Marktübersicht Endpoint Detection and Response (EDR), Teil 1

Hersteller	Bitdefender	BlackBerry	Cisco	CrowdStrike	Cybereason	Cynet	Eset	F-Secure	Fortinet	Kaspersky	Malwarebytes
Produktname	Bitdefender GravityZone Ultra	BlackBerry Optics / BlackBerry Guard	Cisco Secure Endpoint	CrowdStrike Falcon	The Cybereason Defense Platform	Cynet 360	ESET Enterprise Inspector	F-Secure Elements Endpoint Detection and Response	FortiEDR	Kaspersky Endpoint Detection and Response	Malwarebytes Endpoint Detection and Response
Lizenzierung											
Lizenzbasis (Gerät / Benutzer)	– / ✓	✓ / ✓	✓ / –	✓ / –	✓ / ✓	✓ / –	✓ / –	✓ / –	✓ / –	✓ / –	✓ / –
allgemein											
Architektur (Endpunktagent / zentrale Konsole / Netzwerksensoren)	✓ / ✓ / ✓	✓ / ✓ / –	✓ / ✓ / –	✓ / ✓ / –	✓ / ✓ / –	✓ / ✓ / –	✓ / ✓ / –	✓ / ✓ / –	✓ / ✓ / ✓	✓ / ✓ / –	✓ / ✓ / –
Betriebsmodelle für das zentrale Management (on Premises / Cloud / Hybrid)	✓ / ✓ / –	✓ / ✓ / ✓	✓ / ✓ / –	– / ✓ / –	✓ / ✓ / ✓	✓ / ✓ / ✓	✓ / – / –	– / ✓ / –	✓ / ✓ / ✓	✓ / – / ✓	– / ✓ / –
unterstützte Betriebssysteme (Windows / Linux / macOS / Android / iOS)	✓ / ✓ / ✓ / – / –	✓ / ✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / – / –	✓ / – / ✓ / – / –	✓ / ✓ / ✓ / – / –	✓ / ✓ / ✓ / – / –	✓ / ✓ / – / – / –	✓ / – / ✓ / – / –
Programmfunktionen unter Linux	EDR, Anti-Malware	EDR, Anti-Malware, Verhaltenskontrolle	EDR, Anti-Malware, Verhaltenskontrolle, Malware-Analyse, DNS-Sicherheit	EDR, Anti-Malware, Verhaltenskontrolle	EDR, Anti-Malware	Anti-Malware, EDR, UEBA, NTA, Deception	n. a.	Anti-Malware, EDR, Vulnerability Management	Anti-Malware, EDR, Endgerätehärtung, Device-Kontrolle	EDR	n. a.
Programmfunktionen unter macOS	EDR, Anti-Malware, Web Threat Protection, Device Control	EDR, Anti-Malware, Verhaltenskontrolle	EDR, Anti-Malware, Verhaltenskontrolle, Malware-Analyse, DNS-Sicherheit	EDR, Anti-Malware, Verhaltenskontrolle	EDR, Anti-Malware	Anti-Malware, EDR, UEBA, NTA, Deception	Anti-Malware, EDR	Anti-Malware, EDR, Vulnerability Management	Anti-Malware, EDR, Endgerätehärtung, Device-Kontrolle	n. a.	EDR
Programmfunktionen unter Android	n. a.	Diagnosefunktionen, Anti-Malware für APK-Dateien, Schutz vor Sideloading, URL-Inspektion, Jailbreak-Erkennung	Anti-Malware für APK-Dateien	Telemetriesensor, Monitoring, App-Isolation,IP-/DNS-Reputationen	Diagnosefunktionen, Anti-Malware für APK-Dateien, Schutz vor Sideloading, URL-Inspektion, Jailbreak-Erkennung, Man-in-the-Middle-Erkennung, Überwachung von Third-Party App Stores	n. a.	n. a.	n. a.	n. a.	n. a.	n. a.
Programmfunktionen unter iOS	n. a.	Diagnosefunktionen, Schutz vor Sideloading, URL-Inspektion, Jailbreak-Erkennung	Anti-Malware, DNS-Sicherheit	Telemetriesensor, Monitoring, IP-/DNS-Reputationen	Diagnosefunktionen, Anti-Malware für APK-Dateien, Schutz vor Sideloading, URL-Inspektion, Jailbreak-Erkennung, Man-in-the-Middle-Erkennung, Überwachung von Third-Party App Stores	n. a.	n. a.	n. a.	n. a.	n. a.	n. a.
Lokationen der Cloud-Daten	USA, EU	weltweit	Nordamerika, EU, Asien-Pazifik	EU, USA	EU, USA, Asien-Pazifik	EU, USA	EU	EU	weltweit	k. A.	USA
unterstützte Sprachen	Englisch, Spanisch, Deutsch, Französisch, Rumänisch, Polnisch, Portugiesisch, Italienisch, Russisch, Tschechisch, Chinesisch, Japanisch	Englisch, Chinesisch, Spanisch, Arabisch, Hindi, Französisch, Russisch	Englisch	Englisch, Japanisch	Englisch, Japanisch	Englisch	Englisch	Englisch, Deutsch, Französisch, Japanisch, Spanisch, Portugiesisch, Italienisch, Finnisch, Schwedisch, Polnisch	Englisch	Englisch, Russisch	Englisch
klassische AV-Funktionen											
statische Analysemethoden (Signaturen / Heuristiken / Hash-Lookups / Codeanalyse / KI-Engine)	✓ / ✓ / ✓ / ✓ / ✓	– / ✓ / – / ✓ / ✓	✓ / ✓ / ✓ / ✓ / ✓	– / ✓ / ✓ / ✓ / ✓	✓ / ✓ / – / – / ✓	✓ / ✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / – / –	✓ / ✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓ / ✓	– / ✓ / – / – / ✓
dynamische Analysemethoden der zentralen Konsole (Sandbox-Analyse / Code-Emulierung)	✓ / ✓	– / –	– / –	✓ / –	– / –	✓ / ✓	✓ / ✓	k. A.	✓ / –	✓ / ✓	✓ / –
integrierte Drittanbieter-Funktionen	–	–	Bitdefender Antivirus, Morphisec Exploit Prevention	–	Bitdefender AV	–	–	–	–	–	–
Logging/Weiterleitung von Events an das zentrale Management											
Dateioperationen (lesen / schreiben / erstellen / löschen)	✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓	– / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓	(✓) / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓	– / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓
Registry-Zugriff (lesen / schreiben / erstellen / löschen)	✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓	– / ✓ / ✓ / ✓	– / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓	– / ✓ / ✓ / ✓	– / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓	– / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓
Netzwerkkommunikation (TCP / UDP / DNS / andere)	✓ / ✓ / ✓ / –	✓ / – / ✓ / –	✓ / – / ✓ / die ersten 25 Netzwerk-Flows jedes Prozesses	✓ / ✓ / ✓ / Verletzungen der lokalen Firewall-Regeln	✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / ICMP	✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / IP	– / – / – / –
Hardwareschnittstellen (USB / Thunderbold / andere)	✓ / – / –	✓ / – / –	– / – / Gerätetreiberdaten	✓ / – / Bluetooth, WLAN	✓ / ✓ / –	✓ / – / CD-ROM	✓ / ✓ / –	k. A.	✓ / – / –	✓ / – / –	– / – / –
Windows-interne Kommunikation (IPC / RPC / COM / andere)	✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / –	k. A.	✓ / ✓ / – / –	✓ / ✓ / ✓ / Erstellen von Named Pipes	✓ / ✓ / ✓ / –	– / – / – / Erstellen von Named Pipes	✓ / ✓ / – / API-Aufrufe	✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / –
Arbeitsspeicherzugriff (Reservierung von Speicher / Schreiben in Speicher fremder Prozesse / Lesen von Speicher fremder Prozesse / andere)	✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / –	k. A.	✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / –	– / ✓ / (✓) / –	– / ✓ / – / –	✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / –
Interaktion mit anderen Prozessen (Starten von Prozessen / Stoppen von Prozessen / Anlegen von Aufgaben / Anlegen von Diensten)	✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓	✓ / – / ✓ / ✓	✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓	✓ / ✓ / (✓) / –	✓ / – / ✓ / ✓	✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓
zusätzliche Überwachung	k. A.	k. A.	Manipulation der lokalen Firewall und Benutzerkontensteuerung, Deaktivierung von Diensten, Änderungen an Schattenkopien, Verwendung von WMI	Laden von Bibliotheken, Starten von Skripten	k. A.	Laden von Bibliotheken	Laden von Bibliotheken, Erstellen/Verändern von Benutzerkonten, Verwendung von WMI, AMSI-Informationen	k. A.	Laden von Bibliotheken	k. A.	k. A.
