

Bitdefender®

GravityZone

LÖSUNGSLEITFADEN

So schützen Sie Ihr mittelständisches Unternehmen über den gesamten Threat Lifecycle hinweg



Alle Rechte vorbehalten. © 2025 Bitdefender. Alle hier genannten Marken, Handelsnamen und Produkte sind Eigentum ihrer jeweiligen Inhaber. Die in diesem Dokument enthaltenen Informationen sind vertraulich und nur für den Gebrauch durch den vorgesehenen Empfänger bestimmt.

Sie dürfen dieses Dokument nicht ohne vorherige Genehmigung durch Bitdefender veröffentlichen oder weiterverbreiten.

Umfang des Sicherheitsschutzes: Die Herausforderung für mittelständische Unternehmen

Laut einer Studie von IBM nutzen Unternehmen durchschnittlich 83 verschiedene Sicherheitslösungen. Es überrascht daher kaum, dass 52 % der Sicherheitsexperten die Komplexität als größtes Hindernis für einen effektiven Betrieb sehen¹. Für IT- oder Sicherheitsverantwortliche in mittelständischen Unternehmen, die um bestehende Sicherheitslücken wissen, mag dies zunächst wie ein Luxusproblem erscheinen.

Die meisten mittelständischen Unternehmen verfügen über die grundlegenden Systeme wie Endpoint Protection Platforms (EPP), E-Mail-Filterung und Patch Management. Viele schöpfen das Potenzial dieser bestehenden Tools jedoch nicht voll aus. Dadurch entstehen einige Sicherheitslücken, und in Kombination mit einem Mangel an präventiven Maßnahmen zur Gefährdungsbewältigung sind diese auf allen Angriffsflächen nicht gut zu erkennen.

Das ist eine nachvollziehbare Herausforderung. Für viele mittelständische Unternehmen können der Zeitaufwand, das benötigte Fachwissen und die Ressourcen, die für die vollständige Implementierung von Sicherheitstools erforderlich sind, überwältigend sein. Die Möglichkeiten, die größere Unternehmen haben, erscheinen ihnen vor diesem Hintergrund vermutlich unerreichbar. Der Schlüssel liegt darin, Wege zu finden, die Abdeckung zu erweitern und den Schutz auszubauen, ohne das Team zu überlasten.

Die Herausforderung für mittelständische Unternehmen: Wie lassen sich Sicherheitslücken schließen, ohne die Komplexität und die Kosten zu erhöhen?

Maximieren Sie Ihren ROI: Nutzen Sie alle Tools optimal

Die meisten mittelständischen Unternehmen haben bereits leistungsstarke Endpoint Detection and Response (EDR)-Systeme als Bestandteil ihres EPP im Einsatz, können diese aber nicht voll ausschöpfen. Die Einrichtung kann komplex sein, und ein hohes Aufkommen von Warnmeldungen führt zu überlasteten Teams und ungelösten Sicherheitsvorfällen.

Die Herausforderung im Zusammenhang mit der Komplexität von EDR hat ihre Wurzeln in seiner Geschichte. EDR wurde ursprünglich als Ergänzung zu EPP entwickelt, um Sicherheitsanalysten in die Lage zu versetzen, laufende Cyberangriffe zu erkennen und darauf zu reagieren. Es handelte sich um ein separates Tool, das für große Unternehmen mit Expertenteams für Sicherheitsoperationen (SecOps) entwickelt wurde, sodass Komplexität kein Problem darstellte.

Heute ist EDR Bestandteil aller führenden Endpoint-Sicherheitsprodukte. Im letzten Jahrzehnt haben EPP-Anbieter EDR-Funktionen aufgenommen, und EDR-Anbieter haben einen vollständigen EPP-Funktionsumfang geschaffen. Das Ergebnis ist, dass viele Implementierungen der Endpoint-Sicherheit ihren Ursprung im Enterprise-Umfeld haben und über einen komplexen Funktionsumfang verfügen, für dessen Verwaltung SecOps-Experten erforderlich sind.

Wenn Ihr EPP ungenutzte Funktionen enthält, deren Wert Ihr IT- und Sicherheitsteam nicht voll ausschöpfen kann, erzielen Sie keine Rendite auf Ihre Investition und setzen Ihr Unternehmen möglicherweise Gefahren aus. Die Lösung besteht darin, die EPP-Funktionen durch eine Lösung zu ersetzen, die EDR beinhaltet und speziell dafür entwickelt wurde, allen IT-Experten die Möglichkeit zu geben, schnell auf einen Vorfall zu reagieren und ihn einzudämmen, bevor er sich zu einer Sicherheitsverletzung ausweitet.

