Een volledig en nauwkeurig overzicht en controle over het IT-landschap

- Ons IT-landschap wordt steeds complexer en uitgebreider. Veel bedrijven beschikken over een berg tools om die infrastructuur te beheren, maar vaak zijn die oplossingen gewoon niet nauwkeurig genoeg en bovendien onbetrouwbaar. Ze integreren niet, zijn traag en gebaseerd op een verouderde architectuur.
- De risico's zijn niet min: securityproblemen, downtime en nodeloos hoge kosten. Zowel voor bedrijven als overheidsdiensten is het belangrijker dan ooit om een holistisch beeld van het IT-landschap te krijgen.
- En dat is precies hoe Tanium voor klanten in de hele wereld het verschil maakt. Dankzij een geïntegreerd platform met één enkele agent voor management en security, en toegang tot meer dan honderd use cases.
- De unieke architectuur maakt het mogelijk om bijna in real-time inzicht en overzicht in het IT-landschap te generen met maar liefst 99,9% betrouwbaarheid. Op die manier kan sneller worden gehandeld en verbetert ook de weerbaarheid van een organisatie.

10 problemen die met Tanium tot het verleden behoren:

Wat Tanium dan precies doet? We draaien de vraag even om en overlopen welke bekende IT-problemen dankzij Tanium zullen verdwijnen:

1. **Een onvolledige en verouderde CMDB**
   Tools zijn zo gevarieerd dat de informatie in de CMDB niet klopt of niet up-to-date is. En dat creëert risico's: wat je niet ziet, kan je niet beschermen.
2. **Software incompliance**
   Door een gebrek aan overzicht draaien er licenties waarover de organisatie helemaal niet beschikt. De kosten hiervoor kunnen bij een audit erg hoog oplopen.
3. **Ongeïdentificeerde kwetsbaarheden**
   Aangezien er geen volledig beeld van alle eindpunten en applicaties bestaat, worden sommige kwetsbaarheden niet geïdentificeerd.
4. **Onvolledig patch management**
   Patches moeten naar alle kwetsbare eindpunten gestuurd worden. Toch zou 80% van de IT-managers volgens een rondvraag van Tanium merken dat niet alle toestellen deze updates ontvangen.
5. **Het lekken van data**
   Belangrijke en gevoelige gegevens lekken, bijvoorbeeld wanneer er software gebruikt wordt die niet is toegestaan.
6. **Blinde vlekken in het IT-landschap**
   Veel organisaties beschikken over veel meer eindpunten dan ze denken. Die blinde vlekken in de zichtbaarheid van het IT-landschap maken hen erg kwetsbaar.
7. **Geen controle over admin accounts**
   Omdat niet duidelijk is welke eindpunten er in de organisatie aanwezig zijn, is het ook niet mogelijk om de controle over de admin accounts te bewaren.
8. **Verstoringen door Change Management**
   Zonder een CMDB die up-to-date is, weet niemand welke services op welke server draaien. Daardoor kunnen diensten plots lange tijd niet beschikbaar zijn.
9. **Geen zicht op de applicatieketen**
   In een keten zijn verschillende applicaties vaak van elkaar afhankelijk. Daarom is het belangrijk om snel te zien met welke componenten een server communiceert.
10. **Onduidelijkheden over tools**
    Bij gebrek aan een overzicht van de gebruikte tools, is het niet mogelijk om snel de juiste tool te raadplegen wanneer een vraag dringend moet worden beantwoord.

> “Nu medewerkers steeds vaker thuiswerken, hebben we meer dan ooit behoefte aan een oplossing die ons volledige IT-landschap in kaart brengt. Thuiswerken wordt het nieuwe normaal, dus is het belangrijk dat we klaar zijn voor de toekomst en de securityrisico’s beperken.”

Lourens Visser
CIO Rijk

Ook governance-uitdagingen lossen we op

Een vals gevoel van veiligheid bestaat niet voor Tanium: dankzij Tanium weten organisaties dat alle taken daadwerkelijk uitgevoerd zijn. Ze zijn er zeker van dat hun tools alle patches of updates wel degelijk geïnstalleerd hebben en ook geactiveerd. Dat is handig bij overheidsdiensten die het IT-beheer decentraal doorvoeren of werken met sourcingpartners. Tanium rapporteert op objectieve basis over de kwaliteit van hun dienstverlening. Gedistribueerde discovery zorgt bovendien voor 100% dekking. De due diligence van Tanium verhoogt de kwaliteit van de dienstverlening en verbetert de efficiëntie.

Dankzij de Unified Management en Security-oplossing van Tanium beschikken klanten over een holistisch beeld van hun IT-landschap. Dat maakt het mogelijk om kwetsbaarheden in slechts enkele uren te verhelpen, terwijl dat anders dagen tot zelfs weken kan duren. Bovendien wordt er dankzij Tanium niet alleen tijd, maar ook heel wat geld bespaard.

Hoe Tanium helpt om kosten te besparen

Wat je niet ziet, kan je onmogelijk beschermen. Op basis van ROI-modellen verwacht Tanium dat ook overheidsinstanties de komende vijf jaar, met dank aan een betere zichtbaarheid en controle van het ITlandschap, zo’n vier tot zes miljoen euro zouden kunnen besparen. De volgende factoren spelen hierbij een cruciale rol:

Beter beheer van bestaande hardware en software

- Ongebruikte assets ontdekken, opeisen of een nieuw doel geven
- Minder uitgaven aan serviceproviders
- Kosten vermijden door het optimaliseren van applicaties op endpoints

Minder operationele onderbrekingen en securityproblemen

- Systemen worden minder gevoelig voor cyberdreigingen
- Minder kosten door securityproblemen, het lekken van data en bijhorende boetes en sancties
- Dankzij een beter overzicht kunnen datacenters met meer vertrouwen naar de publieke cloud migreren

Vervangen en verminderen van het aantal tools in het IT-landschap

- Patches kunnen veel sneller en doeltreffender worden uitgerold
- Vermijden van gefragmenteerde aanpak en dubbele licenties

Processen en de rol van mensen optimaliseren

- Meer tijd om mensen en middelen in te zetten waar ze echt waarde kunnen genereren

Nog meer voordelen van Tanium

Het platform van Tanium helpt om iedere organisatie aan te passen aan de hoge eisen van deze tijd. Ook op de volgende manieren profiteren klanten van Tanium:

1. Tanium is zeer geschikt voor het beheren van werkplekken die niet bekend zijn in het domein of netwerk van een organisatie Denk maar aan de vele thuiskantoren van medewerkers die **thuiswerken**.
2. Tanium vereenvoudigt vraagstukken over **compliance**: wanneer verkopers van software of auditeurs komen checken of de software wel compliant is, duurt het slechts enkele seconden tot minuten om alle informatie te verzamelen. Met andere systemen kan dit heel tijdrovend zijn en zelfs dagen tot weken duren.
3. Het aantal **cyberincidenten** en de **meantime to resolution** (MTTR) nemen aanzienlijk af. Vaak is dit een belangrijke KPI voor een bepaalde rol in de organisatie, zoals bijvoorbeeld de CISO.
4. De **IT-architectuur** wordt **vereenvoudigd** en **geoptimaliseerd**. Tanium helpt om servers uit te zetten en om tools te vervangen en uit te schakelen.

MEER WETEN?

Geïnteresseerd in de vele voordelen die Tanium te bieden heeft? We horen graag wat uw belangrijkste uitdagingen zijn. Laten we daarom eens afspreken, zodat we u meteen kunnen tonen waarom ook uw dienst beter zal worden van een samenwerking met Tanium.

Ja, ik wil een afspraak maken!