August 2025

Marktbericht

Der Ransomware Insights Bericht 2025

Untersuchung der Erfahrungen und Auswirkungen von Ransomware auf Unternehmen weltweit

Barracuda®
Your business, secured.

Inhalt

Einleitung

Ransomware ist eine weit verbreitete und sich weiterentwickelnde Bedrohung, die durch Ransomware-as-a-Service-Kits angetrieben wird, die es immer mehr Cyberkriminellen ermöglichen, Angriffe zu starten. Ransomware-Vorfälle können den Ruf einer Marke schädigen und den täglichen Betrieb lahmlegen, was zu Störungen, Datenverlust, Vertrauensverlust bei Kunden und mehr führen kann. Jedes Unternehmen ist ein potenzielles Ziel.

Dieser Bericht untersucht die Erfahrungen und Auswirkungen erfolgreicher Ransomware-Angriffe auf Unternehmen weltweit in den letzten 12 Monaten. Er basiert auf den Ergebnissen einer internationalen Umfrage unter 2.000 IT- und Security-Entscheidern, die von Barracuda und Vanson Bourne durchgeführt wurde.

Die Ergebnisse lassen sich in drei übergreifende Themen einteilen:

- **Ransomware-Opfer weisen eher fragmentierte Security auf**, mit zu vielen getrennten Security-Tools und unzureichender Abdeckung in wichtigen Security-Bereichen.
- **Ransomware-Angriffe sind multidimensional.** Dabei geht es nicht mehr nur um die Verschlüsselung von Daten, sondern mittlerweile auch um Datendiebstahl und -offenlegung, die Installation zusätzlicher bösartiger Nutzlasten und mehr.

Methodik

Barracuda beauftragte das unabhängige Marktforschungsunternehmen Vanson Bourne mit der Durchführung einer globalen Umfrage unter 2.000 leitenden Sicherheitsexperten in IT- und Geschäftsfunktionen in Unternehmen mit 50 bis 2.000 Mitarbeitern aus einer Vielzahl von Branchen in den USA, dem Vereinigten Königreich, Frankreich, DACH (Deutschland, Österreich, Schweiz), Benelux (Belgien, Niederlande, Luxemburg), den nordischen Ländern (Dänemark, Finnland, Norwegen, Schweden), Australien, Indien und Japan. Die Feldforschung wurde im April und Mai 2025 durchgeführt.

Einleitung

- **Der Einflussbereich eines erfolgreichen Ransomware-Angriffs erweitert** sich und umfasst den Verlust neuer Geschäftsmöglichkeiten sowie Zahlungstaktiken, die Druck auf Mitarbeiter, Partner, Kunden und Behörden ausüben.

Wir hoffen, dass dieser Bericht Unternehmen jeder Größe und Branche dabei hilft, die Bedrohung und die Auswirkungen von Ransomware im Jahr 2025 zu verstehen und Bereiche zu identifizieren und anzugehen, in denen sie potenziell gefährdet sein könnten.

Zentrale Ergebnisse

57 %

der Unternehemn erlebten in den letzten 12 Monaten einen erfolgreichen Ransomware-Angriff

71 %

der Unternehmen, die einen E-Mail-Verstoß erlebt hatten, waren auch von Ransomware betroffen

32 %

zahlten ein Lösegeld, um ihre Daten wiederherzustellen — 41 % von ihnen erhielten nicht alle ihre Daten zurück

65 %

der Ransomware-Opfer konnten Daten aus Backups wiederherstellen

24 %

der Ransomware-Opfer hatten Daten verschlüsselt — während bei 27 % Daten gestohlen wurden und 29 % angaben, dass die Angreifer zusätzliche Payloads installiert hatten

25 %

der Ransomware-Opfer verloren bestehende Kunden — der gleiche Anteil verlor neue Geschäftsmöglichkeiten

Ransomware betrifft mehr als die Hälfte der Unternehmen

Insgesamt waren 57 % der befragten Unternehmen in den letzten 12 Monaten von einem erfolgreichen Ransomware-Angriff betroffen.

