WHITEPAPER

Risikominderung und Prävention durch eine effektive Kill Chain

Minimieren Sie die Auswirkungen von Ransomware mit Akamai Guardicore Segmentation

Übersicht

Zu Beginn war Ransomware nichts weiter als eine lästige Malware, mit der Cyberkriminelle fremde Dateien und Daten verschlüsselten, um den Zugriff darauf einzuschränken und Lösegeld für die erneute Freigabe zu verlangen. Dies hat mittlerweile jedoch extreme Ausmaße angenommen. Nicht genug damit, dass der dauerhafte Verlust von Daten an sich bereits eine schreckliche Bedrohung darstellt – die Methoden der Cyberkriminellen und Hacker, die mitunter sogar mit staatlicher Rückendeckung arbeiten, sind inzwischen so ausgeklügelt, dass sie mithilfe von Ransomware ganze Konzerne, Regierungen, globale Infrastrukturen und Gesundheitsorganisationen durchdringen und lahmlegen.

Der Kryptowurm WannaCry, der 2017 weltweit 230.000 Computer infizierte, indem er eine Schwachstelle von Microsoft Windows ausnutzte, war ein hochkarätiges Beispiel für die immense Bedrohung, die Ransomware darstellen kann. Die Angriffe sind seither noch ausgeklügelter und tiefgreifender geworden. Hacker verkaufen ihre Dienste mittlerweile sogar als Ransomware as a Service (RaaS). Im Bedrohungsbericht zu Ransomware H1 2022 von Akamai werden die Angriffsmuster von Conti, einer berüchtigten RaaS-Gruppe, untersucht. Die offenbar in Russland ansässige Organisation machte erstmals im Jahr 2020 auf sich aufmerksam. Die Analyse weist darauf hin, dass ein starker Schutz vor lateraler Netzwerkbewegung erforderlich ist und dies auch für den Schutz vor Ransomware eine wichtige Rolle spielen. Außerdem geht aus dem Bericht hervor, dass Conti es vornehmlich auf Unternehmen mit einem Umsatz zwischen 10 und 250 Millionen US-Dollar abgesehen hat.

> **Mikrosegmentierung verringert das implizite Vertrauen in das Netzwerk, indem nur ausdrücklich durch die Richtlinie freigegebene Verbindungen zugelassen werden. Dies erzwingt beim Machine-to-Machine-Traffic den Anwendungszugriff mit geringstmöglichen Berechtigungen.**
>
> **– Forrester, Best Practices For Zero Trust Microsegmentation, 27. Juni 2022**

Es zeigt deutlich, dass Unternehmen jeder Größe betroffen sind, die mit veralteter Technologie arbeiten und ihre Verteidigungsstrategien, die sich ausschließlich auf Netzwerke und Endpunkte konzentrieren, als „gut genug“ erachten. Mangelnde Schulung, schlechte Sicherheitsetikette und das Fehlen einer unangreifbaren Lösung tun ihr Übriges dazu. Cybersecurity Ventures geht in seinem Who's Who in Ransomware: 2023 Report davon aus, dass Unternehmen, Verbraucher oder Geräte bis 2031 alle 2 Sekunden einem Ransomware-Angriff ausgesetzt sein werden.

Laterale Netzwerkbewegung als Schlüssel

Bei Ransomware verschaffen sich die Angreifer anfänglich oft über eine Phishing-E-Mail, eine Schwachstelle im Netzwerk oder einen Brute-Force-Angriff Zugang, während sie Sicherheitssysteme gleichzeitig geschickt von ihrer eigentlichen Absicht ablenken. Nachdem die Malware auf einem Gerät oder in einer Anwendung Fuß gefasst hat, dringt sie durch das Erweitern von Berechtigungen und laterale Bewegung über das Netzwerk und zusätzliche Endpunkte weiter vor, um eine möglichst breit gefächerte Infektion und Verschlüsselung zu erzielen. Angreifer übernehmen in der Regel die Kontrolle über einen Domain-Controller, kompromittieren die Anmeldedaten und suchen und verschlüsseln anschließend das Backup, um zu verhindern, dass der Betreiber die lahmgelegten Dienste wiederherstellen kann.

