Bitdefender®

GravityZone

LÖSUNGSLEITFADEN

Sicherheitsabläufe vereinfachen, Risiken minimieren.

Was wäre, wenn alles, was uns über Cybersicherheit erzählt wurde, falsch wäre? Was wäre, wenn die Hinzunahme weiterer Sicherheitsebenen unser Unternehmen nicht sicherer macht, sondern uns noch anfälliger macht? Tatsächlich sind viele unserer Systeme inzwischen so komplex geworden, dass sie heute unsere größten Schwachstellen darstellen.

Jedes neue Sicherheitstool verspricht Schutz, stiftet aber gleichzeitig Verwirrung und schafft blinde Flecken. Cyberkriminelle gehen nicht mit Gewalt vor, sondern nutzen die von uns selbst geschaffenen Schwachstellen aus. Das Weltwirtschaftsforum bestätigt dies: „Der Cyberspace ist aufgrund rasanter technologischer Fortschritte, zunehmender Raffinesse der Cyberkriminellen und eng vernetzter Lieferketten komplexer und herausfordernder denn je."

Die Zukunft der Cybersicherheit besteht nicht darin, immer mehr Sicherheitsebenen zu schaffen. Es geht vielmehr darum, die Sicherheitsfunktionen zu vereinfachen, Unwichtiges auszublenden und sich auf das Wesentliche zu konzentrieren.

Warum sind die heutigen Cyberbedrohungen so schwer zu erkennen und abzuwehren?

Es ist eine vertraute Geschichte: Täglich entwickeln sich Cybersicherheitsbedrohungen weiter, werden immer ausgefeilter und schwieriger abzuwehren. Die Unternehmen agieren in weitläufigen, vernetzten Umgebungen mit Tausenden von Assets. Jede neue Geschäftsinitiative bringt weitere Endpoints, Datenflüsse und Abhängigkeiten mit sich. Sie bieten zwar alle einen Mehrwert, bergen aber auch Risiken.

Je mehr Ihre IT-Umgebung wächst, umso weniger transparent wird Ihre IT, oft sind nur noch Teile sichtbar. Es ist nahezu unmöglich, Daten aus mehreren eigenständigen Quellen miteinander zu korrelieren. Für Ihr personell begrenztes IT- und Sicherheitsteam wird es deshalb immer schwieriger, die Zusammenhänge zu erkennen, und es übersieht dabei möglicherweise Schwachstellen, die von Angreifern schnell ausgenutzt werden können.

Gleichzeitig haben Angreifer ihre bestehenden Exploit-Strategien weiterentwickelt. Sie verlassen sich nicht mehr ausschließlich auf Brute-Force- oder Zero-Day-Ansätze, sondern beherrschen mittlerweile die Technik des „Living-off-the-Land", indem sie ihre schädlichen Aktionen mit legitimen Werkzeugen und Prozessen kombinieren, die bereits in den Systemen ihrer Opfer vorhanden sind.

Deshalb sind die Angriffsversuche für Angreifer viel einfacher durchzuführen und für IT-Teams viel schwieriger zu erkennen. Selbst vergleichsweise einfache Angriffe können, sobald sie präzise ausgeführt werden und „unter dem Radar" ablaufen, verheerende Folgen haben, wenn sie die Verteidigungssysteme lange genug umgehen können. Mittlerweile integrieren die Angreifer Automatisierung und KI in ihre Werkzeugkästen und vergrößern so ihre Reichweite. Zudem werden sie immer schneller, wenn es um das Identifizieren von Schwachstellen, das Ausnutzen von Sicherheitslücken und die Durchführung von Kampagnen in großem Umfang geht

Die Anforderung für IT-Teams wird dadurch noch verschärft, dass die heutigen Bedrohungen selten auf einen einzigen Angriffspunkt beschränkt sind. Sie sind bewusst vielschichtig gestaltet und zielen gleichzeitig auf mehrere Unternehmensebenen ab. So können Hacker mit einer Phishing-E-Mail beginnen, dann auf die Ausweitung von Benutzerrechten übergehen, nachlässig konfigurierte Cloud-Ressourcen ausnutzen und schließlich über verschiedene Endpoints hinweg im internen Netzwerk vordringen. Jede Phase verstärkt die nächste und erzeugt so eine Kette von Ereignissen, die, sobald sie einmal in Gang gesetzt ist, extrem schwer zu unterbrechen ist.

Dieser mehrschichtige Ansatz bedeutet, dass die Auswirkungen eines Angriffs nicht mehr auf ein einzelnes System oder eine einzelne Abteilung beschränkt sind. Hierzu ein Beispiel:

- Mit Ransomware wird oft das Erstellen von Backups deaktiviert, und vertrauliche Daten werden entwendet, sodass der Angriff auf eine doppelte Erpressung hinausläuft.

