G DATA CyberDefense

Ratgeber:

So finden Sie den passenden Managed-XDR-Anbieter

Inklusive Checkliste

Whitepaper

Ratgeber:

So finden Sie den passenden Managed-XDR-Anbieter

Whitepaper

Immer mehr Unternehmen machen sich auf die Suche nach einem Anbieter für Managed Extended Detection and Response (MXDR), um ihre IT-Systeme von externen Fachleuten überwachen zu lassen. Es ist jedoch nicht leicht, aus der Vielzahl von Dienstleistern den richtigen Partner zu finden.

Dieser **Buyer's Guide** gibt allen Entscheider*innen, Fach- und Führungskräften einen Leitfaden an die Hand. Eine Checkliste fasst die Punkte zusammen, die Sie bei der Auswahl eines Managed-XDR-Anbieters beachten sollten.

Inhaltsverzeichnis

Warum Managed XDR?

Etwa 150 bis 250 Tage dauert es, bis Unternehmen einen Cyberangriff bemerken.[1] In dieser Zeit kundschaften Cyberkriminelle das Netzwerk aus, um zum Beispiel die Verschlüsselung von Daten vorzubereiten. Sie hinterlassen dabei zwar Spuren, doch diese aufzuspüren ist für viele IT-Teams nur schwer möglich. Es fehlt Fachpersonal und Zeit, um täglich den Berg an Meldungen aller Sicherheitslösungen durchzuarbeiten und den Kontext auf Angriffe zu prüfen. Denn gleichzeitig braucht wieder ein Kollege Hilfe bei einem Software-Problem und das nächste IT-Ticket wartet.

Eine zusätzliche Herausforderung ist die neue NIS-2-Richtlinie der EU. Mit NIS-2 gelten ab Oktober 2024 für viele Unternehmen und Organisationen in 18 Sektoren verpflichtende IT-Sicherheitsmaßnahmen. Dazu zählt, dass sie Maßnahmen zur Erkennung, Analyse und Reaktion auf Sicherheitsvorfälle umsetzen müssen. Bei Verstößen drohen hohe Geldstrafen.

Immer mehr Unternehmen legen daher die Angriffserkennung und -abwehr in die Hände von spezialisierten IT-Security-Dienstleistern. Managed XDR hilft, die neuen NIS-2-Anforderungen zu erfüllen und stärkt die Resilienz von Unternehmen gegen Cyberangriffe.

Welche Kernelemente enthält Managed XDR?

Mit Managed Extended Detection and Response (MXDR) können sich Unternehmen darauf verlassen, dass Fachleute ihre IT Security immer im Blick haben. Speziell dafür ausgebildete Analyst*innen erkennen, untersuchen und stoppen Cyberangriffe für Sie – rund um die Uhr. So können sie auch Angriffe um 1 Uhr nachts oder am Wochenende direkt aufhalten.

Dazu nutzen die Analyst*innen XDR Software: Auf Endgeräten wie PCs und Servern werden Agenten installiert, die in Echtzeit die Ereignisse auf den Geräten erfassen. Die Agenten schicken die Daten an ein Analyse-Backend, also eine zentrale cloudbasierte XDR-Plattform der Herstellerfirma. Mithilfe von Machine Learning korreliert und analysiert die XDR-Plattform die Daten, um verdächtiges Verhalten festzustellen.

Sobald sie etwas als verdächtig einstuft, löst sie einen Alarm bei den Analyst*innen aus. Je nach Fall kann die XDR-Plattform auch direkt automatisiert reagieren, um zum Beispiel einen PC vom Netzwerk zu isolieren. Die Analyst*innen untersuchen den gesamten Kontext und prüfen mithilfe ihrer Expertise, ob es tatsächlich ein Angriff ist (Detect). Sie greifen bei Bedarf manuell ein, um Angreifende wieder auszusperren (Respond). Die Kunden werden per E-Mail benachrichtigt und in akuten Fällen direkt angerufen.