Maßnahme 1: Implementieren Sie eine Plattform für den Endpoint-Schutz, die Ihr Team in die Lage versetzt, seine Effektivität und Ihren ROI zu maximieren.

Mehr Kontext: **Extended Detection & Response**

Alleinstehende EDR-Funktionen sind hilfreich, konzentrieren sich aber primär auf Endpoint-Signale. Wenn diese Signale in die Schutzmaßnahmen für Identität, Cloud, Netzwerk und E-Mail einfließen, werden die Erkennung und Reaktion wesentlich effektiver. Dieser umfassendere Ansatz wird als Extended Detection and Response (XDR) bezeichnet. Dabei werden Signale aus Ihrer gesamten Umgebung korreliert, um IT- und Sicherheitsteams einen umfassenden Kontext zu liefern, sodass sie die Untersuchung der potenziell gefährlichsten Bedrohungen priorisieren können.

Für mittelständische Unternehmen mit kleinen Teams bedeutet die Implementierung und Verwaltung von Dutzenden einzelner Integrationen zur Bereitstellung dieser Signale jedoch eine erhebliche Komplexität. Die Lösung ist natives XDR. Bei diesem Ansatz stellt der XDR-Anbieter Agenten auf Ihren wichtigsten Assets bereit, um nur die entscheidenden Signale zu erfassen, die Kontext für die aus Ihrem EDR gewonnenen Erkenntnisse liefern. Dadurch werden hochpräzise Erkennungen ermöglicht und die Anzahl der Fehlalarme reduziert, die die Reaktionszeit verlangsamen und Ihr IT- und Sicherheitsteam von anderen Aufgaben abhalten.

Maßnahme 2: Fügen Sie natives XDR hinzu, um die Erkennungsgenauigkeit und die Effektivität Ihres IT- und Sicherheitsteams zu maximieren

Seien Sie proaktiv: **Präventive Sicherheitsmaßnahmen**

Das Mantra „Eine Sicherheitsverletzung ist unvermeidlich“ existiert seit vielen Jahren in der Cybersicherheit und hat die Verbreitung von Erkennungs- und Reaktionstechnologien vorangetrieben. Oftmals geschah dies auf Kosten präventiver Sicherheitsmaßnahmen, die, wenn sie richtig umgesetzt werden, den Aufwand für die Reaktion erheblich reduzieren können.

Effektive Sicherheitsprogramme beinhalten Prävention und Schutz von Anfang an, indem sie die Einstiegspunkte verstecken und blockieren, auf die Angreifer setzen. Prävention hat Priorität, das heißt, Angriffe sollen gestoppt werden, bevor sie sich zu Sicherheitsvorfällen ausweiten, die eine Untersuchung erfordern. Dieser Ansatz reduziert die Arbeitsbelastung Ihres IT- und Sicherheitsteams und ermöglicht es ihnen, sich auf dringendere Aufgaben mit hoher Priorität zu konzentrieren.

Unternehmen verbessern ihre Präventions- und Schutzfähigkeiten durch die Hinzunahme neuer Insellösungen, was den bereits erwähnten Tool-Wildwuchs noch verstärkt. Viele IT-Verantwortliche in mittelständischen Unternehmen erkennen zwar die Vorteile präventiver Sicherheitsmaßnahmen, gehen aber aufgrund von Komplexität und Kosten davon aus, dass diese für sie unerreichbar sind. Es gibt jedoch Sicherheitsplattformen, die die wichtigsten Funktionen von Unternehmenslösungen wie Threat Exposure Management (TEM) und Attack Surface Management (ASM) vereinen.

Maßnahme 3: Implementieren Sie die wichtigsten proaktiven Sicherheitskontrollen, um die Belastung der kleinen IT- und Sicherheitsteams durch Reaktionen auf Sicherheitsvorfälle zu reduzieren

Der Plattformvorteil: Breites Sicherheitsspektrum bei reduzierter Komplexität

Die Cybersicherheitsbranche versucht, die Komplexität der Tool-Vielfalt durch die Konsolidierung der Funktionen auf einer einzigen Plattform zu bewältigen.

„Bis 2029 werden 30 % der mittelgroßen Unternehmen ihre Funktionen für Arbeitsplatz-, Daten- und Identitätssicherheit in einer Arbeitsplatz-Sicherheitsplattform zusammenführen, die ganzheitlichen Schutz und zentrales Richtlinienmanagement bietet.“

Gartner, 2025 Strategic Roadmap for Workspace Security
Peter Firstbrook, Evgeny Mirolyubov, Franz Hinner, 21. April 2025.

