Illumio für DevSecOps

Zero-Trust-Security automatisch in Software integrieren und Policies für die Mikrosegmentierung exakt an Rollen, Anwendungen, Umgebungen und Standorte anpassen.

DevOps darf die Sicherheit nicht vernachlässigen

Agile DevOps-Verfahren beschleunigen die Softwareentwicklung und -bereitstellung, berücksichtigen die Sicherheit aber oft nicht genug. Anwendungen werden schnell gebaut und releast, aber in einer echten Umgebung bereitgestellt, können sie angreifbar sein.

Die Entwicklungszyklen werden immer kürzer, und die Sicherheit muss Schritt halten. DevOps-Teams brauchen eine Methodik, um in jeder Phase – Plan, Build, Test, Deploy und Monitor – Risiken zu berücksichtigen, ohne die Prozesse auszubremsen.

Dass Entwickler oder operative Teams jetzt Security-Experten werden, ist allerdings unrealistisch. Die Sicherheit muss einfach mit dem DevOps-Tempo und dem nötigen Automatisierungsgrad mithalten.

Das bedeutet: Es muss einfacher werden, Software zu entwickeln und bereitzustellen, in die bereits starke, einheitliche Sicherheitsmaßnahmen integriert sind – auch, wenn es schnell gehen muss, und unabhängig davon, wo die Anwendung läuft.

Mit Illumio ganz einfach Zero Trust in DevOps integrieren

Damit Organisationen ihre Software und Netzwerke zuverlässig schützen können, macht Illumio es ihnen leicht, Segmentierungs-Policies festzulegen und schnell durchzusetzen.

Zero Trust bedeutet: Benutzern, Prozessen und Systemen wird grundsätzlich nicht vertraut, es sei denn, sie sind in eine Sicherheitsregel hinterlegt. Illumio blockt den gesamten Netzwerk-Traffic über Ports und Adressen – außer den, der für bestimmte Anwendungen und Personen nötig ist. Das hindert Malware und Hacker daran, sich in Ihrem Netzwerk und den Produktionsumgebungen weiter auszubreiten, und erstickt Cyberangriffe damit im Keim.

Security, die die DevOps-Lücke schließt

Illumio schließt die Security-Lücke von DevOps mit integriertem Schutz vor Ransomware und anderen Bedrohungen.

Zero-Trust-Sicherheit für agile Prozesse
Mit Illumio können DevOps-Teams und Security-Analysten präzise Policies definieren und durchsetzen, ohne Tausende Firewall-Regeln programmieren zu müssen. Illumio übersetzt allgemeine Policies automatisch in detaillierte Regeln.

Security so flexibel, wie DevSecOps es erfordert
Mit Illumio ist es einfach, Segmentierungs-Policies für Rollen, Anwendungen, Umgebungen und Standorte zu definieren und durchzusetzen, sodass DevSecOps-Teams ihre Policies nach Bedarf anpassen können.

Security, die laufende Angriffe stoppt
Mit Illumio können Ransomware und andere Angriffe auf kritische Anwendungen und Daten sofort isoliert werden. Ihre Teams sehen den Datenverkehr in Echtzeit und können infizierte Systeme sofort vom Rest des Netzwerks trennen.

Mit Illumio können DevOps- und Security-Teams gemeinsam festlegen, welchen Traffic die Software unterstützen soll. Jeglicher anderer Datenverkehr wird geblockt.

Anwendungen, die mit DevSecOps-Prozessen entwickelt werden, setzen diese Zero-Trust-Segmentierungsregeln automatisch um und schützen damit vor den unterschiedlichsten Angriffen.

Illumio bietet die Transparenz und Automatisierung, die DevSecOps-Teams brauchen

Durch die automatische Berechnung von Firewall-Regeln anhand allgemeiner Policies macht Illumio es leicht, Security in Software und Services direkt mit einzubauen.

Illumio liefert ein Echtzeit-Mapping des Anwendungs-Traffic, und Sie können genau feststellen, welcher Datenverkehr auf Ihren Kommunikationswegen zugelassen werden sollte.

Nachdem Entwickler, Operations Engineers und Security-Analysten ermittelt haben, welcher Traffic für eine Anwendung oder einen Service erlaubt werden soll, können sie mit Illumio schnell Zero-Trust-Policies definieren, die allen restlichen Datenverkehr blocken. Anschließend lassen sich die Policies anhand verschiedener Faktoren anpassen:

- Rollen innerhalb der Anwendung
- Art der Anwendung
- Umgebung, in der die Anwendung ausgeführt wird (Entwicklung, Test oder Produktion)
- Standort der Umgebung (z. B. Produktionsumgebung in einem Rechenzentrum in Kalifornien)

Um diese Policies durchzusetzen und den Traffic auf laterale Bewegung zu überwachen, fügt das DevSecOps-Team einfach einen Illumio VEN (Virtual Enforcement Node) zum Software-Build hinzu.
Der VEN ist ein leichtgewichtiger, ausfallsicherer Agent, der mit der integrierten Firewall des Anwendungs-Hosts zusammenarbeitet.

Sobald der VEN in der Anwendungsumgebung läuft, setzt er Zero-Trust-Policies durch, gibt Alerts aus, wenn er verdächtige laterale Bewegung erkennt, und schränkt bei aktiven Angriffen den Datenverkehr ein. Infizierte Endpoints werden sofort vom Rest des Netzwerks isoliert.

Illumio bietet eine leicht zu bedienende, flexible zentrale Plattform, mit der sich Security in DevSecOps-Prozesse einbinden lässt – ohne langwierige Schulungen, hohe Kosten oder administrativen Aufwand.

Die Policies können in der Plan-, Build- und Testphase der DevOps-Pipeline definiert und getestet werden. In der Deploy- und der Monitor-Phase wird dann der Traffic überwacht.

Die Illumio-Plattform bietet Zero-Trust-Segmentierung unabhängig davon, wo Anwendungen und Services bereitgestellt werden:

- Rechenzentren
- Public, Private oder Hybrid Cloud
- Endpoints

> „Wir kennen unsere Risiken jetzt besser, haben Security-Policies besser im Griff und können unsere Daten besser schützen. Illumio hat dabei eine entscheidende Rolle gespielt.“
>
> **Security-Verantwortlicher**
> Führendes Finanzinstitut

Segmentierung für DevSecOps

Illumio kann Softwareentwicklungsteams helfen, Anwendungen jeder Art sicherer zu programmieren.

Wenden Sie sich an uns, um mehr zu erfahren:
www.illumio.com

Über Illumio

Illumio, die umfangreichste Zero-Trust-Lösung für Ransomware- und Breach-Containment, schützt Organisationen vor Cyberkatastrophen und Betriebsstörungen, ohne die Komplexität zu erhöhen. Die Illumio-Plattform visualisiert Datenflüsse und legt automatisch Policies für die Segmentierung fest, um unnötigen lateralen Datenverkehr in Multi-Cloud- und Hybrid-Infrastrukturen zu vermeiden – damit kritische Ressourcen geschützt werden und Cyberangreifer sich nicht ausbreiten können.