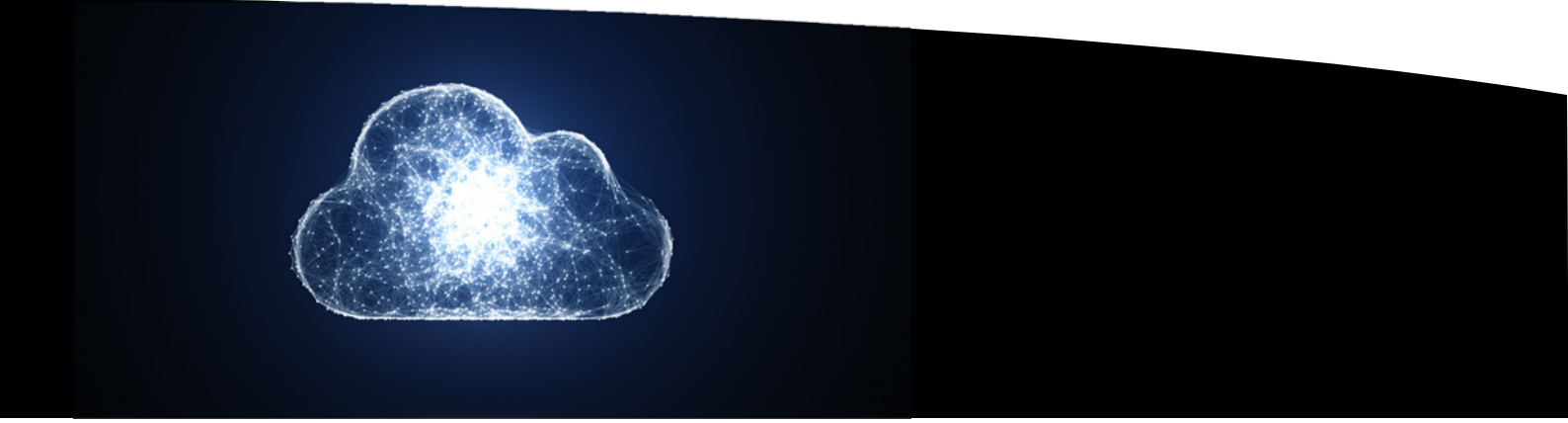
Smarte Netzwerke für Smart Buildings

Mit Cloud Managed Networking Sicherheit erhöhen und Kosten nachhaltig senken

euromicron Deutschland GmbH

cisco Gold Partner

Inhalt



Intelligente Gebäude brauchen leistungsfähige Cloud-Netzwerke

Nur das autonom fahrende Auto beflügelt gegenwärtig stärker die Fantasien: Die Vordenker des „Internet der Dinge“ wollen auch Gebäude zu sogenannten „Smart Buildings“ ausbauen, die sich selbst steuern. Architekten, Bauherren, Gebäudetechniker, Facility-Manager sehen in intelligent vernetzten und zentral gesteuerten Büro- und Verwaltungsgebäuden die Lösung für viele Herausforderungen, vor denen Besitzer, Betreiber und Nutzer von modernen Büro- und Zweckgebäuden, Industriehallen und kritischen Infrastrukturen wie Flughäfen oder Bahnhöfen stehen. Die Vernetzung der Gebäudetechnik mit Sensoren und Aktoren via IP-Technologie steigert Sicherheit, Energieeffizienz und Komfort, reduziert Risiken und Betriebskosten. Smart Buildings passen sich an ihre Nutzergruppen an, orientieren sich an den verschiedenen Bedürfnissen der Menschen und sorgen für eine höhere Sicherheit und einen größeren Komfort. Selbstverständlich erwartet heute jeder Besucher eines Zweckbaus, dass er dort ein WLAN nutzen kann. Bewohnern, Gästen, Arbeitnehmern und Kunden ist der Internetzugriff über die beliebte Funktechnik kaum mehr zu verweigern. Ob für Büro- und Verwaltungsfunktionen, Bildungs- oder Gesundheitseinrichtungen, im Handel oder in einer Mischnutzung: Wer ein Gebäude regelmäßig oder sporadisch betritt, will mit dem eigenen Smartphone, Tablet oder Laptop ins Netz. Moderne Netzwerktechnik ermöglicht zudem neue Services in der Gebäudebewirtschaftung und gewährt Flexibilität für eine Vielzahl unterschiedlicher Nutzungsarten.

Sorgen machen sich über den unausweichlichen Trend aber CIOs, Security-, IT- und Gebäude-Manager sowie Datenschutzbeauftragte.

„Internet of Things“ revolutioniert die intelligente Gebäudetechnik

Es ist noch nicht lange her, da hatte jedes Büro- und Zweckgebäude eine Fülle von singulären Einzelsystemen für die Gebäudetechnik. Isolierte Steuerungen für Heizung, Klima, Zutrittskontrolle, Überwachung und Brandschutz, IT-Netzwerke und Telekommunikation arbeiteten in ihren eigenen Systemwelten. Nur selten ergänzten sie sich oder waren gar verbunden. Dann bullerte die Heizung auf Anschlag, die Fenster waren weit aufgerissen, während anderswo im Haus bereits die Klimaanlage heulte. Beleuchtungssysteme machten die Nacht zum Tage, obwohl niemand sie nutzte – aber abgeschaltet hatte sie auch keiner.

Nachdem in den vergangenen zehn Jahren IT und Telekommunikationsnetzwerke über die IP-Technologie zusammengewachsen sind, revolutioniert das Internet der Dinge nun alle Technikbereiche moderner Gebäude. Das „Internet-Protokoll“ hat sich als Grundlage für die zentrale Datenautobahn längst etabliert und ermöglich die dezentrale Einrichtung, Fernwartung und Steuerung sämtlicher Systeme. Herzstück der Gebäudetechnik ist daher heute nicht mehr die Hausmeisterzentrale oder das Facility-Management, sondern das IT-Netzwerk. Denn alle Gebäudesysteme werden in Smart Buildings via IP vernetzt und zentral gesteuert.

Netzwerk-Architektur übernimmt strategische Aufgaben für Datensicherheit

2018 waren bereits 17,8 Milliarden „ Dinge“ im Internet vernetzt. Bis 2020 sollen es nach einer Studie der Gartner Group schon über 21 Milliarden sein. Ein großer Anteil davon wird aber kein Smartphone oder Laptop mehr sein, sondern eine Heizungs- oder Klimasteuerung, eine Videoüberwachungskamera oder ein Brandmelder. Laut Gartner waren 2015 weltweit bereits 45 Prozent aller „vernetzten Dinge“ in Smart Buildings und Smart Factories verbaut. Und diese vernetzten Dinge in smarten Gebäuden und Fabriken bleiben auch die Treiber des IoT. Der Netzwerk-Architektur kommt bei dieser Entwicklung die strategisch zentrale Aufgabe zu, für die Sicherheit der Daten und der Menschen zu sorgen. Um die Sicherheit in vielen Netzwerken in Smart Buildings ist es allerdings nicht immer zum Besten bestellt, wie IBM in einem Test Ende herausfand. Mit dem „Ethical Hacking Experiment“ simulierten Hacker den Angriff auf ein real vernetztes Gebäude. Sie entdeckten dabei ein gutes Dutzend Sicherheitslücken. Diese ermöglichten es, nicht nur in das Gebäudesystem selbst einzudringen. Noch bedrohlicher an dem Experiment war, dass die Hacker auch Zugriff auf einen zentralen Server erlangten, mit dem über 20 weitere Gebäude in den USA gesteuert werden.

