ENDPOINTS:
DETECTION COMPLEMENTING PREVENTION

Endpoint security solutions are part of the average security posture. But if you're not collecting event logs from your endpoints then you're missing important data required in a comprehensive security practice. Snare helps you address complex audit, compliance and forensic requirements while complementing endpoint security solutions.

Endpoint security is similar to safeguarding a building. Doors and windows are secured with locks, security guards confirm the credentials of tenants and visitors, the interior of the building is monitored for catastrophic events like fire or flooding. The best endpoint security tools provide a myopic view of what is happening at a particular moment in time. Snare improves your security position by collecting and forwarding event logs from your endpoints to your enterprise tools, like a SIEM, for in depth analysis and threat correlation.

Here are 3 reasons why you need to log data on all your endpoints, including desktops and laptops:

1. **Compliance.** Security standards such as SOX & FISMA require assurance of the integrity of the financial systems. This requires end to end logging from the endpoint to any other destination whether it be another endpoint, the server, or to the database where the information may reside to prove that financial systems are true and correct and not compromised.

2. **Completeness.** An endpoint can have changes performed, sensitive data can be stored or copied to it and many of these details are only logged on the endpoint. If a user uses a local login to the work station (a non-active directory account) that information will not go to the domain controller as it only gets logged locally. If they have a local USB or cdrom then using those devices is only recorded locally. They only way to capture activity information is by logging event data on the endpoint.

3. **Scope.** For PCI DSS compliance all systems in scope need to have logging and auditing in place. This means all servers, desktops, databases, web servers, applications, routers, firewalls, switches etc. Any devices that are involved with storing, processing, transmitting or accessing card holder data is in scope for PCI DSS. So users on their laptops and desktops that access systems that contain cardholder data are in scope and need to have their event logs archived. These users could be the office administrators or the systems administrator, application administrators, DBA or network administrators, and service desktop personnel if they take cardholder data over the phone and enter it in a computer, and as such all in scope.

Snare Enterprise agents are the de facto solution for collecting event log data from endpoints and servers. Check out: www.intersectalliance.com/try-snare-eval-now/ to try Snare free, or visit us at www.intersectalliance.com to learn more about how Snare has you covered.