Guardicore

DATA SHEET

Guardicore Centra™ Sicherheitsplattform

Granulare Sichtbarkeits- und Mikrosegmentierungskontrollen für Rechenzentrums-, Cloud- und hybride Cloud-Umgebungen

Die IT-Infrastruktur von Unternehmen entwickelt sich rasant von einem traditionellen Rechenzentrumsmodell zu Cloud- und Hybrid-Cloud-Architekturen mit einer Mischung aus Plattformen und Anwendungsbereitstellungsmodellen. Diese Transformation trägt zwar dazu bei, dass viele Unternehmen eine größere Agilität erreichen und die Infrastrukturkosten senken, schafft aber auch eine größere und komplexere Oberfläche für Sicherheitsangriffe.

Da das traditionelle Konzept eines Netzwerkperimeters immer weniger relevant wird, wird jeder einzelne Server zu einem möglichen Startpunkt für einen Angriff. Angreifer reagieren auf diese Verschiebung, indem sie sich verstärkt darauf konzentrieren, sich lateral zwischen den Ost-West-Verkehrsarbeitslasten zu bewegen.

Die Guardicore Centra™ Security Platform ist eine umfassende Rechenzentrums- und Cloud-Sicherheitslösung, die die einfachste und intuitivste Möglichkeit bietet, Mikrosegmentkontrollen anzuwenden, um die Angriffsfläche zu reduzieren und Verletzungen im Ost-West-Verkehr zu erkennen und zu kontrollieren. Es bietet einen tiefen Einblick in Anwendungsabhängigkeiten und -flüsse sowie die Durchsetzung von Richtlinien auf Netzwerk- und individueller Prozessebene, um kritische Anwendungen und Infrastrukturen zu isolieren und zu segmentieren.

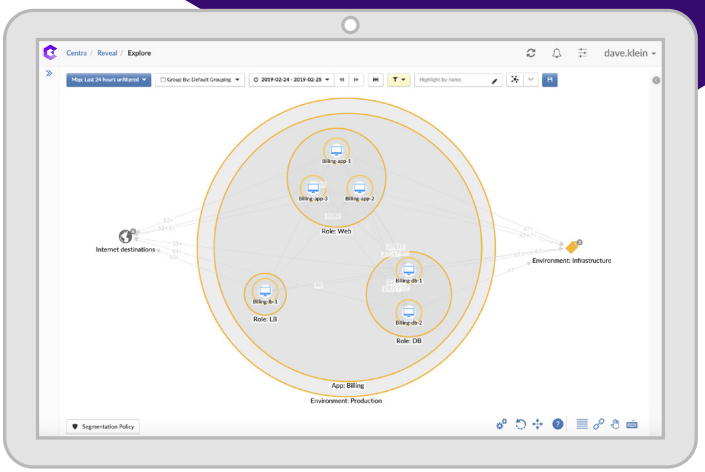
So funktioniert es

Guardicore Centra sammelt detaillierte Informationen über die IT-Infrastruktur eines Unternehmens durch eine Mischung aus agentenbasierten Sensoren, netzwerkbasierten Datensammlern und Flow-Logs der Virtual Private Cloud (VPC) von Cloud-Anbietern. Diese Informationen werden dann durch einen flexiblen und hochautomatisierten Kennzeichnungsprozess in den Kontext gestellt, der die Integration mit allen vorhandenen Datenquellen wie Orchestrierungssystemen und Konfigurationsmanagementdatenbanken beinhaltet. Das Ergebnis ist eine dynamische visuelle Karte der gesamten IT-Infrastruktur, die es den Sicherheitsteams ermöglicht, die Aktivitäten bis auf die einzelne Prozessebene in Echtzeit und auf historischer Basis zu betrachten. Diese detaillierten Einblicke in das Anwendungsverhalten können dann genutzt werden, um schnell granulare Mikrosegmentierungsrichtlinien über eine intuitive visuelle Oberfläche zu erstellen. Die Mikrosegmentfähigkeiten von Centra werden auch durch ein innovatives Set von Funktionen zur Erkennung und Reaktion von Lücken ergänzt. Centra bietet Schutz für Ihre gesamte Infrastruktur. Centra schützt Workloads in hybriden Umgebungen mit einer beliebigen Kombination aus Legacy-Systemen, Bare-Metal-Servern, virtuellen Maschinen, Containern und Cloud-Instanzen in Amazon Web Services, Microsoft Azure und Google Cloud Platform.

