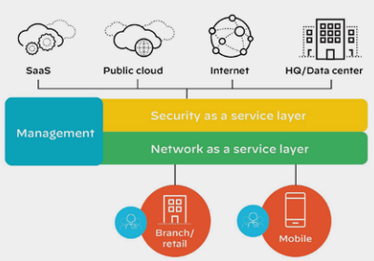
FORTINET

Intelligenter Endpunkt-Schutz in Echtzeit mit FortiEDR

EDR-Lösungen (Endpoint Detection and Response) schützen Unternehmensnetzwerke vor komplexen Cyberbedrohungen, indem sie Angriffe erkennen und geeignete Gegenmassnahmen unterstützen. Dies ist jedoch nur dann effektiv, wenn schnell und automatisiert reagiert wird. EDR-Tools der ersten Generation werden dieser Anforderung nicht gerecht. Demgegenüber reduziert FortiEDR von Fortinet die Angriffsfläche proaktiv und erkennt und entschärft potenzielle Bedrohungen in Echtzeit. Die Reaktion auf Sicherheitsvorfälle und die Fehlerbehebung lassen sich mit anpassbaren Playbooks automatisieren – ohne dass das Security-Team mit einer Flut von Alarmmeldungen überlastet oder der Geschäftsbetrieb beeinträchtigt wird.

- Automatischer Echtzeit-Schutz vor komplexen Bedrohungen
- Proaktive Risikominderung der Angriffsfläche
- Automatisierte Reaktion auf Sicherheitsvorfälle via Playbooks
- Voll integriert in die Fortinet Security Fabric

www.boll.ch/fortinet/fortiedr.html



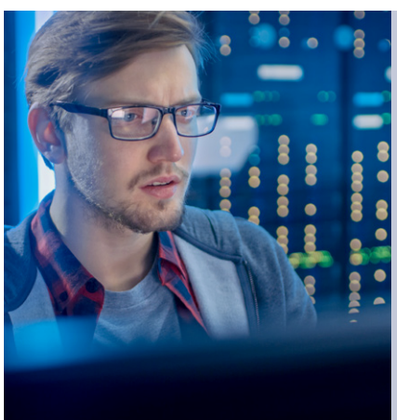
paloalto® NETWORKS

Prisma Access – die umfassende SASE-Lösung von Palo Alto Networks

Mit Secure Access Service Edge (SASE) lassen sich Netzwerke, Filialstandorte und mobile Nutzer schützen. Dabei setzt SASE auf ein cloudbasiertes Betriebsmodell, das WAN- und Security-Funktionalität vereint. Die SASE-Plattform Prisma Access ist in 76 Ländern verfügbar und stellt mehr als 100 Zugangspunkte bereit. Die Sicherheitsfunktionen umfassen Threat Prevention, Web Filtering, Sandboxing, DNS-Sicherheit und Schutz vor Datenabfluss (DLP) bis hin zu Next-Generation Firewalling anhand von User-, Applikations- und Host-Profilen.

- Prisma Access schützt die Unternehmenskommunikation – unabhängig davon, wo Sie arbeiten und welche Dienste Sie nutzen bzw. wo diese zur Verfügung gestellt werden
- Kombiniert Zero Trust Network Access mit Next-Generation-Firewall-Sicherheitsfunktionen
- Inspiziert den gesamten Traffic an allen Ports, für alle Nutzer und Anwendungen
- Cloudbasierter Ansatz (FWaaS) garantiert Skalierbarkeit und höchstmögliche Verfügbarkeit bei voller Kontrolle und Transparenz
- Nutzt die umfassende Threat-Intelligence-Architektur von Palo Alto Networks

www.boll.ch/info/Prisma-Access



Synack

Penetration Testing der neuen Art

Penetration-Tests geben Auskunft über Schwachstellen in der IT-Infrastruktur – auch über Sicherheitslecks, die mit herkömmlichen Vulnerability-Scans nicht zu finden sind. Synack geht mit ihrer Penetration-Testing-Lösung einen höchst innovativen Weg und kombiniert künstliche Intelligenz (KI) und maschinenlernfähige Sicherheitssoftware mit dem Wissen und der Erfahrung der weltweit besten White-Hat-Hacker und Cybersecurity Engineers. Diese sind in einem globalen Netzwerk miteinander verbunden und bilden als Synack Red Team (SRT) den Kern der skalierbaren, effektiven Crowdsourcing-Sicherheitslösung. Die Sicherheitstests stehen über ein Kundenportal als Managed Service rund um die Uhr zur Verfügung.

- Penetration-Tests als Managed Service
- KI-gestützte Technologieplattform für automatisierte Scans
- Synack Red Team: globales Crowdsourcing-Netzwerk aus spezialisierten Hackern
- Tests über sicheres Gateway mit voller Kontrolle durch Kunden

www.boll.ch/synack/index.html