Das „X“ in „XDR“ steht für „Extended“, da XDR die Weiterentwicklung von Endpoint Detection and Response (EDR) ist. EDR sendet zwar auch Daten an eine Plattform, aber analysiert diese nur isoliert pro einzelnen Endpoint. XDR hingegen setzt diese Daten miteinander in Beziehung. Diese Korrelation erlaubt wertvolle Rückschlüsse darauf, was im Netzwerk passiert.

1 Quelle: brand eins, G DATA & Statista: „Cybersicherheit in Zahlen 2023/24“, S. 36

Checkliste: 14 Fragen, um den richtigen Managed-XDR-Anbieter zu finden

Die folgenden Fragen fassen zusammen, was es bei der Auswahl eines Managed-XDR-Anbieters zu beachten gibt. Sie können die Antworten einfach recherchieren oder die Anbieter direkt danach fragen.

Umfang der Dienstleistung

1. Handelt es sich um reine XDR Software oder um Managed XDR?

Bei manchen Angeboten ist der Umfang nicht klar ersichtlich, sodass sie auf den ersten Blick günstiger erscheinen. Prüfen Sie daher immer: Handelt es sich um eine reine XDR Software? Dann benötigen Sie ein eigenes Analysten-Team mit hohen Fachkenntnissen, um die XDR-Meldungen zu untersuchen und die richtigen Gegenmaßnahmen zu ergreifen – und das im Schichtbetrieb rund um die Uhr. Ansonsten bleibt der Sicherheitsgewinn aus, den XDR bieten kann. Mit Managed XDR übernimmt dies komplett der Dienstleister für Sie.

2. Umfasst der Service auch die Reaktion auf Angriffe?

Achten Sie darauf, was genau der Managed-XDR-Anbieter für Sie übernimmt – und was nicht. Manche beschränken sich darauf, Angriffe zu erkennen und Sie lediglich zu informieren. Damit liegt jedoch die gesamte Arbeit der Reaktion wieder bei Ihnen – also kein echter Zeit- und Sicherheitsgewinn. Ein guter Dienstleister übernimmt die komplette Reaktion für Sie. Das heißt: Die Analyst*innen rekonstruieren, wie die Angreifenden eindringen konnten. Sie dämmen den Angriff ein und bereinigen ihn, indem sie zum Beispiel persistente Malware entfernen und Registry-Einträge säubern. Es sollte nur noch in wenigen Fällen Ihr Mitwirken nötig sein.

Tipp:

Zeitangaben sind nur schwer zu vergleichen. Die „Mean Time To Detect (MTTD)“ oder „Mean Time To Respond (MTTR)“ sind zwar hilfreiche Kennzahlen. Doch sie können je nach Anbieter etwas ganz anderes bedeuten – etwa eine automatisierte Reaktion oder aber eine Reaktion durch Analyst*innen.

3. Ist der Managed-XDR-Anbieter rund um die Uhr im Einsatz?

Ein häufiger Grund, warum sich Unternehmen für Managed XDR entscheiden, ist die 24/7-Abdeckung. Denn das eigene IT-Team arbeitet nur zu Geschäftszeiten – aber Angreifende schlagen auch um 1 Uhr nachts zu. Prüfen Sie daher, ob der Anbieter rund um die Uhr Ihre IT-Systeme überwacht, auch an Feiertagen und an Wochenenden.

