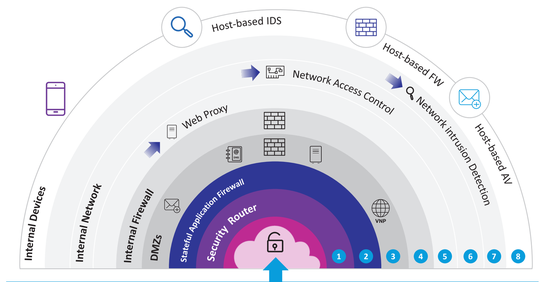
Why App Security?

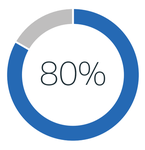
Existing Network and Perimeter Based Security is Insufficient



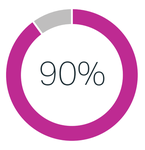
84% of breaches exploit vulnerabilities in the application layer
Yet the ratio of spending between perimeter security and application security is 23

Gartner Maverick Research: Stop Protecting Your Apps: It's Time for Apps to Protect Themselves (2014)

The Majority of Security Breaches Today are from Application Vulnerabilities



Percentage of applications containing at least one critical or high vulnerability.[1]



Security incidents from exploits against defects in the design or code of software.[2]

Homeland Security

12017 Application Security Research Update" by the HPE Software Security Research team, 2017
2U.S. Department of Homeland Security's U.S. Computer Emergency Response Team (US-CERT)

AppSec Risk by the Numbers

1,900,000,000
Records lost globally in the first half of 2017

1,400,000
Sensitive PII lost in a single US breach

15%
Survey respondents reporting a breach

23%
Respondents citing their application as source

References: breachlevelindex.com and SANS 2017 Application Security survey

Application Security Today is Complex

Internet of Things
Suppliers
Managed Cloud
Public Cloud

Monitoring / Protecting Production Software

Securing legacy applications

Legacy Software

Demonstrating Compliance

Certifying new releases

In-house Development

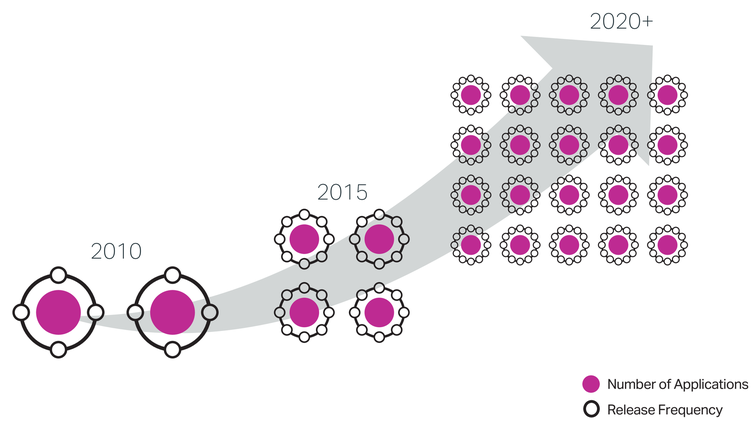
Procuring secure software

Outsourced
Commercial
Open Source

Security Must be Integrated Into the New SDLC

Application security for the SDLC

Today's Business Needs are Dramatically Increasing the Number of Applications and the Frequency of Releases



Document version 4.0