DATENBLATT

ThreatSync+ SaaS

Unified Network Security leicht gemacht

ThreatSync+ SaaS ist eine Erweiterung der ThreatSync XDR-Lösung von WatchGuard. Sie wird in der WatchGuard Cloud verwaltet und bietet eine hocheffektive Lösung für Erkennung und Abwehr bei Cloud- und SaaS-Anwendungen für Cybersicherheitsteams, die sich mit dem Schutz von Cloud-Umgebungen befassen. ThreatSync+ SaaS nutzt KI-gesteuerte Sicherheitsrichtlinien und stellt Risiken und Bedrohungen für M365, Azure, Google Workspace, Google Cloud und AWS Cloud übersichtlich dar, die durch intelligente Warnungen, Untersuchungsansichten und Compliance-Berichte priorisiert werden.

Sobald Risiken und Bedrohungen für Cloud-Anwendungen identifiziert wurden, sendet ThreatSync+ SaaS sie zur Behebung an ThreatSync Core und bietet somit eine einheitlich orchestrierte Reaktion. Gemeinsam optimieren sie die Cybersicherheit in der Cloud, verbessern die Transparenz, beschleunigen die automatisierten Reaktionsmaßnahmen im gesamten Unternehmen, reduzieren Risiken und Kosten und bieten mehr Präzision.

Risiken und Bedrohungen in Ihrer gesamten Cloud-Umgebung identifizieren

Betriebsleiter von Hybrid-Netzwerken und Cloud-Umgebungen erhalten mit ThreatSync+ SaaS einen umfassenden Überblick über abnormale riskante Aktivitäten in Cloud-Umgebungen und SaaS-Anwendungen. Dadurch können sie gefährdete Benutzer- und Administratorkonten, Cloud-Anwendungen und Dateiaktivitäten schnell identifizieren, ohne die IT überzustrapazieren.

Bedrohungen erkennen und stoppen, Verweildauer verkürzen

ThreatSync+ SaaS ermöglicht eine automatisierte, kontinuierliche Überwachung von Bedrohungen aller Cloud-Plattformen und SaaS-Anwendungen. Mit einer einzigartigen Kombination aus Cyber-TTP-Richtlinien, Threat Intelligence und KI stellt es eine kurze, priorisierte Liste mit intelligenten Warnungen und Bedrohungsberichten bereit. Cyber- und IT-Manager können Cyberangriffe so rund um die Uhr schnell untersuchen und beheben.

Kontinuierliche Compliance nachweisen

ThreatSync+ SaaS umfasst zahlreiche Compliance-Kontrollen für Cloud-Plattformen und SaaS-Anwendungen, die mit ISO 27001, NIST 800-53 und Cyber Essentials kompatibel sind. Diese Kontrollen sind leicht zu aktivieren und stellen die Steuerung von Effektivität, SLA und Compliance-Zielverfolgung sofort übersichtlich dar. Fügen Sie WatchGuard Compliance Reporting für vorgefertigte, automatisierte Compliance-Richtlinien und Berichte zur Kontrolleffektivität hinzu, die FFIEC, NIST, ISO, NIAC, CMMC und mehr abdecken.