enthaltene Eventinformationen (gesamte Datei / Metadaten / Dateiheader / Arbeitsspeicherinhalte / andere)	✓ / ✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / – / konfigurierbar	✓ / ✓ / ✓ / – / –	✓ / ✓ / ✓ / ✓ / –	k. A.	– / ✓ / ✓ / – / –	✓ / ✓ / ✓ / – / Datei-Hashes, Dateisignaturen	– / ✓ / – / – / –	– / ✓ / – / – / z. B. Benutzernamen, digitale Zertifikate, Prozessdaten, Produktbeschreibung	✓ / ✓ / ✓ / ✓ / –	– / ✓ / ✓ / – / –
Erkennung/Alarmierung											
Mechanismen zur Erkennung von schadhaftem Verhalten (statisches Regelwerk / musterbasierte IoCs / Punktesystem / andere)	✓ / ✓ / ✓ / –	✓ / ✓ / – / KI-Modell	✓ / ✓ / – / –	✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / KI-Modell	✓ / ✓ / ✓ / Anomalieerkennung	✓ / – / ✓ / –	✓ / ✓ / ✓ / –	✓ / – / – / –	✓ / ✓ / ✓ / –	✓ / ✓ / – / –
Parameter zur manuellen Definition von Ausnahmen bei der Alarmierung im Prozessverhalten (bestimmte Dateioperationen / IP-Adressen, Ports, Protokolle / Windows-interne Kommunikation / Zugriff auf bestimmte Registry-Keys / USB-Gerätedaten / andere)	✓ / ✓ / ✓ / ✓ / ✓ / –	k. A.	– / ✓ / – / – / – / Dateitypen	k. A.	✓ / ✓ / k. A. / k. A. / k. A. / –	✓ / ✓ / ✓ / ✓ / ✓ / Datei-Hashes, Prozesspfad, Prozess-Hashes	✓ / ✓ / ✓ / ✓ / – / beliebige Events	k. A.	– / – / – / – / ✓ / Events und Policies	✓ / ✓ / ✓ / ✓ / – / beliebige Events	✓ / – / – / ✓ / – / –
Parameter zur manuellen Definition von Ausnahmen aufgrund der Prozessumgebung (Datei-Hash / Dateispeicherort / Benutzerkontext / Elternprozess / Dateiherkunft / andere)	✓ / ✓ / ✓ / ✓ / ✓ / –	✓ / ✓ / – / ✓ / – / –	✓ / ✓ / ✓ / ✓ / ✓ / Versionsinformationen von Programmen	✓ / ✓ / – / – / – / –	✓ / ✓ / k. A. / k. A. / ✓ / –	✓ / ✓ / ✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / ✓ / ✓ / Dateisignatur, Dateireputationen	k. A.	✓ / ✓ / ✓ / ✓ / ✓ / –	✓ / ✓ / – / ✓ / – / –	✓ / ✓ / – / ✓ / – / –
Referenzen zum MITRE-ATT&CK-Framework (Taktik / Technik / Empfehlung)	✓ / ✓ / ✓	✓ / ✓ / ✓	✓ / ✓ / ✓	✓ / ✓ / ✓	✓ / ✓ / ✓	✓ / ✓ / –	✓ / ✓ / –	✓ / ✓ / –	✓ / ✓ / –	✓ / ✓ / ✓	✓ / ✓ / –
Beispielkriterien für die Erkennung einer Rechteerweiterung	LSASS-Prozessüberwachung, Verwendung von Mimikatz, unregelmäßige Interprozesskommunikation	LSASS-Prozessüberwachung, Überwachung der Benutzerkontensteuerung	LSASS-Prozessüberwachung, abnormale Benutzung von Named Pipes, Überwachung der Benutzerkontensteuerung	LSASS-Prozessüberwachung, SAM, NTDS.dit, Registry-Operationen, Benutzerkontensteuerung	LSASS-Prozessüberwachung, Überwachung der Benutzerkontensteuerung, Anlegen von Benutzern	LSASS-Prozessüberwachung, Überwachung der Benutzerkontensteuerung, Registry-Operationen, Verwendung von Mimikatz	LSASS-Prozessüberwachung, Überwachung der Benutzerkontensteuerung, Anlegen von Benutzern	k. A.	k. A.	LSASS-Prozessüberwachung, Verwendung von Mimikatz	k. A.
Beispielkriterien für die Erkennung eines Netzwerkscans	Log-in-Versuche	k. A.	k. A.	hohe Anzahl von Verbindungsversuchen	Verwendung verdächtiger Netzwerktools	Deep Packet Inspection, Anomalieerkennung	Deep Packet Inspection	k. A.	k. A.	Suricata-Regeln (mit Netzwerksensor)	k. A.
Beispielkriterien zur Erkennung von Lateral Movement	Unregelmäßigkeiten im SMB-Verkehr, Verwendung von PSEXEC und DCOM, Verwendung bekannter Exploits	k. A.	Verwendung von PSEXEC und WMI, Auslesen von Anmeldedaten	z. B. Verwendung von WMI oder RDP	Verwendung von WMI, PSEXEC, RunAs, Auslesen von Anmeldedaten	Verwendung von WMI, PSEXEC, DCOM, RunAs, Auslesen von Anmeldedaten, Zugriff auf administrative Freigaben	Verwendung von WMI, PSEXEC, PowerShell Remoting, Auslesen von Anmeldedaten, Log-in-Versuche, Schreiben in SMB-Shares	k. A.	k. A.	k. A.	k. A.
Beispielkriterien zur Erkennung von C&C-Kommunikation	IP-Reputationen, Blocklisten, Anomalieerkennung	k. A.	Domain-Reputationen, Verwendung von Net use, WebDav, MSBuild, Installation lokaler Proxydienste	auffällige Verwendung spezieller Netzwerkprotokolle (z. B. DNS), Verwendung von Proxys, Änderungen an der lokalen Firewall, Starten von Netzwerk-Listenern	auffällige Verwendung spezieller Netzwerkprotokolle, Kommunikation mit verdächtigen Adressen	Domain-/IP-Reputationen, auffällige Verwendung spezieller Netzwerkprotokolle (z. B. ICMP, DNS)	Kommunikation mit verdächtigen Adressen	k. A.	k. A.	Suricata-Regeln (mit Netzwerksensor)	IP-Reputationen, Blocklisten
Beispielkriterien zur Erkennung von Datendiebstahl	Deep Packet Inspection: Alarmierung bei Abfluss von Benutzernamen und Passwörtern, Kreditkartendaten, Dokumenten und ZIP-Archiven	Überwachung von Screenshot- und Keylogging-Funktionen	k. A.	k. A.	unregelmäßig hohes Kommunikationsaufkommen, unregelmäßige Dateioperationen	Überwachung von Screenshot- und Keylogging-Funktionen	Überwachung von Screenshot- und Keylogging-Funktionen	k. A.	k. A.	Überwachung von Screenshot- und Keylogging-Funktionen	–
Beispielkriterien zur Erkennung von Ransomware	hohe Anzahl an Verschlüsselungsoperationen, Verwendung bekannter Dateiendungen	k. A.	hohe Anzahl an Dateioperationen (Verschieben, Verschlüsseln, Löschen)	Zugriff auf Schattenkopien, Verwendung von Verschlüsselungsoperationen	Zugriff auf Schattenkopien oder Canary-Dateien	Zugriff auf Canary-Dateien	hohe Anzahl an Dateioperationen (Verschieben, Verschlüsseln, Löschen), Verhaltensanalyse	hohe Anzahl an Dateioperationen	k. A.	Löschen von Schattenkopien, Verschlüsseln oder Löschen wichtiger Dateien	Verschlüsselungsoperationen
Beispielkriterien zur Erkennung schadhafter Office-Makros	Überwachung von API-Aufrufen	k. A.	z. B. Aufruf von PowerShell	z. B. Ausführung von Skripten oder codierten Befehlen	z. B. Aufruf verdächtiger Unterprozesse, WMI, Verhaltensanalyse	Aufruf verdächtiger Unterprozesse wie z. B. WinAPI-Aufrufe	Office-Anwendung, die Prozesse startet	k. A.	z. B. Ausführung von Skripten	k. A.	k. A.