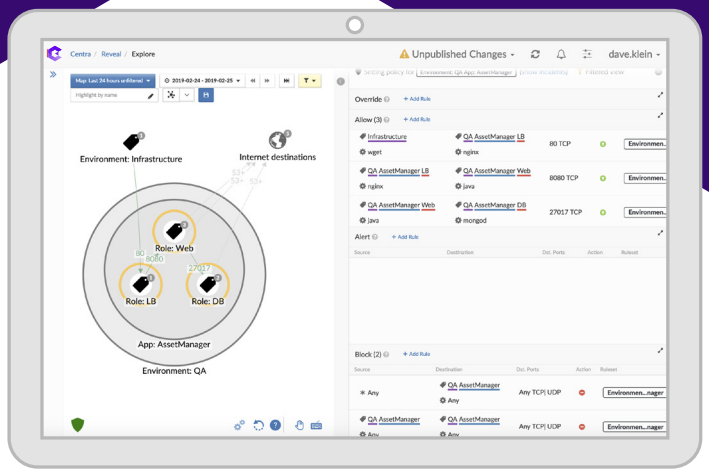
Highlights

- **Unübertroffene Sichtbarkeit**
  Abbildung von Anwendungsabhängigkeiten und -abflüssen bis auf die Prozessebene mit Kontext in Echtzeit und historisch.
- **Plattformunabhängig**
  Mikrosegmentierung auf jedes Betriebssystem über eine beliebige Kombination von Legacy-Systemen, Bare-Metal-Servern, VMs, Containern oder Cloud-Instanzen anwenden.
- **Granulare Durchsetzung von Richtlinien**
  Definition und Durchsetzung von L4 und L7 Segmentierungsrichtlinien über alle Server und Betriebssysteme hinweg.
- **Umfassende Unterstützung für Anwendungsfälle**
  Unterstützt die breiteste Palette von Anwendungsfällen für Segmentierung und Mikrosegmentierung, von der Umweltsegmentierung bis hin zur Anwendungsabgrenzung und mehr.
- **Breiter Schutz**
  Integrierte Funktionen zur Erkennung von Verletzungen und zur Reaktion auf Vorfälle ergänzen die Maßnahmen zur Mikrosegmentierung und erhöhen den Schutz und den ROI.

Einfache und intuitive Mikro-Segmentierung



Guardicore Centra entdeckt automatisch Anwendungsabhängigkeiten und -flüsse und generiert eine visuelle Karte, um ein vollständiges Verständnis zu gewährleisten, bevor Segmentierungsrichtlinien angewendet werden.
Reduzierung der Angriffsfläche, Sicherung kritischer Anwendungen



Direkt aus der visuellen Karte heraus können Administratoren schnell Anwendungs- und Mikrosegmentierungsrichtlinien erstellen, die auf automatisch generierten Regelempfehlungen und dem historischen Kontext basieren

Einfache und intuitive Mikro-Segmentierung

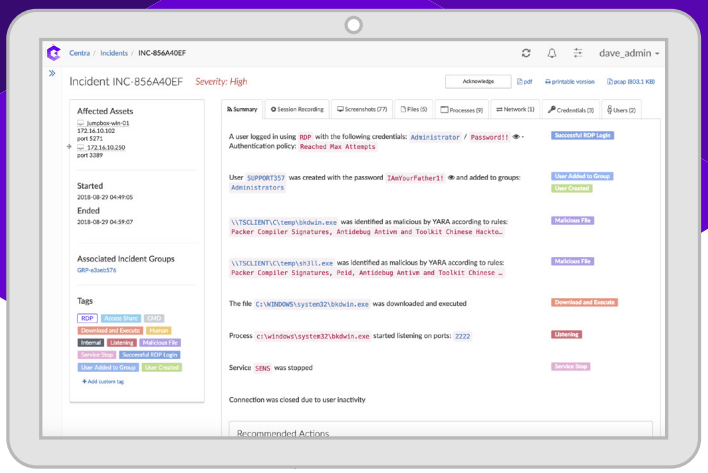
- **Breite Abdeckung:** Wenden Sie Mikrosegmentierungsrichtlinien überall dort an, wo Ihre Anwendungen in öffentlichen, privaten oder hybriden Cloud-Umgebungen ausgeführt werden.
- **Tiefe Sicht:** Anwendungsbezogene Transparenz, damit Sie die Abhängigkeiten der Anwendung vollständig verstehen, bevor Sie Sicherheitsrichtlinien für die Mikrosegmentierung definieren.
- **Intuitiver Workflow:** Ein hochvisueller Workflow und eine leistungsstarke Verbundregellogik ermöglichen die schnelle und intuitive Erstellung von Mikrosegmentierungsrichtlinien.
- **Granulare Richtlinien:** Festlegung und Durchsetzung von Regeln auf Prozessebene zur strikten Kontrolle der Abläufe zwischen den Anwendungskomponenten, was zu einem optimalen Sicherheitsniveau führt.

