HADRIAN

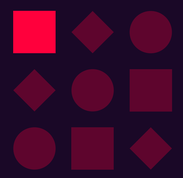
# Zehn Gründe, warum Sie Ihre Angriffsfläche kontinuierlich überwachen sollten

Mit der Digitalisierung von Organisationen ist es entscheidend, ständig die Angriffsfläche - die Punkte, die anfällig für unautorisierten Zugriff sind - zu überwachen, um mit der stetig fortschreitenden Bedrohung durch Cyberangriffe Schritt zu halten. Durch die proaktive Identifizierung und Behandlung von Risiken können sich Organisationen gegen diese Bedrohungen schützen. Hadrian scannt kontinuierlich die Angriffsfläche und identifiziert Risiken, sobald sie auftreten, um die Wahrscheinlichkeit eines erfolgreichen Angriffs zu verringern.


Innerhalb von **15 Minuten** nach der Offenlegung scannen Bedrohungsakteure nach Vulnerabilitäten.

**10%**

aller CVEs werden als kritisch eingestuft.



**Eine von zehn Vulnerabilitäten** im Internet exponierten Anwendungen wird als hochriskant oder kritisch betrachtet.

Hochrisikovulnerabilitäten sind in den Netzwerkperimetern von **84%** der Unternehmen vorhanden.

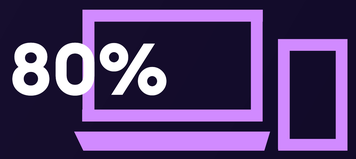

Es wird erwartet, dass der Prozentsatz großer Organisationen, die täglich Code in Produktion deployen, von **5%** im Jahr 2021 auf **70%** im Jahr 2025 steigen wird.

Nicht gepatchte Vulnerabilitäten waren in **60%** der Datenschutzverletzungen involviert.

**80%** der öffentlichen Exploits werden vor der Veröffentlichung der CVEs publiziert.


der Organisationen haben einen Angriff auf unbekannte, unverwaltete oder schlecht verwaltete, im Internet exponierte Asset erlitten.

Berichte über schlechte Konfigurationen von Websites sind im letzten Jahr um **151%** gestiegen.




der CISOs sagen, dass kritische Updates oder Patches, von denen sie dachten, sie hätten sie eingesetzt, tatsächlich nicht alle Geräte aktualisiert haben.