Produkt-Code: **CIXE** = Central Intercept X Essentials | **CIXA** = Central Intercept X Advanced | **CIXAXDR** = Central Intercept X Advanced with XDR | **SVRCIXE** = Central Intercept X Essentials for Server | **SVRCIXA** = Central Intercept X Advanced for Server | **SVRCIXAXDR** = Central Intercept X Advanced with XDR for Server | **MDR-COMPLETE** = Central Managed Detection and Response Complete

Beschreibung der Anforderungen	Wichtigkeit	MDR-COMPLETE	SVRMDR-COMPLETE	Bemerkung
Zentrale Verwaltung				
Die zentrale Verwaltung wird als SaaS Lösung bereitgestellt		x	x	
Die Verwaltungsdaten werden in einem deutschen Rechenzentrum gespeichert	!	x	x	
Das deutsche Rechenzentrum verfügt über ein Testat nach den Anforderungen des Anforderungskatalogs Cloud Computing (Cloud Computing Compliance Controls Catalogue, C5) des Bundesamts für Sicherheit in der Informationstechnik (BSI)		x	x	
Es sind weitere Rechenzentren in USA und Europa verfügbar		x	x	
Die Verwaltungsoberfläche kann über einen Web-Browser bedient werden		x	x	
Alle geforderten Funktionalitäten können über eine gemeinsame, zentrale Verwaltung bedient werden	!	x	x	
Die zentrale Verwaltungsöberfläche und die dazugehörige Dokumentation/Hilfe wird in folgenden Sprachen angeboten:				
Deutsch		x	x	
Englisch		x	x	
Fränzösich		x	x	
Spanisch		x	x	
Portugiesisch		x	x	
Italienisch		x	x	
Japanisch		x	x	
Chinesisch		x	x	
Koreanisch		x	x	
Import von Benutzer-/gruppen ist über Active Directory Anbindung möglich		x	x	
Der Active Directory Synchronisationsdienst erfüllt folgende Anforderungen:				
Kann auf Windows Server Systemen installiert und betrieben werden		x	x	
Verschlüsselte Kommunikation per LDAP over SSL (LDAPS)		x	x	
LDAP Port ist konfigurierbar		x	x	
Für eine erfolgreiche Kommunikation müssen keine Port von außen (Internet) nach innen (LAN) geöffnet werden		x	x	
Unterstützt Umgebung mit mehreren AD-Domains		x	x	
Unterstützt den Import von Benutzer- und Gruppen Objekten		x	x	
Unterstützt den Import von Organisationseinzeit (OU, organizational unit)		x	x	
Unterstützt den Import von Computer-Objekten		x	x	
Die Suchbereiche für den Import von Benutzer- und Gruppen-Objekten per Distinguished Name können vorgegeben werden		x	x	
Beliebige LDAP-Filter können anhand von Attributen zur Einschränkung der Objektauswahl definiert werden		x	x	
Automatisiert Synchronisation auf Basis definierbarer Intervalle: zweimal täglich / täglich (Uhrzeiten), wöchentlich (Wochentag/Uhrzeit) / mehrfach monatlich (Anzahl / Uhrzeit)		x	x	
Interne Benutzerverwaltung: Benutzer-/gruppen können manuell über die Verwaltungsoberfläche erzeugt werden		x	x	
Die Listen der Computer, Server und Benutzer im Verwaltungssystem lassen sich als CSV-Datei exportieren.		x	x	
Die Azure AD-Synchronisierung erfüllt folgende Anforderungen:				
Synchronisierung aller Benutzer und Gruppen		x	x	
Benutzer über Gruppen-ID hinzufügen		x	x	
Benutzer über Gruppen-Filter hinzufügen		x	x	
Benutzer über Benutzer-Filter hinzufügen		x	x	
Die Richtlinienverwaltung erfüllt folgende Anforderungen: Eine Richtline kann vom Administrator ...				
einem oder mehreren Benutzerobjekten zugewiesen werden		x		
einer oder mehreren Benutzergruppen zugewiesen werden	!	x		
einem oder mehreren Computer / Server / Gerät zugewiesen werden		x	x	
einer oder mehreren Computer-, Server-, Geräte-Gruppe zugewiesen werden	!	x	x	
jederzeit manuell aktiviert oder deaktiviert werden, ohne dass die Zuweisung geändert werden müsste		x	x	
automatisch zu einem definierbaren Zeitpunkt (Datum und Uhrzeit) deaktiviert werden		x	x	
Die Richtlinienverwaltung ermöglicht die Erstellung mehrerer invidueller Richtlinien		x	x	
Richtlinienverteilung: Änderungen an zentralen Vorgaben sowie Richtlinienänderungen werden auch dann umgehend an alle betroffenen System verteilt, wenn Systeme nicht mit dem LAN verbunden sind (auch keine VPN Verbindung), sondern nur über ein beliebiges Netz eine Internetverbindung besteht.	!	x	x	

Beschreibung der Anforderungen	Wichtigkeit	MDR-COMPLETE	EVRMDR-COMPLETE	Bemerkung
Das Lizenzmodell ist benutzerbasierend.		x		
Das Lizenzmodell ist computerbasierend			x	
Lizenzmodell bei Education/Health/Goverment Kunden: Wahlweise benutzerbasierend oder computerbasierend	!	x		
Die Verwaltungsoberfläche erfüllt mindestens folgende Anforderungen an ein rollenbasiertes Administrationskonzept:				
Es können mehrere personalisierte Administratoren-Zugänge im Verwaltungssystem angelegt werden		x	x	
Administratoren können Administrationsrollen zugewiesen werden. Durch die Rolle werden die Handlungsmöglichkeiten (Berechtigungen) innerhalb der Verwaltung festlegen.		x	x	
Über AD-Import erzeugte Benutzerobjekte können zu Administratoren umgewandelt werden		x	x	
Superadmin-Rolle: hat Vollzugriff, keine Einschränkungen		x	x	
Admin: hat Vollzugriff, Einschränkung: kann kein Administratoren erzeugen oder ändern		x	x	
Helpdesk-Rolle: Kann Protokolle/Bericht einsehen, Alarme empfangen/löschen und Computer-Scan ausführen, Einschränkung: kann keine Einstellungen ändern oder Richtlinien bzw. Administratoren erzeugen/ändern		x	x	
Revisor-Rolle: Nur lesenden Zugriff auf alle Informationen/Einstellungen		x	x	
Alle Aktivitäten und Änderungen durch Verwalter werden in einem Audit-Protokoll aufgezeichnet und können - Berechtigungen vorausgesetzt - über die Verwaltungsoberfläche eingesehen werden.		x	x	
Mandantenfähigkeit: Die Mandantenfähigkeit der Lösung erfüllt folgende Anforderungen:				Enterprise Dashboard https://support.sophos.com/support/s/article/KB-000036993?language=en_US
Jeder Mandant ist eigenständig, verfügt über eigene Einstellung, Richtlinien und Benutzer-/Computer-/Gruppen-Objekte und Administratoren		x	x	
Die Verwaltungsdaten der Mandanten sind voneinandern separiert		x	x	
Ein Administrator hat nur Zugriff auf die Verwaltungsdaten seines Mandanten		x	x	
Es existiert ein übergreifendes Dashboard (Organisations-Dashboard) im dem die Alarme aller Mandanten konsolidiert dargestellt und eingesehen werden können	!	x	x	
Im Organisations-Dashboard werden alle angebundenen Mandanten angezeigt und es können neue Mandanten angelegt oder vorhandene Mandanten gelöscht werden		x	x	
Der Zugriffsrechte der Verwalter im Organisations-Dashboard können durch die Zuweisung einer Verwalter-Rolle und der Zuweisung von Mandanten festgelegt werden.		x	x	
Über ein Organisations-Dashboard kann man sich direkt in die Verwaltungsoberfläche eines Mandanten anmelden		x	x	
Über ein Organisations-Dashboard kann das Lizenz-Management der Mandanten vorgenommen werden				
Alle Aktivitäten und Änderungen durch Verwalter im Organisations-Dashboard werden in einem Audit-Protokoll aufgezeichnet und können - Berechtigungen vorausgesetzt - über die Verwaltungsoberfläche eingesehen werden.		x	x	
Globale Vorlagen: Es können globale Vorlage erstell werden, sodass globalen Einstellungen und Basisrichtlinien auf alle oder eine Auswahl von Mandanten angewendet werden können.		x	x	
Azure AD Federation: Eine Azure AD Verbundanmeldung kann aktiviert werden, sodass Administratoren und Benutzer sich an der zentralen Verwaltung bzw. am Self-Serivce Portal mit ihren Microsoft Anmeldedaten anmelden können.		x	x	
OpenID Connect Verbundanmeldung kann aktiviert werden, sodass Administratoren und Benutzer sich an der zentralen Verwaltung mit ihren Anmeldedaten anmelden können		x	x	
Microsoft AD FS Verbundanmeldung kann aktiviert werden, sodass Administratoren und Benutzer sich an der zentralen Verwaltung mit ihren Anmeldedaten anmelden können		x	x	
MFA: Zwei Faktor Authentisierung (2FA) - Es werden folgende Anforderungen an eine 2FA erfüllt:				
Die Anmeldung an der Verwaltungsobfläche kann über eine integrierte Zwei-Faktor-Authentisierung (2FA) zusätzlich abgesichert werden	!	x	x	
Das verwendete 2FA-Verfahren ist kompatible mit Google Authenticator		x	x	
SMS und E-Mail steht alternativ als 2FA-Verfahren zur Verfügung		x	x	
Pro Verwalter-Konto kann festgelegt werden, ob bei der Anmeldung mit diesem Konto eine 2FA zum Einsatz kommen muß		x	x	
Erweiterbarkeit - Der Funktionsumfang der zentrale Verwaltung kann um folgenden Funktionen erweitert werden:	!			
