Cisco Tetration Analytics Platform

Het Cisco Tetration Analytics™platform pakt belangrijke operationele en beveiligings-uitdagingen van het datacenter aan door op applicatiegedrag gebaseerde inzichten te bieden, het genereren van whitelistpolicy te automatiseren en zero-trust beveiliging in te schakelen met behulp van applicatiesegmentering.

Productoverzicht

Applicaties bepalen het ontwerp van datacenterinfrastructuren. Moderne Applicaties zijn dynamisch, maken gebruik van virtualisatie, containerisatie, microservices en technologieën voor workloadmobiliteit, waarbij sprake is van voortdurend veranderende communicatiepatronen tussen applicatiecomponenten. Nu is 76% van het datacenterverkeer oost-west, een fundamentele verandering in vergelijking met verkeerspatronen in het verleden. Deze technologische verschuiving heeft bijgedragen aan een vergroot aanvalsgebied en gaten in policyshandhaving. Deze dynamische omgeving heeft diverse uitdagingen opgeworpen die organisaties moeten aangaan:

- Een statisch beveiligingsmodel dat aan de buitengrens van het netwerk wordt geïmplementeerd is niet langer voldoende.
- Organisaties moeten diepgaande zichtbaarheid verkrijgen in de communicatie en afhankelijkheden van Applicaties en een whitelistpolicy genereren voor segmentering.
- Organisaties moeten een consistent zero-trust model voor Applicaties implementeren in een heterogene omgeving, maar tegelijkertijd flexibel genoeg zijn om dat policy up-to-date te houden.

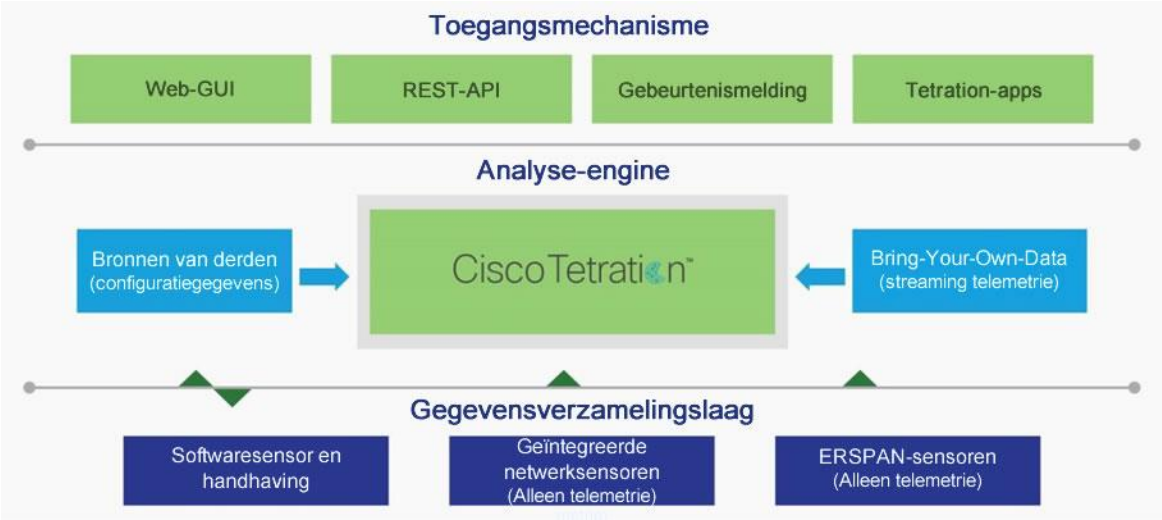
Het Cisco Tetration™-platform is ontwikkeld om deze uitdagingen doeltreffend aan te gaan op basis van uitgebreide telemetriegegevens over verkeersflows die afkomstig zijn van zowel servers als Cisco Nexus®-switches. Het platform voert geavanceerde analyses uit op basis van algoritmen en dwingt een consistent whitelistpolicy voor Applicaties af. Bij deze algoritmische verwerking wordt gebruikgemaakt van onbeheerde technieken voor machine learning en gedragsanalyse. Het platform vormt een kant-en-klare oplossing.

- Het biedt volledige zichtbaarheid van Applicatiecomponenten, hun communicatie en afhankelijkheden voor implementatie van een zero-trust model in het datacenter.
- Het voert real-time asset-tagging uit, zodat beheerders zakelijke mechanismen kunnen koppelen aan telemetriegegevens over verkeersflows en workloads.
- Het genereert automatisch segmenteringspolicy op basis van het gedrag van Applicaties. Het biedt tevens een mechanisme voor de opname van beveiligingspolicy op basis van bedrijfsvereisten.
- Organisaties kunnen dit segmenteringspolicy consistent op heterogene infrastructuren uitvoeren om segmentering van Applicaties te implementeren.

Voor al deze functies worden uitgebreide Cisco Tetration telemetriegegevens verzameld met behulp van speciaal ontwikkelde sensoren. De volgende typen sensoren worden gebruikt: softwaresensoren, hardwaresensoren en ERSPAN-sensoren (Encapsulated Remote Switched Port Analyzer). Met deze verschillende typen sensoren kan deze oplossing zowel bestaande (brownfield) als nieuwe (greenfield ofwel niet Cisco infrastructure) datacenters en openbare cloudinfrastructuren ondersteunen.

In afbeelding 1 wordt de overkoepelende architectuur van het Cisco Tetration platform weergegeven.

Afbeelding 1. Architectuur van het Cisco Tetration-platform



Het Cisco Tetration platform heeft vier hoofdfunctielagen:

- **Gegevensverzamelingslaag:** deze laag bestaat voornamelijk uit sensorfuncties. Sensoren vormen de ogen en oren van het Cisco Tetration Analytics™platform. Er worden twee typen sensoren gebruikt:
  - **Softwaresensoren:** deze lichtgewicht sensoren worden uitgevoerd als gebruikersprocessen en kunnen op elke gewenste server (gevirtualiseerd of bare-metal) in datacenters op locatie en in een openbare cloud worden geïnstalleerd. Deze softwaresensoren kunnen telemetriegegevens verzamelen en fungeren tevens ten behoeve van Policy Enforcement.
  - **Hardwaresensoren:** deze sensoren zijn geïntegreerd in switches van het type Cisco Nexus 93180YC-EX, 93108TC-EX, 93180YC-FX en 93108TC-FX.
  - **ERSPAN-sensoren:** deze out-of-band sensoren zijn ontwikkeld om Cisco Tetration telemetriegegevens te genereren aan de hand van kopieën van netwerkpakketten. Deze gekopieerde pakketten worden met ERSPAN aan deze sensoren geleverd.

