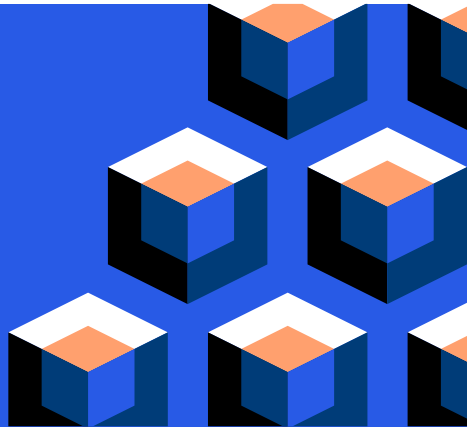
imperva

DATENBLATT

Imperva Application Security

Flexible Sicherheit, wann und wie Sie sie benötigen.



Einführung

Anwendungen sind für Organisationen, die ein rasches Wachstum vorantreiben wollen, missionskritisch geworden. Eine zunehmende Abhängigkeit vom Web hat dafür gesorgt, dass Anwendungen für Unternehmen, die exponentielles Wachstum anstreben, ein kritischer Teil des Wegs geworden sind. Für viele Unternehmen, wie zum Beispiel solche, die ausschließlich online aktiv sind, sind Anwendungen zu ihrem primären Geschäftsmodell geworden, was ihnen hilft, Kunden auf der ganzen Welt zu erreichen und ein schnelles finanzielles Wachstum zu erzielen. Unternehmen wissen, dass Endverbraucher eine qualitativ hochwertige Erfahrung beim Zugriff auf Anwendungen verlangen, unabhängig davon, wo sie sich auf der Welt befinden. Die Erfahrung des Endverbrauchers muss sicher, konsistent und nahtlos sein, was das Risiko einer Störung des Einnahmenmodells unzähliger Organisationen auf der ganzen Welt verringert, die auf ihre Anwendungen angewiesen sind, um ihr Geschäft zu betreiben. Imperva Application Security befähigt Unternehmen, ihre Anwendungen zu schützen und gleichzeitig sicherzustellen, dass ihre Kunden ein optimales Benutzererlebnis haben. Durch Imperva können Unternehmen nicht nur unvorhergesehene Störungen ihres Geschäfts verhindern, sondern auch Risiken mildern.

Auf kritische Erkenntnisse reagieren

Mit der komplexen und sich ständig verändernden Bedrohungslandschaft von heute ist es wichtiger denn je, einen Einblick in die Daten und Anwendungen zu erlangen. Eine Explosion von Sicherheitswarnungen kann Organisationen davon abhalten, die kritischen Angriffe zu entdecken, die tatsächlich eine unmittelbare Bedrohung darstellen, die oft zu einer Verletzung der Datensicherheit durch ein Anwendungs-Exploit führen kann. Viele Sicherheitsteams, die nicht in der Lage sind, mit der Lawine von Sicherheitswarnungen fertig zu werden, erliegen oft einer „Alarmmüdigkeit“, die dazu führt, kritische Vorfälle zu ignorieren, die tatsächlich von Bedeutung sind. Die Anwendungssicherheit „Attack Analytics“ von Imperva macht es Unternehmen möglich, kritische Sicherheitswarnungen herauszufiltern, die von Sicherheitsteams schnell untersucht und bearbeitet werden können. Mithilfe von künstlicher Intelligenz kann Attack Analytics wirklich wichtige Sicherheitseinsichten aus Millionen von Sicherheitswarnungen herausfiltern, auf die Sie dann reagieren können. Dies kann Organisationen helfen, das Ausmaß des Cyberrisikos zu erkennen, dem sie in ihrer gesamten Umgebung tatsächlich ausgesetzt sind.