Laterale Netzwerkbewegungen entscheiden über den Erfolg eines Angriffs. Malware, die sich von ihrem Eindringpunkt nicht weiter ausbreiten kann, ist nutzlos. Daher ist es wichtig, die laterale Netzwerkbewegung zu unterbinden. Durch die Transparenz- und Segmentierungsfunktionen einer Lösung wie Akamai Guardicore Segmentation können Sie schnell Richtlinien festlegen, die verhindern, dass Malware eindringt und sich verbreitet. Außerdem werden Sie auf laterale Netzwerkbewegung und andere verdächtige Verhaltensmuster aufmerksam gemacht, um Malware frühzeitig zu erkennen und entsprechend zu reagieren.

Teil 1: Risikominderung und Prävention durch eine effektive Ransomware-Kill-Chain

Ransomware verbreitet sich nicht, indem sie an einem einzelnen Gerät Schaden anrichtet. Cyberkriminelle verwenden Ransomware, um möglichst viele Systeme in einem Netzwerk zu verschlüsseln und die Lösegeldzahlung sicherzustellen.

Da Ransomware ein vielschichtiger Angriff ist, kann die Implementierung mehrerer Verteidigungsebenen dazu beitragen, umfassende Schäden, Datenverlust und Ausfallzeiten zu verhindern. Das Ziel der ersten Verteidigungsebene besteht darin, die Ransomware-Infektion zu verhindern.

Die Kill Chain von Ransomware

1. **Erstzugriff**
   (Spear) Phishing oder vulnerable Services
2. **Laterale Netzwerkbewegungen**
   Verbreitung über das Netzwerk für maximale Auswirkungen
3. **Extraktion**
   Wertvolle Daten finden und stehlen
4. **Verschlüsselung**
   PKI für die Verschlüsselung zum Schutz vor Cracking
5. **Lösegeldforderung**
   Wallpaper, E-Mail, txt-Datei usw.
6. **Auswirkungen**
   Daten, Finanzen, Marke usw.

Erstinfektion vermeiden

Die ersten anfälligen Stellen für jedes Netzwerk sind immer die Kontaktpunkte mit dem Internet. Viele Ransomware-Angriffe basieren zwar auf Spear-Phishing, doch im Prinzip können auch Services mit Verbindung zum Internet das Einfallstor sein.

Dank der Transparenz von Akamai Guardicore Segmentation können Sie online geschaltete Services überwachen und den Zugriff darauf durch Richtlinien schützen:

- Remotezugriffsdienste (RDP, SSH, TeamViewer, AnyDesk, VPNs)
- Potenziell anfällige Services (Apache, IIS, Nginx)
- Potenziell anfällige Rechner (Erkennung von Computern mit ungepatchtem Betriebssystem mithilfe der zusätzlichen Insight-Funktion)
- Ungewollt ungeschützte Services (Datenbanken, Domain-Controller, interne Web- oder Fileserver)

Verbesserung der Kill Chain durch Segmentierung

Früher oder später werden Angreifer in ein Netzwerk eindringen – das ist unvermeidbar. Dies kann durch Spear-Phishing, menschliches Versagen oder einen Server verursacht werden, auf dem ein anfälliger Service ausgeführt wird, der nicht ordnungsgemäß abgesichert wurde. Deshalb ist es wichtig, dass Sie über angemessene Strategien zur Risikominderung verfügen.