  Sensoren zijn ontwikkeld voor het bewaken van elk pakket en elke flow. Ze verzamelen geen informatie afkomstig van de payload en er wordt geen sampling uitgevoerd.

- **Analyselaag:** gegevens afkomstig van de sensoren worden verzonden naar het Cisco Tetration platform waar alle analyses worden uitgevoerd. Dit big data platform met meerdere knooppunten verwerkt de informatie afkomstig van de sensoren en maakt gebruik van zowel onbeheerde als begeleide machine learning, gedragsanalyse en intelligente algoritmen om een kant-en-klare oplossing (ofwel gestructureerde) voor de volgende use cases te bieden:
    - Nauwkeurig inzicht in communicatie van Applicatiecomponenten op basis van waargenomen gedrag
    - Geautomatiseerde groepering van vergelijkbare endpoints (zoals webserver- en databaseclusters)
    - Binnen enkele minuten aanbevelingen voor consistent whitelistpolicy voor Applicaties en controle op niet-naleving
    - Analyse van policysimpact voordat een policy op het netwerk wordt toegepast en gehandhaafd
    - Geautomatiseerde policyshandhaving die consistente segmentering van Applicaties mogelijk maakt
    - Bewaking om policysnalevingsafwijkingen te traceren en policy in real-time bij te werken
    - Diepgaande, real-time zichtbaarheid van de gehele datacenterinfrastructuur
    - Langdurig gegevensbehoud voor historische analyse zonder verlies van gedetailleerdheid
    - Diepgaand forensisch onderzoek met behulp van krachtige zoekfilters en visuele query's
- **Handhavingslaag (Enforcement Laag):** softwaresensoren met volledige zichtbaarheid fungeren als het handhavingspunt voor het segmenteringspolicy dat door het platform wordt gegenereerd, waardoor segmentering van Applicaties mogelijk wordt. Met de mogelijkheden voor softwaresensoren en besturingssystemen biedt het Cisco Tetration platform stateful en consistente handhaving op implementaties in de publieke, private cloud en in het datacenter op locatie. Deze laag zorgt er tevens voor dat policy meebeweegt met de workload, zelfs wanneer een applicatiecomponent wordt gemigreerd van een bare-metal server naar een gevirtualiseerde omgeving. Bovendien garandeert de handhavingslaag schaalbaarheid met consistent policy dat wordt geïmplementeerd voor duizenden Applicaties met tienduizenden workloads.
- **Toegangslaag (Access Laag):** het Cisco Tetration platform maakt verwerking van deze gegevens mogelijk via een gebruiksvriendelijke en schaalbare web-GUI en REST-API's (Representational State Transfer). Bovendien biedt het platform op Apache Kafka gebaseerde push-meldingen waarop 'northbound' systemen zich kunnen abonneren voor berichten over afwijkingen van policysnaleving, abnormaliteiten in verkeersflows, enzovoort. Ervaren gebruikers hebben toegang tot de Hadoop data lake en kunnen aangepaste Applicaties schrijven in programmeertaal, zoals Python en Scala, die op het platform worden uitgevoerd met de krachtige beschikbare computingresources.
- **Andere gegevensresources:** naast de sensoren worden aanvullende configuratiegegevens verzameld afkomstig van bronnen van derden, zoals load balancers, DNS-serverrecords (Domain Name System) en de database voor IP-adresbeheer. Deze configuratiegegevens worden gebruikt als aanvulling op de informatie afkomstig van het analyseplatform. Dit platform ondersteunt tevens het gebruik van streaming telemetriegegevens afkomstig van andere bronnen voor analyses en correlatie.

Software-, hardware- en ERSPAN-sensoren

De software- en hardwaresensoren verzamelen drie typen telemetriegegevens:

- **Flow informatie:** dit betreft informatie over endpoints, protocollen en poorten van flows (wanneer de flow begon, hoe lang de flow actief was, enzovoort).
- **Variaties tussen pakketten:** dit betreft informatie over variaties tussen pakketten die binnen de flow zijn waargenomen. Voorbeelden hiervan zijn variaties in de TTL (Time To Live), IP/TCP-vlaggen en payloadlengte van het pakket.
- **Contextdetails:** contextinformatie die afkomstig is van buiten de pakketheader. In het geval van een softwaresensor omvat deze informatie details over het proces, waaronder welk proces de flow heeft gegenereerd, de proces-ID en de gebruiker die aan het proces is gekoppeld.

ERSPAN-sensoren verzamelen alleen flowinformatie en variaties tussen pakketten. ERSPAN-sensoren kunnen worden gebruikt in specifieke delen van het netwerk waar het gebruik van hardware- en softwaresensoren niet haalbaar is. Softwaresensoren worden nog steeds beschouwd als de voornaamste methode voor het verzamelen van telemetriegegevens, terwijl ERSPAN wordt gebruikt om ‘de gaten te vullen’.

Voor het Cisco Tetration platform moet u softwaresensoren gebruiken om de grootste hoeveelheid informatie te verzamelen en de hoogste nauwkeurigheid te behalen. Hardware- en ERSPAN-sensoren kunnen worden gebruikt om de gegevens uit te breiden die aan het platform worden geleverd.

Aanvullende kenmerken van sensoren

Softwaresensoren voor volledige zichtbaarheid ondersteunen een configureerbaar CPU-servicecontract (SLA). Als de SLA-waarde te laag wordt ingesteld, of als het verkeersvolume op de server te hoog is, zal het platform selectief de kans missen om elk pakket te inspecteren zodat aan de SLA wordt voldaan. Deze gemiste kansen worden vastgelegd en weergegeven in de gebruikersinterface van de beheerder, die optionele aanpassingen van de SLA kan doorvoeren.

Hardwaresensoren in de switch hebben een eindige capaciteit voor het vastleggen van flows en zijn onderhevig aan compromissen op het gebied van schaalbaarheid, metadata resolutie en kosten. Als het verkeersvolume te groot is, of als grote aantallen flows kortstondig zijn, kan deze capaciteit het aantal vastgelegde pakketten tijdens een bepaald interval (tussen 100 milliseconden en 4 seconden) beperken. In dat geval is filtering mogelijk en wordt dan ook aanbevolen. Klanten kunnen Applicaties en IP-adressen met hoge prioriteit opgeven waarvan Cisco Tetration telemetriegegevens moet verzamelen.