WICHTIGE MERKMALE UND VORTEILE

- Entdecken und reagieren Sie auf wichtige kritische Sicherheitsvorfälle, indem Sie künstliche Intelligenz und maschinelles Lernen nutzen.
- Sichern Sie sich gegen OWASP-Top 10-Bedrohungen sowohl in der Cloud als auch in den WAF-Einsätzen vor Ort.
- Schwächen Sie potenziell verheerende DDoS-Attacken ab, bevor sie Ihre Anwendung erreichen.
- Beschleunigen Sie die Bereitstellung von Webinhalten und gewährleisten Sie eine optimale Benutzererfahrung.
- Unterstützen Sie schnellere Release-Zyklen für die Anwendung und stellen Sie gleichzeitig den Schutz der Anwendung während der Laufzeit sicher.
- Sichern Sie sich eine hohe Verfügbarkeit Ihrer Anwendung trotz Webausfällen wegen Überlastung.

CISOs können Berichte auf hoher Ebene einsehen, die die Länder angeben, in denen Angriffskampagnen gegen ihre Organisation gestartet wurden, welche Art von Sicherheitsangriffen und Malware-Tools während jeder Angriffskampagnen eingesetzt wurden.

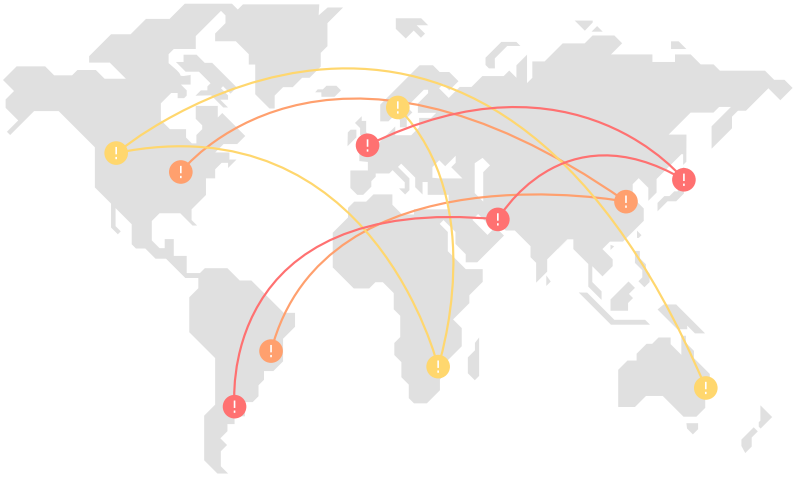


Bild 1: Kritische Einblicke in die Angriffe, die wichtig sind

Sichern Sie Ihre kritischen Anwendungen

Bei Imperva setzen wir ein Sicherheitsmodell ein, das einen geschichteten Ansatz zur Durchsetzung der Sicherheit von der Anwendung bis zum Endverbraucher bietet. Wir können den kompletten Schutz innerhalb der Anwendung, in der Cloud oder in Bereitstellungen vor Ort gewährleisten. Auf Anwendungsebene können wir Anwendungen direkt durch Imperva Autonomous Application Protection (AAP) schützen, eine Leichtgewicht-Komponente, die während des Software-Entwicklungszyklus integriert wird. AAP erlernt das einzigartige Verhalten der Anwendung und stärkt das Sicherheitsmodell um inhärente Sicherheitslücken. Dies verringert den Druck auf die Entwicklungsteams, kritische Schwachstellen sofort beheben zu müssen, bevor sie eine Anwendung für die Produktion freigeben, während gleichzeitig ein sofortiger und effektiver Schutz vor bösartigen Exploits gewährleistet wird. Imperva bietet auch Web Application Firewalls (Webanwendungsfirewall, WAF) an, die gegen alle OWASP Top 10-Bedrohungen wie SQL-Injektion, standortübergreifendes Scripting, illegaler Ressourcenzugriff und Remote File Inclusion schützen. Für einen breiteren Schutz können Kunden Imperva Cloud WAF einsetzen, die die Kontrolle und Durchsetzung des Nutzerverkehrs über das globale Netzwerk von Imperva von PoPs ermöglicht. Bei Webverkehr, der für Kunden-Websites bestimmt ist, kann schnell zwischen legitimem und bösartigem Datenverkehr unterschieden werden. Böswilliger Datenverkehr wird bei der nächstgelegenen Imperva PoP schnell behoben, sodass nur legitimer Datenverkehr sicher zu einer Kundenwebsite fließt. Für Kunden mit Vor-Ort-Bereitstellungen bietet Imperva Web Application Firewall (WAF)-Gateways an, die auf Kundenseiten eingesetzt werden können und einen sofortigen Schutz bieten, indem sie das automatische Lernen der Anwendung mit aktuellen Schutzrichtlinien und Signaturen vom Imperva Security Research-Team kombinieren.

