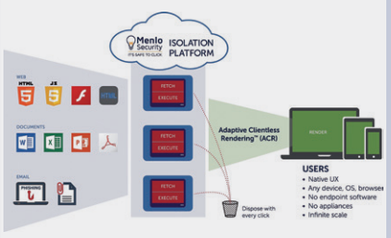


Menlo Security

Next-Gen Proxy – IT-Sicherheit ohne Kompromisse

Viele IT-Security-Lösungen basieren auf dem Prinzip «Detection». Dabei werden bereits bekannte Malware oder als gefährlich gemeldete Websites erkannt und der Zugriff darauf unterbunden. Bei neuer Malware jedoch sowie bei unbekannten oder neu infizierten Websites stösst dieser Ansatz an seine Grenzen. Diesbezüglich Abhilfe schafft Menlo Security mit ihrer innovativen Isolation-Technologie. Dabei werden sämtliche Websites, deren Dokumente sowie Links oder Attachments in E-Mails isoliert. Sie werden in einem abgeschotteten Container «ausgeführt» und dem Benutzer als gerenderte Darstellung ohne aktiven Code auf das Endgerät übermittelt. Nun hat Menlo Security den patentierten «Isolation»-Kern in einen Next-Gen Proxy integriert, um Endgeräte ohne Kompromisse vor Attacken aus dem Internet zu schützen. Dadurch werden die User von jeglicher Malware isoliert.

- Web- und E-Mail-Security-Lösung mit revolutionärer Isolation-Technologie
- 100% sicherer Zugriff auf alle Websites (Secure Browsing)
- Eliminiert Drive-by Infections, Zero-Day Malware und Ransomware
- Security für Cloud-Anwendungen
- Erhältlich als globaler Cloud-Service oder als virtuelle Appliance

Informationen:
www.boll.ch/info/Menlo-de

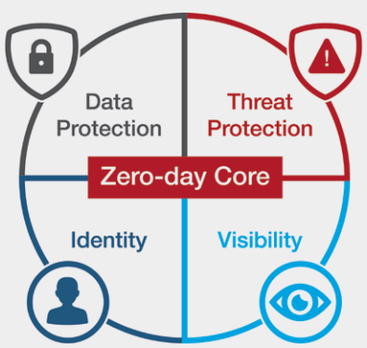
RAPID7

Verdächtige Aktivitäten frühzeitig erkennen

Oft nutzen Hacker gestohlene oder schwache Passwörter, um ins Firmennetzwerk einzudringen und bleiben dadurch über Wochen oder Monate unerkannt. Nun bietet Rapid7 mit ihrer InsightIDR-Lösung die Möglichkeit, verdächtige Aktivitäten im Firmennetzwerk frühzeitig zu erkennen. Endgeräte werden mittels eines lokalen Agenten an InsightIDR angebunden und Log-Files von anderen IT-Komponenten wie Firewall, Active Directory oder Web Proxy eingelesen. Die cloudbasierte Insight-Plattform korreliert die Daten und analysiert diese auf Auffälligkeiten. Da Rapid7 viele Angriffsmuster und Alarmtrigger bei InsightIDR mitliefert, entfaltet die Lösung bereits innerhalb weniger Tage die volle Stärke.

- Cloudbasierte User-Behaviour-Analytics-Lösung mit Fokus auf Hackerangriffe über Endpoints
- Vordefinierte Automation- und Remedation-Workflows für rasche Beseitigung
- Zentralisiertes Log Management
- Sammelt und analysiert auch Aktivitäten auf Azure und AWS
- Schnittstellen zu Palo Alto Wildfire, Splunk, CyberArk, FireEye, ServiceNow
- Update von neuen Angriffsmustern dank Quellen wie Metasploit, Project Heisenberg oder Sonar

Informationen:
www.boll.ch/rapid7/index.html



bitglass

Maximale Sicherheit in der Cloud

Die «Cloud Access Security Broker»-Plattform (CASB) von Bitglass ermöglicht Unternehmen jeder Grösse, bei der Nutzung von Cloud-Diensten Sicherheitsrichtlinien über die Grenzen ihrer eigenen IT-Infrastruktur hinaus durchzusetzen. Demnach bietet die Lösung einen agentenlosen Zero-Day-, Daten- und Bedrohungsschutz – dies an jedem Standort, für jede Anwendung und für jedes Endgerät. Mit der Unterstützung von SaaS-Anwendungen wie Office 365, IaaS-Plattformen wie AWS und privaten Cloud-Anwendungen sorgt Bitglass für einen umfassenden Echtzeitschutz über alle wichtigen Geschäftsanwendungen hinweg. Ferner bietet die innovative CASB-Lösung ein lückenloses Identitätsmanagement und eine beeindruckende Sichtbarkeit. Darüber hinaus ermöglicht Bitglass über eine Reverse-Proxy-Funktionalität eine Field/File-Verschlüsselung in Echtzeit (bei Uploads und Downloads). Dank Bitglass ist es möglich, Compliance-Anforderungen sowie Anforderungen an die Datensicherheit gemäss DSGVO/GDPR in Cloud-Umgebungen einfach einzuhalten.
Die vier Schlüsselfaktoren für ein Maximum an Cloud-Security und Compliance:

- Datenschutz
- Identitätsmanagement
- Bedrohungsschutz
- Visibilität

Informationen:
www.boll.ch/bitglass/index.html