Endpoint/Server Protection: Endpoint Detection & Response (EDR)				Je nach Erweiterungswunsch ggf. entfernen
Unified Endpoint Management (UEM)		x	x	Je nach Erweiterungswunsch ggf. entfernen
Mobile Security für Android (Anti-Virus, Sicherheit für persönliche Daten, Authenticator, Sichere QR Code Scanner)		x	x	Je nach Erweiterungswunsch ggf. entfernen
Bitlocker & FileVault2 Management		x	x	Je nach Erweiterungswunsch ggf. entfernen
Email Gateway (Anti-Virus & Anti-Spam, cloudbasiert)		x	x	Je nach Erweiterungswunsch ggf. entfernen
Wireless/Access Point-Management		x	x	Je nach Erweiterungswunsch ggf. entfernen
Firewall Management (Perimeter/Netzwerk-Firewall, nicht Client Firewall)		x	x	Je nach Erweiterungswunsch ggf. entfernen
Phishing Simulation und Training		x	x	Je nach Erweiterungswunsch ggf. entfernen

Beschreibung der Anforderungen	Wichtigkeit	MDR-COMPLETE	EVRMDR-COMPLETE	Bemerkung
Cloud Security Posture Management		x	x	Je nach Erweiterungswunsch ggf. entfernen
Zero Trust Network Access (ZTNA)		x	x	Je nach Erweiterungswunsch ggf. entfernen
Reporting				
Ereignisse und sonstige allgemeine Status- und Fehlermeldung werden an das zentrale Management übermittelt.		x	x	
Ereignisse werden auch dann von Systemen umgehend an das zentrale Management übermittelt, wenn das Endgerät selbst nicht mit dem LAN verbunden ist (auch keine VPN Verbindung), sondern nur über ein beliebiges Netzwerk eine Internetverbindung besteht.	!	x	x	
Alle Ereignisse werden durch das zentrale Management der Lösung mindestens 90 Tage gespeichert		x	x	
Eine Suche in den Daten der zentralen Ereignisanzeige muss mindestens anhand folgenden Kriterien / Filter möglich sein:				
Zeitraum (Start/Ende-Datum)		x	x	
Benutzername		x	x	
Computername		x	x	
Name der Bedrohung		x	x	
Schweregrad (niedrig/mittel/hoch)		x	x	
Computergruppen		x	x	
Benutzergruppen		x	x	
Ereignistyp (Botnet-Kommunikation, Exploit-Erkennung, Ransomware etc.)		x	x	
Schwerwiegende Ereignisse müssen als Alarme automatisch per Email an ein oder mehrere Administratoren versendet werden können		x	x	
Es können benutzerdefinierte Berichte mit selbst definierten Filtern erstellt und gespeichert werden		x	x	
Benutzerdefinierte Berichte können dem Verwalter automatisch per Email als Link oder in Dateiform (PDF/CSV) in vorgebbaren Zeitintervallen zugestellt werden		x	x	
Berichte können mindestens im CSV- und PDF-Format erstellt werden		x	x	
Es steht einer Schnittstelle zur Verfügung, die es ermöglicht, die Ereignisse und Alarme automatisiert an Security Information and Event-Management (SIEM) Systeme zu übergeben	!	x	x	
Allgemeine Funktionen - Agent				
SSL-basierte Client/Server Kommunikation		x	x	
Message Relay: Die Management-Kommunikation zwischen den Endgeräten im LAN und der zentralen Verwaltung kann gebündelt über ein Relay-Server erfolgen. Der Relay Server erfüllt dabei folgende Anforderungen:				
Er nimmt nimmt Daten von Endgeräten (z.B. Protokollierungsdaten) entgegen und leitet diese an die zentrale Verwaltung weiter		x	x	
Die zentral Verwaltung sendet Daten (z.B. Richtlinien) an das Relay, welches die Daten an das Endgerät weiterleitet		x	x	
Es können ein oder mehrere Relay-Server in einem Netzwerk betrieben werden		x	x	
Dem Agent auf dem Endgerät werden von der zentrale Verwaltung alle vorhandenen Relay Server mitgeteilt. Diese Liste wird mindestens täglich aktualisiert.		x	x	
Der Agent auf den Endgeräten verbindet sich automatisch zum nächstgelegenen (Vergleich der IP-Adressen) Relay-Server im Netzwerk		x	x	
Ein Endgerät kann über die zentral Verwaltung fest mit einem Relay-Server verbunden werden		x	x	
In der zentralen Verwaltung wird der aktuelle Status für jedes Relay-Server angezeigt		x	x	
Befindet sich ein System nicht im LAN oder ist kein Relay-Server erreichbar, kommuniziert das System direkt über das Internet mit der zentralen Verwaltung		x	x	
Installation auf einem Windows 2008 R2 (oder höher) Server			x	
Automatische Isolation: Folgende Anforderungen an eine automatische Isolation von Systemen mit kritischen Systemzustand werden erfüllt:				
Ist eine Richtlinienoption und kann für ein System, ein oder mehrere Computer-Gruppen oder alle Systeme aktiviert werden		x		
Geräte mit kritischen Systemzuständen isolieren sich selbständig vom Netzwerk (Layer 3 TCP/UDP) und lassen keine ein- oder ausgehende Kommunikation zu. Der Systemzustand ist kritisch, wenn eine Bedrohung / Infektion erkannt wurde oder bedingt durch Manipulation oder Fehlfunktion das Gerät nicht richtig geschützt ist.		x		
Standardmäßig ist in einem kritischen Systemzustand nur Kommunikation vom und zum Verwaltungssystem freigeschaltet, sodass ein Client in diesem Zustand noch verwaltet werden und sich ggf. selbständig aktualieren kann.		x		
Über das Management können weitere Ausnahme für die automatische Isolation definiert werden. Die Ausnahmen können auf Basis folgender Angaben erstellt werden: Richtung (Eingehende/Ausgehende Verbindung oder beide), Lokaler Port, Remote Port, Remote Adresse (IPv4, IPv6 oder CIDR), Kommentar		x		
Sobald sich der Systemzustand wieder normalisiert hat, wird die Isolation durch das Gerät automatisch aufgehoben.		x		
Administrator gesteuerte Isolation: Folgende Anforderungen an eine durch den Administrator gesteuerte Isolation werden erfüllt:				
Über das Management kann ein Verwalter jederzeit beauftragen, dass sich ein Endgerät selbständig vom Netzwerk isolieren soll. Nach der Isolation (Layer 3 TCP/UDP) läßt das Endgerät keine ein- oder ausgehende Kommunikation mehr zu.		x	x	

Beschreibung der Anforderungen	Wichtigkeit	MDR-COMPLETE	EVRMDR-COMPLETE	Bemerkung
Standardmäßig ist nur Kommunikation vom und zum Verwaltungssystem freigeschaltet, sodass ein Client in diesem Zustand noch verwaltet werden und sich ggf. selbständig aktualieren kann.		x	x	
Ist das Endgerät aktuell nicht online, wird dieser Befehl / Auftrag zur Isolation für mindestens 7 Tage zwischengespeichert und zu einem späteren Zeitpunkt nachgeholt.		x	x	
Über das Management können weitere Ausnahme für die Isolation definiert werden. Die Ausnahmen können auf Basis folgender Angaben erstellt werden: Richtung (Eingehende/Ausgehende Verbindung oder beide), Lokaler Port, Remote Port, Remote Adresse (IPv4, IPv6 oder CIDR), Kommentar		x	x	
Der Administration kann jederzeit über das Managment die Aufhebung der Isolation eines Endgerätes veranlassen.		x	x	
Interaktion mit Sophos Firewall	!			Setzt Sophos Firewall voraus: Entfernen sofern keine Sophos Firewall im Einsatz oder geplant ist
Der Agent sendet der Sophos Firewall seinen Sicherheitsstatus kontinuierlich und proaktiv zu		x	x	
Der Agent unterscheidet mindestens drei Sicherheitstatis: Konform, teilweise konform, nicht konform		x	x	
Automatisierter Austausch von Sicherheitsstatusinformationen zur Isolierung kompromittierter Systeme		x	x	
Lateral Movement Prevention: Sobald ein infiziertes System identifiziert wurde, informiert die Firewall proaktiv alle anderen Systeme in einem Netzwerk. Daraufhin werden alle Verbindungen vom und zum infizierten Gerät von allen anderen Systemen abgelehnt.		x	x	