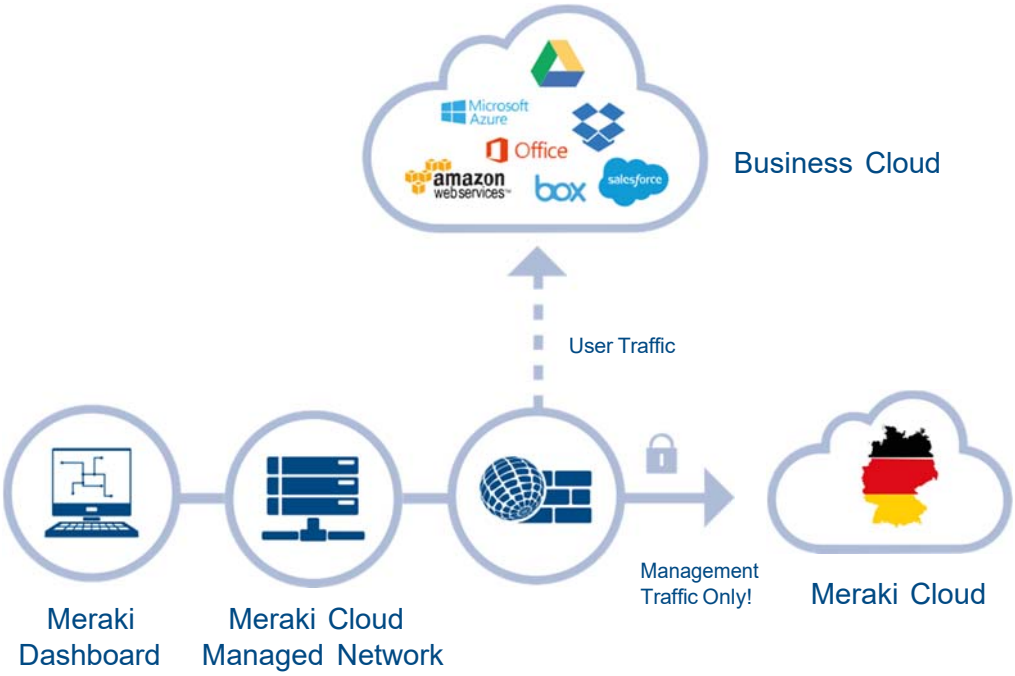
Sorglosigkeit ist die größte Gefahr im „Schatten-IoT“

Vernetzte Gebäude schaffen eine Art „Schatten-IoT“. So bezeichnen die Experten die unaufhaltsam wachsende Anzahl an Geräten, die mit dem Internet verbunden sind, häufig aber gar nicht oder kaum überwacht würden. Die Vorstellung macht nachdenklich: Gebäude, die über das IoT eingebunden sind, sind gegen Cyberattacken offensichtlich wenig geschützt. Und die damit verbundenen Risiken unsicherer Netzwerke stellen nicht nur für die Daten eine Gefahr dar. Angriffe auf sensible IT-Systeme zur Gebäudesteuerung können schnell auch massive Schäden für Menschen und die Infrastruktur bedeuten. Wenn Aufzüge, Rolltreppen, Brandmeldeanlagen, dynamische Fluchtwegesysteme gestört sind und gebäudeinterne Sicherheitseinrichtungen im Ernstfall versagen, sind Katastrophen vorprogrammiert. Es scheint so, als wäre die Sorglosigkeit mit dem IoT in Smart Buildings die größte Gefahr. Dabei gibt es längst sichere und hochverfügbare Netzwerktechnik, die fast alle Risiken im Griff hat und neue Risiken im IoT minimiert.

In diesem E-Book lesen Sie, wie Sie die Implementierung und den Wartungsaufwand eines IT-Netzwerkes in einem Smart Building reduzieren und gleichzeitig die Kosten senken. Sie erfahren, wie Sie parallel die Performance und die Netzwerkproduktivität steigern und Ihr Unternehmen vor Cyberattacken wirksam schützen können. Denn mit den cloudbasierten Lösungen von euromicron Deutschland steuern Sie Ihr Netzwerk von einem zentralen Dashboard mit bisher unerreichter Managementeffizienz.

Cloud Managed Networking

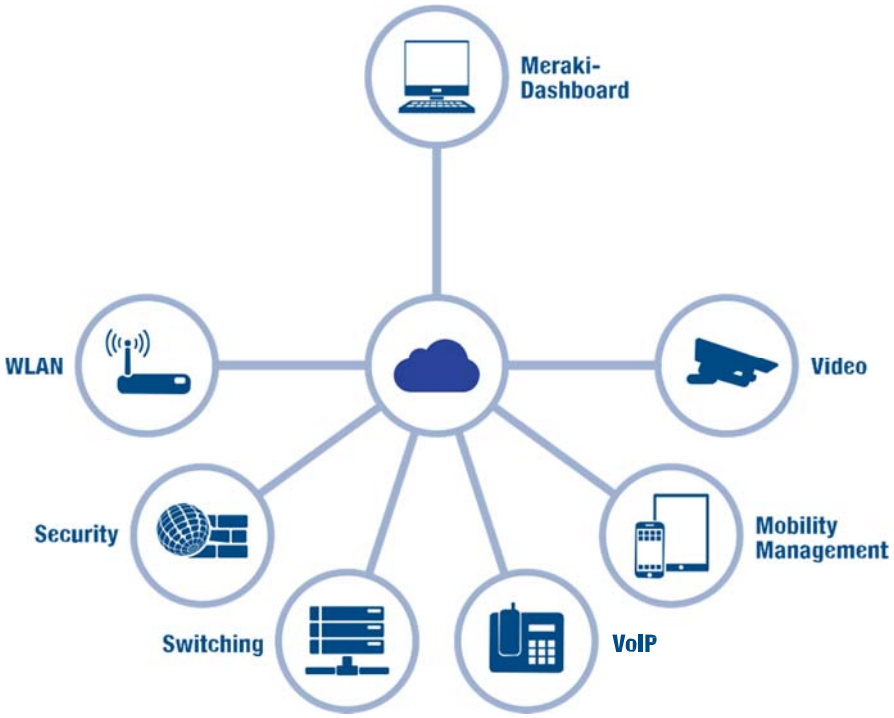
Als Cisco Gold Partner empfiehlt euromicron Deutschland den Einsatz der cloudbasierten Netzwerklösung Cisco Meraki. Die in der Cloud gehostete Lösung, die eine zentrale Einrichtung und Verwaltung von Unternehmensnetzwerken via Dashboard ermöglicht, wird u. a. als Managed Service bereitgestellt. Im ersten Schritt bietet euromicron Deutschland eine umfassende Beratung an und entwickelt gemeinsam mit Ihnen maßgeschneiderte Anwendungskonzepte. Im Rahmen der kurzfristig realisierbaren Installation wird dem Nutzer dann eine schlüsselfertige Netzwerkplattform zur Verfügung gestellt, in die sämtliche erforderliche Netzwerkgeräte und Managementanwendungen bereits integriert sind – von WLAN Access Points, Access und Core Switches über Voice-over-IP und Security-Kameras bis hin zu Mobile Device Management und IT Security Appliances. Diese werden aber nicht mehr als einzelne Instanzen im Netzwerk singulär programmiert und verwaltet. Vielmehr sind sie in einem cloudbasierten virtuellen Netzwerk zusammengeschlossen. Diese Zusammenführung führt in der Praxis zu einer schnelleren, sicheren und zentralen Verwaltung von Netzwerken und den auf ihnen basierenden Hardware-Komponenten. Diese müssen nicht mehr einzeln konfiguriert werden, sondern lassen sich von einer zentralen Steuerungsinstanz einrichten, warten, skalieren und vor allem auch sichern. Anders als in einer klassisch-linearen Netzwerkinfrastruktur muss beispielsweise nicht mehr jeder Switch oder jede Firewall manuell vor Ort programmiert werden. Techniker verkabeln lediglich die Hardware. Administratoren steuern anschließend die Einrichtung über das Meraki Dashboard von überall her.