Jedes dritte Opfer (31 %) war zwei Mal oder häufiger betroffen.

Die Häufigkeit mehrerer erfolgreicher Angriffe lässt darauf schließen, dass Security-Lücken nicht nach jedem Vorfall umfassend untersucht und behoben werden. In diesem Bericht untersuchen wir die Unterschiede zwischen Unternehmen, die einmal betroffen waren, und solchen, die mehrfach betroffen waren, um zu ermitteln, welche Erkenntnisse aus den Daten gewonnen werden können und wie Unternehmen diese nutzen können, um ihre Security zu verbessern.

Die am stärksten betroffenen Branchen in unserer Umfrage waren das Gesundheitswesen (mit 67 % betroffenen Unternehmen), Kommunalverwaltungen (65 %) und der Einzelhandel (61 %). Den Daten zufolge war die verarbeitende Industrie am wenigsten betroffen. Knapp die Hälfte (46 %) der Befragten gab an, dass sie erfolgreich getroffen wurden.

Die Größe scheint bei Ransomware keine Rolle zu spielen, da die Ergebnisse über alle untersuchten Unternehmensgrößen hinweg, von 50 bis 2.000 Mitarbeitern, konsistent bleiben.

71 % der Unternehmen, die einen E-Mail-Verstoß erlebt hatten, wurden auch von Ransomware betroffen — was den Zusammenhang zwischen den beiden Arten von Angriffen unterstreicht.

Ransomware-Opfer haben ein anderes Profil für Security-Tools und -Prioritäten

Security-Ausuferung und das Risiko von Ransomware

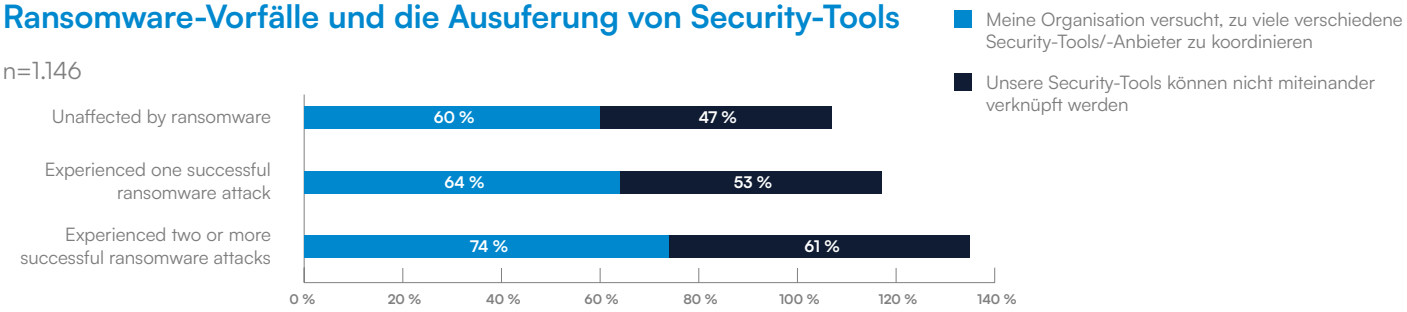
Die Umfrage zeigt, dass ein Übermaß an Security-Tools — bekannt als Security-Ausuferung — zusammen mit einer mangelnden Integration das Risiko erhöhen und zu Schutzlücken führen kann, da es für Unternehmen schwieriger wird, aktive Bedrohungen, einschließlich Ransomware, zu erkennen und abzuwehren.

Die Daten zeigen, dass der Anteil der Unternehmen, die von Security-Ausuferung oder mangelnder Integration betroffen sind, entsprechend ihrer Erfahrung mit Ransomware zunimmt.