- BEC-Kampagnen (Business Email Compromise) können weit mehr Schaden anrichten als nur einen Posteingang zu kompromittieren; oft gehen sie mit Finanzbetrug oder der Unterwanderung von Lieferketten einher.

Dadurch, dass Angreifer mehrere Angriffsvektoren gleichzeitig ausnutzen können, erhöhen sie ihre Erfolgswahrscheinlichkeit und somit das Potenzial für Störungen des Geschäftsbetriebs. Das führt zu einer äußerst kritischen Lage: Immer komplexere Unternehmensumgebungen werden von immer effizienteren Gegnern heimgesucht. Ohne die richtige Transparenz, das nötige Verständnis und die entsprechenden Reaktionsmöglichkeiten fällt es den Unternehmen schwer, die beste Vorgehensweise zur Priorisierung von Schutzmaßnahmen zu bestimmen.

Mehr Tools = mehr Hintergrundrauschen

Die heutigen, hochkomplexen Unternehmensumgebungen bedeuten nie dagewesene Belastungen für die IT-Sicherheitsteams. Jedes neue Gerät, jede neue Anwendung oder jeder neue Cloud-Dienst bringt wieder neue Warnmeldungen, Protokolle und Schwachstellen mit sich. Um damit Schritt zu halten, nutzen die meisten Unternehmen eine Reihe von Sicherheitstools, darunter:

- Endpoint detection and response
- Firewalls
- Identitätsschutz
- Cloud- und SaaS-Sicherheit
- Schwachstellen-Management
- und weitere

Selbstverständlich erfüllt jedes Tool seinen Zweck. Doch wenn man einfach versucht, diese Elemente zu einem zusammenhängenden Verteidigungssystem zu verschmelzen, schafft man oft mehr Probleme, als man löst. Warum ist das so?

- **Ungleiche Daten:** Jede Plattform verfügt über ihre eigenen Datenformate, Alarmierungslogiken und Dashboards. Ihr Sicherheitsteam muss daher viel Zeit für die Angleichung inkonsistenter Schemata und die Bearbeitung doppelt gemeldeter Ereignisse aufwenden, anstatt sich auf die vorrangigen Bedrohungen konzentrieren zu können.
- **Redundanzen und Hintergrundrauschen:** Durch sich überschneidende Funktionalitäten verschiedener Tools kommt es dazu, dass dasselbe Ereignis mehrere Alarme auslösen kann. Dies überfordert die Analysten, kostet Zeit und untergräbt das Vertrauen in den gesamten Erkennungsprozess.
- **Probleme bei der Integration:** Die Integration zwischen Tools verläuft nur selten reibungslos. APIs ändern sich, Konnektoren funktionieren nicht mehr, und die Anpassung von Korrelationsregeln erfordert einen kontinuierlichen technischen Aufwand, den viele Teams schlichtweg nicht stemmen können.

Mit zunehmender Komplexität der Sicherheitsarchitektur sinkt die Gesamttransparenz. Laut der Gigamon-Studie „Hybrid Cloud Security Survey 2024“ äußerten 41 % der CISOs Bedenken hinsichtlich der unkontrollierten Ausweitung des Tool-Einsatzes und der damit einhergehenden Transparenzlücken und Schwachstellen. Diese entstehen durch die schwierige Integration und die Probleme bei der Verwaltung der einzelnen Tools. Anstatt ein einheitliches Bild zu erhalten, müssen Analysten mehrere Konsolen nutzen, die jeweils nur einen Teil der Umgebung abdecken. Diese eingeschränkte Sicht verlangsamt die Untersuchung von Sicherheitsvorfällen. Die Teams müssen zwischen verschiedenen Plattformen wechseln, um den Ablauf eines Angriffs zu rekonstruieren, was die mittlere Erkennungszeit (MTTD) und die mittlere Reaktionszeit (MTTR) erhöht.

Um diesem Problem zu begegnen, setzen viele Unternehmen auf SIEM- (Security Information and Event Management) und SOAR-Plattformen (Security Orchestration Automation and Response), um Daten zu zentralisieren und Arbeitsabläufe zu automatisieren. Allerdings sind SIEM- und SOAR-Systeme selbst sehr komplex und verursachen enorme Kosten für die Protokollerfassung, bieten nur unzuverlässige Erkennungsregeln und benötigen Spezialisten für deren Anpassung und Pflege.