Functies en voordelen

Tabel 1 bevat een overzicht van de belangrijkste functies en voordelen van het Cisco Tetration platform.

Tabel 1. Belangrijkste functies en voordelen

Functie	Voordeel
Software- en hardwaresensoren	• Een combinatie van hardware- en softwaresensoren legt alle oost-west verkeersflows vast, waarbij geen blinde vlekken voorkomen. • Softwaresensoren zijn ontworpen voor gebruik binnen door de beheerder gedefinieerde computing-SLA's (de standaard is binnen 3% van CPU-benutting). • Zowel software- als hardwaresensoren bevinden zich buiten het gegevenspad en hebben geen invloed op de applicatieprestatie. • Sensorverkeer voegt minder dan 1% aan bandbreedteoverhead toe.
Uitgebreide telemetriegegevens	• Uitgebreide telemetriegegevens maken op applicatiegedrag gebaseerde analyses en bewaking van gedragsafwijkingen mogelijk. • Informatie is onafhankelijk van het feit of er sprake is van versleutelde of niet-versleutelde payload. • De verzameling van contextinformatie van flows en gegevens van pakketheaders maakt beter inzicht mogelijk.
Real-time asset-tagging	• Bedrijfscontext kan worden gekoppeld aan de telemetriegegevens in de vorm van tags. • Tags bieden de flexibiliteit om te zoeken naar inventaris en verkeer, en zelfs om policy te definiëren op basis van deze metadata gegevens. • Beheerders kunnen bedrijfspolicy koppelen aan policy inzake segmentering van Applicaties. • De 'northbound' REST-API wordt gebruikt om deze informatie up-to-date te houden.
Resourcetags van VMware vCenter en Amazon Web Services (AWS)	• Er kan worden geïntegreerd met VMware vCenter om kenmerken van virtuele machines te gebruiken in de vorm van tags in een datacenter op locatie. • Er kan worden geïntegreerd met AWS om AWS-resourcetags toe te wijzen binnen het Cisco Tetration-platform. • Op basis van deze bekende kenmerken kan policy worden gedefinieerd of worden gezocht naar inventaris en verkeer.
Softwaresensoren met beperkte zichtbaarheid	• De dekking van de sensoren wordt uitgebreid naar bepaalde oudere besturingssystemen. • Vereiste verbindingsinformatie wordt getraceerd voor applicatieinzicht van Cisco Tetration. • Met deze sensoren kan specifieker en nauwkeuriger policy voor Applicaties worden opgesteld.
ERSPAN-sensoren	• Rijke telemetriegegevens kunnen worden verzameld van delen van het netwerk waar software- en hardwaresensoren niet aanwezig zijn. • Gegevens kunnen worden verzameld vanuit meerdere invalshoeken voor betere correlatie en analyse.
Ondersteuning van Network Address Translation (NAT) en Port Address Translation (PAT) door sensoren	• Sensoren kunnen worden geïmplementeerd in omgevingen waar NAT of PAT wordt toegepast tussen servers en het Cisco Tetration platform. • NAT en PAT zijn geschikt voor implementaties met meerdere domeinen met overlappende IP-adressen.
Real-time zichtbaarheid van flows	• Tientallen miljarden flows worden doorzocht en binnen een seconde wordt bruikbaar inzicht geboden. • Problemen worden sneller opgelost en abnormaliteiten sneller gedetecteerd, zodat datacenterprocessen effectiever verlopen. • Afwijkingen in applicatiegedrag worden effectief geïdentificeerd en naleving van netwerkpolicy wordt beter gehandhaafd.
Ondersteuning voor schaalbaarheid van datacenters	• Telemetriegegevens van elk pakket in het datacenter kunnen zonder sampling worden verzameld. • Het platform kan miljoenen unieke flows per seconde verwerken. • Langdurig gegevensbehoud ondersteunt forensisch onderzoek en analyses.
Implementatie- en gebruiksgemak	• Het platform werkt als een applicatie met kant-en-klare ondersteuning voor cruciale operationele use cases. • Onbeheerde machine learning vermindert de noodzaak van menselijke interactie.
Platformbeveiliging	• Gebruikerstoegang wordt geregeld via op rollen gebaseerd toegangsbeheer (RBAC) voor zowel de GUI als REST-API. • Communicatie tussen verschillende platformcomponenten verloopt volledig beveiligd dankzij een ingebouwde firewall.
Zelfcontrole van platform	• Dankzij zelfcontrole is er geen uitgebreide interne expertise op het gebied van big data meer nodig om dit platform te gebruiken. • Deze controle strekt zich uit tot de sensoren om processen te vereenvoudigen. • Er kan een optie worden gebruikt om de functie Cisco® Call Home in te schakelen en bekende foutstatussen te melden.
Integratie van Microsoft Active Directory	• Er vindt gebruikersverificatie plaats via de externe Active Directory. • Dankzij deze integratie is het niet nodig aanmeldingsgegevens van gebruikers lokaal op het Cisco Tetration platform op te slaan.

Functie	Voordeel
Multitenancy-ondersteuning	• Dankzij de multitenant GUI en back-end kan het platform met meerdere groepen en organisaties worden gedeeld. • RBAC-mechanismen worden geïmplementeerd zodat alleen geautoriseerde gegevens worden weergegeven.
Open interface	• Open REST-API kan worden gebruikt voor 'northbound' systeemintegratie. • Het meldingsmechanisme kan worden gebruikt om op naleving gebaseerde gebeurtenissen eenvoudig te controleren en abnormaliteiten te detecteren. • Ontwikkelaars hebben toegang tot de Hadoop data lake en kunnen hun eigen Applicaties schrijven met Python of Scala.

Use cases voor datacenters

De kenmerken en functies van het Cisco Tetration platform ondersteunen cruciale use cases voor datacenterbeveiliging en processen. Tabel 2 bevat een overzicht van de use cases.