Upgrade auf die ThreatSync+ Suite

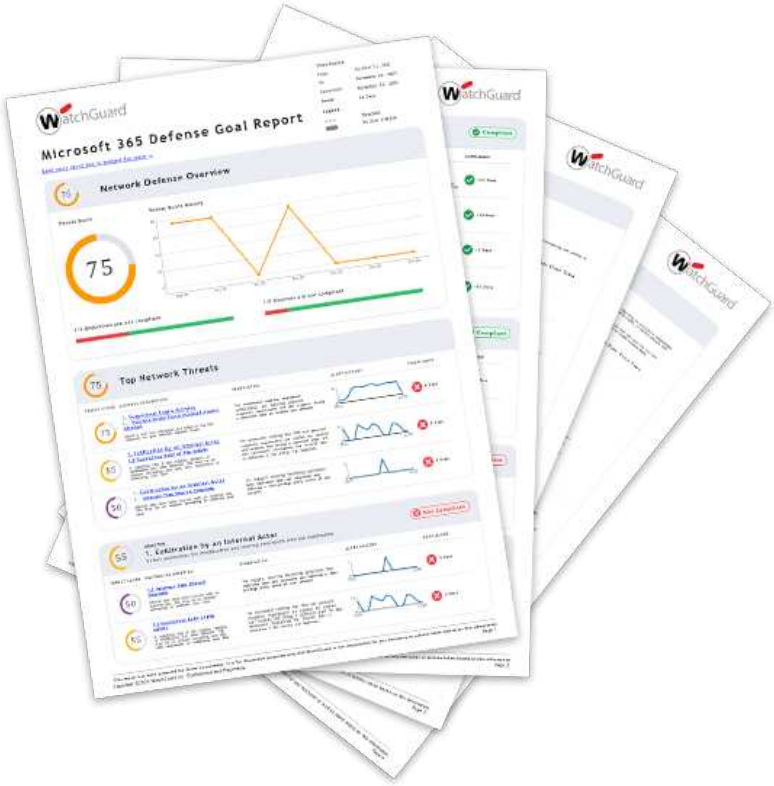
ThreatSync+ SaaS ist vollständig in die ThreatSync+ Suite integriert. Das Upgrade auf die Suite erweitert die Abdeckung der Bedrohungserkennung um komplette hybride Netzwerk- und Cloud-Infrastrukturen und fügt automatisierte Compliance-Berichte hinzu – alles zu einem günstigen Preis. Die ThreatSync+ Suite beinhaltet ThreatSync Core, ThreatSync+ NDR und SaaS sowie WatchGuard Compliance Reporting.

Vorteile

- Machen Sie sich weniger abhängig von den komplexen und kostspieligen „integrierten“ Cloud-Bedrohungserkennungssystemen, die für Azure, Google und AWS entwickelt wurden.
- Verschaffen Sie sich einen einheitlichen Risiko- und Bedrohungsüberblick über mehrere Cloud-Plattformen und SaaS-Anwendungen, einschließlich M365 und Google Workspaces.
- Verringern Sie die Kosten für Sicherheit und Compliance von Cloud-Plattformen, indem Sie Überwachungs-, Warn- und Behebungs- sowie Compliance-Kontrollberichte automatisieren.
- Stellen Sie sofort einsatzbereite M365-Risiko- und Bedrohungsberichte bereit, um Sicherheitsstatus und Verbesserungen nachzuweisen.

Bedrohungserkennung für M365

Überwachen Sie Nutzung, Risiken und Bedrohungen aller M365-SaaS-Anwendungen kontinuierlich, einschließlich Office, Teams, OneDrive und SharePoint. Mithilfe von KI-gestützter Bedrohungsmodellierung können Sie Verhaltensweisen und Aktivitäten, die zu kompromittierten Benutzerkonten, anwendungsbasierten Angriffen und Verlust vertraulicher Daten führen, leicht identifizieren und mindern.