Im Bericht „State of SIEM Detection Risk 2025“ von CardinalOps wurde festgestellt, dass SIEM-Systeme trotz der Verarbeitung hunderter Protokollquellen typischerweise nur einen Bruchteil bekannter Angreifertechniken abdecken und somit gefährliche Sicherheitslücken hinterlassen. Die Unternehmen erleben nach wie vor keine angemessene Verbesserung der Abdeckung, wenn sie in SIEM-Systeme investieren, um ihre heterogene Tool-Landschaft zu konsolidieren.

Was ist also zu tun? Die Lösung besteht eindeutig nicht darin, weitere Tools hinzuzunehmen, sondern vielmehr in einem integrierten Ansatz, der die Komplexität reduziert und gleichzeitig die Abdeckung und die Ergebnisse verbessert.

Bitdefender

Einheitliche Tools für einfache Sicherheit

Angesichts zunehmender Bedrohungen, fragmentierter Tools und unter Druck stehender, personell begrenzter Teams ist heute ein sorgfältig und gut durchdachter Ansatz für Ihre Cybersicherheit vonnöten. Das Hinzufügen von Produkten zum Endpoint-Schutz vervielfacht lediglich den Integrationsaufwand und verstärkt das Datenrauschen. Ihr IT-Sicherheitsteam benötigt eine einheitliche Plattform, die den Betrieb vereinfacht, die Transparenz verbessert, Erkennung und Reaktion automatisiert und bei Bedarf die richtige Expertise bereitstellt.

Dieselbe Sprache sprechen

Eine einheitliche Sicherheitsplattform vereint das gesamte Spektrum an Sicherheitstools und -funktionen unter einem Dach und sorgt dafür, dass alle dieselbe Sprache sprechen. Anstelle von separaten Konsolen und isolierten Daten können die Unternehmen die Sicherheit von Endpoints, Identitäten, Cloud, Netzwerk und SaaS-Anwendungen in einer einzigen integrierten Umgebung verwalten.

Vorteile dieser Konsolidierung:

- → Weniger Redundanz
- → Geringerer Aufwand im Betrieb
- → Es wird sichergestellt, dass Warnmeldungen, Protokolle und Telemetriedaten in eine zentrale Informationsschicht fließen, in der sie korreliert und in Echtzeit analysiert werden können.

Das Ergebnis: Vereinfachte Sicherheitsabläufe mit besserer Erkennungs- und Reaktionsfähigkeit über Ihre gesamte Angriffsfläche hinweg.

Einheitlichkeit bei Prävention, Schutz, Erkennung und Reaktion

Eine einheitliche Sicherheitsplattform stärkt die Abwehrfähigkeit des Unternehmens, indem sie Prävention, Schutz, Erkennung und Reaktion in einem zusammenhängenden System vereint. Anstatt diese Bereiche als separate Funktionen zu behandeln, korreliert die Plattform kontinuierlich Telemetriedaten über Endpoints, Identitäten, Cloud-Workloads, Netzwerke und SaaS-Anwendungen hinweg. Dies ermöglicht eine frühzeitige Erkennung von Schwachstellen, Fehlkonfigurationen oder anormalen Aktivitäten, bevor Angreifer diese ausnutzen können, und verringert so die Wahrscheinlichkeit, dass Angriffe tiefer in die Umgebung eindringen.

Prävention und Schutz werden durch die Durchsetzung einheitlicher Richtlinien und ein effektives Schwachstellenmanagement weiter optimiert. Sicherheitsmaßnahmen, Zugriffsrichtlinien und Konfigurations-Baselines können über eine einzige Konsole in der gesamten Umgebung einheitlich angewendet werden. Wenn Aktualisierungen der Erkennungslogik oder der Intelligence-Feeds eingeführt werden, findet gleichzeitig eine Verteilung dieser Updates statt, sodass die Abwehrmaßnahmen stets auf dem neuesten Stand und synchronisiert bleiben. Dies verbessert die Abdeckung und verringert die Komplexität, die mit der Aufrechterhaltung angemessener Cybersicherheitskontrollen einhergeht.

Durch diese Konsolidierung der Tools wird auch die Sichtbarkeit verbessert, sodass das Team eine bessere Übersicht über die Angriffsfläche hat. Analysten können schnell erkennen, welche Ressourcen am gefährdetsten sind, Maßnahmen zur Behebung von Sicherheitslücken anhand des tatsächlichen Geschäftsrisikos priorisieren und die Reaktionsaktivitäten mithilfe korrelierter Kontextinformationen beschleunigen. Dank dieser durchgängigen Sequenz von Prävention bis Reaktion können Bedrohungen früher gestoppt, Untersuchungen vereinfacht und Abhilfemaßnahmen schneller und sicherer durchgeführt werden.

