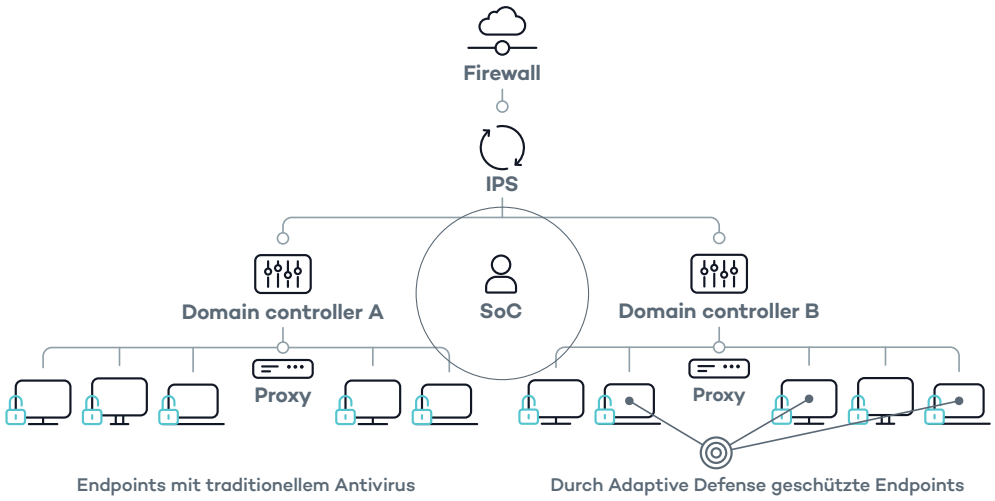
Adaptive Defense bei der Arbeit...

Versteckter Angriff mit anpassungsfähigen lateralen Bewegungen.

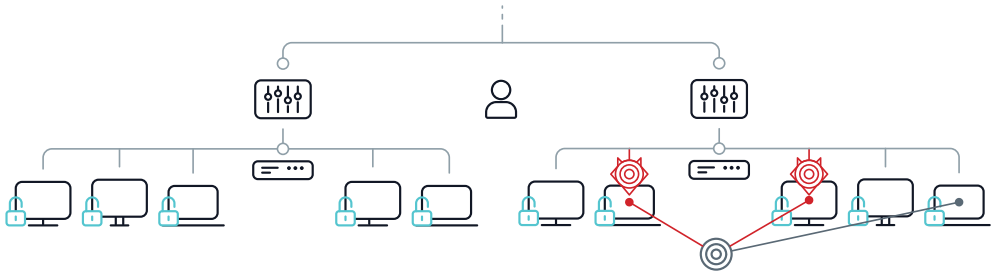
1 Ein scheinbar geschütztes Netzwerk

Key Account-Umgebung mit Tausenden von Endpoints in zwei Domänen, einigen wenigen Domänencontrollern, Firewall, IPS, Antivirus und einem SoC. Die Bereitstellung von Adaptive Defense beginnt an einigen wenigen Endpoints in Domäne B.



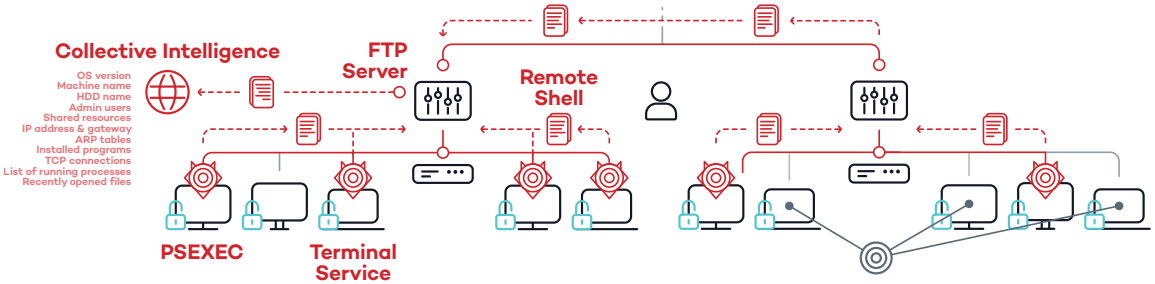
2 Das Adaptive Defense Sicherheitskonzept

Blockiert nicht vertrauenswürdige Programme und sendet geschützte Endpoint-Telemetrie in die Cloud, die dort sofort verarbeitet wird.



3 Threat Hunting and Investigation

Threat Hunting verknüpft vergangene Ereignisse, bei denen sie entdeckten, dass hinter einer scheinbar geschützten Netzwerkdomäne A eine Kompromittierung stattfand, und verwendet dabei administrative Tools, um Daten für die Erstellung von Endpoint-Profilen zu sammeln und an die Collective Intelligence zu senden.



Der Angriff wurde vom Threat Hunting Team entdeckt

Die lateralen Bewegungen des Angreifers, um die Kontrolle über Bereich B zu erlangen, wurden entdeckt und von Adaptive Defense eliminiert, bevor sie Schaden anrichten konnten.