Beispielkriterien zur Erkennung von DLL-Hijacking	k. A.	k. A.	k. A.	k. A.	Laden aus unsicheren Quellen, Reputationen, Speicherort und Dateisignatur	Reputationen, Speicherort und Dateisignatur	Speicherort und Dateisignatur	k. A.	k. A.	k. A.	k. A.
Erkennung von Persistenztechniken (Manipulation der Registry / Aufgabenplanung / Anlegen von Benutzerkonten / andere)	✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / Erstellung von Diensten, WMI-Persistenz	✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / Manipulation des PowerShell-Profils, WMI-Persistenz, Autostart-Manipulation	k. A.	✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / –	✓ / ✓ / – / –
Funktionen zum Schutz vor Exploits (Buffer-Overflow-Schutz / ROP-Schutz / andere)	✓ / ✓ / –	✓ / ✓ / –	– / ✓ / Heap-Spray-Schutz	✓ / ✓ / Heap-Spray-Schutz, Erzwingen von DEP und ASLR, Null Page Allocation, SEHOP	– / – / Limitierung bei der Erstellung von Kindprozessen, Speichermanipulation	k. A.	✓ / ✓ / –	– / – / –	✓ / ✓ / –	✓ / ✓ / –	✓ / ✓ / –
Analyse des Netzwerkverhaltens des Endgeräts	Deep Packet Inspection mit Heuristiken, Regelwerken und Anomalieerkennung	k. A.	Die ersten 25 Netzwerk-Flows jedes Prozesses werden gespeichert.	Überwachung sämtlicher IP-Kommunikation	DNS-/IP-Reputationen, abnormale Verwendung bestimmter Ports und Protokolle, Deep Packet Inspection	Deep Packet Inspection	Deep Packet Inspection	k. A.	k. A.	Überwachung von Netzwerkverkehr und Anomalieerkennung	Überwachung auf Basis von Protokollen und Port
Überwachung bestimmter Netzwerkprotokolle (DNS / HTTP(S) / FTP / SSH / andere)	✓ / ✓ / ✓ / ✓ / ICMP, SSL, RDP, SMTP, POP3, IMAP, MS-Exchange, TelNet, KERBEROS, LDAP, DHCP, VNC, NFS, QUICK, SOCKS, RPC	k. A.	✓ / ✓ / – / – / –	✓ / ✓ / ✓ / ✓ / –	✓ / ✓ / – / – / –	✓ / ✓ / ✓ / ✓ / ICMP	✓ / ✓ / ✓ / ✓ / BitTorrent, DCERCP, IMAP, IRC, POP3, RDP, SIP, SMB, SMB2, SMTP, TOR, VNC, XMPP, RDP	k. A.	✓ / ✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / ✓ / z. B. MSSQL, RDP, SNMP	k. A.
Verwendung von Deception-Techniken	–	–	–	–	Platzierung und Überwachung von Canary-Dateien	Platzierung und Überwachung von Canary-Dateien	–	–	–	Platzierung und Überwachung von Canary-Dateien	–
Möglichkeiten zur benutzerdefinierten Erweiterung der Erkennungsfunktionen	Erstellung eigener Erkennungsregeln	Erstellung eigener Erkennungsregeln	Erstellung eigener Suchabfragen und deren regelmäßige Ausführung	Erstellung eigener Erkennungsregeln und IoCs, über die API	Erstellung eigener Erkennungsregeln	Erstellung eigener Erkennungsregeln, Automatisierungsskripte, über die API	Erstellung eigener Erkennungsregeln, über die API	–	über die API	Import eigener IoA, IoC oder Suricata-Regeln	–
zentrale Sandbox-Analyse											
von der Sandbox unterstützte Dateitypen (ausführbare Dateien / Office-Dokumente / PDFs / Skripte / andere)	✓ / ✓ / ✓ / ✓ / –	✓ / – / – / – / –	✓ / ✓ / ✓ / ✓ / beliebige Dateitypen	✓ / ✓ / ✓ / ✓ / E-Mails, Java-Anwendungen, Linux ELF, SVG	n. a.	✓ / ✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / ✓ / –	k. A.	✓ / ✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / ✓ / –	✓ / – / – / – / –
von der Sandbox unterstützte Betriebssysteme (Windows / Linux / macOS / iOS / Android)	✓ / – / – / – / –	k. A.	✓ / – / – / – / –	✓ / ✓ / – / – / ✓	n. a.	✓ / – / – / – / –	✓ / ✓ / – / – / –	k. A.	✓ / (✓) / – / – / –	✓ / – / – / – / –	✓ / – / – / – / –
zentrales Management											
Darstellung von Incidents (Benutzernamen / Dateinamen / Datei-Hashes / Prozessaufrufbäume / Threat Intelligence / Netzwerkgraphen / Zeitachse)	✓ / ✓ / ✓ / ✓ / ✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓ / – / – / ✓	✓ / ✓ / ✓ / ✓ / ✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓ / ✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓ / ✓ / k. A / ✓	✓ / ✓ / ✓ / ✓ / ✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓ / ✓ / ✓ / – / ✓	✓ / ✓ / ✓ / ✓ / – / – / ✓	✓ / ✓ / ✓ / ✓ / ✓ / ✓ / – / ✓	✓ / ✓ / ✓ / ✓ / ✓ / ✓ / – / –	✓ / ✓ / ✓ / ✓ / ✓ / ✓ / – / –
vordefinierte Benutzerrollen / granular anpassbar / AD-Integration / Multi-Faktor-Authentifizierung	✓ / ✓ / ✓ / ✓	k. A. / ✓ / – / ✓	✓ / (✓) / – / ✓	✓ / (✓) / ✓ / ✓	✓ / – / (✓) / ✓	✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓	(✓) / – / – / –	✓ / – / ✓ / ✓	✓ / ✓ / – / –	✓ / – / ✓ / ✓
maximale Anzahl unterstützter Agenten pro Controllerinstanz	unbegrenzt	unbegrenzt	unbegrenzt (Cloud-Variante), 10 000 (virtuelle Applianace), 100 000 (Hardware-Appliance)	unbegrenzt	unbegrenzt	unbegrenzt	30 000	unbegrenzt	100 000	Windows: 15 000, Linux: 7500	unbegrenzt
Absicherung der Kommunikation zwischen Agent und Managementkonsole	mTLS 1.2	TLS 1.2, SSLv3	TLS 1.2	TLS 1.1 und höher, Zertifikatspinning	TLS, mTLS	verschlüsselte Kommunikation	TLS	TLS	SSL	mTLS	TLS
Dokumentation und Hilfestellung (Handbuch / Trainingsvideos / Schulungen / andere)	✓ / ✓ / ✓ / –	✓ / – / – / Hilfestellung bei der Implementierung	✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / interaktive Anleitung in der Managementoberfläche	✓ / ✓ / ✓ / –	✓ / – / – / –	✓ / ✓ / ✓ / –
Schnittstellen zu SIEM-Plattformen	Splunk, Syslog	Syslog und diverse SIEM-Systeme	Splunk/Phantom, Exabeam, IBM Security, Swimlane, Siemplify	SIEM-Konnektoren über API per Syslog	QRadar, Resilient, Splunk, Demisto, Phantom, ServiceNow, Oracle Cloud Guard, Siemplify, SafeBreach, Vectra, Netskope, Rapid7, Google Chronicle, Sumo Logic, Syslog	z. B. Splunk, QRadar, ArcSight, Elastic	Syslog	Splunk, QRadar	Syslog	Syslog	Syslog, Splunk, QRadar, ArcSight, Azure Sentinel, Logpoint, AlienVault
Reports											
automatische Erstellung von Berichten / konfigurierbar / für einzelne Assets	✓ / ✓ / ✓	✓ / – / ✓	✓ / ✓ / ✓	✓ / ✓ / ✓	✓ / ✓ / ✓	✓ / k. A. / ✓	✓ / ✓ / ✓	✓ / ✓ / –	✓ / – / ✓	✓ / ✓ / –	✓ / ✓ / ✓
Asset-Management											
mögliche Kriterien zur Gruppierung von Geräten	AD-Gruppen	Gerätenamen, Distinguished Name, AD-Gruppen, IP-Adresse, Domain-Name, Betriebssystem	k. A.	z. B. IP, Hostname, Betriebssystem, LDAP-OU, benutzerdefinierte Tags, Gerätehersteller	AD-Gruppen, benutzerdefinierte Tags, Hostname	Betriebssystem, IP-Segment, AD-Gruppen	z. B. AD-Gruppen, benutzerdefinierte Tags, Softwareversionen, Betriebssystem	benutzerdefinierte Tags	k. A.	k. A.	Betriebssystem, Lokation, Policy