Lateral Movement Prevention: Es lassen sich Ausnahmen definieren, sodass definierte Systeme auch mit infizierten Geräten kommunizieren können.		x	x	
Um am Client automatisiert Prozesse zu identifizieren und zu bereinigen, welche mit einem Botnet kommunizieren		x	x	
Der Agent liefer der Sophos Firewall zur Identifikation der Kommunikation automatisiert Informationen zu Anwendungen		x	x	
Kommunikation: Zur Synchronisation mit der zentralen Verwaltung ist nicht zwingend eine LAN Verbindung nötig. Für eine erfolgreiche Kommunikation muß das Endgerät nur über ein beliebiges Netzwerk mit dem Internet verbunden sein.	!	x	x	
Die Kommunikationmechanismen des Agenten unterstützen eine Infrastrukur mit einem Web-Proxy der Authentisierung zwanghaft voraussetzt. Die Proxy-Einstellung (Proxy-Name, Port und Anmeldedaten), die der Agent zur Kommunikation nutzen soll, können zentral über die Verwaltungsobfläche vorgegeben und jederzeit angepasst werden.		x	x	
Unterstütze Betriebssysteme:				https://support.sophos.com/support/s/article/KB-000034074?language=en_US
Windows 7		x		Nur mit Extended Support
Windows 8		x		Support Ende: 07/2023
Windows 8.1		x		Standard Support Ende: 07/2023 danach nur mit Extended Support
Windows 10		x		
Windows 11		x		
MacOS 10.15+		x		https://support.sophos.com/support/s/article/KB-000034670?language=en_US
Windows Server 2008 R2			x	Nur mit Extended Support
Windows Server 2012			x	Standard Support Ende: 07/2023 danach nur mit Extended Support
Windows Server 2012 R2			x	Standard Support Ende: 07/2023 danach nur mit Extended Support
Windows Server 2016			x	
Windows Server 2019			x	
Windows Server 2022			x	
Linux			x	https://support.sophos.com/support/s/article/KB-000033389?language=en_US
Die Benutzerobfläche wird in folgenden Sprachen zur Verfügung gestellt:				
Deutsch		x	x	
Englisch		x	x	
Fränzösich		x	x	
Spanisch		x	x	
Portugiesisch		x	x	
Italienisch		x	x	
Japanisch		x	x	
Chinesisch		x	x	
Koreanisch		x	x	
Client / Server -Virtualisierung				
Die Installation des vollständigen Agents in VMs auf folgenden Virtualisierungsplattformen wird unterstützt:				https://support.sophos.com/support/s/article/KB-000034062?language=en_US
VMware vSphere/ESX		x	x	
VMware Workstation		x	x	
Microsoft Hyper-V		x	x	

Beschreibung der Anforderungen	Wichtigkeit	MDR-COMPLETE	VRMDR-COMPLETE	Bemerkung
Citrix XenServer		x	x	
Ein off-board Malware-Scan für VMs über einen Light-Agent und eine Scan-VM wird für folgende Virtualisierungsplattformen unterstützt:				https://support.sophos.com/support/s/article/KB-000036517?language=en_US
VMware ESXi 5.5 / 6.0 / 6.5 / 6.7 / 7.0		x	x	
Microsoft Hyper-V Server 2012 R2 / 2016 / 2019		x	x	
Der Light-Agent für den off-board Scan unterstützt folgende Gast-VMs Betriebsysteme:		x	x	
Windows 7 SP1		x		
Windows 8.1		x		
Windows 10		x		
Windows Server 2008 R2 SP1			x	
Windows Server 2012 /R2			x	
Windows Server 2016			x	
Windows Server 2019			x	
Folgende Anforderungen an den off-board Malware-Scan werden erfüllt:				
Es können mehrere Scan-VMs pro Host betrieben werden		x	x	
Ausfallsicherheit: Es existiert ein Mechanismus, dass eine Gast-VM beim Ausfall seiner aktuell verwendeten Scan VM automatisch auf eine andere Scan VM wechselt		x	x	
Lastverteilung: Es existiert ein Mechanismus, dass eine Gast-VM automatisch zu einer Scan VM mit angemessener Scan-Performance verbindet.		x	x	
Bei Malware-Fund wird eine automatische Bereinigung der Gast-VM vorgenommen		x	x	
In der zentralen Verwaltung werden alle installierten Scan VMs angezeigt		x	x	
In der zentralen Verwaltung werden alle geschützten Gast VMs angezeigt		x	x	
In der zentralen Verwaltung wird pro Scan VM der Versionsstand und Malware-Fund angezeigt		x	x	
Über die zentral Verwaltung kann ein Full-Scan einer Gast-VM ausgeführt werden		x	x	
Installation / Produkt Updates				
Über die zentrale Verwaltungsobfläche können Emails inkl. Link zum Installationspaket an Anwender versendet werden		x	x	
Das Installationpaket ist skriptierbar und kann mittels gäniger Softwareverteilungswerkzeugen (z.B. SCCM) verteilt werden		x	x	
Der Agent läßt sich in ein (Golden-)Image integrieren, sodass eine Installation in den aus dem Image erstellen Clonen nicht mehr notwendig ist		x	x	
Der Installer verfügt über einen Mechanismus zur Erkennung und Deinstallation von Drittanbieter-Lösungen		x	x	
Die Produktsprache wird bei der Installation anhand der konfigurierten Systemsprache des Betriebssystem festgelegt		x	x	
Es existiert ein Installationspaket, welches sowohl für Server als auch für Client Systeme genutzt werden kann		x	x	
Das Installationspaket verfügt über Parameter, welche die Erfüllung folgende Anforderungen ermöglichen:				
Produktsprache(Installer) kann unabhängig von der Systemsprache des Betriebssystems festgelegt werden		x	x	
Proxy-Einstellungen können definiert werden, mindestens Proxy-Adresse, Proxy-Benutzername und Passwort		x	x	
Die Deinstallationsfunktion von Drittanbieter-Lösungen, kann de-/aktiviert werden		x	x	
der Benutzername, des Benutzer, dem dieses System in der Verwaltungsoberfläche zugeordnet werden soll, kann vorgegeben werden		x	x	
Der Gruppenname, der Gruppe, der dieses System in der Verwaltungsoberfläche zugeordnet werden soll, kann vorgegeben werden		x	x	
Der Computername, mit dem das System in der Verwaltungsobfläche identifizierbar ist, kann vorgegeben werden		x	x	
Der Domain-Name, dem dieses System in der Verwaltungsoberfläche zugeordnet wird, kann überschrieben werden.		x	x	
Die zu installierenden Produktbestandteile lassen sich einzeln auswählen		x	x	
Eine Installation ohne Benutzerinteraktion ist de-/aktivierbar		x	x	
Die zur Installation notwendig Kommunikation der Endgeräte mit der zentralen Verwaltung läßt sich gebündelt über einen Relay Server steuern.		x	x	
Die Installation kann aus einer lokalen Updatequelle (kein Nachladen von Software aus dem Internet) durchgeführt werden	!	x	x	
Produkt-Updates - Folgende Anforderungen werden erfüllt:				
Produkt-Update werden nach Verfügbarkeit automatisch auf alle System installiert		x	x	
Produkt-Updates können manuell gesteuert werden, sodass Updates erst nach manueller Freigabe durch den Administrator installiert werden	!	x	x	
Die manuelle Steuerung von Produkt-Update kann für Client und Server unabhängig voneinander durchgeführt werden		x	x	
Es kann gesteuert werden, dass Produkt-Updates zuerst auf auswählbaren Testsystemen installiert werden, bevor das Update zur Installation auf anderen Systemen zur Verfügung steht		x	x	

Beschreibung der Anforderungen	Wichtigkeit	MDR-COMPLETE	EVRMDR-COMPLETE	Bemerkung
Produkt-Updates können für eine definierbare Zeitspanne von bis zu 90 Tagen pausiert werden. In diesem Zeitraum werden nur Signatur-Update, aber keine Produkt-Updates, eingespielt		x	x	
Der Verwalter wird per Email über die Veröffentlichung neue Produkt-Versionen informiert		x	x	
Es kann festgelegt werden, an welchen Wochentagen und zu welcher Uhrzeit ein System Produkt-Updates installieren soll		x	x	
Die Bandbreite, die der Agent zum Herunterladen von Produkt-Update verwendet, kann limitiert werden	!	x	x	
Die Bandbreite, die der Agent zum Laden von Signatur-Updates verwendet, kann limitiert werden.		x	x	