Tabel 2. Ondersteunde use cases

Use case	Beschrijving
Inzicht in Applicaties	U moet inzicht verkrijgen in de Applicatiecomponenten en hun afhankelijkheden binnen het datacenter om segmentering van Applicaties te kunnen implementeren en uit te voeren. Deze mogelijkheid kan ook worden gebruikt om Applicaties te migreren en strategieën voor noodherstel te plannen. Het Cisco Tetration-platform gebruikt real-time gegevens over de communicatie tussen Applicatiecomponenten en machine learning en algoritmen voor gedragsanalyse om applicatiegroepen, hun communicatiepatronen en serviceafhankelijkheden te identificeren. Dankzij inzicht in Applicaties kunnen gebruikers en beheerders: • Endpointhosts en applicatiesclusters groeperen om applicatiesweergaven te maken, uitgebreid met kenmerken van VMware vCenter- en AWS-tags • Nauwkeurig inzicht verkrijgen in de relatie tussen klanten en providers op basis van communicatiepatronen • Inzicht verkrijgen in de serviceafhankelijkheden voor elke component Organisaties kunnen ook informatie afkomstig van apparaten van derden, zoals taakverdelers en de database voor IP-adresbeheer, op een slimme manier integreren om een end-to-end beeld van de applicatiescommunicatie te krijgen.
Geautomatiseerde aanbeveling voor whitelistpolicy	U moet automatisch een betrouwbaar whitelistpolicy kunnen genereren en dat vrijwel in real-time ka bijwerken naarmate Applicaties evolueren. Hierdoor wordt de beveiliging verbeterd en wordt consistente handhaving van de policy in verschillende omgevingen toegepast, inclusief workloads die in de cloud worden uitgevoerd, en kunnen abnormaliteiten eenvoudiger worden geïdentificeerd. Via het Cisco Tetration-platform kunt u automatisch zeer specifiek whitelistpolicy genereren op basis van de daadwerkelijke communicatie tussen endpoints. Het platform prioritiseert een ander vooraf gedefinieerde policy van entiteiten op hoger niveau, zoals InfoSec of Coprorate policy. U kunt policy specificeren door gebruik te maken van informatie op netwerkniveau en van abstracte informatie, zoals inventaristags. Beveiligingspolicy kan bijvoorbeeld aangeven dat productieservers niet mogen communiceren met niet-productieservers. Deze policy kan dan dankzij Cisco Tetration-policy handhaving worden afgedwongen (segmentering van Applicaties). Als u ervoor kiest de policy te handhaven met andere technologieën, kan de policy worden geëxporteerd in programmeerbare indelingen (JSON, XML en YAML) via de webgebaseerde GUI of REST-API.
Segmentering van Applicaties	Via de Cisco Tetration-functie voor segmentering van Applicaties kunt u een beveiligd zero-trust model implementeren met een whitelistpolicy voor Applicaties. Deze policy wordt vervolgens genormaliseerd op basis van prioriteit en hiërarchie voordat het wordt afgedwongen. Wanneer policy handhaving is ingeschakeld voor een applicatie, wordt de policy afgedwongen via softwaresensoren die gebruikmaken van native besturingssysteemfuncties (zoals ipsets en iptables op Linux-servers en de geavanceerde firewall op Microsoft Windows-servers). Op die manier wordt geschaalde stateful en consistente segmentering binnen de heterogene infrastructuur mogelijk (op locatie en in publieke en private clouds). In een gevirtualiseerde omgeving beweegt de segmenteringspolicy bovendien mee met de workload, zodat de applicatiesmobiliteit toeneemt en u zich niet bezig hoeft te houden met infrastructuurspecifiek segmenteringspolicy. Wanneer applicatiesafhankelijkheden en communicatiepatronen veranderen, zorgt het platform ervoor dat policy automatisch wordt bijgewerkt.
Impactanalyse en naleving van policy	Via het Cisco Tetration-platform kunt u de whitelistpolicy simuleren en de impact ervan beoordelen voordat het in het productienetwerk wordt toegepast. Deze impactanalyse kan worden uitgevoerd met historische gegevens of real-time gegevens zonder dat dit het productieverkeer beïnvloedt. Hierdoor kunt u nagaan wat de impact van de whitelistpolicy zou zijn op de daadwerkelijke verkeersflows in het netwerk. U kunt ook direct zien welke flows worden geclassificeerd als compatibel, niet compatibel of verloren gegaan. Nadat de policy is afgedwongen, controleert het platform op doorlopende naleving. U kunt meldingen ontvangen over niet-naleving, zodat u proactief elk probleem kunt aanpakken. U kunt met één klik de policy aanpassen als sprake is van een daadwerkelijke policysafwijking.

Use case	Beschrijving
Inventaris van serverprocessen en proceshashes	Dankzij softwaresensoren kan nu via het Cisco Tetration-platform de volledige procesinventaris worden verzameld in combinatie met informatie over proceshashes voor de applicatiesservers. Gebruikers kunnen voor elke server zoeken op basis van de procesgegevens of de hashinformatie. Hierdoor kan via het platform meer informatie worden verzameld en gebruikt dan alleen informatie over netwerkverkeer. Informatie over proceshashes biedt ook aanvullende beveiligingsmogelijkheden.
Nabijheidsgrafieken voor Applicaties	Met de nabijheidsgrafieken voor Applicaties kunnen gebruikers zoeken naar een specifieke applicatiesserver en een tweehopsbeeld krijgen van de communicatie van die server met andere servers binnen het datacenter. Gebruikers kunnen inzoomen op verkeers- en communicatiepatronen tussen een of meer van deze servers. Zij kunnen ook een query uitvoeren om na te gaan of er sprake is van een communicatiepad tussen twee servers en om het aantal logische serverhops tussen die twee applicatiesservers te bepalen. Vooraf geconfigureerde en door de gebruiker gedefinieerde waarschuwingen kunnen worden gegenereerd op basis van bepaalde gedragsveranderingen.
Visualisatie van virtuele desktopinfrastructuur (VDI)	Wanneer VDI wordt gebruikt in het datacenter, kan het Cisco Tetration-platform zichtbaarheid bieden van de verkeers- en applicatiesworkspaces die door deze VDI-instanties worden bezocht. Deze zichtbaarheid wordt verkregen door de installatie van softwaresensoren in de virtuele VDI-machines. Op deze manier kan volledige zichtbaarheid worden verkregen van de communicatie die extern en binnen het datacenter plaatsvindt voor de virtuele VDI-machines.
Visualisatie en forensisch onderzoek	Het Cisco Tetration-platform kan uw zoekmachine zijn voor alle flows in het datacenter. U kunt met de krachtige zoekmogelijkheid die door het platform wordt geboden tientallen miljarden flowrecords doorzoeken in minder dan een seconde. Bovendien kunnen zoekacties met complexe filterexpressies en visuele query's worden uitgevoerd om details te vinden die cruciaal zijn voor datacenteractiviteiten. Dankzij deze zoekmogelijkheid kunt u niet alleen bekende problemen detecteren, maar ook abnormaal gedrag dat anders onopgemerkt zou blijven.

