

CLAROTY HEALTHCARE

MEDIGATE
by Claroty



Markus Bloem

Biljana Cabrilo



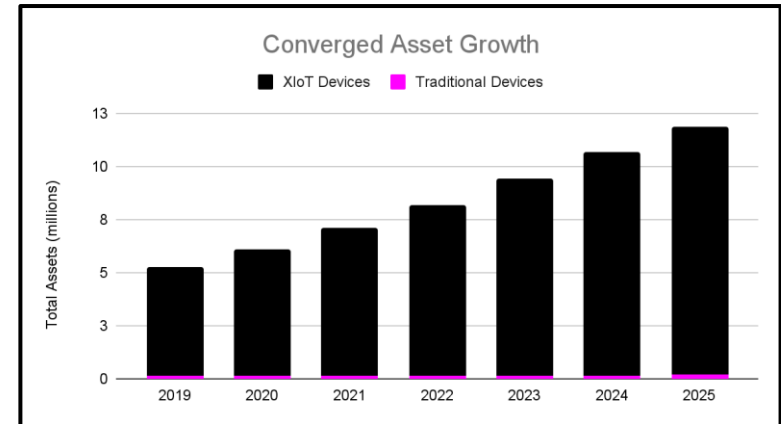
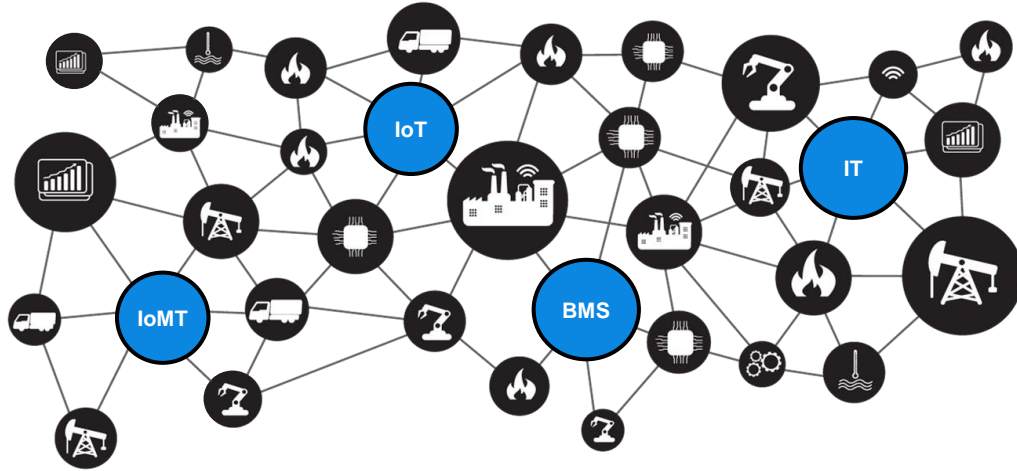
Franz Großmann



Boosting Resilience

Introducing Medigate by Claroty

The rapidly growing Extended Internet of Things (XIoT) is reshaping care delivery



HDOs are increasingly embracing *cyber-physical systems (CPS)* that span a diverse, ever-expanding range of *highly connected devices*.