Lokale Update Server versorgen die im LAN befindlichen Systeme mit Software-Updates	!	x	x	
Lokale Update Server versorgen die im LAN befindlichen Systeme mit Signatur-Updates (Anti-Virus)		x	x	
Installation eines lokalen Update-Caches auf einem Windows 10 (64 bit) Client	!	x		
Installation eines lokalen Update-Caches auf einem Windows 2008 R2 (oder höher) Server			x	
Update Cache: Folgende Anforderungen an die Update-Server Infrastruktur werden erfüllt:				
Es können ein oder mehrere Update Server in einem Netzwerk betrieben werden		x	x	
Dem Agent auf dem Endgerät werden von der zentralen Verwaltung alle vorhandenen Update Server mitgeteilt		x	x	
Der Agent auf den Endgeräten verbindet sich automatisch zum nächstgelegenen (Vergleich der IP-Adressen) Update-Server im Netzwerk	!	x	x	
Ein Endgerät kann über die zentrale Verwaltung fest mit einem Update-Server verbunden werden		x	x	
Konnte ein Update-Server sich selbst seit mehr als einer Stunde nicht aktualisieren, wird dieser Server aus der Liste, der im Netzwerk verfügbaren Update-Server entfernt		x	x	
In der zentralen Verwaltung wird für jeden Update-Server der Status, die Zeitspanne seit dem letzten erfolgreichen Update und eine Liste der über diesen Server aktualisierenden Endgeräte angezeigt		x	x	
Befindet sich ein System nicht im LAN oder ist keiner der Update-Server erreichbar, aktualisiert sich das System direkt über das Internet		x	x	
Überwachung/Protokollierung von Dateien und RegKeys: Er werden folgende Anforderungen erfüllt				https://support.sophos.com/support/s/article/KB-000038360?language=en_US
Es handelt sich um eine Richtlinienoption die für ein oder mehrere Systeme aktiviert und konfiguriert werden kann			x	
In der Standardeinstellung werden alle systemkritische Datei und Registrierungsschlüssel eines Windows-System überwacht und Änderungen werden protokolliert . Die Konfiguration der Standardeinstellungen ist dokumentiert.			x	https://support.sophos.com/support/s/article/KB-000038115?language=en_US
Es können zusätzliche Überwachungsregeln auf Basis einzelner Dateien, Ordner, Registrierungsschlüssel und Registrierungswerte hinzugeführt werden. Die Verwendung von Systemvariablen wird unterstützt.			x	
Es können Ausschlüsse für die Überwachung auf Basis einzelner Dateien, Ordner, Registrierungsschlüssel und Registrierungswerte hinzugeführt werden. Die Verwendung von Systemvariablen wird unterstützt.			x	
Anti-Virus				
Der signaturbasierte Echtzeit Schutz (on-access) erfüllt folgende Anforderungen bzw. kann zentral wie folgt konfiguriert werden:				
über Richtlinie de-/aktivierbar		x	x	
Überprüft Zugriffe auf lokalen Laufwerken		x	x	
Überprüft Zugriffe auf Netzlaufwerken		x	x	
über Richtlinie de-/aktivierbar, dass lesende Zugriffe überprüft werden			x	
über Richtlinie de-/aktivierbar, dass schreibende Zugriffe überprüft werden			x	
Überprüft Download		x	x	
Blockiert den Zugriff auf schädliche Websites		x	x	
Erkennt und blockiert potenziell unerwünchte Anwendungen / Adware		x	x	
Erkennt und blockiert schädliches Verhalten (HIPS, Host Intrusion Prevention System)		x	x	
Die Lösung verfügt über eine Überprüfung von Downloads anhand eines reputationsbasierten Verfahren, welches zur Bewertung zumindest die Download-Häufigkeit und die Download-Quelle heranzieht		x	x	Download Reputation
Die Lösung verfügt über einen Live-Schutz (online Datenbank), der folgende Anforderungen erfüllt:				
Verdächtige Dateien werden online gegenüber einer Live-Datenbank mit den neusten Informationen zu Bedrohungen geprüft		x	x	
Der Live-Schutz kann über eine Richtinie de-/aktiviert werden		x	x	
Eine Weitergabe von Malware-Samples findet nicht statt bzw. kann per Richtlinie deaktiviert werden		x	x	
Der Live-Schutz wird auch zur Überprüfung im Rahmen von geplanten Scans verwendet		x	x	
Erkennt und blockiert Kommunikation mit Botnetzen	!	x	x	Malicious Traffic Detection (MTD)
Schädlichen Netzwerkverkehr mit Packet Inspection (IPS) verhindern		x	x	
Die Lösung verfügt über eine automatisch Malware-Bereinigungsfunktion		x	x	
Geplante Scans: Die Lösung verfügt über eine Möglichkeit geplante Scans einzurichten und erfüllt folgende Anforderungen:				
Ein oder mehrere Wochentage und die Uhrzeit, an welcher der Scan ausgeführt werden soll, können festgelegt werden		x	x	

Beschreibung der Anforderungen	Wichtigkeit	MDR-COMPLETE	VRMDR-COMPLETE	Bemerkung
Scan von Archivdatenen (.zip, .cab, etc.) kann de-/aktiviert werden		x	x	
Folgende Anforderungen an einen On-Demand Scan werden erfüllt:				
Bei Bedarf kann über die zentrale Verwaltung ein vollständiger Scan eines System initiiert werden		x	x	
Ist das System zum Zeitpunkt der Initiierung eines Scans offline, wird der Scan durchgeführt, sobald das System wieder online ist		x	x	
Bereinigungsereignisse werden an die zentrale Verwaltung übermittelt		x	x	
Der Benachrichtigungstext, der dem Anwender im Falle eines Virenfundes angezeigt wird, kann angepasst werden.		x	x	
Scan Ausschlüsse: Im Bereich der Scan Ausschlüsse werden folgende Anforderungen erfüllt:				
Dateien oder Ordner können über einen Ausschluß von Scan ausgenommen werden		x	x	
Prozesse können über einen Ausschluß vom Scan ausgenommen werden		x	x	
Webseiten können über einen Ausschluß vom Scan ausgenommen werden		x	x	
Potenziell unerwünschte Anwendungen können über einen Ausschluß vom Scan ausgenommen werden		x	x	
Pro Ausschluß kann definiert werden, ob dieser für den Echtzeitscan und/oder für geplante Scans angewendet werden soll		x	x	
Für die Anwendungen Microsoft Exchange und Microsoft SQL werden automatisch nach Herstellervorgaben Ausschlüsse defniert			x	
In der zentralen Verwaltung werden pro System detailliert alle installierten Komponenten inkl. Versionsnummer angezeigt		x	x	
In der zentralen Verwaltung kann eine Aktualisierung des Endpoint Agenten initiiert werden		x	x	
Anti-Exploit				
Die Exploit Prevention verfügt über nachstehende Anti-Exploit Technologien:				
Enforce Data Execution Prevention (DEP): Unterbindet die missbräuchliche Nutzung von Pufferüberläufen		x	x	
Mandatory Address Space Layout Randomization (ASLR): Verhindert vorhersagbare Code-Speicherorte		x	x	
Bottom Up ASLR: Optimiert die Randomisierung von Code-Speicherorten		x	x	
Null Page (Null Dereference Protection): Stoppt Exploits, die Sprungbefehle über die Zero-Page beinhalten		x	x	
Heap Spray Allocation: Reserviert beim Programmstart Speicherbereiche, die häufig für das Einbringen von Schadcode verwendet werden, um solche Angriffe abzuwehren		x	x	
Dynamic Heap Spray: Stoppt Angriffe, die verdächtige Sequenzen an verschiedene Stellen des Heaps schreiben		x	x	
Stack Pivot: Stoppt missbräuchliche Nutzungen des Stack Pointers		x	x	
Stack Exec (MemProt): Stoppt Code von Angreifern auf dem Stack		x	x	
Stack-based ROP Mitigations (Caller): Stoppt „Return-Oriented Programming“-Standardangriffe		x	x	
Branch-based ROP Mitigations (Hardware Augmented): Stoppt Angriffe die komplexe „Return- Oriented Programming“-Angriffe	!	x	x	
Structured Exception Handler Overwrite Protection (SEHOP): Stoppt missbräuchliche Nutzungen des Ausnahmehandlers		x	x	
