NGSS

Next Generation Simple Solutions Pvt Ltd

CUSTOMER SECURITY & TECHNOLOGY BULLETIN

SIEM or XDR? Yes

Vendor: Sophos | Product: SIEM | Published: 2026-11-05



From EDR to XDREDR effectively became a cloud-based store of endpoint data. To make that data actionable, a lot has to happen:Data must be correlated to surface threats and generate alerts.Alerts must be prioritized, triaged to confirm they are true positives, and managed.Actions must be taken to disrupt threats, with automation and playbooks for repeatable patterns.Data must be searchable as investigations progress, and reports must be generated.The system must integrate with IT service management (ITSM) tools to fit into operational processes.Attackers also target multiple entry points and move laterally once inside. So, the industry rightly concluded that threat detection and response become far more insightful and effective when endpoint data is combined with data from other threat vectors and sources such as network, identity, cloud, and email. The result was a purpose-built, integrated system focused singularly on security outcomes rather than on the endpoint alone. EDR evolved into extended detection and response (XDR).Same logs, two places, overlapping outcomesIf you have EDR, you most likely have a security team handling triage, investigation, and response, and very likely a SIEM as well.At a minimum, a SIEM handles data ingestion, analytics, alert management, investigation, and response. If that sounds familiar, it is because that is exactly what XDR does. The SIEM is the original detection and response platform, the forerunner of every DR product, but it is neither cost-efficient nor easy to maintain. So why do organizations run both and pay twice? In most cases, the reasons are astonishingly simple:If it aint broke, dont fix it.Other projects take priority, and taking this on would leave no one for anything else.Almost every auditor asks for a SIEM, and some may even use the word SIEM as a generic term.The SIEM is an established budget line item (most likely due to the previous bullet).To be fair, there is one legitimate reason XDR and the SIEM co-exist, and it is the endpoint. For a SIEM to fully overlap with XDR, there must, by definition, be an endpoint, and the SIEM depends on an agent to supply it. The industry differs on what that agent looks like. It could be a complete endpoint agent with superior built-in protection capabilities, or a detection-focused sidecar agent that runs alongside an incumbent protection solution and forwards alerts and telemetry to an XDR or a

Prepared by:

Source: https://www.sophos.com/en-us/blog/siem-or-xdr-yes

NGSS | Customer Technology Advisory | support@ngss.in