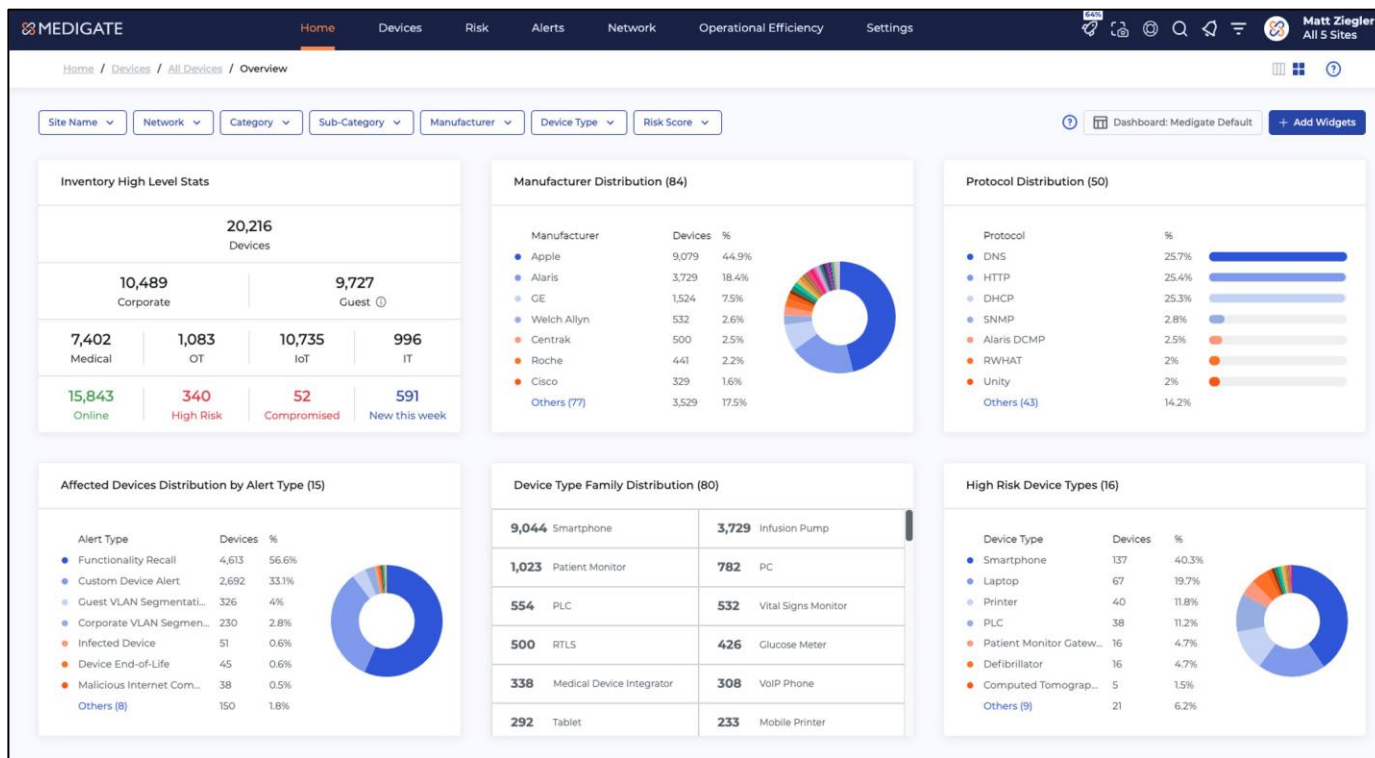
The Cyber-Physical Systems Security Maturity Journey