GARTNER ist eine Marke von Gartner, Inc. und den verbundenen Unternehmen.

Die heutigen Sicherheitsplattformen haben sich von EPP/EDR über XDR bis hin zu Präventionsfunktionen weiterentwickelt, um die Systeme zu härten und das Eindringen von Angreifern abzuwenden. Sie verfügen außerdem über Schutzmechanismen, um Bedrohungen vor ihrer Ausführung zu blockieren. Diese Fähigkeiten verringern den Bedarf an ressourcenintensiven Erkennungs- und Reaktionsmechanismen im späteren Verlauf des Sicherheitslebenszyklus.

Native Integrationen und sofort einsatzbereite Arbeitsabläufe vereinfachen den täglichen Betrieb und machen die Entwicklung spezieller Integrationen oder die individuelle Anpassung von Erkennungsregeln überflüssig. Und die von vielen Plattformen bereitgestellten präventiven Funktionen weiten diese Einfachheit auf Risikomanagement und Compliance aus. Das Ergebnis ist eine umfassendere Sicherheit sowie eine verbesserte Prävention und ein besserer Schutz ohne die Nachteile von Enterprise-Lösungen.

Um mehr über die Vor- und Nachteile der so genannten Plattformisierung zu erfahren, lesen Sie [Die Sicherheitsplattform ist tot. Es lebe die Sicherheitsplattform.](#)

Maßnahme 4: Stellen Sie eine Plattform bereit, die für Sicherheit im gesamten Bedrohungslebenszyklus optimiert ist – Prävention, Schutz, Erkennung und Reaktion

Erweitern Sie Ihr Team mit MDR

Eine einheitliche Plattform bietet umfassende Abdeckung. Sie können diese Sicherheit durch Managed Detection and Response (MDR) weiter ausbauen, um eine Rund-um-die-Uhr-Überwachung der Plattform zu gewährleisten. MDR ergänzt und unterstützt Ihr Team, indem es ihm hilft, verdächtige Aktivitäten zu erkennen und zu untersuchen, bevor diese eskalieren können. Wenn es zu Sicherheitsvorfällen kommt, ergreifen die MDR-Analysten rasche und entschlossene Maßnahmen, um Bedrohungen einzudämmen, die Behebung zu koordinieren und die Wiederherstellung zu beschleunigen.

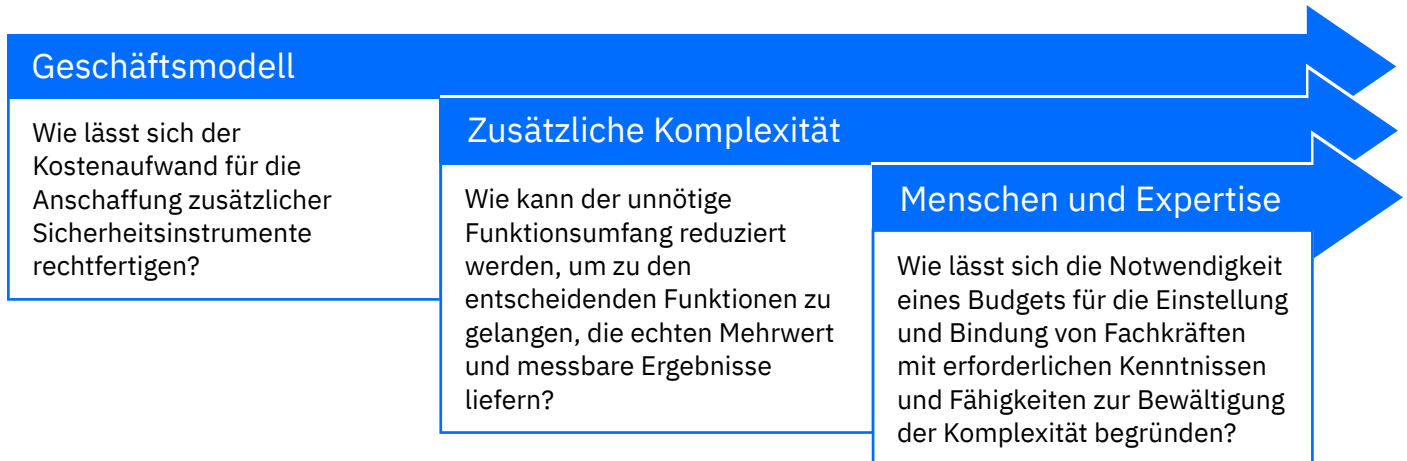
Viele Dienste erweitern die präventiven Fähigkeiten Ihrer Plattform, indem sie Experteneinblicke und Empfehlungen bieten, mit denen die Sicherheitslage verbessert werden kann. Dies stärkt und qualifiziert Ihr Team für die entsprechenden Aufgaben und festigt Ihr gesamtes Sicherheitsprogramm, ohne dass eine große interne Sicherheitsabteilung aufgebaut werden muss.