Schnittstellen zu ITSM-Tools	k. A.	k. A.	über die API	z. B. ServiceNow über die API	k. A.	k. A.	AD-Integration, über die API	über die API	über die API, ServiceNow	-	ServiceNow, BigFix, über die API
Response-Workflow											
Aufzeichnung administrativer Tätigkeiten (auf den Endgeräten ausgeführte Kommandos / Suchanfragen / Response-Schritte / Zugriff auf Logs / vollständiges Audit-Trail / andere)	✓ / ✓ / ✓ / – / – / –	✓ / ✓ / ✓ / ✓ / ✓ / –	– / ✓ / ✓ / – / – / Anpassen von Richtlinien und Gruppenzugehörigkeiten, Anfertigung eines forensischen Abbilds	✓ / ✓ / ✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / ✓ / ✓ / –	– / – / ✓ / – / – / –	✓ / ✓ / ✓ / ✓ / ✓ / –	✓ / – / ✓ / – / – / –	– / – / ✓ / ✓ / – / –
Alarmierungsmöglichkeiten (E-Mail / SMS / Telefonanruf / andere)	✓ / – / – / –	✓ / – / – / SIEM-Integration	✓ / – / – / API	✓ / – / ✓ / Slack-Benachrichtigung	✓ / ✓ / – / Syslog	✓ / – / ✓ / Mobile App	✓ / – / – / –	✓ / – / – / API	✓ / – / – / –	✓ / – / – / –	✓ / – / – / API
aktive Response-Möglichkeiten über die zentrale Konsole (Stoppen von Prozessen / Dateiwiederherstellung / Fernzugriff per Konsole / Client-Isolation / Löschen von Dateien / andere)	✓ / ✓ / ✓ / ✓ / ✓ / Schwachstellenscan, Sandbox-Analyse	✓ / – / ✓ / ✓ / ✓ / –	– / – / – / ✓ / – / Dateiquarantäne	✓ / ✓ / ✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / ✓ / ✓ / –	✓ / – / ✓ / ✓ / ✓ / Benutzer sperren, Dateiquarantäne	✓ / – / ✓ / ✓ / – / –	– / – / – / ✓ / – / –	✓ / ✓ / – / ✓ / ✓ / –	✓ / ✓ / – / ✓ / ✓ / Starten von Programmen	✓ / ✓ / – / ✓ / – / –
konfigurierbare Auslöser für automatische Response-Schritte	Erreichen eines definierbaren Risikoschwellenwert	k. A.	beliebige Events	beliebige Events	beliebige Events	k. A.	beliebige Events	beliebige Events	beliebige Events ab einer bestimmten Kritikalität	k. A.	n. a.
mögliche automatische Response-Schritte (Stoppen von Prozessen / Unterbrechen von Prozessen / Client-Isolation / Löschen von Dateien / Dateiwiederherstellung / andere)	✓ / – / – / ✓ / ✓ / –	✓ / ✓ / ✓ / ✓ / – / –	– / – / ✓ / – / – / Anfertigung eines forensischen Abbilds, Datei-Analyse	✓ / ✓ / ✓ / ✓ / (✓) / Bereinigung der Registry, Ausführung beliebiger Kommandos und Skripte	✓ / – / ✓ / ✓ / – / –	✓ / ✓ / ✓ / ✓ / ✓ / Benutzer sperren, Dateiquarantäne	✓ / – / ✓ / ✓ / – / –	– / – / ✓ / – / – / –	✓ / – / ✓ / ✓ / ✓ / –	✓ / – / – / ✓ / ✓ / –	n. a.
Möglichkeiten zur manuellen Abfrage von Information vom Endgerät (Dateien / Prozess-Dumps / Prozessliste / forensisch verwertbare Speicherabbilder / andere)	✓ / – / ✓ / – / –	k. A. / k. A. / k. A. / ✓ / –	✓ / – / ✓ / – / –	✓ / ✓ / ✓ / ✓ / Registry-Keys, Datei-Hashes, Forensikdaten über ein spezielles Auswertungstool	✓ / ✓ / ✓ / ✓ / Forensikdaten über ein spezielles Auswertungstool	✓ / ✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / – / diverse Logs	– / – / – / – / Logs, Registry, Netzwerkdiagnosedaten, installierte Software, Interface-Status, bestimmte Systemdateien	✓ / ✓ / – / ✓ / –	✓ / – / ✓ / – / Liste von Dateien	n. a.
Möglichkeiten zur Kollaboration mehrerer Analysten (integriertes Ticket-Tool / Kommentarfunktion / Jira-Integration / andere)	– / ✓ / – / –	– / – / – / Integration in ServiceDesk und Splunk	✓ / ✓ / – / Integration in Cisco SecureX	✓ / ✓ / – / –	– / ✓ / – / –	– / ✓ / – / –	– / ✓ / – / Incident Management System geplant	– / ✓ / – / –	– / ✓ / ✓ / –	✓ / ✓ / – / –	✓ / – / – / –
Threat Hunting											
mögliche Suchkriterien für IoCs (Dateinamen / Datei-Hashes / Registry-Keys / IP-Adressen / Domain-Namen / Netzwerkartefakte / andere)	✓ / ✓ / ✓ / ✓ / ✓ / – / Taktiken und Techniken	✓ / ✓ / ✓ / ✓ / ✓ / – / Prozessparameter	✓ / ✓ / – / ✓ / ✓ / – / TTPs	✓ / ✓ / ✓ / ✓ / ✓ / ✓ / Prozessnamen	✓ / ✓ / ✓ / ✓ / ✓ / ✓ / TTPs, WMI-Aktivitäten, bestimmte Verhaltensmuster, ausgeführte Befehle, Log-in-Versuche	✓ / ✓ / – / ✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / ✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / ✓ / ✓ / – / –	k. A.	✓ / ✓ / ✓ / ✓ / ✓ / ✓ / –	✓ / ✓ / – / ✓ / ✓ / – / Prozess-Hashes
eingebundene Threat-Intelligence-Datenbanken	z. B. Honeypots, VirusTotal, Google, RecordedFuture, TTPs, Telemetriedaten von anderen Kunden	VirusTotal, eigene Threat-Intelligence-Quellen	Cisco Talos, Cisco AMP Dateireputationen, Cisco Umbrella, VirusTotal, und diverse Drittanbieter für Threat Intelligence	eigene Threat Intelligence, VirusTotal, diverse zusätzliche Quellen	eigene Threat Intelligence, VirusTotal	VirusTotal, MalwareBazaar, Cisco Talos, VirusShare, ANY.RUN, Ministerium für Innere Sicherheit der Vereinigten Staaten	VirusTotal, diverse OSINT-Quellen	VirusTotal	FortiGuard Labs, MITRE CVE Datenbank, VirusTotal	Kaspersky Threat Intelligence, VirusTotal	VirusTotal
integrierbare Drittquellen zur Informationsanreicherung	k. A.	k. A.	z. B. AbuseIPDB, AlienVault, CyberCrime Tracker, Farsight Security DNSDB, Google Chronicle, Google Safe Browsing, IsItPhishing, Micrrosoft Graph Securrity API, Pulsedive, Qualys IOC, Security Trials, Shodan, Signal Sciences, Sixgill Darkfeed, SpyCloud, Threatscore	diverse Möglichkeiten über den CrowdStrike Store, z. B. Hunters.ai	G Suite, O365, Azure AD, Salesforce, OKTA, GitHub	diverse Möglichkeiten über die API zu Cynet SIEM	k. A.	–	k. A.	MITRE ATT&CK knowledgebase	–
Integration von externer Werkzeuge während der Analyse	Sandbox-Analyse	k. A.	z. B. TheHive, Phantom, Siemplify	Splunk Phantom, Demisto, Sixgill, RiskIQ, DomainTools, OPSWAT, diverse Möglichkeiten über die API	Sandbox-Analyse	Sandbox-Analyse, Code-Analyse	Sandbox-Analyse, Such-Engines	–	k. A.	Sandbox-Analyse	–
Managed Service											
angebotene Dienstleistungen durch den Hersteller (Management der zentralen Konsole / manuelle Verifikation von Alarmen / Incident Response im Unternehmen / Analyse von Binärdateien / aktive Response-Tätigkeiten / Überwachung der Agenten / Hunting / forensische Analysen / andere)	✓ / ✓ / ✓ / ✓ / ✓ / ✓ / ✓ / ✓ / ✓ / Überwachung von OSINT-Informationen	✓ / ✓ / ✓ / ✓ / ✓ / ✓ / ✓ / ✓ / ✓ / –	k. A.	✓ / ✓ / ✓ / ✓ / ✓ / ✓ / ✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / – / ✓ / ✓ / ✓ / ✓ / ✓ / Analyse der IT-Sicherheit im Unternehmen	✓ / ✓ / ✓ / ✓ / – / – / ✓ / – / –	✓ / ✓ / ✓ / ✓ / ✓ / ✓ / ✓ / ✓ / ✓ / –	k. A.	✓ / ✓ / – / ✓ / ✓ / ✓ / ✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / ✓ / ✓ / ✓ / ✓ / ✓ / ✓ / –	–

