A Dynamic Attack Surface Requires Dynamic, Extended Security

To stay ahead of attackers, organizations need dynamic, proactive security that can identify new or emerging threats and react in real-time to block an attack. Legacy AV is no match for unknown threats. So, in order to better secure an organization, they need to think of their attack surface as a whole rather than just individual endpoints. Today’s dangerous threats are unknown—i.e., custom, brand-new (zero-day), or polymorphic exploits and payloads. Other common attack surface tactics include:

- Memory Exploits
- Unauthorized Applications
- Cloud Resources and Infrastructure

The cloud must not be a weak link in your attack surface. Cloud and container services must be protected from misconfiguration. The security from your remote resources needs to be extended to the cloud and provide consistent protection.

Reduce Your Attack Surface with AI-Driven Security Solutions

Try as they might, organizations will never be able to completely eliminate vulnerability. To manage the modern and dynamic attack surface, organizations need to ensure they have the right set of security controls in place that reduce the chance that an attacker can/uni00A0gain access.

In order to better secure an organization, they will need to convert their security stack into an AI-driven endpoint and network security solution. Legacy AV is no match for unknown threats. To stay ahead of attackers, organizations need dynamic, proactive security that can identify new or emerging threats and react in real-time to block an attack. Legacy AV is no match for unknown threats. Legacy AV is no match for unknown threats. Legacy AV is no match for unknown threats. Legacy AV is no match for unknown threats. Legacy AV is no match for unknown threats. Legacy AV is no match for unknown threats.