Cisco Tetration-Applicaties

Het Cisco Tetration-platform biedt toegang tot de Hadoop data lake in de cluster via Cisco Tetration-Applicaties. Ontwikkelaars, programmeurs en datawetenschappers hebben met Cisco Tetration-Applicaties toegang tot de informatie in de data lake en kunnen hun eigen Applicaties schrijven met Python, Scala of Spark SQL. Deze Applicaties kunnen worden uitgevoerd als microservices op het platform zelf en kunnen worden geactiveerd met behulp van diverse mechanismen:

- Een applicatie kan als een eenmalige taak worden uitgevoerd.
- Applicaties kunnen worden ingesteld om periodiek te worden uitgevoerd (per uur, dag, week, enzovoort).
- Applicaties kunnen worden geactiveerd op basis van gegevensafhankelijkheden.

Ontwikkelaars kunnen op JSON-gebaseerde streaming telemetriegegevens van andere gegevensbronnen gebruiken en deze vergelijken met de flowinformatie in het data lake. Applicaties kunnen zo nodig externe waarschuwingen genereren via de Kafka-gegevensbus of de verwerkte gegevens weergeven in het dashboard van de webinterface van Cisco Tetration. Er kunnen streaming telemetriegegevens afkomstig van maximaal 10 verschillende gegevensbronnen tegelijk worden gebruikt.

Tabel 3 bevat een overzicht van de specificaties van de Cisco Tetration-Applicaties.

Tabel 3. Specificaties van Cisco Tetration-Applicaties

Gegevenspunten van Cisco Tetration-Applicaties	Specificatie
Maximum aantal gebruikers applicaties dat gelijktijdig op het platform kan worden uitgevoerd	14
Maximum aantal Applicaties dat kan worden verwerkt	100
Gegevenslimiet bij het uploaden van externe gegevens voor gebruik in een applicatie	5 terabyte (TB), te delen door alle Applicaties
Containerspecificatie voor elke applicatie (bovengrens)	Virtuele CPU (vCPU) met 3 cores Ongeveer 6 GB RAM
Python-versie	Release 3.0
Scala-versie	Release 2.11.0
Spark SQL	Release 1.6.2 (niet volledig ANSI-compatibel)

Licentieverlening

Cisco Tetration Analytics-software wordt gelicentieerd op basis van het aantal workloads (virtuele machines en bare-metal servers) waarop het platform analyses uitvoert. Telemetriegegevens kunnen worden verzameld met software-, hardware- of ERSPAN-sensoren, of een combinatie hiervan. Er zijn twee licenties beschikbaar:

- **Base-licentie:** met deze licentie kunnen de volgende gegevens worden verzameld van uitgebreide telemetriegegevens, inzicht in Applicaties, forensisch onderzoek, policysaanbeveling en policyssimulatie worden gebruikt.
- **Add-on-licentie voor policyshandhaving en segmentering van Applicaties:** de licentie voor policyshandhaving wordt afzonderlijk van de basis sensor gelicentieerd. Klanten moeten de licentie voor policyshandhaving kopen als zij geautomatiseerde handhaving via het platform willen toepassen.

Als een klant meerdere Cisco Tetration-clusters heeft, kunnen softwarelicenties op deze clusters worden samengevoegd.

Licentievoorwaarden

Cisco Tetration-software is niet alleen onderhevig aan de bepalingen in de Cisco-gebruiksrechtovereenkomst (EULA, zie https://www.cisco.com/go/eula), maar ook aan de bepalingen in de aanvullende Cisco-gebruiksrechtovereenkomst (SEULA, zie https://www.cisco.com/c/dam/en_us/about/doing_business/legal/docs/cisco-tetration.pdf).

Implementatiemodellen en -schaal

Cisco Tetration Analytics biedt een applicatieachtige ervaring. Het programma biedt flexibele implementatieopties op basis van de grootte van het datacenter en of implementatie op fysieke hardware of in een openbare cloud gewenst is door de organisatie. Er zijn momenteel drie implementatieopties beschikbaar.

Cisco Tetration-L platform (grote appliance)

Deze implementatieoptie bestaat uit 36 servers en 3 Cisco Nexus 9300-platformservers. Deze optie is geschikt voor datacenters die meer dan 5.000 servers hosten (virtuele machine of bare-metal).

Tabel 4 bevat een overzicht van de geverifieerde en ondersteunde schaal. In tabel 5 worden de voedings- en koelingsvereisten van het Cisco Tetration-platform aangegeven.

Tabel 4. Schaal van standaardplatform van Cisco Tetration Analytics

Platformkenmerken	Specificatie
Aantal gelijktijdige servers (virtuele machine of bare-metal) waarvan telemetriegegevens kunnen worden geanalyseerd	Maximaal 25.000

Aantal flowgebeurtenissen dat per seconde kan worden verwerkt	2 miljoen per seconde

Tabel 5. Voedings- en koelingsspecificaties voor LLF-optie

Platformvereisten	Specificatie
Piekvermogen voor Cisco Tetration Analytics (enkel rack, 39 RU)*	22,5 kW
Maximale koelingsvereisten voor Cisco Tetration Analytics (enkel rack, 39 RU)*	14,6 kW
Totale gewicht voor Cisco Tetration Analytics (enkel rack, 39 RU)	800 kg (1800 lb)
Power Distribution Unit (PDU) en voeding (enkel rack, 39 RU)	4 x 3-fasige PDU's (flow- en spanningswaarden kunnen per geografisch gebied verschillen)
Piekvermogen voor Cisco Tetration Analytics (dubbel rack, 39 RU)	11,25 kW per rack (22,5 kW totaal)
Maximale koelingsvereiste voor Cisco Tetration Analytics (dubbel rack, 39 RU)	7,3 kW per rack
Totale gewicht voor Cisco Tetration Analytics (dubbel rack, 39 RU)	400 kg (900 lb) per rack
Power Distribution Unit (PDU) en voeding (dubbel rack, 39 RU)	4 x eenfasige PDU's per rack (flow- en spanningswaarden kunnen per geografisch gebied verschillen)

*Bij configuratie met enkel rack worden 8 van de 36 servers afzonderlijk verzonden gezien de gewichtsvereisten. Deze moeten op locatie in het rack worden geplaatst en worden bekabeld.