4. Wird eine „Garantie“ angeboten, bei der Sie genauer hinschauen sollten?

Manche Dienstleister bieten zusammen mit Managed XDR eine „Garantie“ an. Häufig sind diese jedoch an Bedingungen und Nachweise geknüpft. Schauen Sie daher ins Kleingedruckte: Welchen Betrag bekommen Sie im Schadensfall unter welchen Bedingungen tatsächlich erstattet? Handelt es sich ggf. nur um ein Guthaben statt einer Auszahlung? Die Erstattungen stehen häufig in keinem Verhältnis zu den Verlusten durch etwa Produktionsausfälle. Zudem hilft es nicht viel, wenn das Geld erst ein Jahr später kommt. Im Gegensatz zu vollwertigen Cyber-Versicherungen gelten solche „Garantien“, die nicht als „Versicherung“ bezeichnet werden dürfen, in der Branche nicht als seriös.

Datenschutz

5. Wo sitzt der Dienstleister?

Ein Managed-XDR-Anbieter erhält einen tiefen Einblick in Ihre IT-Infrastruktur und hat sogar hohe Einwirkungsmöglichkeiten. Deshalb sollten Sie diesem Anbieter sehr vertrauen können. Einen wichtigen Hinweis hierfür liefert der Unternehmenssitz. Anbieter aus Deutschland sind den strengen deutschen und europäischen Datenschutzgesetzen verpflichtet. Zudem sind sie verpflichtet, Daten nur in Verdachtsfällen einzusehen – und zwar nur so viele, wie absolut nötig sind für die Analyse. In vielen anderen Ländern gibt es diese Vorgabe nicht.

6. Wo stehen die Server zur Datenhaltung?

Wenn es um sensible Daten und Cloud-Lösungen geht, ist der Server-Standort besonders wichtig. Erkundigen Sie sich beim Anbieter, in welchem Land die Server zur Datenhaltung stehen und welchen Firmen diese Server gehören. Bei manchen Anbietern liegen die Daten in Übersee, wo sie eventuell nicht ausreichend vor Fremdzugriff – auch durch Regierungen – geschützt sind. Am besten ist es daher, wenn die Server in Deutschland stehen und vom Managed-XDR-Anbieter selbst oder einem deutschen Cloud-Anbieter betrieben werden.

7. Wie gut ist die Datenübertragung abgesichert?

Die Kommunikation zwischen den Software-Agenten auf Ihren Geräten und der XDR-Plattform darf auf keinen Fall von Dritten eingesehen werden. Der Kanal sollte daher mehrstufig gesichert sein. Die gesamte Kommunikation sollte über TLS nach aktuellsten Standards verschlüsselt stattfinden. Das gilt besonders für den Response-Rückkanal, der die Möglichkeit zum Eingreifen in Ihre IT-Systeme bietet. Hier sollte zusätzlich der Inhalt jeder Nachricht von intern autorisiert und protokolliert werden. Autorisierte Nachrichten sollten mit Hilfe von Public-Key-Kryptographie signiert und vom Software-Agenten überprüft werden.

Individuelle Betreuung

8. Gibt es Support in deutscher Sprache, der sich genug Zeit für Sie nimmt?

Egal ob Sie Hilfe bei einer Handlungsempfehlung brauchen oder sonstige Fragen haben: Gerade bei einem so wichtigen Thema sollten Sie immer jemanden telefonisch erreichen können, der Ihnen weiterhilft. Hier sind die Unterschiede zwischen Managed-XDR-Anbietern oft sehr groß. Viele bieten Telefonsupport erst ab teureren Service-Leveln an, ansonsten nur per E-Mail. Dann können Sie auch in dringenden Fällen nur hoffen, nicht zu lange auf eine Antwort warten zu müssen. Und wenn es Telefonsupport gibt, landen Sie oft bei anonymen Callcentern, wo Sie in wenigen Minuten und in schlechtem Englisch abgehandelt werden. Prüfen Sie daher:

- Sitzt das Support-Team in Deutschland, im Idealfall am Hauptsitz des Anbieters?
- Ist telefonische Erreichbarkeit rund um die Uhr in allen Service-Leveln enthalten?
- Nimmt sich der Support genug Zeit für Sie, um Ihr Anliegen zu klären?