Funktionsweise eines Meraki Cloud Managed Network.

Zentraler Überblick mit dezentraler Steuerung und geringerem Wartungsaufwand

Für Sie als Betreiber oder Nutzer eines Smart Buildings/Extended Enterprise und für Ihre CIOs, Datenschützer und Facility-Manager eröffnet Cloud Managed Networking völlig neue Möglichkeiten. Sie kontrollieren alle Datenverkehre, konfigurieren Hardware über ein zentrales Dashboard. Eine physische Präsenz eines IT-Mitarbeiters vor Ort für die Programmierung, Wartung und Kontrolle von u. a. Switches, Firewalls oder WLAN Access Points entfällt praktisch. Die Hardware wird lediglich einmal verbaut und verkabelt. Danach steuern Sie per Fernwartung alle Systeme. Und egal welches Ding mit einem Netzwerkknoten verbunden ist, ein Sensor, ein Aktor, ein Fahrstuhl oder eine Heizungsanlage oder ein Mobile Device. eines Mitarbeiters: Sie greifen über Ihr virtuelles Netzwerk darauf zu. Entscheidende Vorteile für die Sicherheit und die Leistungsfähigkeit bieten die fein aussteuerbaren Regeln, die Sie frei definieren können. Sie öffnen oder schließen Ports für Anwendungen. Sie legen fest, welche Anwendungen Vorfahrt haben. So können Sie VoIP-Telefonie priorisieren, Datenpakete mit Facebook und Co. hingegen blockieren. Sie können sicherheitsrelevante Systeme völlig abschotten. So schützen Sie geschäftskritische Datenverkehre, halten Ihr Netz sauber und leistungsfähig.

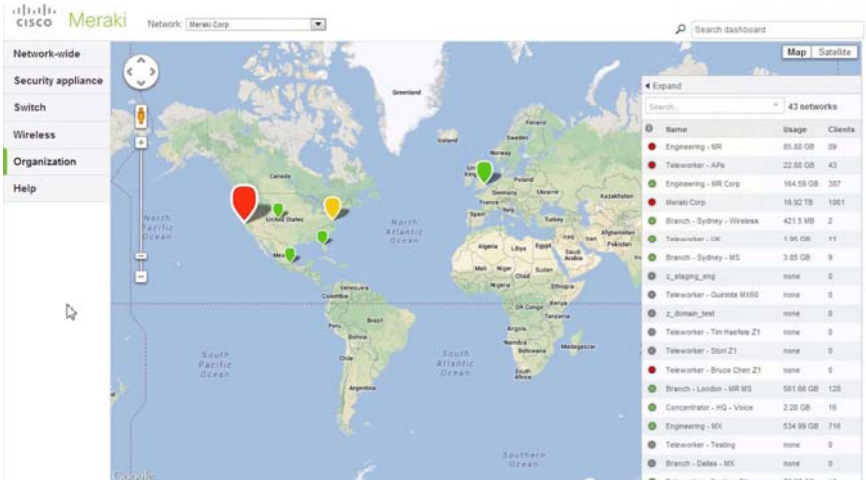


Das Cisco Meraki Ökosystem und seine Produkte bieten einen völlig neuen und erfrischenden IT-Ansatz.

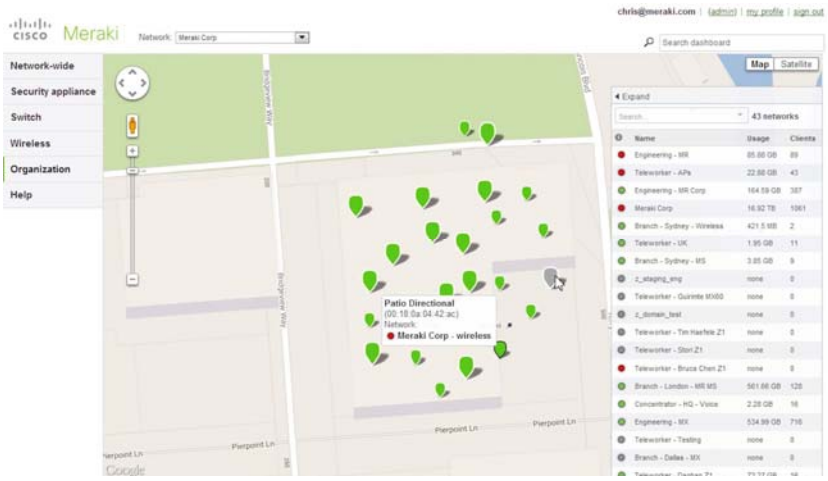
Cisco Meraki Cloud Management:
die Steuerung für Smart Buildings

Cisco Meraki vereinfacht Unternehmensnetzwerke deutlich. Es ermöglicht ein zentrales Cloud-Management für WLAN, Switching, Security Appliances und Mobile Device Management. Meraki reduziert die Komplexität von traditionellen Netzwerkarchitekturen, senkt dadurch enorm die Kosten und erhöht die Sicherheit.

