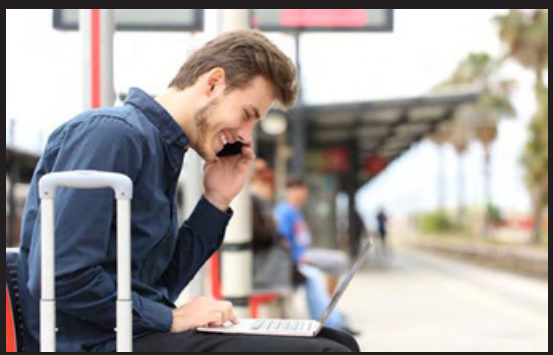

Mobile
Endpoint Security

Beskyt de enheder, der forbinder dine medarbejderes professionelle og personlige liv.

Luk sikkerhedshullet for dine medarbejderes mobile enheder med branchens førende løsning inden for mobil Endpoint Detection and Response (EDR). Lookout Mobile Endpoint Security, kombineret med CapMons Managed Service koncept giver dig optimal beskyttelse mod sikkerhedsbrud uden ekstra brug af interne ressourcer.

Lookout Mobile Endpoint Security

Lookout Mobile Endpoint Security giver dig omfattende realtidsbeskyttelse mod alle mobile trusler på tværs af alle iOS, Android og Chrome OS-enheder. Vi stopper kendte og ukendte phishing angreb, beskytter mod skadelige apps, enheds-jailbreaks og risikable netværk, hvor du hurtigt kan ende med at miste data. Alt dette udføres samtidig med, at vi giver slutbrugeren mulighed for selv at afhjælpe sikkerhedsproblemer, hvilket i høj grad mindsker behovet for support til slutbrugere.

Lookout Managed Services

Vores Managed Service koncept er designet til dig der ønsker at beskytte dine medarbejderes mobile enheder. Vi har designet to forskellige pakker: ***Essentials*** og ***Advanced.***

Essentials giver dig beskyttelse mod de 4 primære mobiltrusler, phising-, enheds-, app- og netværkstrusler.

Advanced pakken giver dig udover alt fra Essentials pakken, 24/7 overvågning og mulighed for at få udført proaktive analyser på alle virksomhedens mobile enheder.

En Managed Service aftale giver jer:

- Implementering og opsætning
- Dansk Support 08:30 - 16:00 med mulighed for tilkøb af 24/7 service og eskalering til 3rd level support.
- Overvågning med proaktiv assistance:
  - Identificering og blokering af malware fx. cookies, spyware og ransomware
  - Identificering af uautoriseret kamera- og mikrofon-adgang fra overvågningssoftware
  - Identificering/forhindring af identifikationstyveri og dataeksfiltrering gennem netværksangreb
  - Identificering af kompromitteret udstyr (root/jailbreak)
  - Identificering og blokering af phishing forsøg
  - SIEM integration (fx. Elastic, Splunk, ArcSight, Qrader, Azure Sentinel)
  - Mobile risk API for workflow automatisering
  - Klient opgradering
- Kunderapportering 1 gang om måneden

CapMon A/S | Lyskær 9 | 2730 Herlev Denmark | Tel.: +45 4485 5060 www.capmon.dk | E-mail: salg@capmon.dk

Implementering og opsætning
Essentials og Advanced Capmon hjælper med implementering og opsætning af Lookout, så du ikke behøver at gøre det selv. Vi hjælper gerne med at opsætte det på din Mobile Device Management (MDM)-platform, hvis det er nødvendigt. Som en integreret del af opsætnings- processen tilbyder vi skræddersyet undervisning, hvor du og dine medarbejdere bliver grundigt instrueret i effektiv brug af Lookout. Vores mål er at sikre, at du føler dig komfortabel med brug af løsningen.

Dansk support
Essentials og Advanced CapMon har et dansk supportteam der sidder klar (hverdage i tidsrummet 08:30 til 16:30). Ved tilkøb af 24/7 overvågning kan CapMon kontaktes alle døgnets timer hele året rundt. Dette kan ske enten via mail, telefon eller en remote forbindelse.

Overvågning med proaktiv assistance
Essentials: Hverdage 08:30 til 16:30 Advanced: 24/7
CapMon Support Team kombinerer mere end 20 års erfaring inden for cyber security med konstant overvågning af din virksomheds infrastruktur for at sikre din virksomhed en robust sikkerhedsløsning. Med Lookout Mobile Endpoint Security er vi i stand til nøjagtigt at identificere og analysere forskellige signaturer, hvilket giver os mulighed for at skelne mellem potentielt skadelig og harmløs aktivitet på alle mobile enheder. Alle hændelser håndteres hurtigt og effektivt. Vi genererer månedlige rapporter baseret på de individuelle hændelser, og stræber efter at levere en omfattende sikkerhedsløsning, der giver dig en sikker digital drift.

Klient opgradering (hverdage 08:30 til 16:30)
Essentials og Advanced CapMons support team vil tilsikre, at alle klienter er blevet opdateret senest 24 timer efter frigivelsen af en ny Lookout release. Er der stadig klienter i kundens infrastruktur der ikke er opgraderet vil kunden blive notificeret om dette.

Cyber Threat notifikation
Advanced Som en del af vores Advanced pakke vil du modtage adviseringer om alle potentielle sårbarheder i den software, der anvendes på dine mobile enheder. Lookout har adgang til en omfattende database, der gør det muligt for os at identificere og informere dig om eventuelle sikkerhedsrisici i realtid.

cap:mon THE MONITORING COMPANY

Lookout

Managed Services	Advanced	Essentials
Implementering og opsætning	■	■
Dansk Support 08:30 til 16:00 på alle hverdage med eskalering til 3. level support	■	■
Overvågning 08:30 til 16:00 alle hverdage, med proaktiv assistance, herunder	■	■
Identificere, om signaturer er gode eller dårlige		
Identificering og blokering af malware fx. rootkits, spyware og ransomware		
Identificering af uautoriseret kamara- og mikrofonadgang fra overvågningssoftware		
Identificering/forhindring af identifikations-tyveri og dataeksfiltrering gennem netværksangreb		
Identificering af kompromitteret udstyr (root/jailbreak)		
Identificering og blokering af phishing forsøg		
SIEM integration (fx. Elastic, Splunk, ArcSight, Qrader, Azure Sentinel)		
Mobile risk API for workflow automatisering		
Incident reporting		
Klient opgradering	■	■
Kunderapportering 1 gang pr. måned	■	■
24/7 overvågning med proaktiv assistance og hurtige svar-tider, med eskalering til 3. level support.	■	
Identificere, om signaturer er gode eller dårlige		
Identificering og blokering af malware fx. cookies, spyware og ransomware		
Identificering af uautoriseret kamara- og mikrofon-ad-gang fra overvågningssoftware		
Identificering/forhindring af identifikations-tyveri og dataeksfiltrering gennem netværksangreb		
Identificering af kompromitteret udstyr (root/jailbreak)		
Identificering og blokering af phishing forsøg		
SIEM integration (fx. Elastic, Splunk, ArcSight, Qrader, Azure Sentinel)		
Mobile risk API for workflow automatisering		
Incident reporting		
Cyber threats notifikation	■	