Wenn ein Computer infiziert wurde, müssen Sie die Ausbreitung innerhalb des Netzwerks begrenzen. Dies kann auf drei Arten erfolgen:

1. Segmentierung durch Abschirmen von Anwendungen

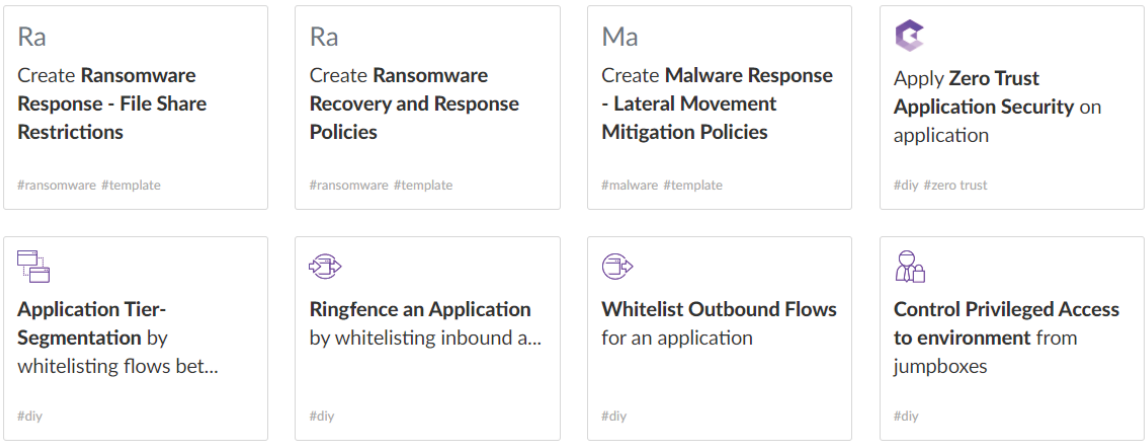
Das Netzwerk sollte nach Anwendung, Nutzung oder Umgebung in operative Segmente aufgeteilt sein, und unnötige Verbindungen zwischen und innerhalb dieser Segmente sollten nicht zugelassen werden.

Hier sind vier Segmentierungsrichtlinien, die Sie berücksichtigen sollten:

- Blockieren Sie jegliche Kommunikation zwischen Laptops/Workstations.
- Blockieren Sie die Kommunikation von Prozessen, die mit „weitreichenden“ Domain-Nutzerberechtigungen ausgeführt werden, wie z. B. Domain-Administratoren.
- Schränken Sie Nutzer ein, die Prozesse auf Ihren Servern ausführen können.
- Beschränken Sie den Zugriff von Laptops/Workstations auf Rechenzentrumsserver und Cloud-Instanzen.

Mit Akamai Guardicore Segmentation ist es ganz einfach, Ihr Netzwerk vor Ransomware zu schützen. Vorlagen helfen Ihnen, Richtlinien in drei einfachen Schritten festzulegen, um Angriffe abzuwehren:

1. **Legen Sie ein Ziel fest**, wie etwa das Abschirmen kritischer Anwendungen, das Erstellen von Abwehrrichtlinien für Ransomware oder das Sichern aktiver Verzeichnisse.
2. **Identifizieren Sie die zu schützenden Assets**, z. B. die abzuschirmenden E-Commerce-Anwendungsressourcen, die Active-Directory-Workloads im Rechenzentrum oder die Endpunkte, die Sie vor der Ausbreitung von Ransomware schützen möchten. Dieser Schritt wird in vielen Fällen automatisch durch das AI Labeling von Akamai erreicht.
3. **Schützen Sie Ihre Assets durch Richtlinien**. Die KI von Akamai Guardicore Segmentation schlägt automatisch basierend auf dem realen Traffic in der Umgebung Richtlinien vor und lernt die Kommunikationsmuster von Anwendungen in Hunderten von Netzwerken.