Die Vorzüge im Überblick:



- Sie verwalten Ihr gesamtes, weltweit verteiltes Netzwerk von jedem beliebigen Endgerät über eine browserbasierte Anwendung. Egal wo der Administrator sitzt, er kann auf alle angeschlossenen Netzwerkstandorte und alle eingebundenen Systeme zugreifen.



- Sie erhalten zu jeder Zeit eine Übersicht über alle WLAN Access Points, Switches, Security Devices, Nutzer, Endgeräte und Anwendungen.
- Sie können regelbasiert Zugriffsrechte definieren und jedem Nutzer, jedem Endgerät und jeder Anwendung zuteilen. Unterbinden Sie YouTube-Videos und geben Sie Ihren eigenen Anwendungen wie VoIP Vorfahrt.

Die wichtigsten Argumente für Cisco Meraki im Überblick

- Browserbasiertes Cloud Managed Network für IoT in Smart Buildings
- Hochverfügbare Datencenter in Europa (Frankfurt am Main, München [SLA 99,9 Prozent])
- Volle Netzwerkfunktionalität auch ohne Verbindung in die Cloud
- Sie benötigen keine weitere Controller-Hardware oder Management-Software
- Durch das Meraki Managementprinzip erzielen Sie kurze IT-Rollouts, Software- und Feature- Updates direkt aus der Cloud
    - Verbinden Sie Standorte und Endgeräte mit wenigen Mausklicks
    - Überwachen Sie Software-Updates auf allen Endgeräten und greifen Sie direkt auf jedes Endgerät zu, bei dem Sicherheitslücken entstehen
- Cisco Meraki ist standortübergreifend skalierbar, für kleine und große Netzwerke
- HIPAA-/PCI-konform mit Level-1-Zertifizierung; höchste Sicherheit vor dem Zugriff Dritter
    - Health Insurance Portability and Accountability Act (HIPAA) ist der amerikanische Standard zur sicheren digitalen Weitergabe und Verarbeitung von Patientendaten
    - Payment Card Industry Data Security Standard (PCI) umfasst alle Regeln für die Abwicklung eines sicheren Zahlungsverkehrs der großen Kreditkartenunternehmen der Welt
- Automatische Firmware- und Software- sowie Security-Updates nach vorgegebenen Zeiträumen
- Desaster-Recovery und Preparedness-Prozess
- Sie haben geringere Kosten bei der Implementierung und Wartung Ihres Netzwerks

Hardware: das komplette Cloud-Managed-IT-Portfolio „Out of the Box“

Meraki besteht aus Hard- und Software-Komponenten, die lediglich verkabelt und dann zentral gesteuert werden.

Hardware:

- MR WLAN Access Points (mit 802.11ac und Bluetooth)
- MS Ethernet Switches (Distribution und Edge Layer)
- MX Security Appliances (NG.-Firewall, VPN, SD-WAN, AWS-vMX)
- MV Security Cameras (inkl. Analytics Tools, On-Device Storage)
- MC Communication (Voice-over-IP)

Software:

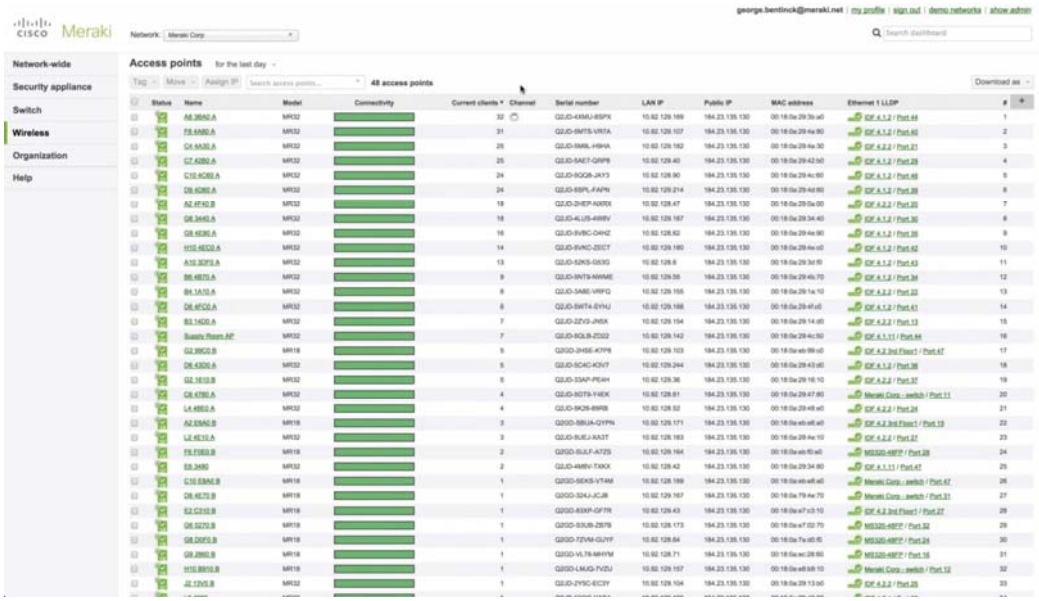
Mit dem SM Systems Manager für iOS, Android, Mac und Windows steuern Sie diese Hardware-Komponenten über das Meraki Dashboard. Das Mobile Device Management System installiert, konfiguriert und managt alle Komponenten über Standorte hinweg.

Meraki Dashboard: das Cockpit für die komplette Netzwerksteuerung

Das Meraki Dashboard ist eine benutzerfreundliche und browserbasierte Oberfläche, die intuitiv alle Funktionen der Netzwerksteuerung integriert. Sie bietet einen sicheren Administratoren-Zugriff mit einer Zwei-Faktor-Authentifizierung mit SSL/TLS. Secure Socket Layer und Transport Layer Security ist ein hybrides Verschlüsselungsprotokoll zur sicheren Übertragung sensibler Daten über das Internet mit einer 256-Bit-Verschlüsselung. Eine einfache Übersicht ermöglicht die Überwachung von WLANs, Switches und Security-Funktionen.

Access Control und Priorisierung

WLAN Access Point, Switches, Security Devices und Endgeräte können Sie mit Cisco Meraki einzeln managen. Sie erhalten einen vollen Überblick über die aktuelle Performance Ihres Netzwerkes, erfassen den Durchlauf, die Auslastung und haben Zugriff auf alle Verbindungsdaten. Sie erteilen per Mausklick ausgewählten Datenverkehren Vorfahrt, vergeben Bandbreiten für weniger wichtige Datenströme. Alle Berechtigungen für die Netzwerknutzung lassen sich für jeden Anwender und für jede Anwendung einzeln konfigurieren. So verteilen Sie Rechte und Rollen, unterbinden bei Bedarf bestimmte Apps oder Websites, die die Nutzer über Ihr Netzwerk nicht aufrufen dürfen.



Eine Übersicht über alle Access Points zeigt auf einen Blick,
ob und wo es Störungen gibt. Der grüne Balken signalisiert: alles okay!