Cisco Tetration-M platform (medium appliance)

De implementatieoptie Cisco Tetration-M bestaat uit 6 servers en 2 Cisco Nexus 9300-platformswitches. Deze optie is geschikt voor datacenters met minder dan 5.000 servers (virtuele machine of bare-metal).

Tabel 6 bevat een overzicht van de geverifieerde en ondersteunde schaal. In tabel 7 worden de voedings- en koelingsvereisten van het Cisco Tetration-M-platform (de SFF-optie) aangegeven.

Tabel 6. Schaal van Cisco Tetration-M-platform

Platformkenmerken	Specificatie
Aantal gelijktijdige servers (virtuele machine of bare-metal) waarvan telemetriegegevens kunnen worden geanalyseerd	Maximaal 5.000
Aantal flowgebeurtenissen dat per seconde kan worden verwerkt	500.000 per seconde

Tabel 7. Voedings- en koelingsspecificaties voor Cisco Tetration-M

Platformvereisten	Specificatie
Piekvermogen voor Cisco Tetration-M (8 RU)	5,5 kW
Maximale koelingsvereiste voor Cisco Tetration-M (8 RU)	4,0 kW

Cisco Tetration Cloud platform (optie voor openbare cloud in AWS)

Met de openbare cloudimplementatie voor AWS kan de Cisco Tetration-software in een AWS-instantie worden uitgevoerd. U moet de benodigde AWS-instanties rechtstreeks bij AWS aanschaffen om de Cisco Tetration-software te kunnen uitvoeren. Deze optie is geschikt voor datacenters met minder dan 1000 servers (virtuele machine of bare-metal). Als softwaresensoren zijn geïmplementeerd op workloads in een private cloud of op locatie, is AWS Direct Connect vereist om verbinding te kunnen maken met het Cisco Tetration Cloud-platform. Tabel 8 bevat een overzicht van de vereisten ten aanzien van het type AWS-instantie, Amazon Elastic Block Storage (EBS) en Amazon Elastic IP-adres (EIP) voor het gebruik van Cisco Tetration Cloud in AWS. In tabel 9 wordt de schaal van het platform aangegeven.

Tabel 8. Maximale AWS-instantievereisten voor Cisco Tetration Cloud

AWS-instantietype	Specificatie
t2.medium	6 instanties
m4.large	15 instanties
m4.2xlarge	2 instanties
m4.xlarge	3 instanties
r4.large	13 instanties
r4.2xlarge	23 instanties
r4.xlarge	4 instanties
m4.4xlarge	8 instanties
Amazon EBS: solid-state drive voor algemeen gebruik (SSD; gp2)	65 TB
Amazon EIP	50 adressen

Tabel 9. Schaal van Cisco Tetration Cloud-platform

Platformkenmerken	Specificatie
Aantal gelijktijdige servers (virtuele machine of bare-metal) waarvan telemetriegegevens kunnen worden geanalyseerd	Maximaal 1000
Aantal flowgebeurtenissen dat per seconde kan worden verwerkt	200.000 per seconde

Ondersteunde platforms en compatibiliteit

In tabellen 10, 11, 12 en 13 is informatie opgenomen over software- en hardwareondersteuning en compatibiliteit voor het Cisco Tetration-platform.

Tabel 10. Ondersteunde besturingssystemen voor sensoren met volledige zichtbaarheid

Servermodus	Besturingssysteem	Distributie en release
Virtuele machines en bare-metal servers	Linux	• Red Hat Enterprise Linux, release 5.0 en hoger • Red Hat Enterprise Linux, release 6.0 en hoger • Red Hat Enterprise Linux, release 7.1, 7.2 en 7.3 • CentOS, release 5.0 en hoger • CentOS, release 6.0 en hoger • CentOS, release 7.1, 7.2 en 7.3 • Oracle Linux, release 6.0 en hoger • Oracle Linux, release 7.1, 7.2 en 7.3 • SUSE Linux, release 11.2, 11.3 en 11.4 • SUSE Linux, release 12.0, 12.1 en 12.2 • Ubuntu, release 12.04, 14.04, 14.10 en 16.04
	Microsoft Windows Server (servercore en volledige desktop)	• Microsoft Windows Server 2008 Standard, Enterprise, Essentials en Datacenter Editions • Microsoft Windows Server 2008 R2 Standard, Enterprise, Essentials en Datacenter Editions • Microsoft Windows Server 2012 Standard, Foundation, Essentials en Datacenter Editions • Microsoft Windows Server 2012 R2 Standard, Foundation, Essentials en Datacenter Editions • Microsoft Windows Server 2016 Standard, Essentials en Datacenter Editions
Virtuele machines als VDI-desktops	Microsoft Windows Desktop (alleen use case VDI)	• Microsoft Windows 7 Desktop • Microsoft Windows 8 Desktop • Microsoft Windows 10 Desktop

Tabel 11. Ondersteunde besturingssystemen voor handhaving

Servermodus	Besturingssysteem	Distributie en release
Virtuele machines en bare-metal servers	Linux (64-bits)	• Red Hat Enterprise Linux, release 6.0 en hoger • Red Hat Enterprise Linux, release 7.1, 7.2 en 7.3 • CentOS, release 6.0 en hoger • CentOS, release 7.1, 7.2 en 7.3 • Oracle Linux, release 6.0 en hoger • Oracle Linux, release 7.1, 7.2 en 7.3 • Ubuntu, release 14.04, 14.10 en 16.04 • SUSE Linux, release 11.2, 11.3 en 11.4 • SUSE Linux, release 12.0, 12.1 en 12.2
	Microsoft Windows Server (servercore en volledige desktop)	• Microsoft Windows Server 2008 Standard, Datacenter, Enterprise en Essentials • Microsoft Windows Server 2008 R2 Standard, Datacenter, Enterprise en Essentials • Microsoft Windows Server 2012 Standard, Datacenter, Foundation en Essentials • Microsoft Windows Server 2012 R2 Datacenter, Foundation en Essentials • Microsoft Windows Server 2016 Standard, Essentials en Datacenter Editions