Import Address Table Filtering (IAF) (Hardware Augmented): Stoppt Angriffe, die nach API-Adressen in der IAT suchen		x	x	
Load Library: Unterbindet das Laden von Libraries von UNC-Pfaden		x	x	
Reflective DLL Injection: Verhindert das Laden einer Library vom Speicher in einen Host-Prozess		x	x	
VBScript God Mode: Verhindert die Ausnutzung von VBScript in IE zur Ausführung von Schadcode		x	x	
WoW64: Stoppt Angriffe, die auf die 64-Bit-Funktion des WoW64- Prozesses abzielen		x	x	
Syscall: Stoppt Angreifer, die versuchen, Sicherheitsmaßnahmen zu umgehen		x	x	
Hollow Process: Stoppt Angriffe, die legitime Prozesse nutzen, um Schadecode zu verbergen		x	x	
DLL Hijacking: Gibt System-Libraries für heruntergeladene Anwendungen Priorität		x	x	
Squiblydoo AppLocker Bypass: Verhindert die Ausführung von Remote-Skripte und -Code durch regsvr32		x	x	
APC Violation (Double pulsar/AtomBombing): Entdeckt den Missbrauch von Application Procedure Calls	!	x	x	
Process Privilege Escalation und Process Owner Changing: Verhindert Process Priviliege Escalation und Process Ower Changing indem es Kernel Token / Ticket Diebstahl erkennt und die Wiederverwendung durch einen Fremd-Prozess verhindert		x	x	
Weitere Schutzmaßnahmen				
Diebstahlschutz für Anmeldedaten und Hash-Informationen: Schützt Windows-Systeme vor unautorisierte Interaktionen mit dem LSASS-Laufzeitspeicher, der SAM DB Registry und den Sektoren mit Hash Inforationen auf der Festplatte	!	x	x	
Code Cave Verwendung: Erkennt sogenannte Code Cave Inhalte in Anwendungen und verhindert deren Ausführung	!	x	x	
Man-in-The-browser (MITB) Schutz: Überwacht Webbrowser um MITB Angriffe durch (Banking-)Trojaner zu erkennen und zu verhindern.		x	x	
Malicious Process Migration: Erkennt und verhindert unautorisierte Prozess Migration mittels Pen Test Tools (z.B. Metasploit Meterprecter Shell).		x	x	
Registry Protection: Schützt die Windows Sticky Key Einträge vor Manipulationen und verhindert den Missbrauch von Application Verifier (DoubleAgent).		x	x	
Schutz vor Ransomware				

Beschreibung der Anforderungen	Wichtigkeit	MDR-COMPLETE	EVRMDR-COMPLETE	Bemerkung
Ransomware Dateischutz: Verhaltensbasierte Erkennung schadhafter Dateiverschlüsselungsoperationen an Dateien auf lokalen Datenträgern oder auf Netzlaufwerken	!	x	x	
Der Ransomware Dateischutz ist in der Lage legitime Dateiverschlüsselungslösungen (z.B. SafeGuard Enterprise) zu erkennen und blockiert diese nicht in ihrer Funktionsweise		x	x	
Automatische Wiederherstellung verschlüsselter Dateien: Beim Öffnen einer Datei wird durch einen Backup-Mechanismus der Lösung eine Kopie erstellt und diese im Bedarfsfall (Modifikation durch schadhafte Verschlüsselung) automatisch wiederhergestellt	!	x	x	
Schutz vor remote ausgeführter Ransomware: Schadhafte Verschlüsselungsoperationen werden auch dann erkannt und gestoppt, wenn diese nicht durch einen lokalen Prozess, sondern durch ein anderes System über das Netzwerk (remote) ausgeführt werden	!	x	x	
Der Ransomware-Schutz unterstützt den Einsatz auf Windows Terminal Servern.	!		x	
Festplatten und Boot Record Schutz: Erkennt und verhindert die schadhafte sektorbasierte Verschlüsselung von Festplatten und die Manipulation des Master Boot Record (MBR)	!	x	x	
Schutz von Anwendungen und Erkennung von Anomalien				
Alle installierten Anwendungen müssen automatisch klassifiziert und gemäß Ihrer Klassifizierung mit einem Verhaltens- und einem Schutzprofil ausgestattet werden. Das Verhaltensprofil dient zur Erkennung von Anwendungsanomalien. Das Schutzprofil legt die Schutzeinstellungen fest.		x	x	
Die Aktivitäten folgender Anwendungstypen werden überwacht und sofern Verhaltensanomalien festgestellt werden, wird die entsprechende Anwendung automatisch blockiert:				
Web Browser		x	x	
Browser Plugins		x	x	
Java Anwendungen		x	x	
Medienanwendungen		x	x	
Office Anwendungen		x	x	
Die Verwendung von Angriffstechniken in HTML-Anwendungen (kurz HTA) wird erkannt.		x	x	
Der Start und die Verwendung von PowerShell durch Anwendungen der Office-Pakete wird erkannt und verhindert		x	x	
In der Verwaltung können Anwendungen von der Überwachung durch die Exploit Mitigation ausgenommen werden		x	x	
Über das Management müssen für Benutzer/Benutzergruppen und/oder Computer/Computergruppen Ausnahmen von der Exploit Migration vorgenommen werden können		x	x	
Machine Learning				
Zur Erkennung neuer Malware wird ein auf Machine Learning Technolgie basierendes Verfahren eingesetzt		x	x	
Zur Erkennung von potenziell unerwünschten Anwendungen wird ein auf Machine Learning Technolgie basierendes Verfahren eingesetzt.		x	x	
Die eingesetzte Machine Learing Technolgoie erfüllt folgende Anforderungen:				
Verwendet einen Deep Learing Ansatz		x	x	
Anhand einer veröffentlichten ROC-Kurve (Receiver-Operating-Characteristic) kann eine hohe Erkennungsrate und eine niedrige Fehlerkennungsrate nachgewiesen werden		x	x	
Das Modell wird nachweislich mit Daten geschult, die repräsentativ für Bedrohungen aus der realen Welt sind		x	x	
False Positives können über das Management auf Basis eines Hash-Wertes oder anhand eines hinterlegten Code-Signing Zertifikats von der erneuten Erkennung ausgenommen werden		x	x	
Bereinigung unbekannter Malware				
Signaturloser on-demand Malware-Scanner	!	x	x	
Wird bei erkannter Bedrohung automatisch gestartet		x	x	
Forensische Erkennung bisher unbekannt Malware		x	x	
Entfernt persistente Malware		x	x	
Ersetzt infizierte Windows-Resourcen durch sichere Originalversionen		x	x	
Bedrohungsanalyse und Endpoint Detection & Response (EDR)				
Die Lösung verfügt über eine Bedrohungsanalyse, die bei einer Erkennung lokal gesammtelte Meta-Daten in die Verwaltung hochlädt und diese dort in aufbereiteter Form anzeigt. Die angezeigten Daten umfassen die vollständige Angriffskette, vom Eintritt ins System bis hin zur Erkennung.	!	x	x	
Es könne alle Bedrohungsanalysen der letzten 90 Tagen über das Management eingesehen werden.		x	x	
Es werden durch die Bedrohungsanalyse mindestens folgende Informationen zu Vorfällen im Management bereitgestellt:				
Name des angemeldeten Benutzers zum Zeitpunkt der Erkennung		x	x	
Computername		x	x	
Zeitpunkt der Erkennung (Datum und Uhrzeit)		x	x	

Beschreibung der Anforderungen	Wichtigkeit	MDR-COMPLETE	EVRMDR-COMPLETE	Bemerkung
Name aller aktive Prozesse zum Zeitpunkt der Erkennung inkl. vollständiger Pfadangabe, Prozess-ID, Datei-Hash (SHA256), Start/End Time, Interaktionen, Datei Reputation Bewertungen (bekannt gut/schadhaft, unbekannt) und Befehlszelenaufrufe / Parameterübergabewerte (z.B. Powershell)		x	x	
Bei Ransomware: Namen aller angegriffene Geschäftsdateien inkl. vollständiger Pfadangabe		x	x	
Aktive Netzwerkverbindungen inkl. IP-Adresse / DNS Name / URL		x	x	
Zugriff auf die Registry unter Angabe der Registry-Pfade		x	x	
Threat Intelligence - Im Rahmen der Bedrohungsanalyse werden für jeden Prozess erweiterte Analysedaten bereitgestellt (bei bekannten Dateien) bzw. können diese Daten angefordert werden (bislang unbekannte Dateien). Werden die erweiterten Analysedaten angefordert wird die Datei zur Analyse in eine Sandbox-System übertragen und ausgeführt. Folgende Daten werden mindestens angezeigt:	!			