In der Einzelansicht analysieren Sie aktuelle und historische Daten zu Performance, Anzahl der Nutzer, Ausfallzeiten und Auslastung.

Location Analytics – nicht nur für den Handel ein attraktives Screening

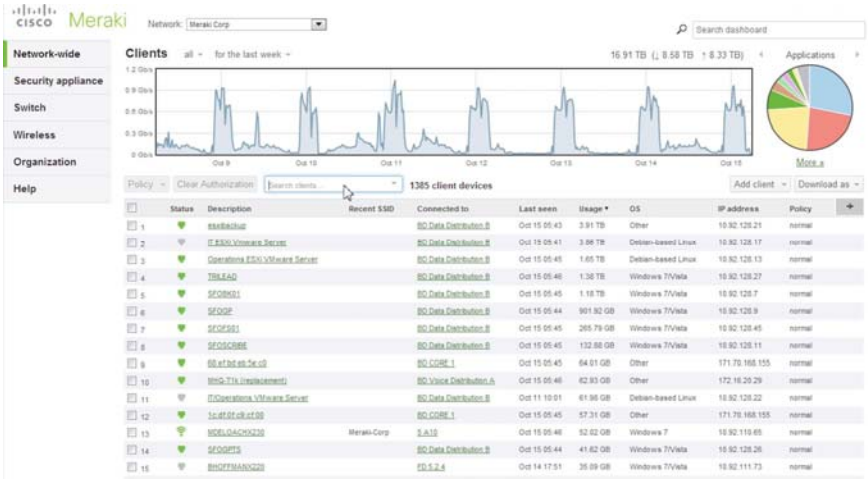
Mit der Standortanalyse können Sie messen und vergleichen, wie viele Nutzer in verschiedenen Gebäuden die öffentlich zugänglichen WLANs nutzen. Jedes Endgerät mit eingeschaltetem WLAN wird erfasst. So können Sie zum Beispiel über Location-Heatmaps analysieren:

- Wie viele potenzielle Kunden laufen an dem Standort vorbei?
- Wie viele kommen ins Gebäude?
- Wie viele nutzen das WLAN?
- Wie lange sind sie verbunden?
- Wie oft kommen sie am Gebäude vorbei und loggen sich ein?

Für den Einzelhandel ergeben sich aus den gewonnenen Daten Hinweise für die Gestaltung der Auslagen und des Angebotes oder einer Werbekampagne. Auch der Vergleich von verschiedenen Niederlassungen bietet sich an. Vor allem in Verbindung mit den Tools zur User Analytic ergeben sich weitere Analyse-Routinen, um auch das Nutzerverhalten zu analysieren.

User Analytics und Anwenderkontrolle

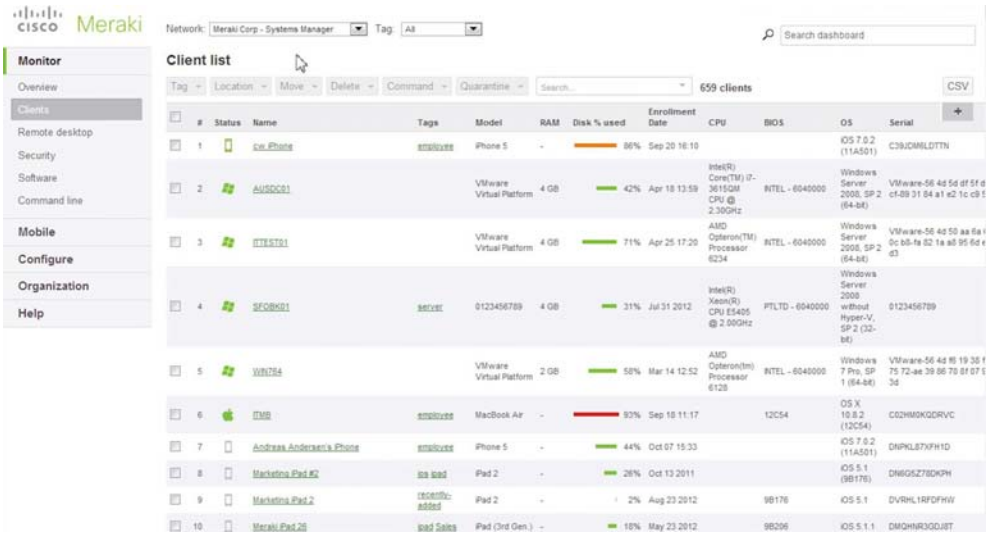
Für die Netzwerksicherheit ist es wichtig, sowohl die Nutzer als auch deren Verhalten zu überwachen. Cisco Meraki ermöglicht aber weitaus mehr als lediglich die Überwachung. Durch Regeln und Eingriffe bis hin zur Endgeräteebene sorgen Sie für eine hohe Performance und Integrität Ihres Netzwerkes. Stellen Sie beispielsweise Regeln für das Software-Update in den Endgeräten auf. Geräten ohne Updates senden Sie eine Nachricht. Bei Verbindungsproblemen loggen Sie sich in das betroffene Endgerät ein und beheben die Störung. Oder Sie geben lediglich bestimmte Anwendungen frei, die in einer Bildungs- oder Healthcare-Einrichtung wichtig sind. Gleichzeitig unterbinden Sie für bestimmte Nutzergruppen beispielsweise Social Media und geben diese anderen frei. Oder Sie wollen bei einer hohen Auslastung eines Netzwerkbereiches die Datenströme beschränken? Reduzieren Sie die Bandbreite oder sperren Sie beispielsweise Videostreaming.



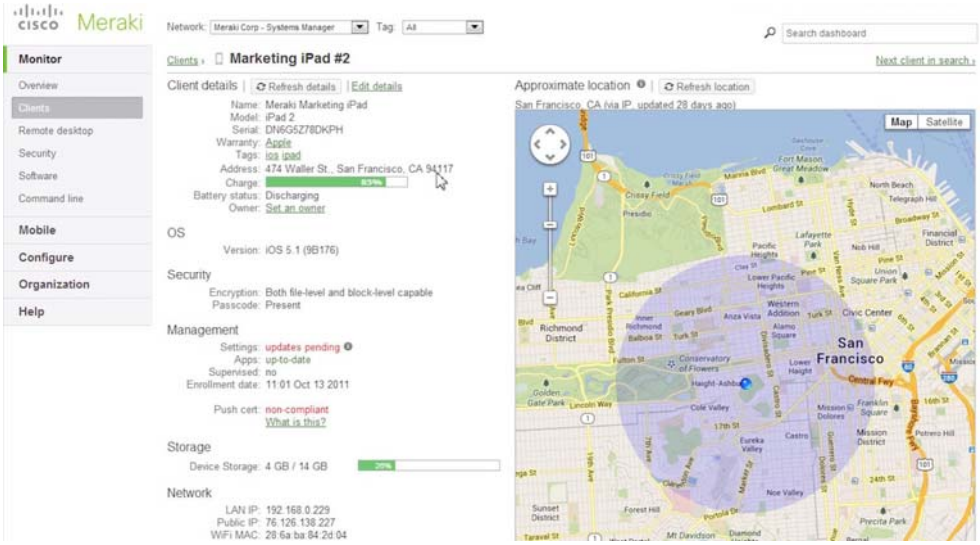
Feingranulare Analyse, Überwachung und Steuerung aller Netzwerkaktivitäten der Nutzer und Kontrolle über alle Anwendungen.