Tabel 12. Ondersteunde besturingssystemen voor universele softwaresensoren

Servermodus	Besturingssysteem	Distributie en release
Virtuele machines en bare-metal servers	Linux	• Red Hat Enterprise Linux, release 4.0 (32-bits en 64-bits) • CentOS, release 4.0 (32-bits en 64-bits) • Red Hat Enterprise Linux, release 5.0 (32-bits) • CentOS, release 5.0 (32-bits)
	AIX	• AIX, release 5.3, 6.1, 7.1 en 7.2
	Solaris	• Solaris, release 11.0 (64-bits) op x86-architectuur
	Microsoft Windows Server	• Microsoft Windows Server (64-bits)

Tabel 13. Ondersteunde hardwaresensoren

Productlijn	Platform	Softwarerelease
Cisco Nexus 9300-platformswitches (NX-OS-modus)*	Cisco Nexus 92160YC-X	Cisco NX-OS, release 7.0(3)I5(2) en hoger
	Cisco Nexus 93180YC-EX en 93108TC-EX	Cisco NX-OS, release 7.0(3)I5(2) en hoger
	Cisco Nexus 93180YC-FX en 93108TC-FX	Cisco NX-OS, release 7.0(3)I7(2) en hoger
Cisco Nexus 9300-platformswitches (ACI-modus)*	Cisco Nexus 93180YC-EX en 93108TC-EX	Cisco Application Centric Infrastructure (Cisco ACI™), release 2.2(2e) en hoger
	Cisco Nexus 93180YC-FX en 93108TC-FX	Cisco Application Centric Infrastructure (Cisco ACI™), release 2.3(1f) en hoger

* Vereist afzonderlijke Cisco Nexus 9300-telemetrielicentie

Bestelinformatie

Tabel 14 bevat een overzicht van artikelnummers van hardware- en softwarebundels voor Cisco Tetration Analytics (LFF-optie).

Tabel 14. Bundels van hardware abonnementssoftware voor Cisco Tetration Analytics (LFF-optie)

Artikelnummer van bundel	Artikelnummers opgenomen in bundel	Beschrijving
C1-TETRATION		Artikelnummer voor Cisco Tetration Analytics-bundel die hardware, softwareabonnementslicentie en AS-Fixed-service (Cisco Advanced Services–Fixed) voor implementatie omvat. AS-Fixed wordt zonder extra kosten meegeleverd.
	TA-CL-G1-39-K9	Cisco Tetration Analytics-hardwareplatform met 36 servers en 3 switches dat de verwerking van Cisco Tetration Analytics-telemetriegegevens afkomstig van maximaal 25.000 servers (virtuele machine of bare-metal) ondersteunt.
	C1-TA-SW-K9	Artikelnummer van bundel voor Cisco Tetration Analytics-softwareabonnementslicentie. Zie tabel 16 voor details.
	ASF-DCV1-TA-QS-M	AS-Fixed-artikelnummer voor Cisco Tetration Analytics-implementatieservices.

Tabel 15 bevat een overzicht van artikelnummers van hardware- en softwarebundels voor Cisco Tetration-M (SFF-optie, 8 RU).

Tabel 15. Bundels van hardware abonnementssoftware voor Cisco Tetration-M (SFF-optie)

Artikelnummer van bundel	Artikelnummers opgenomen in bundel	Beschrijving
C1-TETRATION-M		Artikelnummer voor Cisco Tetration Analytics-bundel die hardware, softwareabonnementslicentie en AS-Fixed-service (Cisco Advanced Services–Fixed) voor implementatie omvat. AS-Fixed wordt zonder extra kosten meegeleverd.
	TA-CL-G1-SFF8-K9	Cisco Tetration Analytics-hardwareplatform met 6 servers en 2 switches, vereist voor Cisco Tetration-M.
	C1-TA-SW-K9	Artikelnummer van bundel voor Cisco Tetration Analytics-softwareabonnementslicentie.
	ASF-DCV1-TA-QS-M	AS-Fixed-artikelnummer voor Cisco Tetration Analytics-implementatieservices.

Tabel 16 bevat een overzicht van artikelnummers van bundels van abonnementssoftware voor Cisco Tetration Analytics (LFF-optie) en Cisco Tetration-M (SFF-optie).

Tabel 16. Licentie voor abonnementssoftware voor Cisco Tetration Analytics (LFF-optie) en Cisco Tetration-M (SFF-optie)

Artikelnummer van bundel	Artikelnummers opgenomen in bundel	Beschrijving
C1-TA-SW-K9		Artikelnummer van bundel voor Cisco Tetration Analytics-softwareabonnementslicentie.
	C1-TA-BASE-1K-K9	Licentie voor Cisco Tetration Analytics-abonnementssoftware in veelvouden van 1000 servers (virtuele machine of bare-metal). Kies een hoeveelheid tussen 1 en 25. Bij een aantal van 5 wordt bijvoorbeeld de licentieprijs voor maximaal 5000 softwaresensorinstanties getoond.
	C1-TA-ENF-1K-K9	Add-on-licentie voor handhaving voor Cisco Tetration Analytics-abonnementssoftware in veelvouden van 1000 servers (virtuele machine of bare-metal). Kies een hoeveelheid tussen 1 en 25. Bij een aantal van 5 wordt bijvoorbeeld de licentieprijs voor maximaal 5000 softwaresensorinstanties getoond.

Houd ook rekening met de volgende aanvullende informatie over het artikelnummer van de softwareabonnementslicentie:

- U kunt kiezen voor een abonnementsduur van 1, 3 of 5 jaar.
- De abonnementsprijs omvat softwareondersteuning.
- Het abonnementsniveau wordt automatisch geselecteerd op basis van de ingevoerde hoeveelheid.

- Handhaving is een add-on-licentie en kan niet worden besteld zonder de base-softwarelicentie.
- U kunt kiezen voor jaarlijkse facturering of vooruitbetaling voor de gehele abonnementsduur.
- U kunt meer licenties voor softwaresensorinstanties toevoegen.
- Deze softwareabonnementslicentie kan worden gebruikt met zowel Cisco Tetration-hardwareclusters als de Cisco Tetration Cloud-optie.