Mikro-Segmentierung vereinfacht

- **Visualisieren:** Guardicore Centra bietet branchenführende Transparenz, die automatisch alle Anwendungsabhängigkeiten und Kommunikationsflüsse im Kontext der Prozessebene erkennt und abbildet. Diese Visualisierung, ergänzt durch den automatischen Import von Orchestrierungsmetadaten, ermöglicht es Sicherheitsteams, alle Assets und Anwendungen einfach zu kennzeichnen und zu gruppieren und die Richtlinienentwicklung zu optimieren.
- **Bauen:** Guardicore vereinfacht die Entwicklung und Verwaltung von Richtlinien zur Mikrosegmentierung. Ein einziger Klick auf einen Kommunikationsfluss generiert automatisierte Regelvorschläge basierend auf historischen Beobachtungen und erstellt schnell eine starke Richtlinie. Ein intuitiver Workflow und eine flexible Policy-Engine unterstützen die kontinuierliche Weiterentwicklung der Richtlinien und reduzieren kostspielige Fehler.
- **Durchsetzen:** Mit der Möglichkeit, Kommunikationsrichtlinien auf Netzwerk- und Prozessebene sowohl auf Windows- als auch auf Linux-Systemen durchzusetzen, gewährleistet Centra die Sicherheit unabhängig von den Einschränkungen der Durchsetzung von Betriebssystemen. Integrierte Funktionen zur Erkennung und Reaktion auf Verstöße ermöglichen es Ihnen, Richtlinienverletzungen im Zusammenhang mit einem aktiven Verstoß zu erkennen und die Angriffsmethode zu identifizieren.

Guardicore

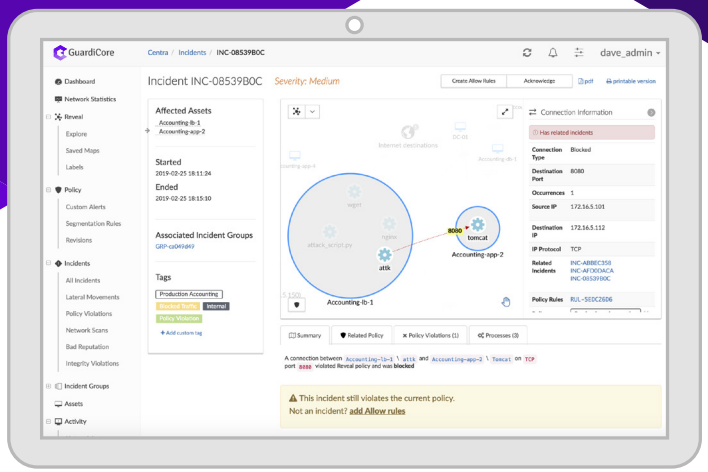
Erkennen Sie mehr Bedrohungen schneller und reagieren Sie mit mehr Intelligenz



Guardicore Centra bietet High-Fidelity-Sicherheitsvorfälle im Kontext mit Details zu Angreifer-Tools und -Techniken, die IR-Teams helfen, die Untersuchung von Vorfällen zu priorisieren und die Verweildauer zu verkürzen.

Über die Mikro-Segmentierung hinaus: Datendiebstahlerkennung und - reaktion

- **Mehrere Erkennungsmethoden:** Drei Erkennungsmethoden - Dynamic Deception, Reputation Analysis und Policy-Based Detection - bilden ein starkes Sicherheitsnetz, um Live-Angriffe umzuleiten oder einzudämmen.
- **Entwickelt für die Cloud:** Patentierte dynamische Täuschung mit zusätzlichen Methoden, die auf die besonderen Anforderungen der Cloud zugeschnitten sind, bietet Abdeckung gegen Angriffsvektoren, die andere Produkte nicht nutzen.
- **Integrierte Antwort:** Verwertbare Informationen und die Aufzeichnung der genauen Tools und Methoden der Angreifer ermöglichen eine Echtzeit-Reaktion auf Verstöße und die kontinuierliche Verbesserung der Mikrosegmentierungsrichtlinien.
- **Detaillierte Forensik:** Vorfallsdaten werden in einer für den Menschen lesbaren Form neben Beweismitteln dargestellt, einschließlich Indikatoren für Kompromisse, relevante Artefakte und die Identifizierungsmerkmale von menschlichen Angreifern gegenüber Bots.



