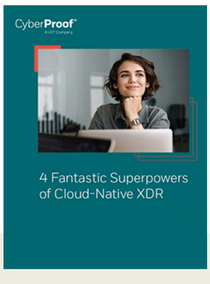
CyberProof®
A UST Company

Why You Need Cloud-Native XDR

When it comes to securing your enterprise, “good enough” is never good enough. When anyone in sweatpants can purchase a ransomware kit for $66 and cause millions in financial damage, organizations need to secure every corner of their environment.

If you’re migrating your Security Operation Center (SOC) to the cloud, you need to know exactly how your processes, talent requirements, costs, and security approach will change. Check out how on-premises, cloud-based, and cloud-native detection and response compare before making your migration.

	On-Premises	Cloud-Based	Cloud-Native
LOG MANAGEMENT	Security teams manually collect, parse, tag, and filter security data from their on-premises data center	Built for an on-premises architecture but stored in a cloud-hosted environment	Cloud computing and AI enables automated and dynamic log collection
COSTS	Expensive data centers increase CapEx and infrastructure costs, and can’t scale cost-effectively in periods of high demand	Experience cost advantages of the cloud, including paying only for what you need, but spend on pricey integrations to connect on-prem and cloud	Pay only for the space you use and easily integrate data streams
ANALYTICS	Analytics limited by capacity and compute restraints of on-prem data centers, while siloed data leads to poorly informed decision-making	Achieve faster time to insights and deploy AI and ML to run models that require cloud-computing to function	Use custom tools that maximize your cloud infrastructure and rapidly accelerates data analysis. Automate many of the manual tasks that bog down analysts
USE CASE MANAGEMENT	On-premises detection rules, but no CI/CD capability	On-premises and cloud detection rules	Cloud detection rules, response playbooks, integrations for automation, CI/CD capability for fast deployment and rapid changes
THREAT DETECTION SKILLSETS	Typical threat detection and basic skills required to manually triage and validate alerts	Improve threat detection speed and accuracy but still experience bottlenecks due to retrofitted integrations or poorly mastered data	Requires advanced skills to maximize capabilities of XDR. Typically, enterprises engage a third party to handle cloud-native threat detection



As you can tell, **Cloud-Native XDR** give you more control, greater visibility, and superior cost management compared to cloud-based security or on-premises detection and response. But to keep up with evolving cyberthreats, you need four more essential capabilities. Find out what those capabilities are in the eBook, The 4 Fantastic Superpowers of Cloud-Native XDR.

DOWNLOAD THE EBOOK