kaspersky

Vergleich neue/alte Produktlinie

	Kaspersky Next EDR Foundations	Kaspersky Next EDR Optimum	Kaspersky Next XDR Expert	Kaspersky Next Complete Security	Kaspersky Endpoint Security Cloud	Kaspersky Endpoint Security Cloud Plus	Kaspersky Endpoint Security Cloud Pro	Kaspersky Endpoint Security for Business Select	Kaspersky Endpoint Security for Business Advanced
Detaillierter Funktionsumfang: Schutz									
	Next EDR Foundations	Next EDR Optimum	Next XDR Expert	Next Complete Security	KES Cloud	KES Cloud Plus	KES Cloud Pro	KESB Select	KESB Advanced
Datei-Schutz	+	+	+	+	+	+	+	+	+
Web-Schutz	+	+	+	+	Nur für Workstations	+	+	Nur für Workstations	+
Mail-Schutz	+	+	+	+	Nur für Workstations	+	+	Nur für Workstations	+
Netzwerk-Schutz	+	+	+	+	+	+	+	+	+
Verhaltenskontrolle	+	+	+	+	+	+	+	+	+
Wiederherstellung	+	+	+	+	+	+	+	+	+
Exploit Prevention	+	+	+	+	+	+	+	+	+
HIPS	+	+	+	+	+	+	+	+	+
AMSI	+	+	+	+	+	+	+	+	+
Anti Cryptor	+	+	+	+	+	+	+	+	+
Bad USB Attack Prevention	+	+	+	+	-	-	+	+	+
Detaillierter Funktionsumfang: Kontrollmechanismen									
Firewall	+	+	+	+	+	+	+	+	+
Web-Kontrolle	+	+	+	+	-	+	+	+	+
Gerätekontrolle	+	+	+	+	-	+	+	+	+
Programmkontrolle	+	+	+	+	-	-	+	+	+
Adaptive Anomaly Control**	-	+	+	+	-	-	+	-	+

* Verfügbar in separater Konsole

** Erkennt und blockiert Anomalien im Hinblick auf dateilose Angriffe und Angriffe mit legitimen Tools nach der Selbstlernphase. Diese Art von Angriffen ist i.d.R. extrem schwieg zu erkennen.

kaspersky

Vergleich neue/alte Produktlinie

Detaillierter Funktionsumfang: Cloud-Schutz & Training

	Next EDR Foundations	Next EDR Optimum	Next XDR Expert	Next Complete Security	KES Cloud	KES Cloud Plus	KES Cloud Pro	KESB Select	KESB Advanced
Cloud Discovery & Blocking	Nur Cloud Discovery	+	Pro View*	+	Nur Cloud Discovery	+	+	-	-
Schutz für Security for MS O 365	-	Pro View	Pro View*	Pro View	-	+	+	Add-On für KS4Mail	Add-On für KS4Mail
Data Discovery	-	Pro View	Pro View*	Pro View	-	-	+	-	-
SIEM: Export von Ereignissen via Syslog	Expert View On-Prem	Expert View On-Prem	Expert View On-Prem	Expert View On-Prem	-	-	-	+	+
SIEM: Export von Ereignissen via CE/LEEF	-	Expert View On-Prem	Expert View On-Prem	Expert View On-Prem	-	-	-	-	On-Prem
Cybersicherheitstraining für IT-Admins	-	Pro View	Pro View*	Pro View	-	-	+	-	-

Detaillierter Funktionsumfang: Verschlüsselung, Schutz für mobile Geräte, IT-Szenarien

Verschlüsselungs-Management (BitLocker, FileVault)	-	+	+	+	-	+	+	-	+
Verschlüsselung (Kaspersky Crypto-Modul)	-	Expert View On-Prem	Expert View On-Prem	Expert View On-Prem	-	-	-	-	+
Schutz, Kontrolle und Verwaltung für mobile Geräte	+	+	+	+	+ Schutz für Android	+ Schutz für Android	+ Schutz für Android	+	+
iOS MDM Server	+	Pro View, Expert View On-Prem	Expert View On-Prem	Pro View, Expert View On-Prem	+	+	+	On-Prem	On-Prem
Vulnerability Assessment & Patch Management	Nur Vulnerability Assessment	+	+	+	Nur Vulnerability Assessment	+	+	Nur Vulnerability Assessment	+
Datenlöschung	-	+	+	+	-	-	+	+	+
Software-Inventarisierung	Expert View On-Prem	Expert View On-Prem	+	Expert View On-Prem	-	-	-	-	+
Hardware-Inventarisierung	Expert View On-Prem	Expert View On-Prem	+	Expert View On-Prem	-	-	-	-	+
Patch Management	-	Expert View On-Prem	+	Expert View On-Prem	-	-	-	-	+
OS Deployment	-	On-Prem	On-Prem	On-Prem	-	-	-	-	On-Prem

kaspersky

Vergleich neue/alte Produktlinie

Detaillierter Leistungsumfang: E(X)DR-Funktionen

	Next EDR Foundations	Next EDR Optimum	Next XDR Expert	Next Complete Security	KES Cloud	KES Cloud Plus	KES Cloud Pro	KESB Select	KESB Advanced
EDR-Basisfunktionen • Ursachenanalyse • IoC Scan • Automatisierte Reaktion	Nur Ursachenanalyse	+	+	+	-	Nur Ursachenanalyse	+	-	-
Erweiterte EDR-Funktionen • Erfassung von Telemetriedaten • Threat Hunting • Erkennung von Angriffsindikatoren • MITRE ATT&CK-Mapping	-	-	+	-	-	-	-	-	-
XDR-Basisfunktionen • Zusammenführung von Warnmeldungen • Fallmanagement*** • Sandbox • Anomaly Detection • Anreicherung mit Threat Intelligence	-	-	+	-	-	-	-	-	-
Erweiterte XDR-Funktionen • Kreuzkorrelation**** • Threat Hunting • Drittanbieteranbindung • Playbooks • Untersuchungsdiagramm***** • Protokollverwaltung und Datenspeicher	-	-	+	-	-	-	-	-	-

Detaillierter Leistungsumfang: MDR-Funktionen

Sicherheitsüberwachung rund um die Uhr (24x7)	-	-	-	+	-	-	-	-	-
Automatisiertes Threat Hunting	-	-	-	+	-	-	-	-	-

*** Die effektive Untersuchung von Incidents und Koordination von Arbeitsabläufen
**** Bei der Kreuzkorrelation werden sowohl vordefinierte als auch benutzerdefinierte Regeln verwendet, um Angriffe und Bedrohungen zu identifizieren
***** Zeigt die Details zu einem Incident, d. h. die entsprechenden Warnmeldungen und ihre gemeinsamen Eigenschaften