Die Durchsetzung auf Prozessebene erkennt, warnt und blockiert den Zugriff unbefugter Prozesse auf kritische Anwendungskomponenten, reduziert die Angriffsfläche und begrenzt Querbewegungen.

Sehen Sie sich den gesamten Angriff an, blockieren Sie seitliche Bewegungen und reduzieren Sie die Verweildauer

- **Erkennen:** Centra verfügt über mehrere Erkennungsmethoden, die für Angriffe auf die Cloud- und Rechenzentrumsinfrastruktur entwickelt wurden, darunter die richtlinienbasierte Erkennung nicht genehmigter Aktivitäten, eine hochinteraktive Täuschungsmaschine, die Angreifer stört und Angriffsdetails erfasst, und eine Reputationsanalyse, die verdächtige Domainnamen, IP-Adressen und Dateihashes innerhalb von Verkehrsströmen erkennt.
- **Untersuchen:** Centra sammelt den gesamten Angriffsfußabdruck - die Dateien und Tools, die verwendet und hochgeladen werden, sowie das Arsenal an Waffen, die der Eindringling aktiviert - und führt Tiefenforensik durch, um Benutzeranmeldungen, Angriffsmethoden, Verbreitungsstrategien und vieles mehr offenzulegen.
- **Reagieren Sie:** Beschleunigen Sie die Reaktion auf Vorfälle durch automatische Exporte von Kompromissindikatoren an Sicherheitsgateways und Sicherheitsinformations- und Ereignismanagementsysteme, Aktualisierungen von Segmentierungsrichtlinien mit einem Klick, um Verkehrsverstöße zu beheben, und die Möglichkeit, Aktionen an VMs auszulösen - Suspendieren, Anhalten, Trennen oder Snapshot -, um die Ausbreitung von Schäden durch Ransomware-Angriffe zu verhindern.

Guardicore

Umfassender Schutz bei der Cloud-Skala

Jede Umgebung

Schützen Sie Workloads in hybriden Cloud-Umgebungen mit einer Kombination aus lokalen Workloads, virtuellen Maschinen, Containern und Cloud-Instanzen über Amazon Web Services, Microsoft Azure und Google Cloud Platform.

Vereinfachung der Sicherheit

Vereinfachung des Sicherheitsmanagements mit einer Plattform, die Flow-Transparenz, Mikrosegmentierung, Datendiebstahlerkennung und -reaktion bietet.

Skalierbarkeit und Leistung des Unternehmens

Skalierbar, um die Leistungs- und Sicherheitsanforderungen einer Umgebung jeder Größe zu erfüllen.

Unterstützung für die moderne Enterprise IT-Infrastruktur

Guardicore Centra is designed to integrate with your infrastructure

Speicher- und Systemanforderungen
Management Server: 32 GB RAM min, 64 GB RAM empfohlen, 12 vCPUs, 400 GB Speicherplatz

Deception Server: 32 GB RAM min, 64 GB RAM empfohlen, 8 vCPUs, 100 GB Speicherplatz

Aggregator: 2 GB RAM min, 4 GB RAM empfohlen, 2 vCPUs min, 4 vCPUs empfohlen, 30 GB Speicherplatz

Kollektor: 2 GB RAM min, 4 GB RAM empfohlen, 2 vCPUs min, 4 vCPUs empfohlen, 30 GB Speicherplatz

Public Cloud Anbieter
Amazon Web Services, Microsoft Azure, Oracle OPC, Google Cloud Plattform

Container Orchestrierung & Engines
Docker, Kubernetes, OpenShift

Orchestrierung
VMware vSphere und VMware vCenter Server 5.5.x und höher, VMware NSX Manager 6.1.x, Nuage Networks, CloudStack, Mission Critical Cloud, Openstack (Vanila/Mirantis)

Sicherheits-Gateways
Palo Alto Netzwerke, Check Point Software Technologien, Cisco

Hypervisor(s)
KVM, XenServer, Microsoft Hyper-V, VMware ESX 5.1 oder höher für jeden Server.

Intelligence-Sharing-Exportprotokolle
STIX, Syslog, CEF,
Open REST API öffnen

Über Guardicore

Guardicore ist ein innovativer Anbieter im Rechenzentrums - und Cloud Securitybereich. Der Fokus liegt hierbei einem sehr effektiven und akkuraten Weg um hoch anspruchsvolle Bedrohungen durch Echtzeit Breach Detection und Response zu erkennen und zu stoppen. Entwickelt von top Cybersicherheitsexperten verändert Guardicore die Art und Weise wie Unternehmen Cyber Attacken in Ihren Rechenzentren und der Cloud abwehren.

www.guardicore.com

v. 4.0

Guardicore