Mobile Device Management: Konfiguration von hunderten Endgeräten gleichzeitig

Mobile Device Management ist in großen Unternehmen eine Herausforderung, die den Sicherheitsverantwortlichen viele Sorgen macht. Und viel Arbeit, denn jedes Gerät muss konfiguriert und regelmäßig auf Updates geprüft werden. Ob im Unternehmen oder in einer Bildungseinrichtung: Immer wieder sind viele Endgeräte gleichzeitig einzubinden. Sie wollen bestimmte Software aufspielen oder aktualisieren, andere Anwendungen wollen Sie löschen. Früher war mit einer solchen Aufgabe ein Mitarbeiter der IT je nach Anzahl der Geräte ein paar Tage beschäftigt. Mit Cisco Meraki gehören solche Konfigurationsarbeiten der Vergangenheit an. Sie verteilen einfach die Endgeräte an Studenten, Mitarbeiter oder Gäste und weisen ihnen ihr VLAN zu. Sie weiten Ihre Standards auf jedes Gerät automatisch aus. Dafür definieren Sie einmal in Cisco Meraki die Regeln für diese Nutzergruppe, die auf den Geräten laufen soll.



Mit dem Mobile Device Management in Cisco Meraki behalten Sie den Überblick.



Geht ein Endgerät verloren, orten Sie es via GPS und können die Rückgabe organisieren.

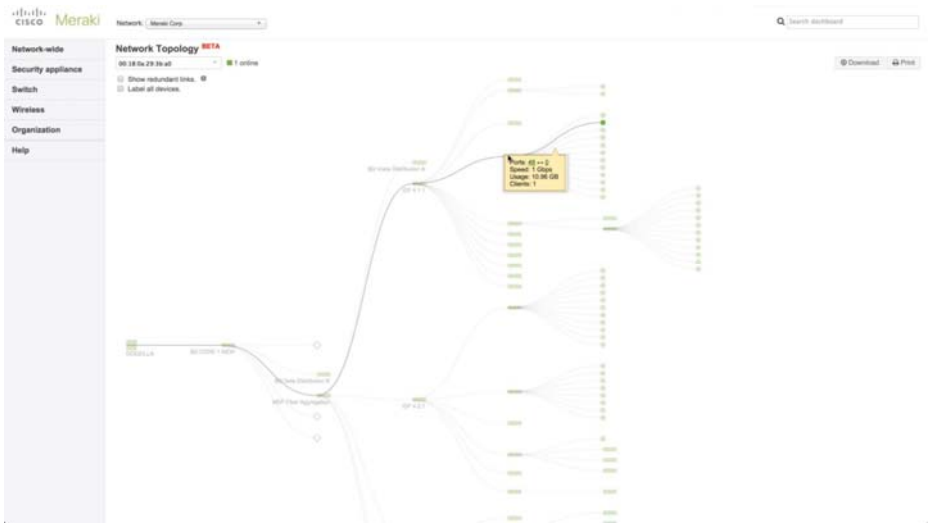
Video-Überwachung 2.0

Zu der Produktfamilie von Cisco Meraki gehört eines der leistungsfähigsten marktverfügbaren Video-Überwachungssysteme. Die Hardware besteht aus Kameras für den In- und Outdoor-Einsatz. Jede Kamera verfügt über einen auf anspruchsvolle Umgebungen ausgelegten 128-GB-Solid-State-Speicher, der Platz für bis zu 20 Tage an Videomaterial bietet. Ein Video-Server ist deshalb nicht nötig. Das System ist geeignet für alle Einsatzgebiete und Gebäudegrößen: von einer bis über 1.000 Kameras.

Sie können alle Kameras über das Meraki Dashboard aufrufen und auswerten und benötigen somit keine spezielle Software oder spezielle Browser-Erweiterungen. Intelligente Bewegungsindizierung mit einer Suchmaschine sowie eingebaute Videoanalyse-Werkzeuge ermöglichen es Ihren Sicherheitsmitarbeitern, mit einem Mausklick direkt auf die Videosequenzen zuzugreifen, in denen ein Ereignis stattfand. Die Videoaufzeichnungen können anschließend einfach exportiert und digital ausgetauscht werden, sodass keine zusätzlichen Speichermedien wie DVDs, VHS-Kasetten oder USB-Sticks benötigt werden.

Safety first in der Netzwerktopologie

Cisco Meraki bietet Ihnen stets einen Überblick über sämtliche im Netzwerk befindlichen Hardware-Komponenten. Egal ob WLAN Access Point, Switches, VoIP-Telefone oder Security-Kameras: Sie erkennen mit einem Blick auf die Netzwerktopologie den Zustand aller Komponenten. So erfahren Sie frühzeitig von Problemen. Sie steuern jedes Gerät einzeln an, spielen neue Firmware auf oder öffnen oder schließen Ports per Mausklick. Eine Kabeldiagnose hilft Ihnen bei der Fehleranalyse. Ebenso können Sie mit „Port Schedule“ für jedes Gerät eine „Terminplanung“ vornehmen. Sie bestimmen damit, wann und wie lange ein Port beziehungsweise ein LAN oder WLAN offen ist und wann er oder es ausgeschaltet wird. So sparen Sie außerhalb der Öffnungszeiten Energie und erhöhen die Sicherheit Ihres Netzwerkes, da beispielsweise das WLAN außerhalb der Betriebszeiten automatisch deaktiviert und demzufolge nicht angegriffen werden kann.



Über die Netzwerktopografie greifen Sie bequem auf alle Hardware-Komponenten zu. Sie spielen Firmware auf, analysieren oder beheben Störungen und nehmen Voreinstellungen auf den Geräten vor.

Wenn ein Kabelproblem auftritt, können Ihre Administratoren mit dem „Kabel-Test-Tool“ dieses über den ausgewählten Switch-Port aufspüren.

SD-WAN-Technologie

Software Defined Wide Area Network (SD-WAN) bietet eine Reihe von Werkzeugen und Fähigkeiten, mit denen es sich an dynamische Netzwerkprozesse anpassen kann. Je nach den eingestellten Regeln muss der Administrator nicht einmal manuell eingreifen. So bietet die Technologie verschiedene fein granulierbare Einstellungen, um ausgewählten IP-Paketen im WAN-Datenverkehr Vorrang einzuräumen. Damit stellt SD-WAN die optimale Performance für kritische Anwendungen im Netzwerk sicher und reduziert Störungen sensibler Verbindungen. Darüber hinaus senkt diese neue Netzwerktechnologie die Betriebskosten und verbessert die Effektivität bei hoher Auslastung.