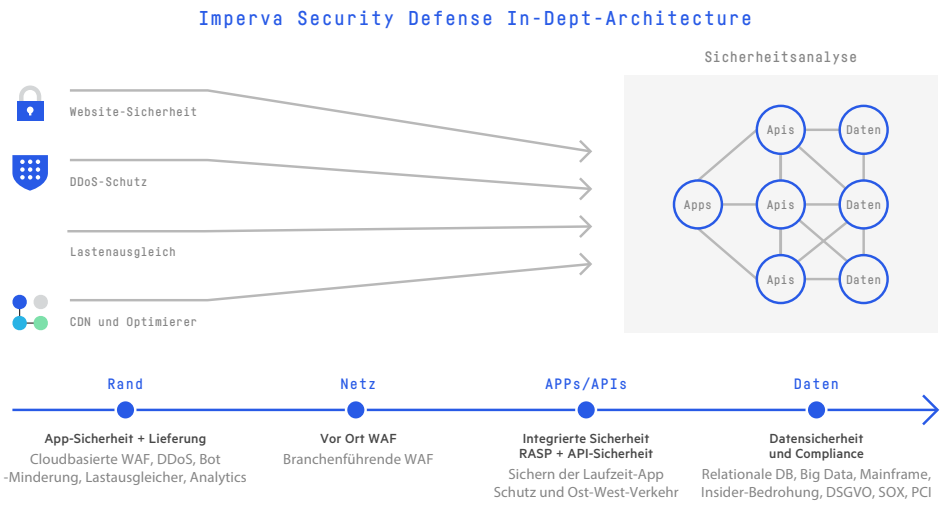


Bild 2: Imperva Security Defense in Depth Architecture

Vermeiden Sie Störungen Ihres Geschäfts

Cyberkriminelle führen oft Störungskampagnen gegen hochkarätige Websites wie Banken, Privatkunden oder politische Organisationen. Sie werden oft von Rache, Erpressung oder politischem Aktivismus getrieben und nutzen riesige Botnetz-Netzwerke für verheerende Distributed Denial of Service (DDoS)-Attacken. Organisationen ohne angemessenen Schutz sind oft DDoS-Angriffen ausgesetzt, die Nutzer vom Zugriff auf ihre Websites vollständig ausschließen oder die Website verlangsamen können. Diese ständigen Angriffskampagnen können die Nutzer davon abbringen, auf eine Website zurückzukehren, womit das Ziel des Angreifers erfüllt wäre. Imperva Application Security bietet einen leistungsstarken DDoS-Schutz, der darauf abzielt, Angriffe direkt zu eliminieren, bevor sie überhaupt auf den Weg gebracht werden, indem der bösartige DDoS-Verkehr über das globalweite Netzwerk von Imperva direkt gestoppt wird, lange bevor der bösartige Datenverkehr die Kundenwebsite erreicht. Imperva bietet zwei DDoS-Schutzlösungen an. DDoS Protection for Websites, ein Always-on-Service, der Schutz für jede Art von DDoS-Angriff jeder Größe, Dauer oder Raffinesse mit nahezu null Latenz bietet – unterstützt durch eine Dienstleistungsvereinbarung. Dieser Dienst kann in wenigen Minuten über einen einfachen DNS-Wechsel aktiviert werden. Es sind keine Hardware- oder Software-Änderungen vor Ort erforderlich und auch keine Änderungen an Ihrem Hosting-Anbieter oder Ihrer Anwendung. Imperva bietet auch DDoS-Schutz für Netzwerke, einen Always-on- oder On-Demand-Service, der IT-Assets vor DDoS-Attacken schützen kann. Der DDoS-Verkehr, der für Kundennetzwerke bestimmt ist, wird sofort über das globale Imperva-Netzwerk abgeschwächt, damit es zu keinen Störungen beim Datenverkehr des Unternehmens kommt.