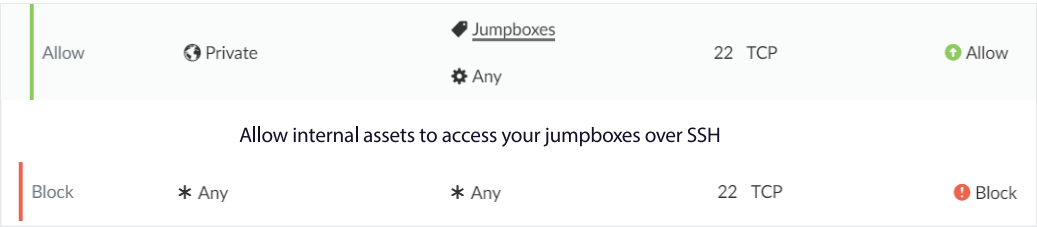


Beispiel: Vorlagen von Akamai Guardicore Segmentation

2. Verhindern lateraler Netzwerkbewegungen mit Regeln, die Protokolle einschränken

Es gibt allgemeine Richtlinien für spezifische Protokolle und Verhaltensweisen. Da einige Protokolle im täglichen Betrieb zum Einsatz kommen, sollte deren Einschränkung sorgfältig geprüft werden. Akamai Guardicore Segmentation ermöglicht die Visualisierung des gesamten Traffics. So können Sie die präzisesten Regeln für Ihre Umgebung rund um risikoreiche Protokolle wie WinRM, SMB, RPC, RDP, SSH oder andere erstellen.

SSH ist beispielsweise nützlich für die Remote-Verwaltung und dient auch zur Sicherung anderer Protokolle (wie SFTP), allerdings ist es auch ein Tool, das von Angreifern verwendet wird, um Computer zu infizieren und sich im Netzwerk zu verbreiten. Sie sollten das netzwerkweite SSH so weit wie möglich einschränken, indem Sie Jump-Boxen für autorisierte Nutzer erstellen.



In Akamai Guardicore Segmentation erstellte Regeln

3. Backups und essenzielle Datendienste schützen

Da Angreifer maximalen Schaden anrichten wollen, zielen Ransomware-Angriffe in der Regel auf die Backup-Server des Unternehmens ab, um die gespeicherten Daten zu verschlüsseln. Ebenso sind Datendienste und Fileserver Ziele für Ransomware.

Verwenden Sie Akamai Guardicore Segmentation, um den Zugriff auf Ihre Backup-Server, Datenbanken und Fileserver zu beschränken und den Zugang von außerhalb des Netzwerks und von Bereichen in Ihrem Netzwerk, die diesen nicht benötigen, einzugrenzen. Um die Kommunikation zu und von den kritischen Backup-Servern zu minimieren, können Sie Anwendungen mit Akamai Guardicore Segmentation abschirmen und deren Kommunikation bis hin zur Prozess- und Nutzerebene sperren. Wenn Sie die Risiken Ihrer Datendienste auf das operative Minimum beschränken, verringern Sie den Risikofaktor für diese Services und verringern die Risiken einer Infektion mit und der Ausbreitung von Ransomware.

Teil 2: Ransomware erkennen und abwehren

Wenn es um den Umgang mit Cyber-Bedrohungen wie Ransomware geht, sind Vorausplanung und Wachsamkeit von entscheidender Bedeutung. Indem Sie schnell auf einen Sicherheitsverstoß reagieren, können Sie den Schaden an Ihrem Netzwerk minimieren. Akamai Guardicore Segmentation verfügt über Funktionen, die Sie sowohl beim Erkennen von Bedrohungen als auch beim Reagieren darauf unterstützen können.

Bedrohungserkennung mit Akamai Guardicore Segmentation

Zu den Vorfällen gehören:

- **Täuschung**: Verdächtige laterale Netzwerkbewegungen werden erkannt, unterbunden und an dynamische Honeypots weitergeleitet, sodass ihre Aktionen überwacht und analysiert werden können. Täuschungen sind High-Fidelity-Vorfälle, die detaillierte Daten über schädliche Aktivitäten und die nächste Phase des Angriffs der Cyberkriminellen bereitstellen.
- **Netzwerk-Scans**: Cyberkriminelle sammeln Informationen, sobald sie sich in einem Netzwerk befinden. Die Netzwerk-Scans stellen eine Aufklärungsmethode dar, um offene Ports oder Services zu erkennen, die von anderen Servern abgefragt werden. Akamai Guardicore Segmentation erkennt Netzwerk-Scans automatisch und benachrichtigt Nutzer sofort.
- **Richtlinienbasierte Erkennung**: Sicherheitsrichtlinien auf Netzwerk- und Prozessebene ermöglichen die sofortige Erkennung von nicht autorisierter Kommunikation und nicht konformem Traffic.

