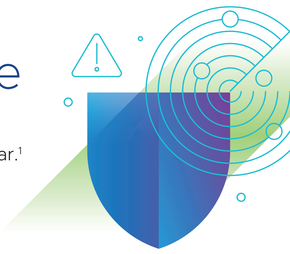
vmware

6 Best Practices for Cyber Vigilance



75% of respondents surveyed said attack volumes have increased by 52% in the past year.[1]

Use the following 6 best practices for cyber vigilance to help fortify your defense against advanced attacks.

1 INCREASE SITUATIONAL AWARENESS

63%

SURVEYED SAY THEY NEED BETTER VISIBILITY OVER DATA AND APPLICATIONS TO PREVENT ATTACKS[1]

Organizations need to take a proactive and comprehensive approach to security, regardless of sector or size. Telemetry is thus fundamental to achieve situational awareness. One must integrate the network detection and response platform with their endpoint protection platform.

2 SECURE WORKLOADS AND KUBERNETES ENVIRONMENTS

98%

SURVEYED ALREADY USE OR PLAN TO USE A CLOUD-FIRST SECURITY STRATEGY

Migration to the cloud shows no sign of slowing down, which must result in security that extends across workloads, containers and Kubernetes environments. Protection across cloud workloads should be the top priority for organizations utilizing public and private clouds to take cloud security to the next level and protect against attacks like cloud jacking.

3 TRACK IDENTITIES ON THE MOVE WITH MULTIFACTOR AUTHENTICATION

PROTECT ALL EXTERNAL-FACING ASSETS WITH MULTIFACTOR AUTHENTICATION

LEVERAGE A SINGLE SIGN-ON (SSO) PROVIDER

APPLY THE PRINCIPLE OF LEVEL PRIVILEGE

Security teams need the ability to accurately track identities as they move throughout networks to ensure adequate protection. This requires just in time administration and two factor authentication.

4 OPERATIONALIZE HARDENING & PATCHING

By leveraging industry best practices for hardening and patching, ensure IT operations and security are on the same page with vulnerability data and have agreed on service-level agreements (SLAs) for patching.

5 APPLY MICRO-SEGMENTATION

COUNTER IR OCCURS

63%

OF THE TIME, ACCORDING TO SURVEYED FINANCIAL INSTITUTIONS[2]

Limit an adversary's ability to move laterally within the organization. Forcing intruders to cross trust boundaries provides an improved opportunity for detection and prevention.

6 ACTIVATE YOUR THREAT HUNTING PROGRAM

81%

OF ORGANIZATIONS REPORT THEY HAVE A THREAT HUNTING PROGRAM IN PLACE

Security teams should assume attackers have multiple avenues into their organization. Threat hunting on all devices can help security teams detect behavioral anomalies as adversaries can maintain clandestine persistence in an organization's system. Organizations have already begun to realize the value of threat hunting.

1. Global Security Insights 2021
2. Modern Bank Heist Report