ABBILDUNG 1

Ransomware-Vorfälle und die Ausuferung von Security-Tools

n=1.146



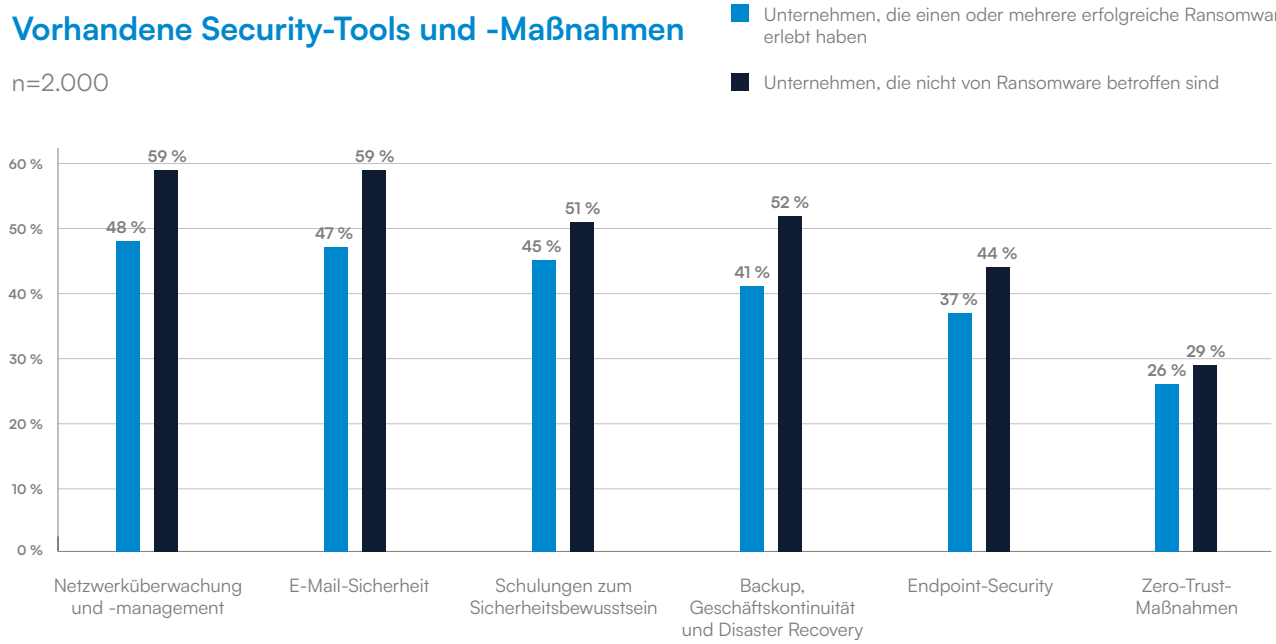
Die verschiedenen Arten von Security Tools und -maßnahmen

Den Befragten zufolge sind die am häufigsten eingesetzten Sicherheitsmaßnahmen E-Mail-Sicherheit (von 52 % implementiert), Netzwerksicherheit (52 %) und Schulung zur Stärkung des Risikobewusstseins (48 %). Unternehmen, die einen erfolgreichen Ransomware-Vorfall gemeldet haben, haben mit geringerer Wahrscheinlichkeit eine dieser Maßnahmen implementiert.

ABBILDUNG 2

Vorhandene Security-Tools und -Maßnahmen

n=2.000



Zum Beispiel:

- 47 % der Ransomware-Opfer hatten eine E-Mail-Sicherheitslösung implementiert — verglichen mit 59 % der Nicht-Opfer.
- 48 % der Ransomware-Opfer hatten Netzwerkmanagement und -überwachung implementiert — im Vergleich zu 59 % der Nicht-Opfer.
- 45 % der Ransomware-Opfer hatten eine Schulung zur Stärkung des Risikobewusstseins absolviert — im Vergleich zu 51 % der Nicht-Opfer
- 37 % hatten Endpoint-Security implementiert — im Vergleich zu 44 % der Nicht-Opfer

Diese Ergebnisse deuten darauf hin, dass Ransomware-Opfer möglicherweise zu wenig in Sicherheitsbereiche investieren, die dazu beitragen könnten, ihr Risiko zu verringern.