Link zu Erkennungen für diese Datei bei bei Virus Total		x	x	
Bewertung des Bekanntheits/Verbreitungsgrad der Datei		x	x	
Analyseergebnis der Dateiattribute der Datei im Vergleich zu bekannten guten und bekannten schädlichen Dateien		x	x	
Analyseergebnis der Code-Ähnlichkeiten der Datei im Vergleich zu bekannten guten und bekannten schädlichen Dateien		x	x	
Analyseergebnis des Dateinamens/Pfads im Vergleich zu bekannten guten und bekannten schädlichen Dateien		x	x	
Datei-Informationen: Produkt, Dateityp, Copyright, Originalname, Interner Name, Dateiversion, Firmenname, Beschreibung, Anmerkungen, Dateigröße, Ziel-Computer, Zeitstempel der Kompilierung, PDB-Pfad, Sprache,		x	x	
Zertifikatsinformationen: Signiert am und Signiert von		x	x	
Aufstellung der PE-Dateiabschnitte inkl. Angabe von Name, Entropie, Virtueller Adresse, Physikalischer Adresse, Physikalischer Größe und Einstellungen		x	x	
Aufstellung der PE-Importe der Datei (DLLs und Funktionen)		x	x	
Aufstellung der PE-Exporte der Datei (DLLs und Funktionen)		x	x	
Die Daten der Bedrohungsanalyse können über das Management mittels einer Volltextsuche durchsucht und gefiltert werden		x	x	
Die Daten der Bedrohungsanalyse können pro Vorfall im CSV-Format exportiert werden		x	x	
Die vollständige Angriffskette, vom Eintritt ins System bis hin zur Erkennung, wird pro Vorfall in visualisierter Form im Management dargestellt	!	x	x	
Forensische Analyse: Folgende Anforderungen werden erfüllt:				https://support.sophos.com/support/s/article/KB-000038358?language=en_US
Bei Bedarf kann über die Verwaltung ein forensicher Snapshot der Geräteaktivitäten auf dem lokalen Endgerät erzeugt und gespeichert werden		x	x	
Dieser Forensische Snapshot enthält alle Daten der Aktivitäten, die der Datenrekorder der Lösung bis zu diesem Zeitpunkt gesammelt hat.		x	x	
Der Forensiche Snapshot kann zur Weiteren Analyse als SQLite Datenbank oder JSON Format konvertiert werden.		x	x	
Es steht eine detaillierte Beschreibung des Datenbank-Schema zur Verfügung.		x	x	https://support.sophos.com/support/s/article/KB-000038469?language=en_US
Datei- und Registrierungsüberwachung (File Integrity Monitoring)			x	
Live Abfragesystem (Threat Hunting und IT Security Compliance) Folgende Anforderungen werden erfüllt:				
Möglichkeit die Sensoren auf den Clients und Servern zentralisiert aus dem Management abzufragen.	!	x	x	
Eine standartisierte Abfragesprache (SQL) kommt zum Einsatz.	!	x	x	
Die Abfragen liefern Ergebnisse zum aktuellen Zustand.	!	x	x	
Historische Informationen über z.B. Dateizugriffe, Netzwerkzugriffe etc. können bis zu 90 Tage abgefragt werden.	!	x	x	
Variablen können in den Abfragen genutzt werden.	!	x	x	
Statistiken (wie z.B. Ausführzeit, übertragende Datenmenge & Systemauswirkung) zur Laufzeit der Abfragen werden dargestellt.	!	x	x	
Abfrageergebnisse können im CSV Format exportiert werden.	!	x	x	
Die Live Abfragemöglichkeiten basieren auf OSQuery	!	x	x	
Im Auslieferungszustand sind bereits umfangreiche vorgefertigte Abfragen integriert (130+)	!	x	x	
Es können individuelle OSQuery Abfragen erstellt werden.	!	x	x	
Externe Datenquellen können für Abfragen genutzt werden	!	x	x	
Abfrageergebnisse können unmittelbar als Ausgangswert für neue Abfragen genutzt werden.	!	x	x	
Cloudbasierter Datenspeicher	!			
Möglichkeit die Telemetriedaten von Clients und Servern zentralisiert aus dem Management abzufragen.	!	x	x	
Eine standartisierte Abfragesprache (SQL) kommt zum Einsatz.	!	x	x	
Die Abfragen liefern Ergebnisse der letzten 90 Tage	!	x	x	
Möglichkeit der Datenspeicherung für 365 Tage	!	x	x	Zusatzlizenz erforderlich
Variablen können in den Abfragen genutzt werden.	!	x	x	

Beschreibung der Anforderungen	Wichtigkeit	MDR-COMPLETE	VRMDR-COMPLETE	Bemerkung
Abfrageergebnisse können im CSV Format exportiert werden.	!	x	x	
Im Auslieferungszustand sind bereits umfangreiche vorgefertigte Abfragen integriert (110+)	!	x	x	
Abfrageergebnisse können unmittelbar als Ausgangswert für neue Abfragen genutzt werden.	!	x	x	
Planbare, wiederkehrende Abfragen	!	X	x	
Automatische Erkennung von verdächtigem Verhalten (KI gestützt) zur weiteren Untersuchung.	!	x	x	
Produktübergreifende Abfragemöglichkeit von Datenquellen	!			
Abfragemöglichkeit von Endpoint Daten	!	x	x	
Abfragemöglichkeit von Server Daten	!	x	x	
Abfragemöglichkeit von Firewall Daten	!	x	x	
Abfragemöglichkeit von E-Mail Daten	!	x	x	
Abfragemöglichkeit von Cloud Security Posture Management	!	x	x	
Live Response (Remote Terminal Zugriff)	!			
Absicherung des Zugriffs über mehrstufige Authentifizierung	!	x	x	
Auditierung des Zugriffs	!	x	x	
Möglichkeit der Nutzung einer Consolen Sitzung mit System-Rechten	!	x	x	
Verwendung von DOS-, UNIX- oder Linux-Befehle (je nach Betriebssystem des Zielgerätes)	!	x	x	
KI gestützte Erkennungen	!			
priorisierte Liste verdächtiger Aktivitäten und anfälliger Konfigurationen	!	x	x	
Zuordnung der Aktivitäten zu den TTPs aus dem MITRE ATT&CK Framework	!	x	x	
Risiko Einstufung verdächtiger Aktivitäten (Skala von 1 bis 10)	!	x	x	
Managed Detection and Response (MDR)	!			
Proaktives Aufspüren und Prüfen von potenziellen Bedrohungen und Vorfällen	!	x	x	
Nutzen aller vorliegenden Informationen, um Ausmaß und Schwere von Bedrohungen zu bestimmen	!	x	x	
Anwenden geeigneter Maßnahmen je nach Risiko-Bewertung der Bedrohung	!	x	x	
Einleiten von Maßnahmen zum Stoppen, Eindämmen und Beseitigen von Bedrohungen	!	x	x	
Bereitstellen konkreter Ratschläge, um die Ursache wiederholt auftretender Vorfälle zu bekämpfen	!	x	x	
24/7 indizienbasierte Bedrohungssuche (Bei dieser Art der Bedrohungssuche werden kausale und angrenzende Ereignisse (schwache Signale) aggregiert und analysiert, um neue „Indicators of Attack (IoA)“ und „Indicators of Compromise (IoC)“ zu enttarnen, die bislang nicht erkannt werden konnten)	!	x	x	
Security Health Check (proaktive Untersuchungen von Betriebsbedingungen und empfohlene Konfigurations-Verbesserungen)	!	x	x	
Aktivitätsreports (Zusammenfassungen der Aktivitäten im Rahmen von Wochen und Monatsreports)	!	x	x	
Angriffserkennung (Erkennung von Angriffs Taktiken, Techniken und Prozessen (TTPs))	!	x	x	
24/7 indizienlose Bedrohungssuche (Mithilfe von Data Science, Threat Intelligence und der Intuition erfahrener Bedrohungsexperten werden verschiedene Informationen kombiniert, um das Verhalten von Angreifern vorherzusagen und neue Angriffsindikatoren (IoA) zu identifizieren)	!	x	x	
Optimierte Telemetriedaten (Bedrohungsanalysen werden um Telemetriedaten ergänzt)	!	x	x	
Proaktive Verbesserung des Sicherheitsstatus	!	x	x	
Dedizierter Ansprechpartner	!	x	x	
Direkter Telefon-Support	!	x	x	
Monatliches Briefing zu aktuellen Bedrohungen	!	x	x	
Stoppen und Eindämmen von Bedrohungen	!	x	x	
Proaktives Aufspüren und Prüfen von potenziellen Bedrohungen	!	x	x	
Korrelieren aller vorliegenden Informationen, um Ausmaß und Schwere zu bestimmen	!	x	x	
Bewertung der Auswirkungen auf das Netzwerk	!	x	x	
Bereitstellen konkreter Ratschläge, um die Ursache wiederholt auftretender Bedrohungsaktivität zu bekämpfen	!	x	x	
Ergreifen von Maßnahmen zum Stoppen, Eindämmen und Beseitigen von Bedrohungen	!	x	x	
Vollständiges Incident-Response: komplette Neutralisierung von Bedrohungen	!	x	x	
Vollständige Ursachenanalyse	!	x	x	
Asset-Erkennung (Asset-Informationen über Betriebssystem-Versionen, Anwendungen und Schwachstellen bis hin zur Identifizierung verwalteter und nicht verwalteter Assets)	!	x	x	
Zielzeit für Fallerstellung 2 Minuten nach Erkennung	!	x	x	

Beschreibung der Anforderungen	Wichtigkeit	MDR-COMPLETE	EVRMDR-COMPLETE	Bemerkung
Zielzeit für die erste Reaktionsmaßnahme 30 Minuten nach der Fallerstellung	!	x	x	
Die Antwortzeiten sind in einem Service-Level-Argement definiert	!	x	x	
Breach Protection Warranty in Höhe von bis zu 1 Mio. US-Dollar für Reaktionsmaßnahmen	!	x	x	
90 Tage Datenspeicherung aller beteiligten Komponenten (inkl. potentieller Integrationen)	!	x	x	
Möglichkeit der Datenspeicherung für 365 Tage	!	x	x	
Integration von Microsoft-Graph-Sicherheit	!	x	x	
Integration von Office 365 Verwaltungsaktivität	!	x	x	
Möglichkeit der Integration von Network Detection and Response Systemen	!	x	x	
Möglichkeit der Integration von Firewall Systemen	!	x	x	
Möglichkeit der Integration von Identitätsanbietern	!	x	x	
Möglichkeit der Integration von Public Cloud Anbietern	!	x	x	
Möglichkeit der Integration von E-Mail Systemen	!	x	x	
Möglichkeit der Integration von Netzwerk Analyse Systemen	!	x	x	
Network Detection and Response (NDR)	!			
