauliche Daten schnell zu identifizieren und zu schützen und sich prozessfähige Erkenntnisse zu Angriffen auf Endpoint-Geräte innerhalb und außerhalb des Netzwerks zu verschaffen. Forcepoint™ TRITON AP-ENDPOINT schützt Ihre Daten, so dass Ihre mobilen Mitarbeiter tätig werden können, wo und wann auch immer es erforderlich ist.

Forcepoint ermöglicht Sicherheit am Endpoint

- Sichern Sie vertrauliche Daten auf Mac OS X- oder Microsoft-Endpoint-Geräten außerhalb Ihres Netzwerks ab.
- Schützen Sie Endpoints außerhalb des Netzwerks vor fortgeschrittenen Bedrohungen.
- Sichern Sie sich an allen Endpoints gegen Bedrohungen von außen ab und verhindern Sie, dass Daten über SSL-Datenverkehr das Unternehmen verlassen.
- Ermöglichen Sie einen sicheren Austausch von Daten mit Partnern durch Verwendung der integrierten, dateibasierten Datenverschlüsselung.
- Führen Sie sicher und vertrauensvoll Cloud-Dienste wie Microsoft Office 365 und Box ein.
- Weisen Sie Prüfern und Führungskräften Ihre icherheitskontrollen problemlos nach, um Compliance-Anforderungen und behördliche Vorschriften zu erfüllen.

Die wichtigsten Funktionen von TRITON AP-ENDPOINT

- Digitale Fingerabdrücke (inkl. partielles Fingerprinting) werden für Endpoint-Geräte innerhalb und außerhalb des Netzwerks unterstützt.
- Unterstützung für Endpoints mit sowohl Mac OS X als auch Microsoft Windows.
- Schutz vertraulicher Daten, die auf USB-Geräte, Wechseldatenträger, Drucker oder Cloud-Dienste wie Microsoft Office 365 oder Box übertragen werden sollen.
- Richtlinienbasierte Dateiverschlüsselung zum Schutz von auf Wechseldatenträgern gespeicherten vertraulichen Daten.
- Erkennung von geistigem Eigentum und Kundendaten, die über E-Mail-Clients oder Webmail verschickt werden sollen.
- Drip DLP berücksichtigt kumulative Datenübertragungsaktivitäten über längere Zeiträume hinweg, um ein langsames Ausschleusen geringer Datenmengen aufzuspüren.
- Effiziente Untersuchung von HTTPS-Datenverkehr mit der Flexibilität zu entscheiden, welche Art von SSL-Datenverkehr inspiziert werden soll.
- Identifizierung von Web-Aktivitäten fortgeschrittener Bedrohungen entlang der gesamten „Kill Chain“ auf Endpoints, die außerhalb der Schutzvorrichtungen des Netzwerks genutzt werden.

"Wir nutzen einen Forcepoint Remote-Agenten, der so vorkonfiguriert ist, dass er Forcepoint im Push-Verfahren auf den Laptops installiert. Wenn ein Laptop unser Netzwerk verlässt, nimmt es wieder die Verbindung zum Netzwerk auf. Dieses wendet dann unsere Internet-Zugangsrichtlinien auf den Laptop an. So gelten für sämtliche Laptops stets dieselben Richtlinien wie für unser internes Netzwerk."

— Jeff Howells, Network Architect, Wollongong City Council

Funktionsumfang von TRITON AP-ENDPOINT

ERMÖGLICHEN SIE ES NUTZERN, AUCH AUSSERHALB DES NETZWERKS AKTIV ZU SEIN

Mitarbeiter benötigen häufig Zugriff auf vertrauliche Informationen, selbst wenn sie sich gerade außerhalb des Büros befinden. TRITON AP-ENDPOINT bietet Kontrollen für Mac OS X- und Microsoft Windows-Laptops, so dass Sie Datendiebstahl verhindern können, ohne diese Nutzer aus Sicherheitsgründen einschränken zu müssen. Finden und sichern Sie kritische Daten auf Endpoints - ganz gleich, ob sich der Benutzer innerhalb oder außerhalb Ihres Unternehmensnetzwerks befindet. Unter anderem erhalten Sie auch leistungsstarke Fingerprinting- Funktionen, die in vielen anderen Endpoint-Data-Loss-Prevention (DLP)-Lösungen fehlen.

WEB-SICHERHEIT FOLGT IHREN MOBILEN MITARBEITERN

Die Risiken webbasierter Angriffe, einschließlich fortgeschrittener Bedrohungen, sind für Benutzer, die außerhalb Ihres Unternehmensnetzwerks tätig sind, noch größer. TRITON AP-ENDPOINT erweitert Web-Sicherheit auf mobile Benutzer, so dass diese geschützt auf webbasierte Ressourcen zugreifen können. Neben einer reinen URL-Filterung können Angriffsaktivitäten entlang der gesamten „Kill Chain" identifiziert und blockiert werden, ohne dass hierfür ein Proxy erforderlich wäre. TRITON AP-ENDPOINT verschafft sich einen Einblick in den SSL-Datenverkehr, um den Web-Kanal für Ihre Roaming-Benutzer abzusichern, selbst wenn diese Cloud-E-Mail-Dienste, soziale Medien oder andere Services mit sicheren Verbindungen nutzen.