So bieten beispielsweise E-Mail-, Netzwerk- und Endpunktsicherheit in Kombination mit Schulungen zur Stärkung des Risikobewusstseins einen robusten Schutz gegen Phishing- und Social-Engineering-Angriffe per E-Mail, deren Ziel der Diebstahl von Zugangsdaten ist und es Angreifern ermöglicht, in Netzwerke einzudringen, Geräte zu kompromittieren und sich lateral zu bewegen — alles Techniken, die für einen Ransomware-Angriff charakteristisch sind.

Ransomware-Banden haben eine Chance von eins zu drei, bezahlt zu werden

32 % der Ransomware-Opfer zahlten ein Lösegeld, um Daten wiederzuerlangen oder wiederherzustellen.

Die Ergebnisse zeigen eine Korrelation zwischen der Neigung einer Unternehmen, Lösegeld zu zahlen, und der Häufigkeit, mit der sie von Ransomware betroffen ist.

Unternehmen, die nur einen erfolgreichen Ransomware-Angriff erlebten, zahlten mit geringerer Wahrscheinlichkeit das Lösegeld (29 %), während 37 % derjenigen, die zweimal oder öfter betroffen waren, das Lösegeld zahlten, um ihre Daten zurückzubekommen.

Diese Zahlen haben sich seit der letzten Umfrage vor zwei Jahren kaum verändert. Im Jahr 2023 ergab die Umfrage, dass 31 % der einmal Betroffenen und 38 % der zweimal oder öfter Betroffenen Lösegeld zahlten, um ihre Daten wiederherzustellen.

Eine mögliche Erklärung für eine Verbindung zwischen mehreren Treffern und Ransomware-Zahlungen ist, dass, sobald gezeigt wird, dass eine Organisation bereit ist zu zahlen, andere Angreifer dasselbe Opfer angreifen oder derselbe Angreifer mehr als einmal zurückkehren kann.

Die gute Nachricht ist, dass die Mehrheit (65 %) der von Ransomware Betroffenen ihre Daten mithilfe von Backups wiederherstellen konnte.

Eine deutliche Erinnerung daran, dass sich die Zahlung des Lösegelds nicht auszahlt: 41 % derjenigen, die zahlten (insgesamt 13 %), bekamen ihre Daten nicht oder nicht einmal teilweise zurück.

Datenverschlüsselung ist mittlerweile nur noch ein Teil eines Ransomware-Angriffs

Abgesehen von der finanziellen Belastung durch die Zahlung eines Lösegelds zeigen die Untersuchungen, dass die kommerziellen, betrieblichen und sogar emotionalen Auswirkungen eines erfolgreichen Ransomware-Angriffs erheblich sind.