Vereinfachte, effizientere Automatisierung

Da alle Tools miteinander verknüpft sind, lassen sich Bedrohungserkennung und -abwehr besser automatisieren und optimieren, wodurch aus ehemals manuellen, fehleranfälligen Prozessen nahtlose, zuverlässige Abläufe werden. Die Plattform ist in der Lage Daten, Ereignisse und Warnmeldungen automatisch zu korrelieren, Bedrohungen mit äußerster Präzision zu erkennen und automatisch Reaktionsmaßnahmen einzuleiten.

Analysten verschwenden keine wertvolle Zeit mehr mit dem Wechsel zwischen Konsolen, der Priorisierung sich überschneidender Warnmeldungen oder dem Versuch, benutzerdefinierte Integrationen zu implementieren, sondern erhalten priorisierte Warnmeldungen mit umfassendem Kontext. Zudem sorgt die Automatisierung für enorme Rentabilität: Der IBM-Bericht „Cost of a Data Breach 2024“ ergab, dass Unternehmen, bei denen die Automatisierung der Sicherheitslösung vollständig implementiert war, Sicherheitsverletzungen 74 Tage eher eindämmen und im Vergleich zu Unternehmen mit minimaler oder ohne Sicherheitsautomatisierung rund 31 % der Kosten einsparen konnten.

Die Automatisierung ermöglicht es Ihrem IT-Sicherheitsteam, Bedrohungen schneller zu erkennen (wodurch die mittlere Zeit bis zur Erkennung (MTTD) verkürzt wird), Sicherheitsvorfälle zuverlässiger zu bestätigen und über die gesamte Angriffskette hinweg effektiver zu reagieren. Dies umfasst die Anreicherung von Warnmeldungen mit Daten zur Bedrohungsaufklärung, die Zuordnung von Aktivitäten zu MITRE ATT&CK-Techniken, die Isolation von betroffenen Ressourcen und das automatische Generieren von revisionssicheren Berichten. Für Teams mit nur wenigen Mitarbeitern kommt dieser Unterschied einer Transformation gleich: Analysten werden von sich wiederholenden Aufgaben zur Ersteinschätzung befreit und können sich auf die proaktive Bedrohungssuche, Resilienzplanung und strategische Sicherheitsverbesserungen konzentrieren.

Automatisierung beschleunigt die Bedrohungserkennung und Reaktion, vereinfacht gleichzeitig Sicherheitsabläufe, verringert die Komplexität und schafft kleinen Teams mehr Freiräume.

Einsatz von Experten zur Unterstützung Ihres Teams

Technologie allein kann eine Organisation nicht schützen; die Teams benötigen auch Dienstleistungen zur Erweiterung ihres Fachwissens und zur Ergänzung ihrer oft nur beschränkten Kapazitäten. So lässt sich Ihre IT-Sicherheit durch die Zusammenarbeit mit einem MDR-Anbieter (Managed Detection and Response) erheblich steigern: Er unterstützt Sie mit Überwachung rund um die Uhr, einer fortschrittlichen Bedrohungserkennung und von Experten geleiteten Reaktionen auf Sicherheitsvorfälle.

Mit MDR erhält Ihr Unternehmen sofortigen Zugriff auf erfahrene Analysten, Experten für die Bedrohungssuche und Forensik, die Warnmeldungen überprüfen, Vorfälle untersuchen und Reaktionen koordinieren können, wodurch die mittlere Zeit bis zur Erkennung und Behebung verkürzt wird. In Kombination mit kontinuierlicher Bedrohungsanalyse, Dark-Web-Überwachung und dem Schutz Ihrer Marke sorgt MDR dafür, dass selbst kleinste Teams Transparenz und Schutz auf Unternehmensebene erhalten.

Einheitliche Plattformen sollten jedoch über die reine Erkennung und Reaktion hinausgehen und präventive sowie beratende Dienstleistungen bieten. Ziehen Sie die Nutzung offensiver Sicherheitsangebote wie Penetrationstests, Red Teaming und Tabletop-Übungen in Betracht. Diese Maßnahmen helfen den Unternehmen dabei, Schwachstellen proaktiv zu erkennen, bevor Angreifer sie ausnutzen können.

Durch Beratungsdienstleistungen wird Ihr Team beim Aufbau und der Weiterentwicklung von Cybersicherheitsprogrammen unterstützt. So wird außerdem sichergestellt, dass Richtlinien, Prozesse und Maßnahmen mit den Geschäftsanforderungen und den Compliance-Vorgaben im Einklang stehen.