Akamai Guardicore Segmentation mit Insight-Funktion

Mit Akamai Guardicore Segmentation können Sie die Transparenz individueller Assets durch eine zusätzliche, auf Osquery basierende Funktion erhöhen. Mit dem damit verbundenen Abfrage-Framework lassen sich ungewöhnliche Aktivitäten, wie etwa eine der Ransomware-Verschlüsselung häufig vorausgehende Volume Shadow Copy, schnell erkennen. Auch zum Einschleusen von Ransomware genutzte Trojaner werden damit erkannt. Dabei wird nach einer gängigen Hollowing-Technik gesucht, die Malware unter dem legitimen Windows-Prozess svchost.exe verbirgt.

Managed Threat Hunting

Der von Akamai Hunt bereitgestellte Service „Managed Threat Hunting“ warnt Nutzer vor ungewöhnlichen Verhaltensweisen in ihrem Netzwerk. Dies erfolgt durch Verfahren wie die Analyse ein- und ausgehender Internetverbindungen und deren zugeordneter GeoIP, die Suche nach neuen ausführbaren Dateien mit zunehmender Netzwerkpräsenz, die auf eine Ausbreitung hinweisen können, und die Analyse von Ressourcenverbindungen, um Hinweise auf laterale Netzwerkbewegung durch Anomalien bei der Anzahl von Nachbarn zu finden.

Unmittelbare Reaktion

Sobald Sie eine Bedrohung, wie z. B. Ransomware, in Ihrem Netzwerk erkannt haben, können Sie umgehend Maßnahmen zur Schadensbegrenzung implementieren, indem Sie Richtlinien auf Prozess- und Nutzerebene anwenden. Schädliche Abläufe werden dadurch aktiv abgewehrt und isoliert.

Stufenweise Infektionstransparenz

Nach dem ersten Hinweis oder Indicator of Compromise (IOC) können Sie nach weiteren Indikatoren suchen, wie Kommunikationsmustern, Prozessen, verwendeten Ports, infizierten Assets und mehr. Akamai Guardicore Segmentation ermöglicht es Ihnen, alle Assets mit diesem Indikator zu finden (alle Assets, die mit dem CnC oder einem eindeutigen Port kommunizieren, oder alle Assets, die einen schädlichen Prozess ausführen). Mithilfe einer Karte Ihrer Umgebung können Sie zudem nach anderen Ähnlichkeiten auf infizierten Computern oder Verbreitungsspuren suchen.

Teil 3: Desinfektion und Wiederherstellung

Sobald Sie eine Liste aller infizierten Geräte und IOCs haben, können Sie mit der Desinfektion beginnen. Teilen Sie Ihre Computer in drei eindeutige Gruppen auf: **Isoliert**, **überwacht** und **unbedenklich**.

Isoliert

- Ressourcen, die durch Malware **infiziert** sind
- Diese Ressourcen sollten in **Quarantäne** verbleiben, bis die Malware entfernt wurde

Überwacht

- Ressourcen, die **infiziert** sein könnten oder auch nicht
- Sie sollten sie **überwachen**, bis Sie sicher sind, dass die Malware **entfernt** wurde