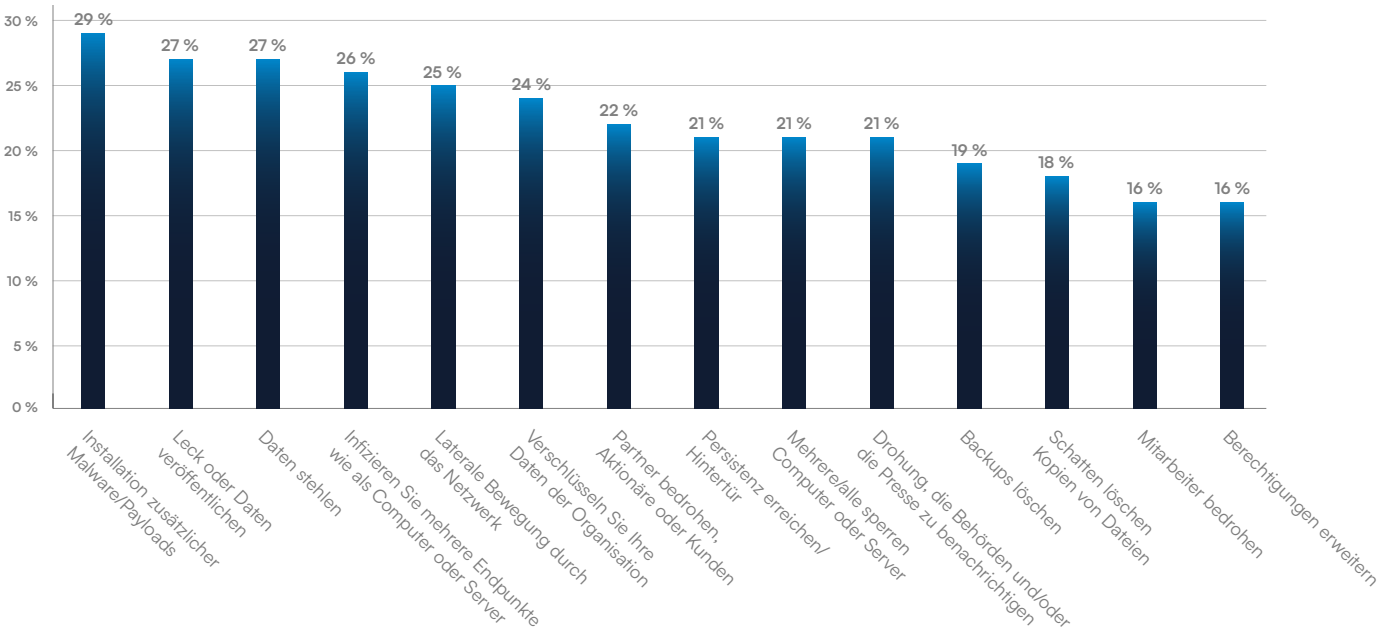
In den meisten Fällen von Ransomware-Angriffen ist die Verschlüsselung von Daten und die Sperrung von Systemen und Computern das Endziel. Dies ist der sichtbarste Teil des Angriffs und daher am ehesten geeignet, das Security-Team auf Eindringlinge aufmerksam zu machen und zur Eindämmung und Beseitigung der Bedrohung zu führen.

Die Forschungsergebnisse unterstreichen die Bandbreite der Aktivitäten, die vor der Ausführung der Ransomware unter dem Radar stattfinden, entweder um den Angriff zu ermöglichen oder möglicherweise den Weg für andere Aktivitäten zu ebnen.

ABBILDUNG 3

Aktivitäten von Ransomware-Banden während des schwerwiegendsten Vorfalls

n=1.146



Etwa ein Viertel der Ransomware-Vorfälle, die die Befragten erlebten, betraf die Verschlüsselung von Daten (24 %), das Sperren von Endpunkten (21 %) und den Diebstahl von Daten (27 %).

Zu den Angriffen zählen außerdem seitliche Bewegungen im Netzwerk (25 %), die Infektion mehrerer Endpunkte wie Computer oder Server (26 %), die Installation zusätzlicher bösartiger Nutzdaten (29 %), die Erhöhung von Berechtigungen (16 %) und die Einbettung von Hintertüren und anderen Persistenzmechanismen (21 %).

Um es den Opfern zu erschweren, ihre Daten ohne Bezahlung wiederherzustellen, griff außerdem etwa jeder fünfte Angreifer auf Backups zu und löschte diese sowie Schattenkopien von Dateien (beides passierte 19 % der Opfer).

Die Ergebnisse zeigen außerdem, dass die Angreifer, sobald die Ransomware ausgeführt und die Zahlungsaufforderung übermittelt wurde, beginnen, durch psychologische Taktiken Druck auf das Opfer auszuüben. Dazu gehören Drohungen gegenüber Partnern, Aktionären oder Kunden (erlebt von 22 %), Drohungen, die Presse oder Behörden zu informieren (21 %) und sogar Drohungen gegenüber Mitarbeitern (16 %).

