The traditional strategy of hardening your perimeter no longer works. That’s because distributed apps have no identifiable perimeter, and when a breach occurs, it’s difficult to prevent the attack from spreading laterally throughout your network. And simply deploying the latest security point solutions for constantly changing applications isn’t effective or sustainable.

Why legacy security falls short

The traditional strategy of hardening your perimeter no longer works. That’s because distributed apps have no identifiable perimeter, and when a breach occurs, it’s difficult to prevent the attack from spreading laterally throughout your network. And simply deploying the latest security point solutions for constantly changing applications isn’t effective or sustainable.
Modern applications require intrinsic security

**Protect the network**
Prevent the lateral spread of threats with micro-segmentation.

**Protect the data center endpoints**
Identify and automatically respond to threats.

**Protect the data**
Encrypt all enterprise data at rest.
Achieve agile, sustainable security with VMware

Maintain a strong security posture as applications and data evolve by architecting security into your environment. Enforce security at the most granular level of the application. And if a breach occurs, stop the attack in its tracks.

Define and automatically provision network security policy for each individual VM or container.

NSX

AppDefense

Enforce the intended state and behavior of applications, instead of chasing threats.

vSAN

Encrypt all enterprise data at rest, all the time.

Learn how this is possible with VMware NSX, VMware AppDefense and VMware vSAN.