Erweiterbare Abfrage-Engine, die ein Deep-Learning-Vorhersagemodell verwendet, um verschlüsselten Datenverkehr auf Muster in nicht zusammenhängenden Netzwerkströmen zu analysieren	!	x	x	Nur mit Zusatzlizenz
Überwachung von sowohl verschlüsselten als auch unverschlüsselten Datenverkehr unter Verwendung bekannter IoCs, um Bedrohungsakteure und TTPs schnell zu identifizieren	!	x	x	Nur mit Zusatzlizenz
Erkennung von Zero-Day-C2-Servern und neuen Varianten von Malware-Familien auf der Grundlage von Mustern, die in der Größe der Sitzung, der Richtung und den Interarrival-Zeiten gefunden werden	!	x	x	Nur mit Zusatzlizenz
Identifizieren das Vorhandenseins einer dynamischen Domain-Generierungstechnologie, die von Malware verwendet wird, um eine Erkennung zu vermeiden	!	x	x	Nur mit Zusatzlizenz
Leistungsstarke Logik-Engine, die Regeln verwendet, die bei einer Vielzahl von sitzungsbasierten Risikofaktoren Alarm schlagen.	!	x	x	Nur mit Zusatzlizenz
Wird als virtuelle Appliance bereitgestellt	!	x	x	
Der Netzwerksensor kann über einen SPAN Port angebunden werden	!	x	x	
Überwachung von Peripheriegeräten (Device Control)				
Die Überwachungsfunktion für Peripheriegeräte kann wie folgt eingestellt werden:				
Die Überwachung für Peripheriegeräte wird vollständig deaktiviert		x	x	
Die Nutzung von Peripheriegeräten wird überwacht und protokolliert, aber nicht eingeschränkt		x	x	
Die Nutzung von Peripheriegeräten wird anhand von Zugriffsrichtlinien für Gerätetypen und einzelne Geräte eingeschränkt (White-/Blacklist-Verfahren)		x	x	
Richtlinien können auf Benutzer(Gruppen) angewandt werden		x	x	
Die Lösung ist in der Lage mindestens auf Basis folgende Gerätetypen Peripheriegeräte zu überwachen und zu blockieren:				
Bluetooth-Geräte		x	x	
Wechseldatenträger		x	x	
Infrarot-Geräte		x	x	
Modem		x	x	
Optische Laufwerke		x	x	
WLAN Geräte		x	x	
MTP/PTP Geräte (Smartphones, Tablets, Kameras und Media Player, deren Verbindung über MTP- oder PTP-Protokolle erfolgt.)		x	x	
Für die Gerätetypen können mindestens folgende Zugriffsrichtlinien definiert werden:				
Erlaubt - Peripheriegeräte dieser Kategorie sind nicht beschränkt		x	x	
Blockieren - Peripheriegeräte dieser Kategorie sind nicht erlaubt		x	x	
Schreibgeschützt - auf Peripheriegeräte dieser Kategorie kann nur lesend zugegriffen werden (Wechseldatenträger und optische Laufwerke)		x	x	
Netzwerkbrücken Speren - verhindert die Nutzung von WLAN bei existierender LAN-Verbindung (WLAN)		x	x	
Folgende Anforderungen an die Erstellung von Ausnahmen (White-/Blacklist) werden erfüllt:				
Ausnahmen können auf Basis eines Geräte-Modells oder für ein einzelnes Gerät (eindeutige ID) erstellt werden		x	x	
Beim Hinzufügen von Ausnahmen wird eine Liste mit allen bislang erkannten Peripheriegeräte inkl. aller relevanten Details zur Identifizierung des Gerätes angezeigt. Ein oder meherere Geräte können aus dem Liste ausgewählt und in die Liste überführt werden		x	x	
Pro Ausnahme können Zugriffsrechte (Zulassen/Blockieren, Schreibgeschützt, Netzwerkbrück verhindern) definiert werden				
Der Benachrichtigungstext, der dem Anwender im Falle einer Geräte-Sperrung angezeigt wird, kann angepasst werden		x	x	

Beschreibung der Anforderungen	Wichtigkeit	MDR-COMPLETE	VRMDR-COMPLETE	Bemerkung
Überwachung von Anwendungen (Application Control)				
Auf Basis von Richtlinien kann festgelegt werden, welche Anwendungen nicht verwendet bzw. nicht installiert werden können. Die Nutzung einer gesperrten Anwendung wird direkt beim Start der Anwendung bzw. bei deren Installation unterbunden		x	x	
Die Überwachungsfunktion für Anwendungen kann wie folgt eingestellt werden:				
Die Überwachung für Anwendungen wird vollständig deaktiviert		x	x	
Die Nutzung von Anwendungen wird überwacht und protokolliert, aber nicht eingeschränkt		x	x	
Die Nutzung von Anwendungen wird anhand von Zugriffsrichtlinien für Anwendungskategorien und einzelnen Anwendungen eingeschränkt (Blacklist-Verfahren)		x	x	
Folgende Anforderungen werden erfüllt:				
Blacklist-Verfahren: Nur Anwendungen deren Nutzung eingeschränkt werden soll, müssen der Lösung bekannt sein		x	x	
Die Lösung stellt die Anwendungskategorien und Erkennungen für Anwendungen, die zur Überwachung und Einschränkung der Nutzung benötigt werden, zur Verfügung.		x	x	
Pro Anwendungskategorie kann festgelegt werden, ob neue / künftige Anwendungen dieser Kategorie automatisch gesperrt werden sollen, oder nicht		x	x	
Die Anwendungskategorien und die Erkennungen für Anwendungen werden regelmäßig durch die Lösungsanbieter aktualisiert und automatisch über einen Kanal zur Nutzung bereitgestellt		x	x	
Mindestens die Erkennungen für alle gängien Anwendungen in den Kategorien Browser (u.a. IE, Chrome, Firefox), Online Speicher (u.a. Dropbox, OneDrive) und Remote Management Tools (u.a. Teamviewer, VNC) müssen bereitgestellt werden		x	x	
Der Benachrichtigungstext, der dem Anwender im Falle einer Geräte-Sperrung angezeigt wird, kann angepasst werden		x	x	
Im Rahmen von On-Demand-Scans kann eine Prüfung vorgenommen und Sperrungen umgesetzt werden, sofern auf einem System eine gesperrte Anwendung installiert ist oder sich ein Instalaltionspaket einer zu sperrenden Anwendung befindet		x	x	
Application Whitelisting (Server Lockdown)	!			