Tipp:

Sie können einen Eindruck erhalten, wieviel Zeit sich der Support für Sie nimmt, indem Sie eine Testversion anfordern und einen Probeanruf machen.

9. Wie detailliert können Sie Ausnahmen definieren?

Haben Sie Server, die die Produktion steuern oder andere Prozesse, die nicht durch Isolation ausfallen sollten? Es ist wichtig, dass Sie sehr fein definieren können, welche Geräte, Prozesse oder Dateien der Anbieter zwar prüfen, aber auf denen er keine Reaktion

vornehmen soll – oder welche er gar nicht einsehen darf. Je granularer, desto besser, damit nicht unnötig viel ausgeschlossen werden muss. Manche Managed-XDR-Anbieter bieten nur global geltende Möglichkeiten für Ausnahmen an. Erkundigen Sie sich daher, wie fein Sie Ausnahmen bestimmen können.

10. Können Sie sehen, was der Anbieter im Hintergrund tut?

Um die Kontrolle zu behalten, ist es vielen Unternehmen wichtig, dass sie stets nachschauen können, was im Hintergrund passiert. Gute Dienstleister bieten daher eine Webkonsole, in der Sie jederzeit in Echtzeit sehen können, welche Security-Vorfälle es gab, was die Analyst*innen für Sie getan haben und ob Handlungsempfehlungen für Sie vorliegen.

11. Sind Handlungsempfehlungen leicht verständlich?

Falls einmal Ihr Mitwirken erforderlich ist, sollten die Handlungsempfehlungen so formuliert sein, dass sie leicht verständlich und umzusetzen sind. Dafür ist es auch hilfreich, wenn sie auf Deutsch sind. Bei manchen Anbietern erfordern die Handlungsempfehlungen jedoch viel Fachwissen und lassen kleinere IT-Teams ratlos zurück.

Tipp:

Fragen Sie, ob es möglich ist, Beispiele für Handlungsempfehlungen zu sehen. So können Sie einen Eindruck bekommen, wie aufwändig diese umzusetzen sind.

Expertise

12. Ist der Anbieter auf IT Security spezialisiert? Wenn ja, wie lange schon?

Ein Grund für die Investition in Managed XDR ist, die eigenen Fähigkeiten mit der Expertise externer Fachleute zu erweitern. Wählen Sie daher einen Dienstleister mit hoher und langjähriger Spezialisierung in IT-Sicherheit. Solche Anbieter verfügen über wertvolles Hintergrundwissen, um Vorfälle genauer zu beurteilen – etwa aus dem Austausch mit der weltweiten Cybercrime Research Community. Wenn er zudem auch Incident Response anbietet, kann er aktuelles Wissen aus IT-Notfalleinsätzen und der Zusammenarbeit mit Strafverfolgungsbehörden ziehen. Die Qualifizierung als APT-Response-Dienstleister vom Bundesamt für Sicherheit in der Informationstechnik (BSI) ist ein weiteres Merkmal für eine hohe IT-Security-Expertise.

13. Hat der Anbieter die XDR Software selbst entwickelt? Wenn ja, wo sitzt die Entwicklung?

Viele Anbieter kaufen die XDR Software lediglich ein und bieten dazu ihren Service an. Dies birgt das Risiko, dass die Analyst*innen die Meldungen falsch interpretieren. Achten Sie daher darauf, dass der Anbieter die XDR Software selbst entwickelt – von den Software-Agenten über das Analyse-Backend bis zur Webkonsole. Dadurch wissen die Analyst*innen genau, wie Meldungen zu verstehen sind und können richtig darauf reagieren. Im Idealfall sitzt die Entwicklung in Deutschland. Unternehmen mit dem TeleTrust-Siegel „IT Security Made in Germany“ haben sich verpflichtet, vertrauenswürdige Lösungen ohne Hintertüren zu entwickeln.

