Lookout

How Lookout Helps with the RANSOMWARE Problem

Ransomware is not a new threat, attackers adapt their tactics to make it an ever-persistent threat even as enterprise architecture evolves. With highly integrated users, devices, networks, apps and data, there are countless points of vulnerability that attackers exploit to make ransomware successful. This makes solving the ransomware problem especially challenging, and while there is no one silver bullet, Lookout is well-positioned to help organizations protect against most parts of a ransomware attack.

Action	How Lookout Helps
Threat actors will first execute recon on the target by discovering vulnerable web-facing apps and assets, phishing for legitimate employee credentials or purchasing exploits and credentials on the dark web. Success with any of these grants the attacker a backstage pass to your infrastructure.	Lookout helps protect against initial compromise via phishing and social engineering across any MacOS, Windows, iOS, Android or ChromeOS device with Secure Web Gateway (SWG) and Phishing and Content Protection (PCP). To protect vulnerable servers, Lookout Zero Trust Network Access (ZTNA) can cloak these servers from discovery on the public internet. Admins can also enhance authentication with policies that implement additional protections such as enforcing multifactor authentication (MFA) where it wasn't present before.
When the attacker successfully enters your infrastructure, they will usually install a persistent backdoor. This will help them come and go as they please so they can observe your security practices and identify where valuable systems, such as database servers, are located.	Identifying unauthorized access to your infrastructure is a critical piece of stopping attacks before serious damage can be done. Lookout Cloud Access Security Broker (CASB) observes contextual signals to help you control data access, downloads or modifications. All activity is logged in the Lookout console ensuring you have a record to remain compliant. Together, Lookout User and Entity Behavior Analytics (UEBA) and Data Loss Prevention (DLP) use contextual clues to detect anomalous or unauthorized access to sensitive data. Admins can leverage policies that enable Lookout to take actions that block users from accessing that data.

Action	How Lookout Helps
Typically, access to something like a database server should only be granted to specific users under particular circumstances. This is usually where the attacker will establish a connection to a remote host and start to copy or modify data for exfiltration to that server.	Again, the combination of UEBA and DLP play a critical role. Together, they can block users and send alerts as soon as Lookout detects privilege escalations, data modifications at rest and in motion, or anomalous access to data, apps and servers. Lookout also detects when the attacker deletes or renames any content as part of their execution process. In addition, SWG will detect the connection to the remote host, as the security intelligence that feeds Lookout phishing protection is also applied to the SWG. This information is critical to help identify, alert and block connections out to a malicious host server.
In the final impact of the attack, the actor will attempt to encrypt sensitive files, exfiltrate some data as leverage, and lock out users and demand payment within a certain timeframe.	To make data useless to the attacker and prevent the possibility of the attacker leveraging data against the victim, Enterprise Digital Rights Management (EDRM) can encrypt data if it's exfiltrated from the infrastructure – even if the attacker encrypts it first.