Die Vorteile der Cisco-Meraki-SD-WAN-Technologie sind:

- Redundanz und Priorisierung für kritische Verbindungen und Anwendungen
- Dynamische Auswahl für den stets optimalen Pfad im Echtzeit-Datenverkehr mit Regeln basierter und variabler Pfadbereitstellung
- Sichere Konnektivität mit integrierter Cisco-Bedrohungsabwehr-Technologie
- Kostengünstige Alternative zu MPLS-Lösungen

Next-Generation Firewall: gibt Cybercrime keine Chance

Neben den Nutzendimensionen und der hohen Usability von Cisco Meraki bieten ausgeklügelte Hard- und Softwarelösungen ein bisher unerreichtes Maß an Netzwerksicherheit. Die Security Appliances von Cisco sorgen dafür, dass 99,2 Prozent aller Bedrohungen blockiert werden und damit höchste Netzwerkintegrität „State of the Art" jederzeit gewährleistet wird. Als einer der ersten großen IT-und Telekommunikationskonzerne integriert Cisco eine bedrohungsorientierte Next-Generation Firewall (NGFW) in die Meraki Produktwelt. Sie vereint neben der bereits skizzierten Anwendungskontrolle alles, was Sie für ein sicheres Netzwerk in einem Smart Building brauchen, in einer umfassenden Lösung.

Firewalls überwachen den kompletten Datenverkehr zwischen dem eigenen Netzwerk und dem Internet. In Firewalls legen Sie fest, wie die Nutzer kommunizieren können. Anfangs fungierten Firewalls als Paketfiltertechnik, die auf Ebene 4 des OSI-Pro- tokolls den Datenverkehr überwachten. Schon bald waren sie aber machtlos gegen Trojaner und andere Viren, die sich geschickt in Anwendun- gen tarnten. So entstanden Firewalls, die auf der Anwendungsschicht (Layer 7 des OSI-Protokolls) arbeiteten. Damit waren sie in der Lage, auch die Inhalte des Datenverkehrs zu überwachen. Und da Cyberkriminelle bisher den Firewall-Technikern immer wieder einen Schritt voraus waren, fanden sie immer wieder Lücken in der Netztopologie, die vor allem durch mobile Endgeräte entstanden. Smartphones und Laptops infizieren sich in ungeschützten WLANs und schleusen Schadcode ins Unternehmensnetz. Viren, Trojaner oder Varianten davon, wie „Wannacry" und „NotPetya", umgehen dann die Firewall. Ein Schaden tritt unweigerlich ein.

Next Generation Firewall (NGFW)

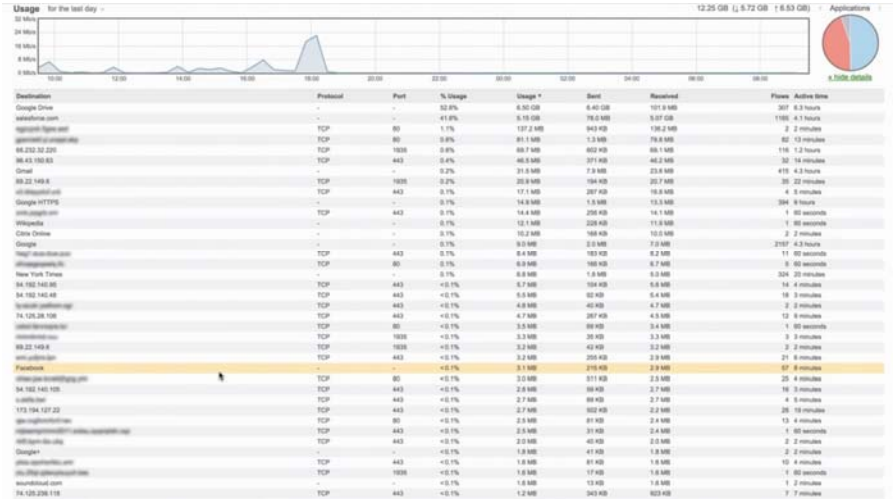
NGFWs übernehmen die bisherigen Funktionen von Firewalls wie Paketfi Netzwerk- und Port-Adressierung (NAT), eine zustandsorientierte IP-Paketübertragung (Stateful Inspection) und ein Virtual Private Network (VPN). Firewalls der nächsten Generation beziehen weitere Schichten des OSI-Modells ein und verbessern die Filterung des Netzwerkverkehrs nachhaltig. Firewalls wie die in Meraki integrierten Security Appliances der neuesten Generation haben sich zu umfassenden Schutzsystemen entwickelt. Sie überwachen den gesamten Datenverkehr regelbasiert. Sie analysieren quasi als selbstlernende Systeme jeden verdächtigen Datenverkehr und können ihn unterbinden, wenn sie eine Bedrohung identifizieren. Vor allem die dynamische Paketfiltertechnik überwacht die Inhalte, ordnet jedes Paket einer Anwendung und dem Nutzer zu. Ergänzend wird jedes Datenpaket dahingehend analysiert, ob es eine Bedrohung darstellen könnte. NGFWs führen damit eine wesentlich tiefere Analyse durch und erkennen potenzielle Bedrohungen schneller.

Nicht nur klassische Firewall-Aufgaben, sondern auch folgende Überwachungsfunktionen sind in die NGFW integriert:

- Intrusion Prevention System (NGIPS)
- Advanced Malware Protection (AMP) mit Threat Grid Intellligenz

Next-Generation Intrusion Prevention System (NGIPS)

NGIPS filtert Pakete oder Ereignisse, die von bekannten Mustern minimal abweichen. Deutet ein IP-Paket auf einen Angriff oder eine Regel- oder Sicherheitsverletzung hin, erkennt NGIPS dies. Es stellt sie im Zweifel auch sofort unter Quarantäne und meldet mit einem Alert dem Admin, dass eine Netzwerkgefahr droht. Dieser kann aktiv eingreifen und entscheiden, ob die Kommunikation fortgesetzt oder endgültig beendet wird. Zudem wird das erkannte Intrusions-Muster in der Zustandstabelle der Next-Generation Firewall eingefügt.



Traffic-Analyse ermöglicht in Echtzeit die Identifikation einer Bedrohung. Datenpakete mit einem potenziell schädlichen Viren- oder Malware-Code-Schnipsel stellt NGIPS sofort unter Quarantäne.

Advanced Malware Protection (AMP)

AMP analysiert in Echtzeit alle Dateiaktivitäten im gesamten Netzwerk und spürt komplexe Malware schneller auf als andere Malware-Programme. AMP stellt sie unter Quarantäne und beseitigt sie, bevor sie Schaden anrichten können. Cisco-Experten aktualisieren AMP täglich. Dafür scannen sie täglich Millionen von Malware. Mit einer kontextbezogenen Threat Intelligence kann AMP sowohl bekannte als auch neue Malware-Bedrohungen proaktiv abwehren.