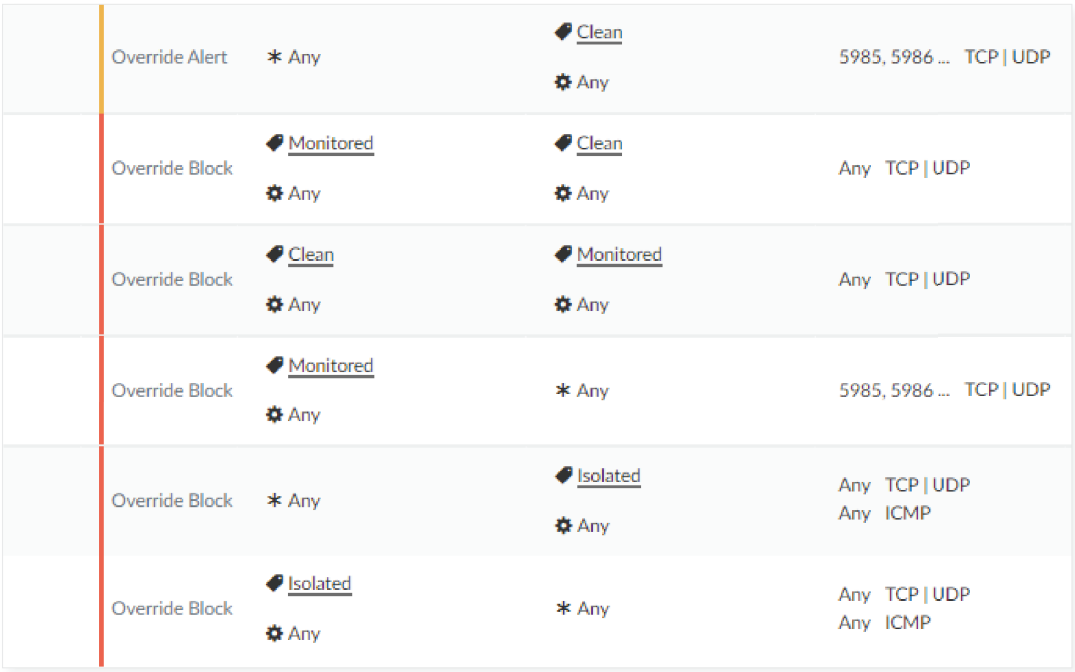
Unbedenklich

- Ressourcen, die nachweislich **nicht infiziert** wurden und **normal funktionieren** können

Segmentierungsrichtlinien für die Wiederherstellung

Nachdem Sie die drei Gruppen festgelegt haben, können Sie mit dem Hinzufügen von Richtlinien beginnen, um Ihr Netzwerk zu segmentieren, indem Sie vier Kommunikationsebenen erstellen:

- **Blockieren** ein- und ausgehender Kommunikation von **isolierten** Computern.
- **Blockieren** der Remote-Verwaltungsprotokoll-Kommunikation zu und von **überwachten** Computern.
- **Warnung** bei jeder Remote-Verwaltungsprotokoll-Kommunikation zu **unbedenklichen** Computern.
- **Blockieren** der gesamten Kommunikation zwischen den Gruppen.