✓: ja / vorhanden / trifft zu; –: nein / nicht vorhanden / trifft nicht zu; n. a: nicht anwendbar; k. A.: keine Angabe

Marktübersicht Endpoint Detection and Response (EDR), Teil 2

Hersteller	McAfee	Microsoft	Palo Alto	SentinelOne	Sequretek	Sophos	Trend Micro	Uptycs	WatchGuard	Wazuh
Produktname	McAfee MVISION EDR	Microsoft Defender for Endpoint	Cortex XDR	SentinelOne ActiveEDR	Sequretek EDPR	Intercept X Advanced with EDR	Trend Micro XDR for Users	Endpoint Secure	Panda Adaptive Defense 360	Wazuh
Lizenzierung										
Lizenzbasis (Gerät / Benutzer)	– / ✓	(✓) / ✓	✓ / –	✓ / –	✓ / –	(✓) / ✓	✓ / –	✓ / –	✓ / –	kostenlos / Open Source
allgemein										
Architektur (Endpunktagent / zentrale Konsole / Netzwerksensoren)	✓ / ✓ / ✓	✓ / ✓ / –	✓ / ✓ / ✓	✓ / ✓ / –	✓ / ✓ / –	✓ / ✓ / ✓	✓ / ✓ / ✓	✓ / ✓ / –	✓ / ✓ / –	✓ / ✓ / ✓
Betriebsmodelle für das zentrale Management (on Premises / Cloud / Hybrid)	✓ / ✓ / ✓	– / ✓ / –	– / ✓ / –	✓ / ✓ / –	✓ / ✓ / –	– / ✓ / –	✓ / ✓ / ✓	✓ / ✓ / –	– / ✓ / –	✓ / ✓ / –
unterstützte Betriebssysteme (Windows / Linux / macOS / Android / iOS)	✓ / ✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / – / –	✓ / ✓ / ✓ / – / –	✓ / ✓ / ✓ / – / –	✓ / ✓ / ✓ / – / –	✓ / ✓ / ✓ / – / –	✓ / ✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / – / –
Programmfunktionen unter Linux	EDR	EDR, Anti-Malware, Verhaltensanalyse, Vulnerability Management	EDR, Anti-Malware	EDR, Anti-Malware, Verhaltensanalyse	EDR, Patch-Management	EDR, Anti-Malware	EDR, Anti-Malware, Endgerätehärtung, Web Threat Protection, Application Control, Exploit-Schutz, Integritätsschutz von Dateien	EDR	EDR, Anti-Malware, Web Threat Protection	EDR, Anti-Malware, Endgerätehärtung
Programmfunktionen unter macOS	EDR	EDR, Anti-Malware, Verhaltensanalyse, Vulnerability Management	EDR, Anti-Malware	EDR, Anti-Malware, Verhaltensanalyse, Device Control	EDR	EDR, Anti-Malware	EDR, Anti-Malware, Endgerätehärtung, Web Threat Protection, Device Control, Integritätsschutz von Dateien	EDR	EDR, Anti-Malware, Web Threat Protection	EDR, Anti-Malware, Endgerätehärtung
Programmfunktionen unter Android	Telemetriedaten über MVISION Mobile, Anti-Malware	Web Threat Protection, Anti-Malware	Anti-Malware	n. a.	n. a.	n. a.	n. a.	n. a.	Anti-Malware, Anti-Theft, Remote Whipe	n. a.
Programmfunktionen unter iOS	Telemetriedaten über MVISION Mobile, Anti-Malware	Web Threat Protection, Anti-Malware	n. a.	n. a.	n. a.	n. a.	n. a.	n. a.	n. a.	n. a.
Lokationen der Cloud-Daten	USA, Deutschland, Singapur, Australien	USA, UK, EU	USA, EU, Singapur, Kanada, Japan, Australien	USA, EU, Asien-Pazifik	USA, Indien	Deutschland, Irland, USA	EU	USA, Australien	EMEA	USA, EU, Singapur
unterstützte Sprachen	Englisch, Deutsch, Französisch, Spanisch, Japanisch	Englisch	Englisch	Englisch, Deutsch, Französisch, Spanisch, Italienisch, Japanisch	Englisch	Deutsch, Englisch, Spanisch, Französisch, Italienisch, Portugiesisch, Japanisch, Chinesisch, Koreanisch	Englisch, Japanisch	Englisch	Englisch, Französisch, Deutsch, Ungarisch, Italienisch, Japanisch, Portugiesisch, Russisch, Spanisch, Schwedisch	Englisch
klassische AV-Funktionen										
statische Analysemethoden (Signaturen / Heuristiken / Hash-Lookups / Codeanalyse / KI-Engine)	✓ / ✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / – / ✓	✓ / – / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓ / ✓	– / – / ✓ / – / –	✓ / ✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓ / –
dynamische Analysemethoden der zentralen Konsole (Sandbox-Analyse / Code-Emulierung)	✓ / ✓	✓ / ✓	✓ / –	– / –	✓ / –	– / –	✓ / –	–	✓ / ✓	–
integrierte Drittanbieter-Funktionen	Windows Defender kann optional verwendet werden	–	–	–	–	–	–	–	–	optionale Integration von AV-Engines
Logging/Weiterleitung von Events an das zentrale Management										
Dateioperationen (lesen / schreiben / erstellen / löschen)	✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓	– / ✓ / ✓ / ✓	– / ✓ / ✓ / ✓	✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓	– / – / ✓ / –	✓ / ✓ / ✓ / ✓	prüft, ob ausgewählte Dateien verändert wurden
Registry-Zugriff (lesen / schreiben / erstellen / löschen)	✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓	– / ✓ / ✓ / ✓	– / ✓ / ✓ / ✓	– / ✓ / ✓ / –	✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓	– / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓	prüft, ob ausgewählte Einträge verändert wurden
Netzwerkkommunikation (TCP / UDP / DNS / andere)	✓ / ✓ / ✓ / HTTP, HTTPS	✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / Socket-Events, HTTP	✓ / ✓ / ✓ / –	✓ / – / ✓ / –	✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / –	– / – / ✓ / HTTP, Socket-Kommunikation	✓ / ✓ / ✓ / –	– / – / – / – / Interfaces und offene Ports
Hardwareschnittstellen (USB / Thunderbold / andere)	✓ / ✓ / z. B. Bluetooth, PCI	✓ / ✓ / –	–	✓ / – / Bluetooth, Bluetooth LE	✓ / – / –	k. A.	✓ / ✓ / Bluetooth	k. A.	✓ / ✓ / –	–
Windows-interne Kommunikation (IPC / RPC / COM / andere)	✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / k. A.	– / ✓ / – / Systemaufrufe	n. a.	✓ / ✓ / ✓ / –	k. A.	✓ / ✓ / ✓ / WMI	✓ / – / – / –	✓ / ✓ / ✓ / –	– / – / – / Systemaufrufe
Arbeitsspeicherzugriff (Reservierung von Speicher / Schreiben in Speicher fremder Prozesse / Lesen von Speicher fremder Prozesse / andere)	✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / –	k. A.	– / ✓ / ✓ / –	– / – / – / Zugriff auf geteilten Speicher	✓ / ✓ / ✓ / –	–
Interaktion mit anderen Prozessen (Starten von Prozessen / Stoppen von Prozessen / Anlegen von Aufgaben / Anlegen von Diensten)	✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / ✓	✓ / – / ✓ / ✓	✓ / ✓ / ✓ / ✓	✓ / – / ✓ / ✓	✓ / ✓ / ✓ / –	✓ / – / – / –	✓ / ✓ / ✓ / ✓	Linux-Logs
zusätzliche Überwachung	z. B. API-Calls, Laden von Bibliotheken	Image Load Events, Änderungen an der Firmware	Windows-Event-Log, Benutzer-Sessions, Gerätestatus	Benutzer-Sessions, Gerätestatus, Netzwerkstatus, Firewallstatus	k. A.	k. A.	k. A.	Benutzer-Sessions, Benutzeraktivitäten, Zugriffe auf Peripheriegeräte	k. A.	Systemaufrufe
enthaltene Eventinformationen (gesamte Datei / Metadaten / Dateiheader / Arbeitsspeicherinhalte / andere))	– / ✓ / – / – / –	– / ✓ / ✓ / – / –	– / ✓ / – / – / –	– / ✓ / – / – / –	k. A.	– / – / – / – / Datei-Hashes, URLs	– / ✓ / – / – / –	– / ✓ / – / – / Compliancestatus	– / ✓ / – / – / –	k. A.