Testmöglichkeiten

14. Gibt es eine Testversion, um Managed XDR in Ihrer eigenen Umgebung auszuprobieren?

Wie gut ein Dienstleister tatsächlich schützt, hängt von den individuellen Systemen, dem Verhalten der Anwender*innen und der eingesetzten Software ab. Prüfen Sie daher, ob der Dienstleister eine Testversion anbietet. Dabei überwacht er für einen bestimmten Zeitraum eine begrenzte Anzahl Ihrer Endgeräte und Server. So probieren Sie Managed XDR unter realen Bedingungen aus. Sie können außerdem durch Probeanrufe herausfinden, wie gut Ihnen der Support bei Fragen weiterhilft.

Aus der Praxis: Interview mit Thomas Rüby, IT-Leiter Landratsamt Dachau

Thomas Rüby ist IT-Leiter im Landratsamt Dachau und setzt auf Managed XDR. Im Interview erzählt er, worauf er beim Kauf geachtet hat, wie der Wechsel von der Endpoint Security zu Managed XDR funktioniert hat und welche Rolle der Datenschutz spielt.

Wieso haben Sie sich entschlossen, Ihre vorherige Endpoint Security Software durch eine Managed-XDR-Lösung abzulösen?

Thomas Rüby: *„Alles begann 2022. Der Vertrag mit dem alten Anbieter hatte nicht mehr viel Laufzeit. Wir haben uns damit auseinandergesetzt, was der Security-Markt bietet und schnell festgestellt, dass rein signaturbasierte Sicherheitslösungen nicht mehr „state of the art“ sind und man wesentlich mehr für die IT-Sicherheit tun kann. Die Weiterentwicklung der Angriffsarten, zum Beispiel durch Künstliche Intelligenz, erfordert andere Abwehrmaßnahmen. Wir haben gemerkt, dass der Einsatz einer Extended-Detection-and-Response-Lösung Sinn macht, wir aber eine gemanagte Variante benötigen.*

Wir betreuen im Landratsamt Dachau über 400 IT-Services, darunter beispielsweise auch Kassenautomaten. Wir sind IT-Allrounder, aber keine Spezialisten für IT-Sicherheit. Außerdem ist der Fachkräftemangel für uns ein großes Problem. Wir können kein 24/7-Team unterhalten, deswegen war schnell klar, dass wir auf externe Expertise setzen müssen. Bei einem Cyberangriff ist es für uns sowohl vom Know-how als auch vom Zeit- und Ressourcenaufwand her schwer, zu schauen, was passiert ist und zu reagieren. Wir wollten nicht nur eine Security Software einkaufen, sondern auch Expertise. Wir haben eine Lösung gesucht, die Schäden und Risiken zuverlässig minimiert und uns mit Wissen und Erfahrung unterstützt – damit im Bedarfsfall die richtigen Maßnahmen erfolgen.“

Haben Sie verschiedene Anbieter verglichen? Was sprach besonders für G DATA?

Thomas Rüby: *„Wir haben uns verschiedene Anbieter angeschaut, die eine gemanagte XDR-Lösung anbieten und um Abgabe eines Angebots gebeten. Wir haben dazu ein Leistungsverzeichnis erstellt und uns aufgrund des Datenschutzes nur auf europäische Unternehmen fokussiert. G DATA hat alle Anforderungen erfüllt und dabei auch das beste Angebot abgegeben. Damit war die Entscheidung gefallen.*

Für G DATA spricht, dass es sich um ein deutsches Unternehmen handelt und sowohl die Produktentwicklung als auch der Support hier in Deutschland sitzen. Der Datenschutz und

die Datenhaltung hier im Inland waren weitere Pluspunkte. Außerdem hatten wir von Beginn an einen sehr guten Kontakt zu G DATA und konnten alle Fragen schnell klären. Die Chemie hat einfach gestimmt.“

Ist Ihnen der Standort des Anbieters und der Ort der Datenhaltung wichtig gewesen?

