kaspersky

Vergleich neue/alte Produktlinie



Kaspersky Next EDR Foundations



EDR Optimum











Kaspersky Endpoint Security Cloud



Kaspersky Endpoint Security Endpoint Security Cloud



for Business

Kaspersky **Endpoint Security** for Business

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 schwieig zu erkennen.

kaspersky

Vergleich neue/alte Produktlinie



Kaspersky Next EDR Foundations



EDR Optimum











Kaspersky
Endpoint Security
Cloud

Kaspersky
Endpoint Security
Cloud
Cloud



Kaspersky Endpoint Security for Business



Endpoint Security

for Business

Detaillierter Funktionsumfang: Cloud-Schutz & Training

Cloud Discovery & Blocking
Schutz für Security for MS O 365
Data Discovery
SIEM: Export von Ereignissen via Syslog
SIEM: Export von Ereignissen via CE/LEEF
Cybersicherheitstraining für IT-Admins

Next EDR Foundations	Next EDR Optimum	Next XDR Expert	Next Complete Security	KES Cloud	KES Cloud Plus	KES Cloud Pro	KESB Select	KESB Advanced
Nur Cloud Discovery	+	Pro View*	+	Nur Cloud Discovery	+	+	-	-
-	Pro View	Pro View*	Pro View	-	+	+	Add-On für KS4Mail	Add-On für KS4Mail
-	Pro View	Pro View*	Pro View	-	-	+	-	-
Expert View On-Prem	Expert View On-Prem	Expert View On-Prem	Expert View On-Prem	-	-	-	+	+
-	Expert View On-Prem	Expert View On-Prem	Expert View On-Prem	-	-	-	-	On-Prem
-	Pro View	Pro View*	Pro View	-	-	+	-	-

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

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

sseiding, Schutz für Mobile Gerate, 11-5zenanen										
-	+	+	+	-	+	+	-	+		
-	Expert View On-Prem	Expert View On-Prem	Expert View On-Prem	-	-	-	-	+		
+	+	+	+	+ Schutz für Android	+ Schutz für Android	+ Schutz für Android	+	+		
+	Pro View, Expert View On-Prem	Expert View On-Prem	Pro View, Expert View On-Prem	+	+	+	On-Prem	On-Prem		
Nur Vulnerability Assessment	+	+	+	Nur Vulnerability Assessment	+	+	Nur Vulnerability Assessment	+		
-	+	+	+	-	-	+	+	+		
Expert View On-Prem	Expert View On-Prem	+	Expert View On-Prem	-	-	-	-	+		
Expert View On-Prem	Expert View On-Prem	+	Expert View On-Prem	-	-	-	-	+		
-	Expert View On-Prem	+	Expert View On-Prem	-	-	-	-	+		
-	On-Prem	On-Prem	On-Prem	-	-	-	-	On-Prem		

kaspersky

Vergleich neue/alte Produktlinie



Kaspersky Next EDR Foundations



EDR Optimum











Kaspersky
Endpoint Security
Cloud

Kaspersky
Endpoint Security
Cloud
Cloud



Kaspersky Endpoint Security for Business



Kaspersky Endpoint Security for Business

Detaillierter Leistungsumfang: E(X)DR-Funktionen

- EDR-BasisfunktionenUrsachenanalyse
- · IoC Scan
- · Automatisierte Reaktion

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

Next EDR Foundations	Next EDR Optimum	Next XDR Expert	Next Complete Security	KES Cloud	KES Cloud Plus	KES Cloud Pro	KESB Select	KESB Advanced
Nur Ursachenanalyse	+	+	+	-	Nur Ursachenanalyse	+	-	-
-	-	+	-	-	-	-	-	-
-	-	+	-	-	-	-	-	-
-	-	+	-	-	-	-	-	-

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