Erkennung/Alarmierung										
Mechanismen zur Erkennung von schadhaftem Verhalten (statisches Regelwerk / musterbasierte IoCs / Punktesystem / andere)	✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / IoA, verdächtiges Verhalten	✓ / ✓ / k. A. / Anomalieerkennung	✓ / ✓ / ✓ / Anomalieerkennung	✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / –	–	✓ / – / ✓ / –	✓ / ✓ / ✓ / –	✓ / ✓ / – / –
Parameter zur manuellen Definition von Ausnahmen bei der Alarmierung im Prozessverhalten (bestimmte Dateioperationen / IP-Adressen, Ports, Protokolle / Windows-interne Kommunikation / Zugriff auf bestimmte Registry-Keys / USB-Gerätedaten / andere)	– / – / – / – / – / Prozesspfade, Kommandozeilenaufrufe, Dateipfade	✓ / ✓ / ✓ / ✓ / ✓ / k. A.	✓ / ✓ / ✓ / ✓ / – / beliebige Events	beliebige Events mit Unterstützung des Supports	✓ / ✓ / ✓ / ✓ / ✓ / –	k. A.	✓ / ✓ / – / ✓ / – / –	✓ / ✓ / ✓ / ✓ / – / beliebige Events	– / – / – / – / – / Dateimerkmale, Prozessverhalten	✓ / ✓ / ✓ / ✓ / ✓ / – / beliebige Events
Parameter zur manuellen Definition von Ausnahmen aufgrund der Prozessumgebung (Datei-Hash / Dateispeicherort / Benutzerkontext / Elternprozess / Dateiherkunft / andere)	✓ / ✓ / ✓ / ✓ / – / –	✓ / ✓ / ✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / ✓ / ✓ / –	✓ / ✓ / – / – / – / –	✓ / ✓ / – / ✓ / – / –	✓ / – / – / ✓ / – / –	✓ / ✓ / – / – / ✓ / Signaturen	✓ / ✓ / – / ✓ / – / –
Referenzen zum MITRE-ATT&CK-Framework (Taktik / Technik / Empfehlung)	✓ / ✓ / ✓	✓ / ✓ / ✓	✓ / ✓ / ✓	✓ / ✓ / ✓	✓ / ✓ / ✓	✓ / ✓ / –	✓ / ✓ / –	✓ / ✓ / ✓	✓ / ✓ / ✓	✓ / ✓ / ✓
Beispielkriterien für die Erkennung einer Rechteerweiterung	LSASS-Prozessüberwachung, Benutzererstellung, UAC-Bypass	k. A.	LSASS-Prozessüberwachung, UAC-Bypass, Named Pipe Impersonation	z. B. LSASS Prozessüberwachung, UAC-Bypass	k. A.	z. B. Zugriff auf die SAM Datenbank, UAC-Bypass	z. B. LSASS-Prozessüberwachung, Prozessintegrität, UAC-Bypass	LSASS-Prozessüberwachung, Prozessintegrität, UAC-Bypass, Verwendung von Mimikatz	Allowlist von Prozessketten, basierend auf Machine Learning und Threat-Intelligence-Daten	Modifizierungen von Nutzern und Gruppen, verdächtige Befehlsausführungen
Beispielkriterien für die Erkennung eines Netzwerkscans	k. A.	k. A.	Verwendung verdächtiger Netzwerk-Tools	n. a.	k. A.	k. A.	k. A.	Verwendung verdächtiger Netzwerktools, YARA-Regeln	Allowlist von Prozessketten, basierend auf Machine Learning und Threat-Intelligence-Daten	k. A.
Beispielkriterien zur Erkennung von Lateral Movement	Unregelmäßigkeiten im SMB-Verkehr, Verwendung von PSEXEC, Verwendung verdächtiger Werkzeuge	k. A.	z. B. unübliche Verwendung von WinRM/WinRS	Verwendung von PSEXEC, WMI, Net use, DCOM, RPC	k. A.	z. B. Verwendung von SMB, DCI oder wmci	z. B. Unregelmäßigkeiten im SMB-Verkehr, Verwendung von PSEXEC	Verwendung von PSEXEC, WMI oder PowerShell	Allowlist von Prozessketten, basierend auf Machine Learning und Threat-Intelligence-Daten	Verwendung verdächtiger Prozesse
Beispielkriterien zur Erkennung von C&C-Kommunikation	auffällige Verwendung spezieller Netzwerkprotokolle, IP-/DNS-Reputation	auffällige Verwendung spezieller Netzwerkprotokolle, Kommunikation mit verdächtigen Adressen	Verwendung des Tor-Netzwerks, Aufbau eines SSH-Tunnels, auffällige Verwendung spezieller Netzwerkprotokolle	Erkennung verbreiteter C2-Werkzeuge	k. A.	IP-Reputationen	auffällige Verwendung spezieller Netzwerkprotokolle, IP-/DNS-Reputation	verdächtige Verwendung von Werkzeugen wie PowerShell, wscript, cscript, wget, curl und rsync	Allowlist von Prozessketten, basierend auf Machine Learning und Threat-Intelligence-Daten	verdächtige Portfreigaben
Beispielkriterien zur Erkennung von Datendiebstahl	Überwachung von Screenshot- und Keylogging-Funktionen	k. A.	Nutzung von Werkzeugen wie curl, wget oder BitTorrent, unüblich große Uploadrate zu unbekannten Zielen	Überwachung von Screenshot- und Keylogging-Funktionen	k. A.	k. A.	Überwachung bekannter Übertragungswege wie USB, SMB oder FTP	Überwachung von Screenshot- und Keylogging-Funktionen	Allowlist von Prozessketten, basierend auf Machine Learning und Threat-Intelligence-Daten	Verbindungen zu bekannten Datenübertragungsports
Beispielkriterien zur Erkennung von Ransomware	Verhaltensanalyse	Zugriff auf geschützte Ordner, Office-Anwendung, die Prozesse startet	Zugriff auf Canary-Dateien	Ändern/Löschen von Dateien, die nicht in Verbindung mit dem Quellprozess stehen	k. A.	hohe Anzahl veränderter Dateien in einer bestimmten Zeit	Dateioperationen	Löschen von Schattenkopien mithilfe von vssadmin	Allowlist von Prozessketten, basierend auf Machine Learning und Threat-Intelligence-Daten	Dateiintegritätsüberwachung
Beispielkriterien zur Erkennung schadhafter Office-Makros	Office-Anwendung, die Prozesse startet	Office-Anwendung, die Prozesse startet	Verhaltensanalyse, Office-Anwendung, die Prozesse startet	spezifische Verhaltensanalyse für Makros	Erkennung bestimmter Schlüsselwörter in Makros	Verhaltensanalyse, Office-Anwendung, die eine PowerShell startet	Verhaltensanalyse	Office-Anwendung, die Prozesse startet	Allowlist von Prozessketten, basierend auf Machine Learning und Threat-Intelligence-Daten	Verhaltensanalyse, verdächtige Dateioperationen
Beispielkriterien zur Erkennung von DLL-Hijacking	k. A.	k. A.	Laden einer DLLs von unsicheren Orten	Überwachung von DLL-Load Events, Laden unsignierter Bibliotheken	k. A.	k. A.	Reputationen und Dateisignatur	Überwachung von DLL-Load Events	Allowlist von Prozessketten, basierend auf Machine Learning und Threat-Intelligence-Daten	k. A.