Bei 27 % der erfolgreichen Ransomware-Angriffe haben die Angreifer die gestohlenen Daten anschließend weitergegeben, offengelegt oder veröffentlicht.

Ransomware-Opfer verlieren Kunden und neue Geschäftsmöglichkeiten

Sobald sich der Staub des eigentlichen Angriffs gelegt hat, stehen die Opfer vor operativen und kommerziellen Folgen.

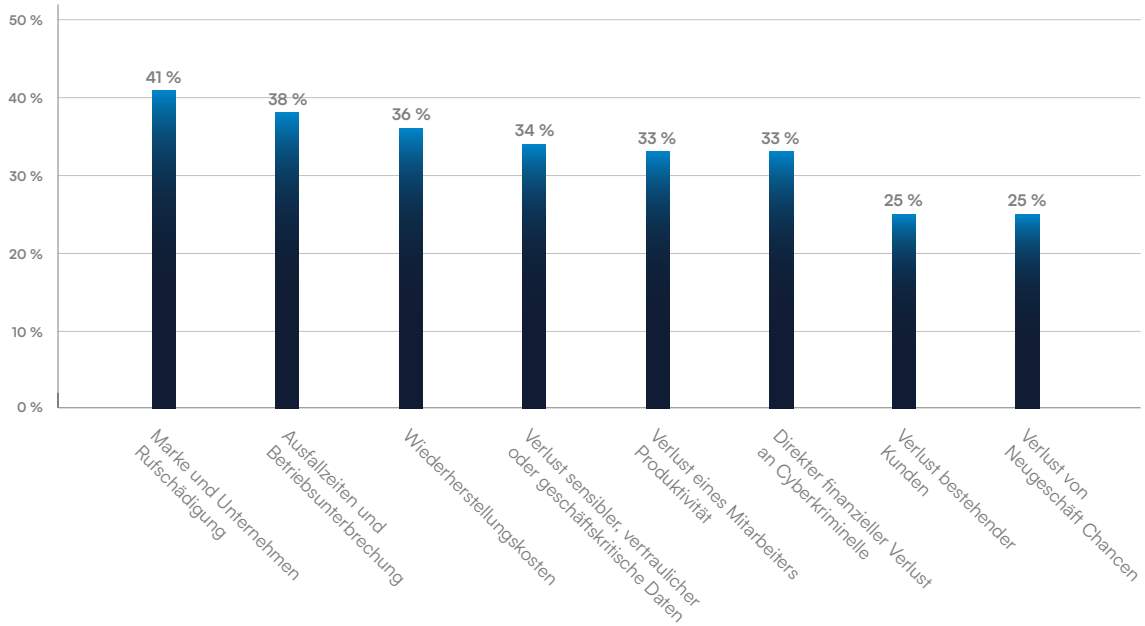
Als größte Auswirkung nannten die Opfer von Ransomware eine Schädigung ihrer Marke und ihres Rufs (41 %). Es folgen Ausfallzeiten (38 %) und Wiederherstellungskosten (36 %). Ein Drittel (34 %) gab zu, sensible Daten verloren zu haben.

Jedes vierte Opfer von Ransomware musste längerfristige geschäftliche Auswirkungen in Form von Verlust bestehender Kunden und entgangener neuer Geschäftsmöglichkeiten hinnehmen (jeweils 25 %).

ABBILDUNG 4

Die Auswirkungen des bedeutendsten Ransomware-Angriffs der letzten 12 Monate

n=1.146



Fazit

Um gegen Ransomware gewappnet zu sein, benötigen Unternehmen eine integrierte, mehrschichtige Security, die ihre ständig wachsende Angriffsfläche vor Cyberbedrohungen schützt.