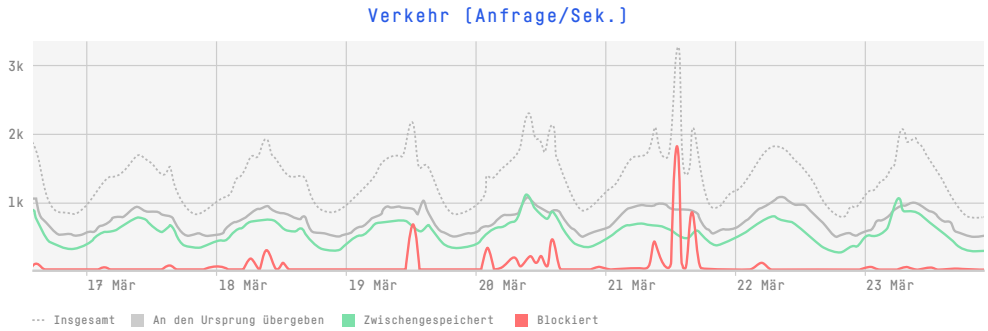


Bild 3: Kunden-DDoS-Angriff wird von Imperva abgeschwächt

Gewährleistung einer nahtlosen Benutzererfahrung

Nutzer verlangen eine konsistente und nahtlose Erfahrung beim Besuch von Websites. Häufige Erfahrungen mit langsamen Website-Downloads können dazu beitragen, dass Nutzer auf andere Websites wechseln. Organisationen, die darauf angewiesen sind, dass Nutzer auf ihre Websites zurückkehren, müssen ihre Website-Infrastruktur so gestalten, dass Webinhalte schnell geliefert werden können, um die Nutzernachfrage jederzeit von überall auf der Welt erfüllen zu können und so eine optimale Benutzererfahrung zu gewährleisten. Das Content Delivery Network (CDN) von Imperva ermöglicht es Unternehmen, die Bereitstellung von Inhalten von Websites, die ihren Endnutzern am nächsten sind, zu optimieren. Mit einem globalen Netzwerk von CDN-Standorten ist Imperva in der Lage, alle Anforderungen an die Bereitstellung von Inhalten zu erfüllen, um sicherzustellen, dass Nutzer schnell und konsistent auf Webinhalte zugreifen können. Unser anwendungssensibles CDN erstellt auf dynamische Weise ein Profil der Website und identifiziert alle zwischenspeicherbaren Inhalte (dynamisch und statisch). Darüber hinaus sorgen die dynamische Profilerstellung und Frequenzanalyse dafür, dass die Ressourcen mit dem häufigsten Zugriff direkt aus dem Speicher erkannt und bedient werden. Dies ermöglicht es Kunden, ihre Website zu optimieren, die Leistung der Website zu verbessern und gleichzeitig die Bandbreitenkosten zu senken.

Um Unternehmen weiter bei der Bereitstellung skalierbarer Anwendungen zu unterstützen, bietet der Imperva-Load-Balancer skalierbaren Lastausgleich an, was teure Geräte durch eine unternehmensgerechte cloudbasierte Lösung ersetzt. Kunden, die verlangen und erwarten, dass ihre Anwendungen auf eine hohe Verfügbarkeit und Redundanz im Falle eines Ausfalls eines Webservers ausgelegt werden, können sicherstellen, dass es keine Auswirkungen auf den Service für ihre Nutzer gibt. Basierend auf einem globalen CDN, unterstützt der Load Balancer von Imperva ein einzelnes Rechenzentrum mit mehreren Servern, Standort-Ausfallsicherung (für DR-Szenarien) und Global Server Load Balancing (GSLB). Die Echtzeit-Zustandsüberwachung und -notifikationen sorgen dafür, dass der Datenverkehr immer auf einen brauchbaren Webserver geleitet wird.