Erkennung von Persistenztechniken (Manipulation der Registry / Aufgabenplanung / Anlegen von Benutzerkonten / andere)	✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / Laden von Kernelmodulen	✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / Erstellen von Systemprozessen, Autostart-Manipulation, Browser-Erweiterung	✓ / ✓ / ✓ / Manipulation des PowerShell-Profils, WMI-Persistenz, Autostart-Manipulation	✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / –
Funktionen zum Schutz vor Exploits (Buffer-Overflow-Schutz / ROP-Schutz / andere)	✓ / – / –	✓ / ✓ / –	✓ / ✓ / Heap-Spray-Schutz, Schutz des Elternprozesses	k. A.	✓ / ✓ / –	✓ / ✓ / Heap-Spray-Schutz, Erkennen von Reflective DLL Injection	✓ / ✓ / –	–	✓ / ✓ / –	– / – / Integration von Windows Defender Exploit Guard
Analyse des Netzwerkverhaltens des Endgeräts	Anomalieerkennung, Deep Packet Inspection möglich mit zusätzlichem Modul	Anomalieerkennung	Überwachung von Netzwerkverkehr	n. a.	k. A.	k. A.	Deep Packet Inspection	Socket-Events, DNS-Lookups, HTTP-Kommunikation	Deep Packet Inspection, Anomalieerkennung	n. a.
Überwachung bestimmter Netzwerkprotokolle (DNS / HTTP(S) / FTP / SSH / andere)	✓ / ✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / – / –	✓ / ✓ / – / – / –	– / – / – / – / –	– / ✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / ✓ / –	✓ / ✓ / – / – / –	✓ / ✓ / ✓ / ✓ / –	n. a.
Verwendung von Deception-Techniken	n. a.	k. A.	Platzierung und Überwachung von Canary-Dateien	Platzierung und Überwachung von Canary-Dateien	Platzierung und Überwachung von Canary-Dateien	k. A.	–	–	–	Honeypot-Ordner
Möglichkeiten zur benutzerdefinierten Erweiterung der Erkennungsfunktionen	Erstellung eigener Erkennungsregeln	Erstellung eigener Erkennungsregeln	Importieren eigener IoCs, Import eigener hashbasierter Block- oder Allowlists	Erstellung eigener Erkennungsregeln über die API, z. B. basierend auf IoCs oder Prozessaktivitäten	k. A.	benutzerdefinierte Echtzeitanfragen an Clients, über die API	über die API	Erstellung eigener Erkennungsregeln, Hinzufügen von YARA-Regeln	–	Erstellung eigener Erkennungsregeln
zentrale Sandbox-Analyse										
von der Sandbox unterstützte Dateitypen (ausführbare Dateien / Office-Dokumente / PDFs / Skripte / andere)	✓ / ✓ / ✓ / ✓ / APK	✓ / – / – / ✓ / –	✓ / ✓ / ✓ / ✓ / APK, Linux ELF	n. a.	✓ / ✓ / ✓ / – / –	✓ / ✓ / ✓ / – / –	✓ / ✓ / ✓ / ✓ / –	n. a.	✓ / – / – / – / –	n. a.
von der Sandbox unterstützte Betriebssysteme (Windows / Linux / macOS / iOS / Android)	✓ / – / – / – / ✓	k. A.	✓ / ✓ / ✓ / – / ✓	n. a.	✓ / ✓ / – / – / –	✓ / – / – / – / –	✓ / – / ✓ / – / –	n. a.	✓ / – / – / – / –	n. a.
zentrales Management										
Darstellung von Incidents (Benutzernamen / Dateinamen / Datei-Hashes / Prozessaufrufbäume / Threat Intelligence / Netzwerkgraphen / Zeitachse)	✓ / ✓ / ✓ / ✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / – / – / – / ✓	✓ / ✓ / ✓ / ✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓ / ✓ / – / ✓	✓ / ✓ / ✓ / ✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / ✓ / ✓ / ✓ / ✓	– / ✓ / ✓ / ✓ / – / ✓ / –	✓ / ✓ / ✓ / ✓ / ✓ / ✓ / ✓	– / ✓ / – / ✓ / – / – / –
vordefinierte Benutzerrollen / granular anpassbar / AD-Integration / Multi-Faktor-Authentifizierung	✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓	✓ / – / ✓ / ✓	✓ / ✓ / – / –	✓ / ✓ / – / ✓	✓ / ✓ / ✓ / ✓
maximale Anzahl unterstützter Agenten pro Controllerinstanz	unbegrenzt	unbegrenzt	unbegrenzt	unbegrenzt	unbegrenzt	unbegrenzt	unbegrenzt	unbegrenzt	unbegrenzt	1500
Absicherung der Kommunikation zwischen Agent und Managementkonsole	z. B. AES256	TLS mit Zertifikatsvalidierung	TLS	TLS	HTTPS	TLS mit Zertifikatspinning	mTLS	TLS 1.3	TLS	AES
Dokumentation und Hilfestellung (Handbuch / Trainingsvideos / Schulungen / andere)	✓ / ✓ / ✓ / Capture the Flag Workshop, Architektur-Workshop	✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / –	✓ / – / ✓ / –	✓ / – / ✓ / –	✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / –	✓ / – / – / –	✓ / ✓ / ✓ / –	✓ / – / – / –
Schnittstellen zu SIEM-Plattformen	Syslog, QRadar, Splunk	Splunk, ArcSight	Syslog	z. B. Syslog, Splunk, QRadar	Syslog	z. B. Splunk, Rapid7, LogRhythm, Cortex XSOAR	Splunk, STIX/TAXII, QRadar	Splunk, Palo Alto Cortex, SumoLogic	SIEM-Feeder als zusätzliches Modul erhältlich	Splunk, Syslog
Reports										
automatische Erstellung von Berichten / konfigurierbar / für einzelne Assets	✓ / ✓ / ✓	✓ / ✓ / ✓	✓ / ✓ / ✓	✓ / ✓ / ✓	✓ / ✓ / ✓	✓ / ✓ / ✓	–	✓ / ✓ / ✓	✓ / ✓ / ✓	✓ / ✓ / ✓
Asset-Management										
mögliche Kriterien zur Gruppierung von Geräten	AD-Gruppen, IP-Segment	AD-Gruppen, Namenskonvention, Betriebssysteme	AD-Gruppen, IP-Segment, Domain, Agent-Version	z. B. AD-Gruppen, IP-Ranges, Domains, Agent-Version, Tags, Endpunktname, OS-Version	AD-Gruppen	AD-Gruppen	–	Tags	AD-Gruppen, IP-Segment	k. A.