Klare Kommunikation und nach außen sichtbarer Mehrwert

Letztlich erleichtert eine einheitliche Plattform nicht nur die Arbeit der Sicherheitsexperten, sondern verändert auch die Art und Weise, wie sicherheitsbezogene Informationen im gesamten Unternehmen kommuniziert werden. Da sämtliche Telemetriedaten, Warnmeldungen und Ergebnisse in eine zentrale Informationsebene einfließen, kann die Plattform die betreffenden Informationen in zielgruppenspezifischen Formaten präsentieren. Analysten profitieren von Warnmeldungen mit umfassendem Kontext sowie von detaillierten forensischen Daten, während für Führungskräfte, Vorstände und Compliance-Beauftragte übersichtliche Dashboards bereitgestellt werden, die Trends, KPIs und die allgemeine Sicherheitslage klar herausstellen.

Durch diese übersichtlichen Informationen werden auch Nicht-Analysten in die Lage versetzt, ihre Aufgaben effektiver wahrzunehmen. Führungskräfte können sich leichter einen Überblick über die aktuelle Lage des Unternehmens verschaffen, Vorstände können Investitionen in die Sicherheit fundiert beurteilen, und Compliance-Teams können ohne technisches Fachwissen die für Audits benötigten Nachweise erstellen. Die Fähigkeit, Sicherheitsergebnisse in einfacher, nicht komplexer Sprache darzustellen, stellt sicher, dass der Wert der Sicherheitsabteilung nicht nur intern erkannt wird, sondern auch extern gegenüber Stakeholdern und Aufsichtsbehörden deutlich werden kann.

Das Ergebnis: Ein Sicherheitsprogramm, das nicht nur leistungsfähiger, sondern auch transparenter, nachvollziehbarer und strategisch auf die jeweiligen Geschäftsziele ausgerichtet ist. Durch Vereinfachung der Informationsnutzung wandelt sich Sicherheit dank der einheitlichen Plattformen von einer rein technischen Disziplin zu einem integrierten Geschäftsfaktor.

Eine speziell für kleine Sicherheitsteams konzipierte Lösung

Im Gegensatz zu Toolsets, die aus verschiedenen Sicherheitsprodukten zusammengesetzt sind, liegt bei einheitlichen Plattformen der Fokus auf Einfachheit, Integration und messbaren Ergebnissen. Diese Konzeption bedeutet eine einfachere Einarbeitung des Personals in weniger Schnittstellen, eine schnellere Bereitstellung und einen Automatisierungsgrad, der die Fähigkeiten kleiner Teams erweitert. Ihr Sicherheitsteam erhält Zugriff auf Funktionen der Enterprise-Klasse, ohne die Last der Verwaltung komplexer Prozesse im Enterprise-Maßstab tragen zu müssen. Die Plattform bietet die notwendige Funktionalität für Transparenz, Prävention, Schutz, Erkennung und Reaktion auf Sicherheitsvorfälle, um das Unternehmen gegen heutige Bedrohungen zu verteidigen, und zwar auf eine Weise, die für Teams mit begrenzter Personalstärke praktikabel und nachhaltig ist.

Zu den Ergebnissen gehören eine schnellere Eindämmung von Bedrohungen, eine proaktive Verringerung von Schwachstellen und die Gewissheit, dass die Sicherheitsmaßnahmen direkt auf das Geschäftsrisiko abgestimmt sind. Durch die Verringerung des Zeitaufwands für die manuelle Ersteinschätzung und Wartung der Tools können auch Teams mit wenigen Mitarbeitern mehr Energie für strategische Initiativen wie Resilienzplanung,die Einhaltung gesetzlicher Vorschriften und die Berichterstattung an die Unternehmensleitung aufwenden.

Konzentrieren Sie sich auf das Wesentliche

Sind Sie bereit, mit weniger mehr zu erreichen? Schaffen Sie eine einheitliche Sicherheitsplattform, indem Sie Ihre Technologie-Tools konsolidieren und mit spezialisierten Dienstleistern zusammenarbeiten. Statt in Daten und unübersichtlichen Warnmeldungen zu ertrinken, können Sie sich auf das Wesentliche konzentrieren: die Sicherheit der Daten und Systeme Ihres Unternehmens.

Benötigen Sie Sicherheit auf Enterprise-Niveau ohne die damit verbundene Komplexität? Die Business-Sicherheitslösungen von Bitdefender helfen Ihnen, Risiken proaktiv zu minimieren und sich gegen Bedrohungen zu verteidigen.

LEARN MORE

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

T: +40 21 4412452

Germany HQ
12 Lohbachstrasse,
58239 Schwerte,
Germany

Erscheinungsdatum: Oktober 2025

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