Die folgenden praktischen Schritte können helfen:

- **Stellen Sie sicher, dass Daten regelmäßig und sicher gesichert** und offline aufbewahrt werden. Führen Sie Tests durch, um sicherzustellen, dass Sie Daten effektiv wiederherstellen können.
- **Implementieren Sie eine Multi-Faktor-Authentifizierung und setzen Sie das Prinzip der minimalen Berechtigung durch**, um den Zugriff auf Unternehmensressourcen und -anwendungen zu beschränken. Dadurch wird verhindert, dass Angreifer selbst mit gestohlenen Zugangsdaten auf wertvolle Daten und Systeme zugreifen können.
- **Halten Sie die Software mit den neuesten** Security-Patches auf dem neuesten Stand, um Sicherheitslücken zu schließen.
- **Bieten Sie Ihren Mitarbeitern regelmäßig Schulungen zur Cybersecurity an**, bei denen der Schwerpunkt auf den neuesten Phishing- und Ransomware-Taktiken liegt.
- **Segmentieren Sie das Netzwerk**, indem Sie kritische Systeme isolieren, um seitliche Bewegungen von Angreifern zu verhindern.
- **Überprüfen Sie alle Konfigurationen**, auch in der Cloud. Fehlkonfigurationen sind eine der Hauptursachen für Sicherheitsverletzungen.
- **Installieren Sie eine robuste E-Mail-Sicherheitslösung.** E-Mail bleibt ein primärer Einstiegspunkt für Ransomware, und fortschrittlicher, KI-gestützter Schutz kann bösartige Payloads erkennen und ausgefeilte Social-Engineering-Taktiken identifizieren, die darauf abzielen, Sicherheitsmaßnahmen zu umgehen.
- **Sichern Sie Web-Applikationen** wie Filesharing-Dienste, Webformulare und E-Commerce-Websites. Applikationen werden dabei oft über die Benutzeroberfläche oder eine API-Schnittstelle angegriffen.
- **Haben Sie einen Incident-Response-Plan — und proben Sie ihn regelmäßig.**
- **Erwägen Sie die Zusammenarbeit mit externen Experten**, einschließlich Managed Service Providers und Security-Anbietern, um zusätzliche Unterstützung zu erhalten. Diese Partner können Sie bei der Implementierung fortschrittlicher integrierter Sicherheitsplattformen und -lösungen unterstützen, mit denen Sie aktive Bedrohungen rund um die Uhr erkennen, blockieren und darauf reagieren können, um Vorfälle einzudämmen und zu neutralisieren, bevor sie ernsthaften Schaden anrichten können.

Über Barracuda

Barracuda ist ein weltweit führendes Cybersecurity-Unternehmen, das Unternehmen jeder Größe umfassenden Schutz vor komplexen Bedrohungen bietet. Unsere KI-gestützte Plattform sichert E-Mails, Daten, Anwendungen und Netzwerke mit innovativen Lösungen, einem verwalteten XDR-Service und einem zentralen Dashboard, um den Schutz zu maximieren und die Cyber-Resilienz zu stärken. Von Hunderttausenden von IT-Experten und Managed Service Providern weltweit als vertrauenswürdig angesehen, bietet Barracuda leistungsstarke Abwehrmaßnahmen, die einfach zu kaufen, bereitzustellen und zu verwenden sind.

Über Vanson Bourne

Vanson Bourne ist ein unabhängiger Spezialist für Marktforschung im Technologiesektor. Der Ruf des Unternehmens für robuste und glaubwürdige forschungsbasierte Analysen beruht auf strengen Forschungsprinzipien und der Fähigkeit, die Meinungen hochrangiger Entscheidungsträger in allen technischen und geschäftlichen Funktionen, in allen Geschäftsbereichen und allen wichtigen Märkten einzuholen. Weiter Informationen erhalten Sie unter vansonbourne.com.