Wichtige Funktionen

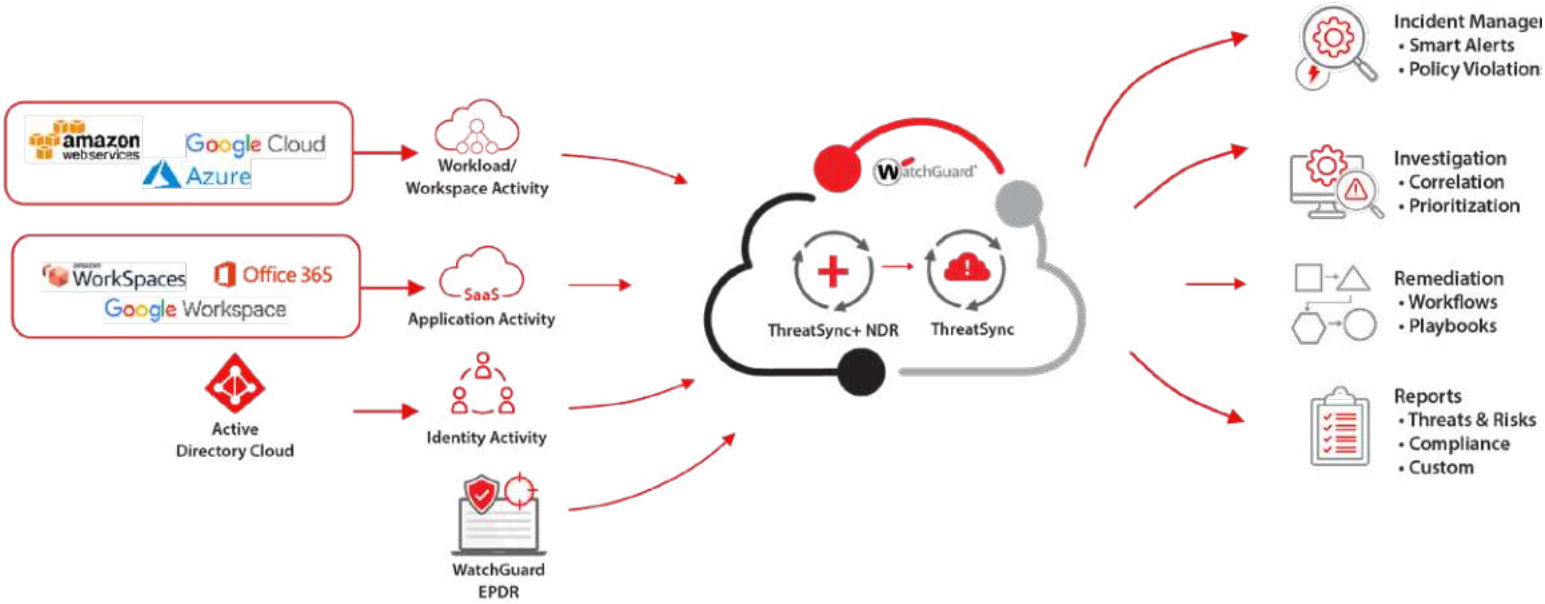
KI-gesteuerte Präzision bei der Erkennung von Angriffen in Ihren beruflichen Cloud-Umgebungen, einschließlich:

- Brute-Passwort-Angriff
- Angriff auf Benutzerkonten mit Zugriffsberechtigung
- Eskalationen von Zugriffsberechtigungen
- Kompromittieren von Benutzerkonten
- Laterale Bewegung
- Diebstahl vertraulicher Dateien
- Staging der Dateiexfiltration
- Datenexfiltration
- Insider-Bedrohungen
- Rogue-/Unmögliches Benutzerverhalten

NIST- und ISO-Richtlinienbasierte, KI-gestützte Kontroll-Frameworks unterstützen eine kontinuierliche Überwachung der Compliance.

ThreatSync+ SaaS unterstützt Azure, M365, Active Directory Cloud, Google, Google Workspace und AWS-Plattformen. Die plattformübergreifende Unterstützung ermöglicht die Koordinierung und Automatisierung mehrerer Prozesse und Tools mithilfe der Sicherheitsorchestrierung zur Förderung eines einheitlichen Sicherheitskonzepts.

ThreatSync und ThreatSync+ SaaS bieten erschwingliche, umfassende und einheitliche Bedrohungsanalysen



DEUTSCHLAND, ÖSTERREICH, SCHWEIZ +49 700 92229333 INTERNATIONALER VERTRIEB: +1 206 613 0895 WEB: www.watchguard.de WatchGuard Technologies, Inc.

Mit diesem Dokument werden keine ausdrücklichen oder stillschweigenden Gewährleistungen gegeben. Alle hier aufgeführten technischen Daten können sich ändern. Informationen zu zukünftigen Produkten, Ausstattungsmerkmalen und Funktionen werden zu gegebener Zeit zur Verfügung gestellt. ©2024 WatchGuard Technologies, Inc. Alle Rechte vorbehalten. WatchGuard, das WatchGuard Logo und ThreatSync sind eingetragene Marken von WatchGuard Technologies, Inc. in den USA und/oder anderen Ländern. Alle weiteren Markennamen sind das Eigentum ihrer jeweiligen Inhaber. Teilenr.WGCE67800_103124