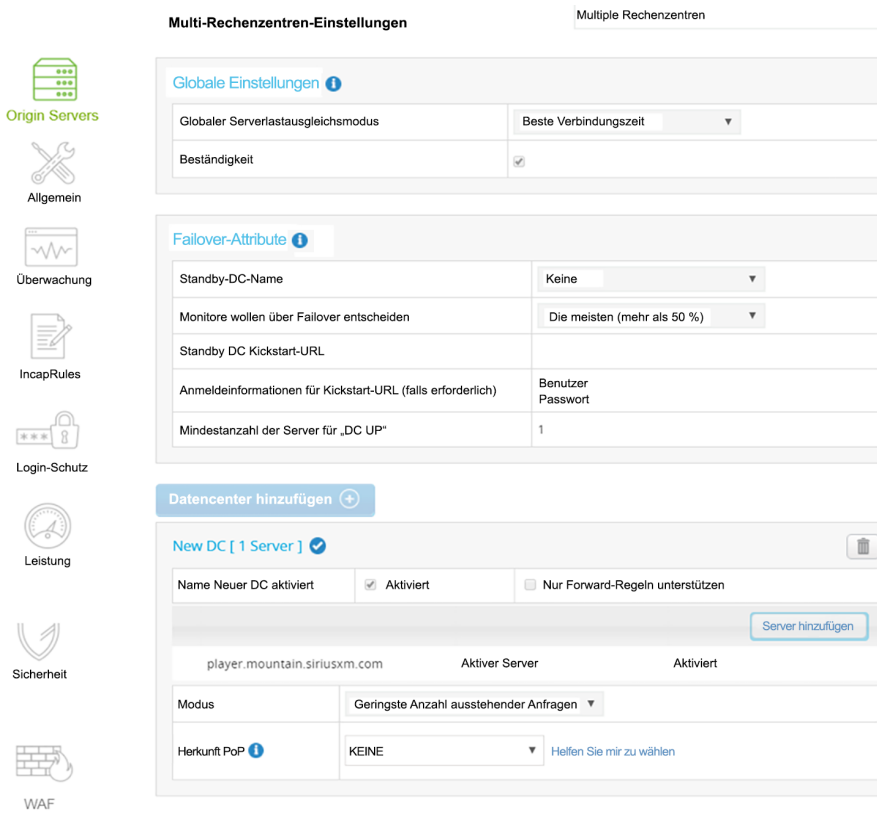


Bild 4: Anwendungsbereitstellung von Imperva: Verbesserung der Websiteleistung

Bietet vollständigen Investitionsschutz

FlexProtect ist ein flexibler Ansatz zur Sicherung von Anwendungen. Eine Einzellizenz bietet Ihnen die Möglichkeit, Imperva Application Security bereitzustellen, wie und wann immer sie es benötigen. FlexProtect for Anwendungen ermöglicht es Kunden, ihre Sicherheit ohne Rücksicht auf Infrastruktur anzupassen. Sie sind geschützt, unabhängig von der Anzahl, dem Ort oder der Art der verwendeten Geräte oder Dienste. FlexProtect hilft Ihnen, Apps überall dort zu schützen, wo Sie sie einsetzen – in der Cloud, am Arbeitsplatz oder als Hybridmodell.

WICHTIGE MERKMALE UND VORTEILE

- Reduzieren Sie die Kosten der Unsicherheit beim Umzug in die Cloud
- Prognostizieren Sie Kosten, auch wenn sich Ihre Cloud- und Vor-Ort-Infrastruktur im Laufe der Zeit verändert
- Skalierbar, um sich dem Wachstum Ihres Geschäfts anzupassen

Imperva ist ein von Analysten anerkannter führender Anbieter von Cybersicherheit, der sich für den Kampf zur Sicherung von Daten und Anwendungen einsetzt, wo immer sie sich befinden.

+ 1 (866) 926-4678
imperva.com

imperva