SETZEN SIE SICHER UND VERTRAUENSVOLL AUF INNOVATION

Wenn Sie die Bedürfnisse Ihrer Kunden befriedigen und konkurrenzfähig bleiben möchten, müssen Sie auch innovativ bleiben und Ihren Mitarbeitern ermöglichen, neue Lösungen und Technologien einzusetzen. TRITON AP-ENDPOINT hilft Ihnen dabei, neue Cloud-Dienste wie Microsoft Office 365 oder Box sicher einzuführen. Sie werden nicht nur im Web vor Bedrohungen geschützt, sondern behalten auch die Kontrolle über Ihre vertraulichen Daten. Benutzer erhalten DLP sowie umfassenden Schutz vor fortgeschrittenen Bedrohungen - ganz gleich, wann und wo sie arbeiten, ob sie Microsoft Windows oder Mac OS X verwenden oder sich inner- oder außerhalb des Netzwerks befinden. Kontrollieren Sie die Verwendung von Wechseldatenträgern wie z.B. USB-Laufwerken, anhand von Optionen zur Blockierung oder Verschlüsselung von Daten, die bestimmten Richtlinien entsprechen. Überwachen Sie den Datenfluss in Richtung Cloud-Dienste, ohne sich dabei hinsichtlich der Innovationen, die Ihr Unternehmen für sein Wachstum braucht, einschränken zu müssen.

PROBLEMLOSE VERWALTUNG MIT IHREN JETZIGEN IT-MITARBEITERN

Das IT-Personalwesen birgt zahlreiche Herausforderungen: die Mitarbeiterzahlen sind oft beschränkt, und die Suche nach geeigneten, qualifizierten Sicherheitsfachkräften ist alles andere als einfach. Die TRITON-Architektur vereint die Verwaltung von Web-, E-Mail-, Daten- und Endpoint-Sicherheit und umfasst Richtlinien, die sich leicht definieren und dort implementieren lassen, wo sie benötigt werden. Reagieren Sie schnell über mehrere Kanäle hinweg auf neue Bedrohungen, und sichern Sie Ihre mobilen Mitarbeiter ab. Schützen Sie Ihr vertrauliches geistiges Eigentum und Ihre personenbezogenen Daten und erfüllen Sie problemlos sämtliche Compliance-Anforderungen und behördlichen Vorschriften mit einer umfangreichen Bibliothek vordefinierter Richtlinien.

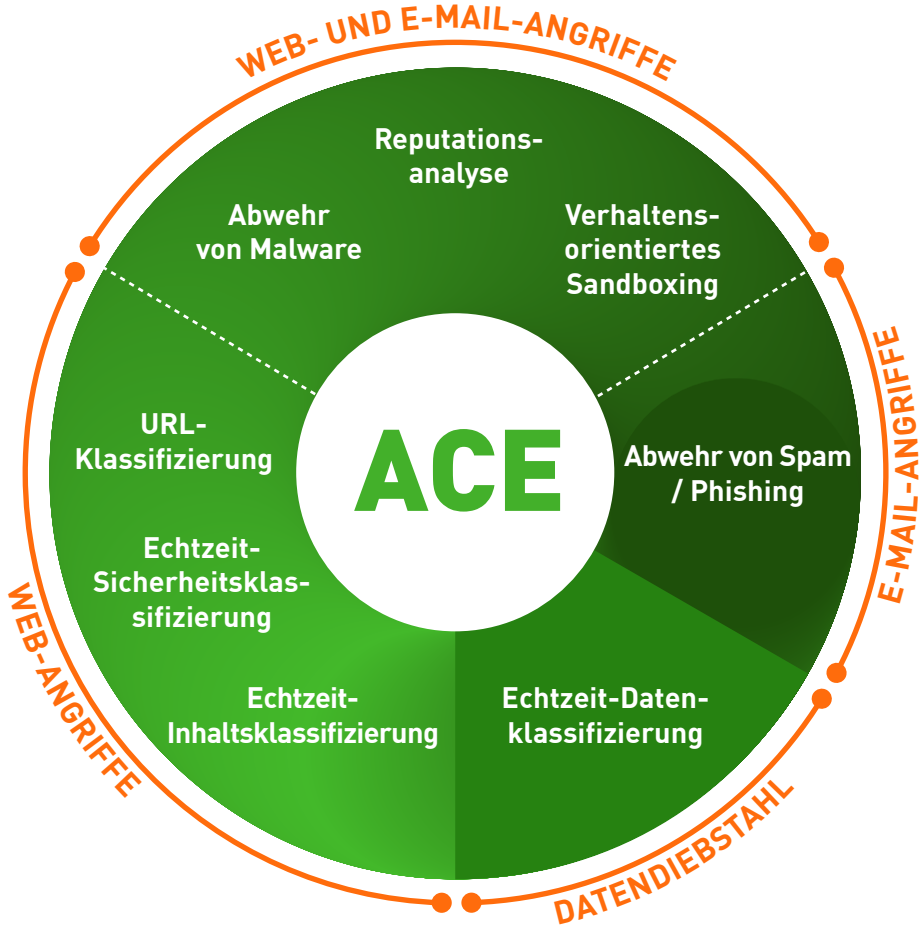
Die treibende Kraft hinter den TRITON Lösungen

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 TRITON-Architektur 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_ENDPOINT_DE.A4] 400005DE.011416

FORCEPOINT
POWERED BY Raytheon