DLP 功能比较

安排演示

传统供应商 — 受限的 DLP 供应商

数据保护功能范围	FORCEPOINT	TRELLIX (MCAFEE)	SYMANTEC	ZSCALER	NETSKOPE	PROOFPOINT	MICROSOFT
一键修复	●						
通过在端点和策略引擎上脚本编程，实现本地修复的可扩展性	●	◑	●	◑			
针对任何出口渠道（终端、网络、云、网站）强制执行超过 1700 多个开箱即用的数据分类器	●	◑	◑	◑	◑	◑	◑
对移动到可移动介质的文件进行本地加密	●	◑	◑				◑
Saas 云应用程序的统一 DLP 策略实施（API/内联）	●	◑	◑	◑	◑	◑	◑
端点检测和执行不需要网络连接	●	◑		◑	◑	◑	◑
电子邮件的全面数据安全（MSFT、Google、行動、無代理程式）	●	●	◑	◑	◑	●	◑
针对 900 多种文件类型的高级真实文件检测	●	◑	◑	◑	●	◑	◑
跨关键云和本地环境的数据发现	●	●	●			◑	◑
300 多个预定义的自然语言处理脚本，准确识别公共数据（PCI、PHI、PCI...）	●	◑	◑	◑	◑	◑	◑
云应用程序保护：实时内联和 API	●	●	●	●	●	●	◑

传统供应商 —— 受限的 DLP 供应商

统一数据保护涵盖范围	FORCEPOINT	TRELLIX (MCAFEE)	SYMANTEC	ZSCALER	NETSKOPE	PROOFPOINT	MICROSOFT
针对传输数据、静止数据和使用中数据的一致性 DLP 引擎	●	●	●	◑	◑	◑	◑
灵活部署；云、混合、本地部署	●	●	●	◑		◑	●
跨网络、电子邮件、云、端点、出口渠道的单一 DLP 策略实施	●	●	◑	◑	●		
跨所有渠道的单一事件警报 UI	●	●		◑	●	◑	

风险自适应保护 (UBA)	FORCEPOINT	TRELLIX (MCAFEE)	SYMANTEC	ZSCALER	NETSKOPE	PROOFPOINT	MICROSOFT
原生端点用户行为异常	●	◑		◑	◑	●	
基于 130 多个行为指标 (IOB) 的风险分析	●						
基于风险的综合数据保护行动计划实施 (基于背景和内容)	●						◑
近实时可调分析	●			●	●		

集成和生态系统	FORCEPOINT	TRELLIX (MCAFEE)	SYMANTEC	ZSCALER	NETSKOPE	PROOFPOINT	MICROSOFT
扫描交换的 PST文件 (邮箱)，静态数据	●	●	●				●
具有自动端点设置的云原生部署	●			◑	◑	◑	◑
Crowdstrike 和 BitDefender 恶意软件扫描	●	◑	◑	●	◑	◑	◑
与任何分类供应商兼容	●	◑	◑	◑	◑		
扫描旧的本地文件和数据存储 (结构化和非结构化)	●	●	●				◑

免责声明：产品比较是基于截至 2024 年 4 月 1 日，同一供应商提供的产品内功能和跨产品组合集成。产品比较不包括与第三方供应商的集成。功能比较是基于截至 2024 年 4 月 1 日，每个供应商的最新版本和现代版本。信息是基于截至 2024 年 4 月 1 日，从公共网站与论坛、分析员论文和产品数据表收集的数据。