Securing the Data Center in Just Four Steps

Implementing any new security approach or solution requires time and commitment from an already stretched-thin security team. The following four-step approach has been used by VMware customers to start small and continually improve data center security over time.

**STEP 1: Crawl - Macro-Segment the Network**

VMware customers have found that the fastest time-to-value is achieved by segmenting the network using an internal firewall.

**Goal:** Begin improving the overall security stance for the data center by preventing lateral movement between zones.

As teams gain more experience in operating a distributed internal firewall, they can continue expanding monitoring and protection of east-west traffic to additional critical or important workloads within the data center.

**Goal:** Use built-in visibility and automation to isolate and secure more workloads, which further reduces the attack surface and strengthens data center security.

**STEP 2: Walk - Micro-Segment Critical Applications**

Typically, the next step on the journey to securing the data center is to start implementing more granular controls on a small number of well understood critical applications.

**Goal:** Isolate and protect critical applications, applying layered security controls specific to the application and preventing lateral movement by attackers either into or out of the network segment where the application runs.

**STEP 3: Jog - Gain Wide Data Center Visibility**

At this point in the journey, security teams are ready to secure all applications in the data center to further mitigate security risk, while easily scaling to protect new workloads and increased traffic.

**Goal:** Extend deployment to inspect and protect all east-west traffic in the data center and provide additional layers of protection for sensitive workloads using the firewall’s IDS/IPS capabilities.

**STEP 4: Run - Secure All Applications**

As teams gain more experience in operating a distributed internal firewall, they can continue expanding monitoring and protection of east-west traffic to additional critical or important workloads within the data center.

**Goal:** Further improve visibility and automation to secure and monitor more workloads, which further reduces the attack surface and strengthens data center security.

**Learn more about this four-phased approach in Securing the Data Center in Just Four Steps.**