Verhindert, dass Software auf dem Server ausgeführt werden kann, die sich nicht auf der systemspezifischen Whiteliste befindet			x	
Folgende Anforderungen an den Whitelist-Erstelllungsprozess werden erfüllt:				
Über die zentral Verwaltung kann ein Automatismus gestartet werden, der eine systemspezifische Whitelist für ausgewählte System erstellt			x	
Alle Betriebsystemkomponenten inkl. Windows Update werden zur Whiteliste hinzugefügt			x	
Alle installlierten Anwendungen inkl. derer Update-Prozesse werden automatisch zur Whiteliste hinzugefügt			x	
Dateien/Odner können über die zentrale Verwaltung zur Whiteliste eines oder mehrerer Systeme hinzugeführt werden			x	
Dateien/Odner können über die zentrale Verwaltung von der Whiteliste eines oder mehrerer System entfernt werden			x	
Bei Bedarf kann das Whitelistverfahren auf einem System über die zentrale Verwaltung unmittelbar und vollständig deaktiviert werden.			x	
Cloud Security Posture Management				
Security Posture Management	!		x	
Inventarisierung von Cloud Ressourcen	!		x	
Überprüfung der Sicherheit von Konfigurationen	!		x	
Compliance-Überprüfung der Richtlinien	!		x	
Integration von AWS und Azure Diensten	!		x	
Anomalieerkennnung im Benutzerverhalten und im Netzwerk	!		x	
Data Loss Prevention (Data Control)				
Auf Basis eines Regelwerks, kann der Transfer von Dateien mit sensiblen Daten überwacht und beschränkt werden		x	x	
Der DLP Schutz kann wie folgt eingestellt werden:				
Die Überwachung des Datentransfers wird vollständig deaktiviert		x	x	
Der Datentransfer wird überwacht, Regelverstöße werden protokolliert und der Benutzer durch einen Dialog auffordert, die Datenübertragung zu bestätigen		x	x	
Der Datentransfer wird überwacht, Regelverstöße werden protokolliert und der Benutzer durch einen Dialog informiert, dass die Übertragung blockiert wurde		x	x	
Der Datentransfer wird überwacht, Regelverstöße werden protokolliert, die Übertragung wird zugelassen		x	x	
Folgende Anforderungen an das Regelwerk der Lösung werden erfüllt:				
Inhaltsregeln: Die Übertragung kann auf Basis des Inhalts einer Datei gesteuert werden		x	x	
Dateiregel: Die Übertragung kann auf Basis des Dateityps oder Dateinamens gesteuert werden		x	x	
Zur Überprüfung des Dateityps kommt ein "True File-Type"-Erkennungsverfahren zum Einsatz. Eine Überprüfung des Dateitypes auf Basis der Dateiendung ist nicht ausreichend.	!	x	x	
Der Datentransfer zu folgenden Anwendungen bzw. über folgende Wege kann überwacht und eingeschränkt werden:				

Beschreibung der Anforderungen	Wichtigkeit	MDR-COMPLETE	VRMDR-COMPLETE	Bemerkung
Email-Clients: Lotus Notes, Outlook, Outlook Express, Thunderbird		x	x	
Internet Browser: Firefox, Internet Explorer, Google Chrome		x	x	
Instant Messaging & VoiP: Microsoft Lync/Skype, WebEx Connect		x	x	
Speicher: Optische Laufwerke, Wechselmedien		x	x	
Die Lösung liefert von Haus aus mindestens folgende Erkennungsmuster, um die Übertragung von Dateien anhand von Inhaltsregel einschränken zu können:				
Kontodaten: Kontonummern, Bankleitzahlen (BLZ), IBAN, SWIFT/BIC, Kredit-/Debitkartennummern		x	x	
Personenbezogene Daten: Sozialversicherungsnummern (VSNR), Renterversicherungsnummern (SV-Nr.), Telefonnummern, Postanschriften, E-Mail Adressen		x	x	
Inhaltsregeln: Zur Erkennung von Daten stehen auf Deutschland / EU angepasste Vorlagen zur Verfügung		x	x	
Inhaltsregeln: Es können manuell weitere Erkennungsmuster angelegt werden		x	x	
Inhaltsregeln: Es können Inhaltsregeln auf Basis von selbstdefinierten Begriffen (Schlagworten) erzeugt werden		x	x	
Inhaltsregeln: Es können Inhaltsregeln auf Basis von selbstdefinierten regulären Ausdrücken erzeugt werden		x	x	
Web Control				
Die Lösung bietet die Möglichkeit den Zugriff auf bestimmte Web-Inhalte und Downloads einzuschränken. Die Einschränkungen werden durch einen lokal installieren Agenten umgesetzt.		x	x	
Der Download folgender riskanter Dateitypen kann über eine True-File-Type Erkennungsverfahren eingeschränkt werden werden:				
ActiveX Controls (ocx)		x	x	
Adobe Flash Video (flv, swf)		x	x	
Adobe PDF (pdf)		x	x	
DOS-Befehlsdatei (com)		x	x	
Java Applet (Class)		x	x	
Java Archiv (jar)		x	x	
Sonstige ausführbare Dateien		x	x	
Windows Bibliotheksdatei (dll)		x	x	
Windows Executable (exe)		x	x	
Windows Installer (msi)		x	x	
Der Zugriff auf folgende Kategorien für Web-Inhalte können eingeschränkt werden:				
Werbung		x	x	
Nicht kategorisierte Seiten		x	x	
Produktivitätsbezogene Kategorien (u.a. Glücksspiel, Jobsuche, Immobilien, Shopping, Sport, Unterhaltung, Reise etc.)		x	x	
Soziale Netzwerke (u.a. Blogs und Foren, Chat, Dating etc.)		x	x	
Jugendgefährdende und potenziell unangebrachte Inhalte (u.a. Alkohol und Tabak, Gewalt, Hacking, Illegale Drogen, Pornografie, Waffen etc.)		x	x	
Übermäßige Bandbreitennutzung (Streaming Medien, Peer-to-Peer)		x	x	
Geschäftsrelevante Kategorien (u.a. Bildung und Forschung, Business, Suchmaschinen, Öffentlicher Dienst, Wohlfahrts- und Berufsverbände etc.)		x	x	
Webbasierte E-Mails und Downloads		x	x	
In den Richtlinien kann pro Kategorie und Unterkategorie festgelegt werden, ob der Zugriff auf die entsprechenden Web-Inhalte erlaubt, verboten oder der Benutzer gewarnt werden soll		x	x	
Ausnahmen und Anpassung der Kategorisierung:				
Es können neue Kategorien für Web-Inhalte erstellt werden, denen Web-Seiten manuell zugeordnet werden können		x	x	
Die Zuordnung einer Web-Seite zu einer Inhaltskategorie kann manuell überschrieben werden		x	x	
Protokollierung: Nur Versuche, infizierte Websites zu besuchen, werden protokolliert.		x	x	
Protokollierung: Alle Versuche, blockierte Websites trotz Warnung zu besuchen, werden protokolliert.		x	x	
Windows Firewall Management				
Überwacht und berichtet den Status (in-/aktiv) der Windows Firewall an die zentrale Verwaltung		x	x	
Berichtet den Status (in-/aktiv) einer 3rd party Firewall an die zentrale Verwaltung		x	x	
Ermöglicht die Konfiguration eines der folgendenden Verbindungstypen pro Firewall Profil (Domain, Private, Public):				
Alle eingehenden Verbindungen erlauben		x	x	
Alle eingehenden Verbindungen blockieren		x	x	

Beschreibung der Anforderungen	Wichtigkeit	MDR-COMPLETE	VRMDR-COMPLETE	Bemerkung
Alle eingehenden Verbindung mit Ausnahmen blockieren		x	x	
Berichtet Block-Ereignisse der Windows Firewall an die zentrale Verwaltung		x	x	
Berichtet, ob die Windows Firewall über Gruppenrichtlinien (GPO) verwaltet wird		x	x	
Manipulationsschutz				
Ein Manipulationsschutz verhindert, dass am System selbst Einstellungen durch Unberechtigte geändert oder Schutz-Mechanismen deaktiviert werden können		x	x	
Der Manipulationsschutz verhnidert mindestens folgende Angriffe auf die Lösung:				
Dienste der Lösung über den Dienste-Bereich des Betriebssystems (services.msc) beenden		x	x	
Dienste der Lösung über den Task Manager des Betriebssystems beenden		x	x	
Dienste der Lösung über die Kommandozeile des Betriebssystem beenden		x	x	
Die Konfiguration der Dienste der Lösung über den Dienste-Bereich des Betriebssystems (services.msc) ändern		x	x	
Die Konfiguration der Dienste der Lösung über die Kommandozeile des Betriebssystems ändern		x	x	
Deinstallation der Lösung		x	x	
Erneute Installation der Lösung		x	x	
Beenden von Prozessen der Lösung über Task Manager		x	x	
Löschen und Ändern geschützer Dateien oder Verzeichnisse der Lösung		x	x	
Löschen und Ändern geschützter Registry-Keys der Lösung		x	x	
Der Maniplationsschutz kann am System selbst durch Eingabe eines Kennwortes deaktiviert werden. Dieser Vorgang wird als Ereignis in der zentralen Verwaltung protokolliert		x	x	
Das Kennwort zur Deaktivierung des Manipuationsschutzes wird automatisch erstellt, ist individuell/systemspezifisch und wird in den zentralen Verwaltung hinterlegt		x	x	
Der Manipulationsschutz kann über die zentrale Verwaltung pro System de-/aktiviert werden.		x	x	
Um eine nachträgliche Deaktivierung zu ermöglichen, werden die Kennwörter zur Deaktivierung des Manipulationsschutzes über den Zeitraum der Löschung eines Systems hinaus in der Verwaltungsobfläche gespeichert		x	x	
Support				
Rund um die Uhr (24x7) direkten Hersteller-Support, telefonisch bzw. Online-Formular bzw. Support Portal		x	x	
Zugriff auf Support Wissensdatenbank und Support Foren		x	x	
Zugriff auf Software-Downloads, Updates und Wartung		x	x	
Alle relevanten Diagnosedaten eines Endgeräts können direkt über das Management angefordert werden.		x	x	