Thomas Rüby: *„Das ist uns sehr wichtig. Die Daten unserer Bürgerinnen und Bürger sind unser Heiligtum und müssen von uns auch gut geschützt werden. Wir haben hier im Haus einen zurecht sehr strengen Datenschützer, der natürlich penibel auf die Einhaltung der Gesetze achtet. Auf einen europäischen Hersteller zu setzen war daher eine klare Voraussetzung bei diesem Projekt. Bei einer gemanagten XDR-Lösung ist auch eine Cloud im Einsatz, da ist es wichtig, wo die Server stehen.*

Der Standort von G DATA hier in Deutschland ist für uns von zentraler Bedeutung. Der Hersteller sitzt in Reichweite und ich habe einen guten Draht dorthin und kann mir im Fall von Problemen und Fragen direkte Unterstützung holen.“

Wie waren Ihre Erfahrungen beim Onboarding von der alten Lösung zu Managed XDR?

Thomas Rüby: *„Wir haben sehr gute Erfahrungen beim Onboarding gemacht. Wir wurden gut betreut. Es gab lediglich Probleme bei der Deinstallation der vorherigen Sicherheitslösung. Diese ließen sich aber auch schnell lösen. Meine Administratoren, die unter anderem auch die Softwareverteilung vornehmen, haben das schlanke Setup und die Ressourcensparsamkeit vom G DATA Agent sehr gelobt.*

Besonders positiv war, dass das Setup Probleme und auch deren Ursachen zurückgemeldet hat. Das war sehr hilfreich, weil eine direkte Reaktion möglich war. Dadurch hat die Installation sehr gut funktioniert.“

Was versprechen Sie sich davon, Managed XDR im Einsatz zu haben?

Thomas Rüby: *„Wir möchten eine höchstmögliche Sicherheit vor Cybergefahren schaffen und das Schadensmaß bei einem Vorfall so gering wie möglich halten. Wir möchten, dass unsere Systeme auch außerhalb der Arbeitszeiten und am Wochenende gut geschützt sind. Wichtig für uns ist die umgehende Reaktion bei Vorfällen und die Unterstützung bei der Analyse. Es muss geklärt werden, was überhaupt passiert ist. Ich muss nach der EU-Datenschutzgrundverordnung und anderen Vorschriften nicht nur den Nachweis eines Datendiebstahls erbringen, sondern wir brauchen auch Transparenz über die Aktivitäten der Schadsoftware. Das ist sehr wichtig für uns.*

Daraus resultiert die Frage, welche Maßnahmen wir ergreifen müssen, um angemessen zu reagieren, zum Beispiel ob wir auf das fünf Tage alte Backup oder ein älteres zurückgreifen müssen, um die Systeme wiederherzustellen.

Natürlich geht es uns auch um eine ständige Verbesserung unserer IT-Sicherheit - unter anderem wollen wir durch die Handlungsempfehlungen von G DATA Lücken im System schließen. Wir möchten auch Angriffe besser verstehen, um zukünftige Attacken zu vermeiden. Wir möchten uns nicht nur auf die Prävention, wie das Einspielen von Updates verlassen. Die Abwehr unbekannter Angriffe wollen wir schon im Vorfeld angehen.

Da setzen wir auf die Erfahrung und das Wissen von G DATA. Wir möchten mit den Angreifergruppen Schritt halten, um schneller und richtig auf Vorfälle reagieren zu können. Bei einem Angriff möchten wir möglichst schnell Zugriff auf die Experten haben. Wir selbst bräuchten viel zu viel Zeit, um Informationen zu beschaffen und Maßnahmen einzuleiten, daher brauchen wir die externe Expertise.“ ■

G DATA: Managed XDR aus Deutschland

Als erfahrener IT-Sicherheitsspezialist aus Deutschland stehen wir Ihnen mit G DATA 365 | MXDR zur Seite: Unsere Analyst*innen überwachen Ihre IT-Systeme – rund um die Uhr, an 365 Tagen im Jahr. Wir erkennen, analysieren und reagieren für Sie auf Angriffe, bevor sie Schaden anrichten. Bei akuten Vorfällen rufen wir Sie direkt an.