Licentievoorwaarden

Cisco Tetration Analytics-software is niet alleen onderhevig aan de bepalingen in de EULA van Cisco (zie https://www.cisco.com/go/eula), maar ook aan de bepalingen in de SEULA van Cisco (zie https://www.cisco.com/c/dam/en_us/about/doing_business/legal/docs/cisco-tetration.pdf).

Tabel 17 en 18 bevatten een overzicht van artikelnummers van bundels voor Cisco Tetration Cloud.

Tabel 17. Softwarebundel voor Cisco Tetration Cloud

Artikelnummer van bundel	Artikelnummers opgenomen in bundel	Beschrijving
C1-TETRATION-V		Artikelnummer van bundel voor Cisco Tetration Analytics die de softwareabonnementslicentie voor de virtuele vormfactor omvat.
	C1-TA-V-SW-K9	Artikelnummer van bundel voor Cisco Tetration Analytics-softwareabonnementslicentie.
	ASF-DCV1-TA-QS-M	Optioneel AS-Fixed-artikelnummer voor Cisco Tetration Analytics-implementatieservices.

Tabel 18. Licentie voor abonnementssoftware voor Cisco Tetration Cloud

Artikelnummer van bundel	Artikelnummers opgenomen in bundel	Beschrijving
C1-TA-V-SW-K9		Artikelnummer van bundel voor Cisco Tetration Analytics-softwareabonnementslicentie; alleen van applicatie op Cisco Tetration Cloud.
	C1-TA-BASE100-K9	Licentie voor Cisco Tetration Analytics-abonnementssoftware in veelvouden van 100 servers (virtuele machine of bare-metal). Kies een aantal tussen 1 en 10. Bij een aantal van 5 wordt bijvoorbeeld de licentieprijs voor maximaal 500 softwaresensorinstanties getoond.
	C1-TA-ENF100-K9	Add-on-licentie voor handhaving voor Cisco Tetration Analytics-abonnementssoftware in veelvouden van 100 servers (virtuele machine of bare-metal). Kies een aantal tussen 1 en 10. Bij een aantal van 5 wordt bijvoorbeeld de licentieprijs voor maximaal 500 softwaresensorinstanties getoond.

Houd ook rekening met de volgende aanvullende informatie over het artikelnummer van de softwareabonnementslicentie:

- U kunt kiezen voor een abonnementsduur van 1, 3 of 5 jaar.
- De abonnementsprijs omvat softwareondersteuning.
- Het abonnementsniveau wordt automatisch geselecteerd op basis van de ingevoerde hoeveelheid.
- Handhaving is een add-on-licentie en kan niet worden besteld zonder de base-softwarelicentie.
- U kunt kiezen voor jaarlijkse facturering of vooruitbetaling voor de gehele abonnementsduur.
- U kunt meer licenties voor softwaresensorinstanties toevoegen.
- Deze softwareabonnementslicentie kan alleen worden gebruikt met een Cisco Tetration Cloud-implementatie.

Licentievoorwaarden

Uw licentie voor Cisco Tetration Cloud-software omvat niet de openbare cloudinstanties (zoals AWS) die nodig zijn om de software te kunnen uitvoeren. U moet de benodigde openbare cloudinstanties rechtstreeks bij de openbare cloudprovider aanschaffen (zoals AWS). Niet alle openbare cloudomgevingen zijn gecertificeerd voor gebruik met Cisco Tetration Cloud. Raadpleeg de Cisco Tetration-documentatie voor informatie over de vereisten die van applicatie zijn op ondersteunde openbare cloudomgevingen. De prestaties van Cisco Tetration Cloud kunnen variëren omdat Cisco de serviceniveaus van de openbare cloud (zoals AWS) niet kan garanderen.

Cisco Tetration Analytics-software is niet alleen onderhevig aan de bepalingen van de EULA van Cisco (zie https://www.cisco.com/go/eula), maar ook aan de bepalingen van de SEULA van Cisco (zie https://www.cisco.com/c/dam/en_us/about/doing_business/legal/docs/cisco-tetration.pdf).

Zet de expertise van Cisco in om uw succes te versnellen

Cisco biedt professionele en ondersteuningsservices zodat organisaties optimaal kunnen profiteren van uw Cisco Tetration-platform. Experts van Cisco Services ondersteunen u bij het integreren van het platform in uw productiedatacenters, het definiëren van use cases die relevant zijn voor uw zakelijke doelstellingen, het afstemmen van machine learning en het valideren van policysregels en naleving om de applicaties- en operationele prestaties te verbeteren. Cisco Solution Support voor Cisco Tetration Analytics biedt ondersteuning op hardware-, software- en oplossingsniveau. Een jaarcontract dekt alle ondersteuningsbehoeften.

Dankzij de expertise van Cisco Tetration Analytics-services bent u verzekerd van een kortere terugverdientijd, uitgebreide adoptie in uw omgeving, geoptimaliseerde policysregels en applicatieprestatie en oplossingsbrede ondersteuning.

Cisco Capital-financiering om u te helpen uw doelen te bereiken

Met financiering van Cisco Capital® kunt u de technologie aanschaffen die u nodig hebt om uw doelen te bereiken en concurrerend te blijven. U kunt besparen op kapitaaluitgaven (CapEx), uw groei versnellen en uw investeringen en ROI optimaliseren. Financiering van Cisco Capital biedt u flexibiliteit bij het aanschaffen van hardware, software, services en aanvullende apparatuur van derden. En dat tegen slechts één voorspelbaar bedrag. Financiering van Cisco Capital is beschikbaar in meer dan 100 landen. Meer informatie.

Meer informatie

Ga voor meer informatie over het Cisco Tetration-platform naar https://www.cisco.com/go/tetration of neem contact op met uw plaatselijke Cisco-accountvertegenwoordiger.

Hoofdkantoor Amerika
Cisco Systems. Inc.
San Jose. CA

Hoofdkantoor Zuidoost-Azië
Cisco Systems (USA) Pte, Ltd.
Singapore

Hoofdkantoor Europa
Cisco Systems International BV Amsterdam,
Nederland

Cisco beschikt wereldwijd over meer dan 200 kantoren. Adressen, telefoonnummers en faxnummers vindt u op de Cisco-website op **www.cisco.com/go/offices**.

Gedrukt in de VS C78-737256-08 10/17