Schnittstellen zu ITSM-Tools	CMDB, AD-Integration, weitere über die API	CMDB, Azure AD, Helpdesk	AD-Integration, über die API	über die API	CMDB, AD-Integration	AD-Integration, über die API, ConnectWise, Kaseya, AUTOTASK	über die API	z. B. ServiceNow, JIRA	über die API	über die API
Response-Workflow										
Aufzeichnung administrativer Tätigkeiten (auf den Endgeräten ausgeführte Kommandos / Suchanfragen / Response-Schritte / Zugriff auf Logs / vollständiges Audit-Trail / andere)	✓ / – / ✓ / – / – / –	✓ / ✓ / ✓ / – / – / –	✓ / ✓ / ✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / ✓ / ✓ / –	✓ / – / ✓ / – / ✓ / –	✓ / – / ✓ / – / – / –	✓ / ✓ / ✓ / ✓ / ✓ / –	✓ / – / – / – / – / –	– / ✓ / ✓ / ✓ / ✓ / –
Alarmierungsmöglichkeiten (E-Mail / SMS / Telefonanruf / andere)	✓ / ✓ / ✓ / Syslog, API, SIEM	✓ / ✓ / – / PowerAutomate, Teams	✓ / – / – / Slack, Syslog	✓ / – / – / Syslog, API, Slack	k. A.	✓ / – / – / API	✓ / – / ✓ / –	✓ / – / – / Slack, PagerDuty	✓ / – / – / –	✓ / – / – / Slack, API
aktive Response-Möglichkeiten über die zentrale Konsole (Stoppen von Prozessen / Dateiwiederherstellung / Fernzugriff per Konsole / Client-Isolation / Löschen von Dateien / andere)	✓ / ✓ / – / ✓ / ✓ / Reboot, Herunterfahren, Log-out, Dumpen eines Prozessspeichers, Löschen von Registry-Werten	✓ / ✓ / ✓ / ✓ / – / –	✓ / ✓ / ✓ / ✓ / ✓ / Schwachstellenscan	✓ / ✓ / ✓ / ✓ / ✓ / –	k. A. / k. A. / ✓ / k. A. / k. A. / k. A.	✓ / ✓ / ✓ / ✓ / ✓ / –	✓ / – / – / ✓ / ✓ / Blockade von IPs, Domains, URLs oder E-Mails	✓ / – / – / ✓ / ✓ / DNS-Blockaden	– / ✓ / – / ✓ / ✓ / Schwachstellenscan	– / – / – / ✓ / ✓ / Schwachstellenscan, Deaktivierung von Benutzerkonten, Blockieren von IPs oder Ports
konfigurierbare Auslöser für automatische Response-Schritte	beliebige Events	k. A.	beliebige Events über die API	beliebige Events	k. A.	beliebige Events	beliebige Events über die API	–	Verstöße gegen Allowlist-basiertes Regelwerk	k. A.
mögliche automatische Response-Schritte (Stoppen von Prozessen / Unterbrechen von Prozessen / Client-Isolation / Löschen von Dateien / Dateiwiederherstellung / andere)	✓ / – / ✓ / ✓ / ✓ / weitere über Custom-Reactions	k. A.	– / – / – / – / – / Quarantäne für Dateien	✓ / ✓ / ✓ / ✓ / ✓ / Quarantäne für Dateien, Hochladen von Dateien	k. A.	✓ / – / ✓ / ✓ / ✓ / –	✓ / – / ✓ / ✓ / – / –	n. a.	✓ / ✓ / ✓ / ✓ / ✓ / –	– / – / ✓ / ✓ / – / AV-Scan, Blockade von IPs und Ports
Möglichkeiten zur manuellen Abfrage von Information vom Endgerät (Dateien / Prozess-Dumps / Prozessliste / forensisch verwertbare Speicherabbilder / andere)	✓ / ✓ / ✓ / – / –	✓ / ✓ / ✓ / ✓ / –	✓ / – / – / – / Ausführen von Skripten	✓ / ✓ / ✓ / ✓ / Ausführen von Skripten	✓ / – / ✓ / ✓ / –	✓ / – / ✓ / – / Windows-Logs	k. A.	✓ / ✓ / ✓ / ✓ / –	✓ / – / ✓ / – / –	–
Möglichkeiten zur Kollaboration mehrerer Analysten (integriertes Ticket-Tool / Kommentarfunktion / Jira-Integration / andere)	✓ / ✓ / – / –	✓ / – / – / –	– / ✓ / – / –	– / ✓ / – / Status	✓ / – / ✓ / –	– / ✓ / ✓ / –	✓ / ✓ / – / –	✓ / ✓ / – / –	✓ / – / – / –	– / – / ✓ / –
Threat Hunting										
mögliche Suchkriterien für IoCs (Dateinamen / Datei-Hashes / Registry-Keys / IP-Adressen / Domain-Namen / Netzwerkartefakte / andere)	✓ / ✓ / ✓ / ✓ / ✓ / ✓ / z. B. Umgebungsvariablen, installierte Treiber, USB-Geräte	✓ / ✓ / – / ✓ / – / ✓ / –	✓ / ✓ / ✓ / ✓ / ✓ / – / –	✓ / ✓ / ✓ / ✓ / ✓ / – / alle übermittelten Daten	✓ / ✓ / k. A. / ✓ / ✓ / – / –	✓ / ✓ / ✓ / ✓ / ✓ / – / –	✓ / ✓ / ✓ / ✓ / ✓ / ✓ / Taktiken und Techniken	– / ✓ / ✓ / ✓ / ✓ / – / –	✓ / ✓ / ✓ / ✓ / ✓ / ✓ / Hashes von Prozessketten, Prozessaktivitäten	✓ / ✓ / ✓ / ✓ / ✓ / – / –
eingebundene Threat-Intelligence-Datenbanken	McAfee GTI, VirusTotal, Phishtank, MVISION Insights	Microsoft Global Threat Optics, diverse Drittanbieter, z. B. Anomali, RiskIQ	VirusTotal, Palo Alto Networks AutoFocus Threat Intelligence Service	VirusTotal, Recorded Future, eigene Threat Intelligence, weitere über API	VirusTotal	–	Trend Micro Smart Protection Network	VirusTotal	–	VirusTotal, AlienVault OTX
integrierbare Drittquellen zur Informationsanreicherung	McAfee-TI-Quellen, VirusTotal, Phishtank, ThreatQ, ThreatConnect, MISP, The Hive, Phantom, ServiceNow	Microsoft 365 XDR und SIEM	k. A.	über die API	Syslog	k. A.	über STIX/TAXII, z. B. Checkpoint, QRadar, Palo Alto	k. A.	Splunk, QRadar	k. A.
Integration externer Werkzeuge während der Analyse	Sandbox-Analyse, Threat-Intelligence-Quellen, diverse Möglichkeiten über die API	z. B. AttackIQ, AzureSentinel, QRadar, Splunk, Demisto, ServiceNow, Swimlane, ThreatConnect, Aruba	Sandbox-Analyse, Threat-Intelligence-Quellen, Firewall	z. B. RecordedFuture, QRadar, Netskope, Splunk, VirusTotal	k. A.	diverse Möglichkeiten über die API	Firewall	Sandbox-Analyse, diverse Möglichkeiten über die API	–	diverse Möglichkeiten über die API
Managed Service										
angebotene Dienstleistungen durch den Hersteller (Management der zentralen Konsole / manuelle Verifikation von Alarmen / Incident Response im Unternehmen / Analyse von Binärdateien / aktive Response-Tätigkeiten / Überwachung der Agenten / Hunting / forensische Analysen / andere)	✓ / – / – / ✓ / – / – / – / – / weitere über zertifizierte Partner	✓ / – / ✓ / – / ✓ / ✓ / ✓ / – / –	✓ / ✓ / ✓ / k. A. / ✓ / ✓ / ✓ / ✓ / k. A.	– / ✓ / ✓ / ✓ / ✓ / ✓ / ✓ / –	✓ / ✓ / – / – / ✓ / – / ✓ / – / –	– / ✓ / – / ✓ / ✓ / ✓ / ✓ / ✓ / –	✓ / ✓ / ✓ / ✓ / ✓ / ✓ / ✓ / ✓ / –	k. A.	✓ / ✓ / ✓ / ✓ / ✓ / ✓ / ✓ / ✓ / –	–

✓: ja / vorhanden / trifft zu; –: nein / nicht vorhanden / trifft nicht zu; n. a: nicht anwendbar; k. A.: keine Angabe