G DATA Managed XDR ist eine gute Wahl für alle, die besonderen Wert auf Datenschutz und persönliche Betreuung legen.

Über G DATA:

- IT-Sicherheitsspezialist mit Hauptsitz in Bochum, Deutschland
- Fast 40 Jahre Erfahrung in der Erforschung und Abwehr von Cybergefahren
- Umfassende Cyber Defense für Privatanwender und Unternehmen
- Services von Managed XDR über Penetrationtests bis Incident Response
- G DATA Advanced Analytics GmbH ist BSI-qualifizierter APT-Response-Dienstleister

SecurITy made in Germany

Ihre Vorteile mit Managed XDR „Made in Germany“:

Höchster Datenschutz

Als deutsches Unternehmen sind wir den strengen deutschen Datenschutzgesetzen verpflichtet. Unsere Analyst*innen sehen Daten nur in Verdachtsfällen ein und nur, soweit Sie es uns beim Onboarding gestatten.

Datenhaltung in Deutschland

Die Datenhaltung erfolgt ausschließlich auf Servern in Deutschland: an unserem Hauptsitz in Bochum sowie auf den Servern unseres Partners, des deutschen Cloud-Anbieters IONOS, in Frankfurt und Berlin.

Prämierter 24/7-Support aus Deutschland

Bei jeglichen Fragen ist unser deutschsprachiger Support am Hauptsitz telefonisch für Sie da. Rund um die Uhr. Komplett kostenfrei. Wir nehmen uns immer Zeit für Sie – und zwar die Zeit, die es braucht.

Kontrolle behalten

Legen Sie mit uns gemeinsam fest, welche Geräte, Prozesse oder Dateien wir zwar prüfen, auf denen wir aber keine Reaktion vornehmen sollen. Oder welche wir gar nicht einsehen müssen.

Alles im Blick

In Ihrer Webkonsole sehen Sie in Echtzeit, welche Vorfälle es gab, was wir für Sie getan haben und ob Handlungsempfehlungen für Sie vorliegen. Diese sind klar verständlich und leicht umzusetzen.

Eigene XDR-Technologie aus Deutschland

Wir entwickeln die XDR Software komplett selbst – ebenfalls in Deutschland. So wissen wir genau, wie Alarme zu verstehen sind und können richtig reagieren. Als Träger des Siegels „IT Security Made in Germany“ haben wir uns verpflichtet, Lösungen ohne Hintertüren zu entwickeln.

Das sagen unsere Kunden

„Der Standort von G DATA hier in Deutschland ist für uns von zentraler Bedeutung. Der Hersteller sitzt in Reichweite und ich habe einen guten Draht dorthin und kann mir im Fall von Problemen und Fragen direkte Unterstützung holen.“

Thomas Rüby

IT-Leiter | Landratsamt Dachau

„Für uns war wichtig, dass der Anbieter in Deutschland sitzt und auch Support in deutscher Sprache anbietet. Einmal wegen des Datenschutzes, aber auch, weil bei einem so wichtigen Thema keine sprachlichen Barrieren bestehen sollten.“

Heiko Streichert

IT-Administrator | etna GmbH

Testsieger 2023 im Umgang mit Kundendaten

Wie vertrauenswürdig sind IT-Sicherheitsunternehmen? Welche Informationen gewinnen sie mit ihrer Software, wie und wo werden die Daten gespeichert und welche Drittanbieter haben Zugang? Das haben Connect und AV-Comparatives genau untersucht.

Ergebnis: G DATA ist das vertrauenswürdigste Unternehmen und wird daher als Testsieger ausgezeichnet.