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.

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.

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.

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.

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.

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.