Blockierungs- und Benachrichtigungsregeln in Akamai Guardicore Segmentation

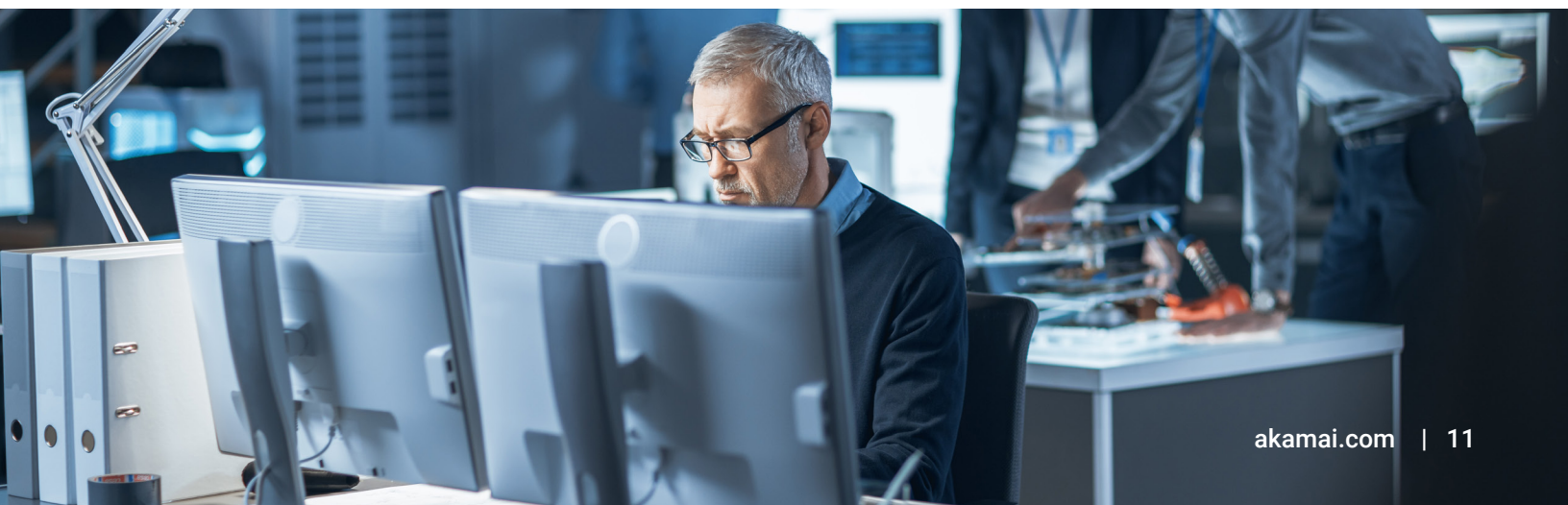
Vorlage für Reaktions- und Wiederherstellungsrichtlinien bei Ransomware-Angriffen

Die in Akamai Guardicore Segmentation enthaltene Vorlage zum Erstellen von Reaktions- und Wiederherstellungsrichtlinien im Falle eines Ransomware-Angriffs bietet Ihnen nutzerfreundliche, vordefinierte Regeln, anhand derer der Zugriff auf Assets beschränkt werden kann, die als **isoliert**, **überwacht** und **unbedenklich** kategorisiert wurden.

Mit dieser Vorlage können Sie die Betriebskontinuität **unbedenklicher** Computer aufrechterhalten – und das ohne das Risiko einer (erneuten) Infektion **isolierter** Geräte.

Fazit

Wenn Sie sich immer noch auf veraltete Firewalls verlassen oder auf eine Verteidigung setzen, die ausschließlich den Netzwerkrand sichert, werden Sie Ransomware nicht daran hindern, sich über Ihr Netzwerk auszubreiten und wichtige Anwendungen und Infrastrukturen lahmzulegen. Sicherheitsverstöße sind unvermeidlich und Sie müssen vorbereitet sein. Mit Akamai Guardicore Segmentation können Sie Bedrohungen in East-West-Traffic im Rechenzentren erkennen und die laterale Netzwerkbewegung blockieren, über die sich Ransomware ausbreitet, um Ihre kritischen Assets zu verschlüsseln und Lösegeld für deren Freischaltung zu verlangen.



Fünf Schritte zur Minderung der Auswirkungen von Ransomware-Angriffen mit Akamai Guardicore Segmentation

Vorbeugen durch die Identifizierung jeder Anwendung und jedes Assets in Ihrer IT

Verhindern durch das Aufstellen von Regeln, um allgemeine Verbreitungstechniken von Ransomware zu blockieren

Erkennen durch das Empfangen von Benachrichtigungen, die Sie auf jeden Versuch eines Zugriffs auf segmentierte Anwendungen und Backups aufmerksam machen

Beheben durch das Initiieren von Maßnahmen zur Eindämmung und zur Isolation von Bedrohungen, sobald ein Angriff erkannt wird

Integrität wiederherstellen durch Visualisierungsfunktionen zur Unterstützung stufenweiser Wiederherstellungsstrategien

Verhindern Sie die lateralen Netzwerkbewegungen von Ransomware in Ihrem Netzwerk. Sie glauben uns nicht? Überzeugen Sie sich selbst unter akamai.com/guardicore