Support und Services

Mit Cisco Meraki profitieren Sie von allen Vorzügen, die eine cloudbasierte Hard- und Softwarelösung zu bieten hat. Tools für Debugging, Benachrichtigungen und Session-Logging sind in die Hardware integriert und lassen sich entweder über das Dashboard aufrufen oder erstatten je nach Voreinstellung selbständig Report. Verliert eine Komponente wegen einer physischen Störung die Verbindung zum Netzwerk, erhalten Sie darüber sofort einen Alert; meistens sogar schneller, als die Nutzer es überhaupt merken. Störungen im Netzwerk werden zudem automatisch in einem Netzwerkzustandsbericht erfasst. Software-Updates für alle Produkte werden vollständig von der Meraki Cloud verwaltet und benötigen nur ein voreinstellbares Wartungsfenster. Wenn Sie Hilfe brauchen, steht Ihnen der Meraki Support direkt aus dem Dashboard zur Verfügung. Das verkürzt die Zeit bis zur Lösung des Problems.

Meraki Support und Services im Überblick:

- Schnelle Bereitstellung: Dank Zero Touch Deployment können Sie eine große Anzahl von Außenstellen innerhalb kürzester Zeit ausstatten.
- Funktions-Audits: Mit der Hilfe des Meraki Dashboards können Sie eine große Anzahl von Netzwerken gleichzeitig überwachen.
- Threat-Reports: Die Meraki Security Appliances bieten Ihnen eine umfassende Übersicht über alle Angriffe auf das Netzwerk.
- Quarterly Network Update Reviews: Sämtliche Informationen zu Netzwerkauslastung, Sicherheit und Verfügbarkeit erhalten Sie einmal pro Quartal in Form eines Reports.
- Integration maßgeschneiderter Apps: Dank API-Zugang zu praktisch allen Daten ist es möglich, maßgeschneiderte Apps zu integrieren.

Wie Sie sehen, erhalten Sie mit Meraki eine Netzwerk-as-a-Service(NaaS)-Management-Lösung für eine Netzwerk-Architektur „State of the Art“. Während jede Hardware-Komponente unabhängig arbeitet, gehört sie doch im Netzwerk zu einer Art Schwarm, der mit jeder weiteren Komponente intelligenter wird. Je mehr Komponenten Sie einbinden, desto intelligenter wird Ihr Netzwerk. Beim Anschließen eines Meraki Access Points oder VoIP-Telefons an einen Meraki Switch zum Beispiel erkennen die Geräte einander. Sofort nach der Erweiterung werden sie für den Administrator sichtbar. Wenn ein neues Produkt zum Dashboard hinzugefügt wurde, erscheint im Menü eine neue Registerkarte, mit der Sie die neuen Funktionen und Dienste freigeben können.

Fazit: Digitalisierte Gebäude denken mit und voraus

In intelligenten Gebäuden öffnen sich dem einen die Türen, dem anderen bleiben sie verschlossen. Biometrische Zugangskontrollsysteme machen es möglich. Betritt ein Mitarbeiter sein Büro, wird das Raumklima automatisch seinen Bedürfnissen entsprechend geregelt. Wie von Zauberhand schalten sich LED-Lichtsysteme ein, wenn ein Bewegungsmelder Besucher registriert. Sie leuchten punktgenau einen Arbeitsplatz aus, aber nur, wenn der berechtigte Mitarbeiter auch anwesend ist. Öffnet jemand ein Fenster, schalten sich Heizung und Klimaanlage aus. Wie gerufen kommt plötzlich der Aufzugsmonteur; der Aufzug bestellt seine Wartung im Smart Building selbständig. Vorausschauende Wartung (Predictive Maintenance) führt dazu, dass Aufzüge, Rolltreppen oder Heizungs- und Klimasysteme nicht mehr unerwartet ausfallen. Schon bei den ersten Anzeichen einer Unwucht in den Umlenkrollen ruft der Aufzug selbständig den Service. Bei einer festgestellten Anomalie ruft die Brandmeldeanlage eigenständig einen Service-Mitarbeiter. Melden Sensoren Fehler im Abgas des Kessels, versendet die Heizung eine SMS an den Wartungsservice. Bei der IT schrillen die Alarmglocken, wenn jemand im Netzwerk versucht, die ihm zugewiesenen Netzbereiche durch unerlaubte Handlungen zu übertreten. Cyberangriffe scheitern schon im Frühstadium an der Cloud Service Security.

Kurzum: Intelligente, digitalisierte Gebäude denken mit und voraus, brauchen aber ein sicheres Netzwerk, um wirklich smart zu sein!

Über euromicron Deutschland GmbH

Die euromicron Deutschland ist eine Tochtergesellschaft der euromicron AG. Mit der Unternehmenszentrale in Neu-Isenburg und einem bundesweit flächendeckenden Niederlassungsnetz ist sie eines der führenden deutschen Systemhäuser im Zukunftsmarkt Internet der Dinge. Geschäftlicher Schwerpunkt sind branchenübergreifende Komplettlösungen im Bereich intelligenter Gebäudetechnologien (Smart Building Solutions) aus den Bereichen Netzwerke, IT-Sicherheit und Sicherheitssysteme. Für unsere Kunden aus Mittelstand, öffentlicher Hand und Großunternehmen legen wir mit leistungsfähigen digitalen Infrastrukturen die Basis für die digitale Transformation.

One-Stop-Shopping im Bereich der intelligenten Gebäudetechnik

Wir kombinieren alle Technologien und Applikationen der Informations- und Kommunikationstechnologie (ITK), um unseren Kunden maßgeschneiderte Lösungen für intelligente Gebäudetechnologien anzubieten. Dabei ist die Kundennähe durch einen Vor-Ort-Service sowie unser zentrales Network Operation Center (NOC) gewährleistet – für Unternehmen und Organisationen aller Größen und Branchen. Mit über 630 Mitarbeitern sind wir ein führender Anbieter kompletter Infrastrukturlösungen für Kommunikations-, Übertragungs-, Sicherheits- und Datennetze mit einem flächendeckenden Niederlassungsnetz in Deutschland.

Als Systemintegrator übernehmen wir das Projektmanagement sowie die komplette Projektabwicklung – von der Planung, Beratung, Systemtechnikauswahl und Installation bis hin zu Service, Wartung und Netzmanagement. Themen wie Sicherheit, Redundanz und Hochverfügbarkeit spielen dabei eine entscheidende Rolle.

Impressum

euromicron Deutschland GmbH Zentrale
Siemensstraße 6
63263 Neu-Isenburg

Tel.: +49 6102 8222-0
E-Mail: info@euromicron-deutschland.de
Web: www.euromicron-deutschland.de