Maßnahme 5: Ziehen Sie MDR in Betracht, um Ihr Team zu stärken und Ihr gesamtes Sicherheitsprogramm zu verbessern.

Erreichbare, verbesserte und nachweisbare Ergebnisse

Für viele mittelständische Unternehmen erscheint diese Bandbreite an Sicherheitsfunktionen unerreichbar. Diese Wahrnehmung ist das Ergebnis einer Reihe von Herausforderungen, bei denen eine zur nächsten führt.

Die Herausforderung für mittelständische Unternehmen



Da Bedrohungen in dynamischen Umgebungen immer schwieriger abzuwehren sind, sind umfassende Transparenz und Verteidigung unerlässlich. Eine Stärkung der Sicherheitsabdeckung erfordert einen strategischen Ansatz und Erkenntnisse, anstatt einfach nur die Personalstärke zu erhöhen, um mehr punktuelle Lösungen zu verwalten.

Ihr 5-Punkte-Aktionsplan zur Gewährleistung von Sicherheit im gesamten Bedrohungslebenszyklus

Wie lassen sich Prävention, Schutz, Erkennung und Reaktion innerhalb der Rahmenbedingungen eines mittelständischen Unternehmens mit einem kleinen IT- und Sicherheitsteam erreichen?

- | | |
|------------------------|---|
| 1
EPP | Implementieren Sie eine Plattform für den Endpoint-Schutz, die Ihr Team in die Lage versetzt, seine Effektivität und Ihren ROI zu maximieren. |
| 2
XDR | Fügen Sie natives XDR hinzu, um die Erkennungsgenauigkeit und die Effektivität Ihres IT- und Sicherheitsteams zu maximieren |
| 3
Prävention | Implementieren Sie die wichtigsten proaktiven Sicherheitskontrollen, um die Belastung der kleinen IT- und Sicherheitsteams durch Reaktionen auf Sicherheitsvorfälle zu reduzieren |
| 4
Plattform | Stellen Sie eine Plattform bereit, die für Sicherheit im gesamten Bedrohungslebenszyklus optimiert ist – Prävention, Schutz, Erkennung und Reaktion |
| 5
MDR | Ziehen Sie MDR in Betracht, um Ihr Team zu stärken und Ihr gesamtes Sicherheitsprogramm zu verbessern. |

Um zu verstehen, wie Sie diesen Plan umsetzen können, lesen Sie den [Buyer's Guide für mittelständische Unternehmen: Auswählen der richtigen Sicherheitsplattform](#)

i. [IBM Institute for Business Value: Capturing the cybersecurity dividend](#)

Als führender Anbieter von Cybersecurity-Lösungen bietet Bitdefender hochwertige Lösungen bei der Prävention, Erkennung und Beseitigung von Bedrohungen. Millionen von Verbrauchern, Unternehmen und staatlichen Organisationen vertrauen auf das Expertenwissen von Bitdefender, wenn es um die Bekämpfung von Cybergefahren, den Schutz von Daten, digitale Identitäten und Privatsphäre und den Aufbau von Cyberresilienz geht. Bitdefenders umfangreiche Investitionen in Forschung und Entwicklung zahlen sich aus: So entdecken die Bitdefender Labs Hunderte neue Bedrohungen pro Minute und prüfen mehrere Milliarden Bedrohungsabfragen pro Tag. Bitdefender zeichnet für zahlreiche bahnbrechende Innovationen im Malware-Schutz, der IoT-Sicherheit, bei Verhaltensanalysen und künstlicher Intelligenz verantwortlich, und die daraus resultierenden Technologien werden von über 200 der bekanntesten Tech-Unternehmen aus aller Welt eingesetzt. Bitdefender wurde 2001 gegründet, betreut Kunden in über 170 Ländern und ist weltweit mit Niederlassungen vertreten.

Stand: November 2025

Weitere Informationen finden Sie unter <https://www.bitdefender.de>.

Romania HQ

Orhideea Towers
15A Orhideelor Road,
6th District,
Bukarest 060071

T: +40 21 4412452

Germany HQ

12 Lohbachstrasse,
58239 Schwerte,
Germany