The Gartner Approach¹

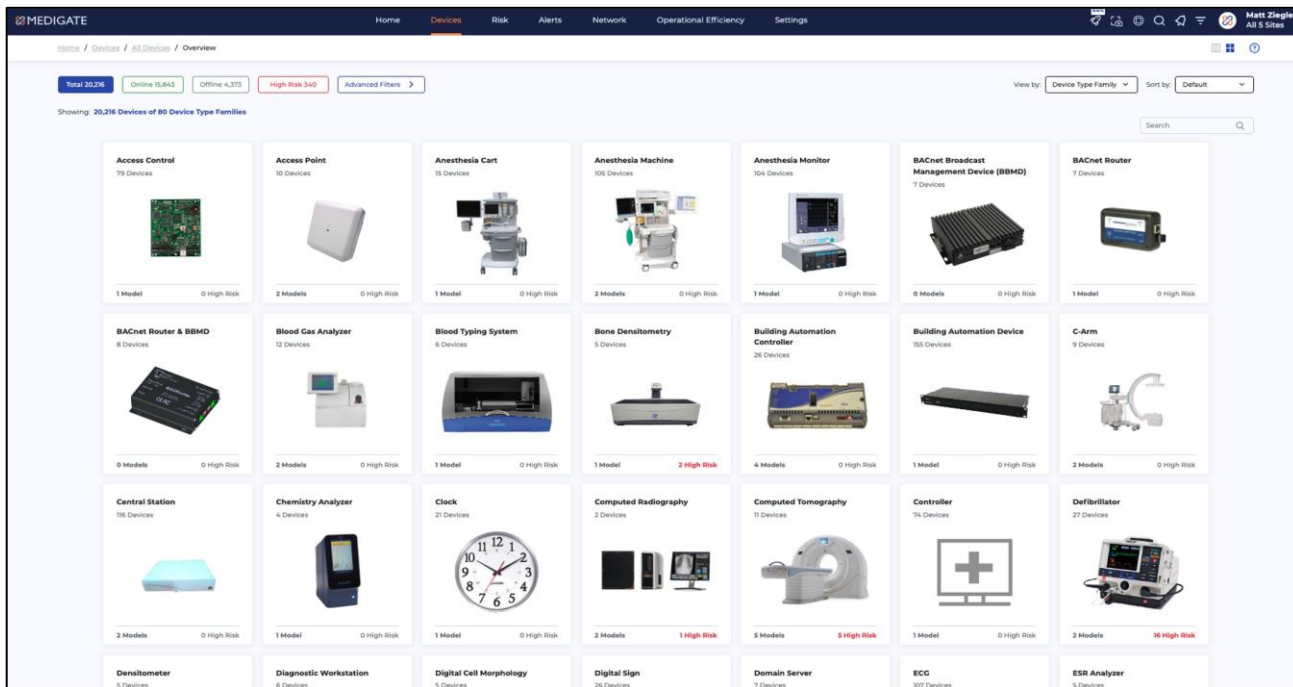


¹Source: Market Guide for Operational Technology Security, Gartner, 2021

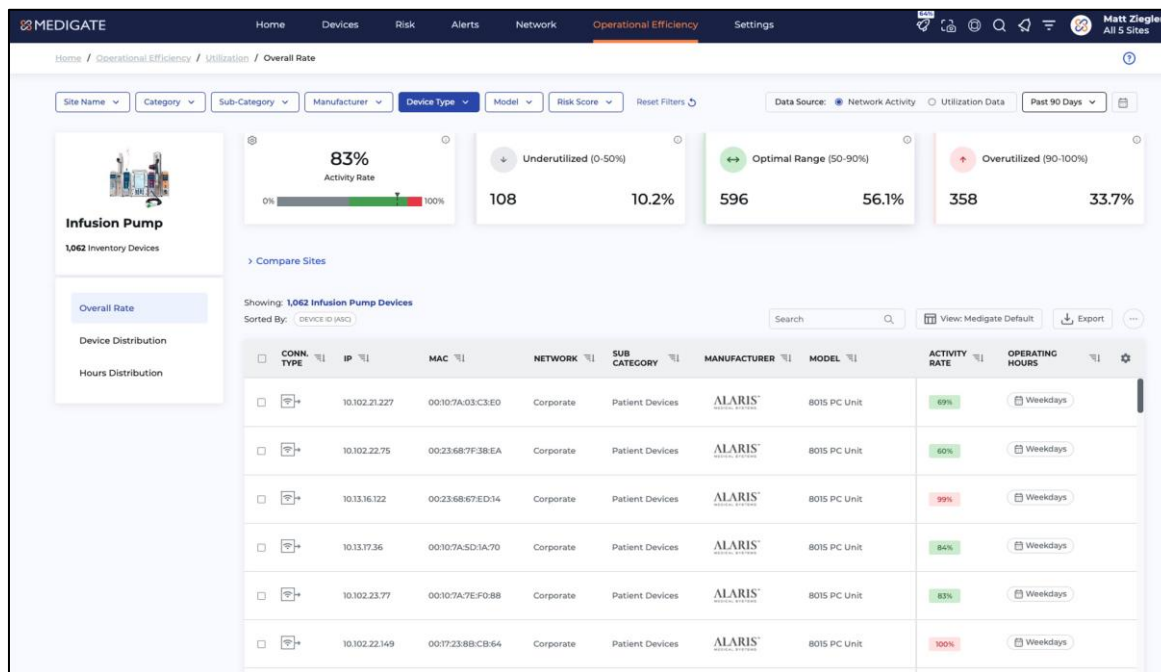
Transparenz



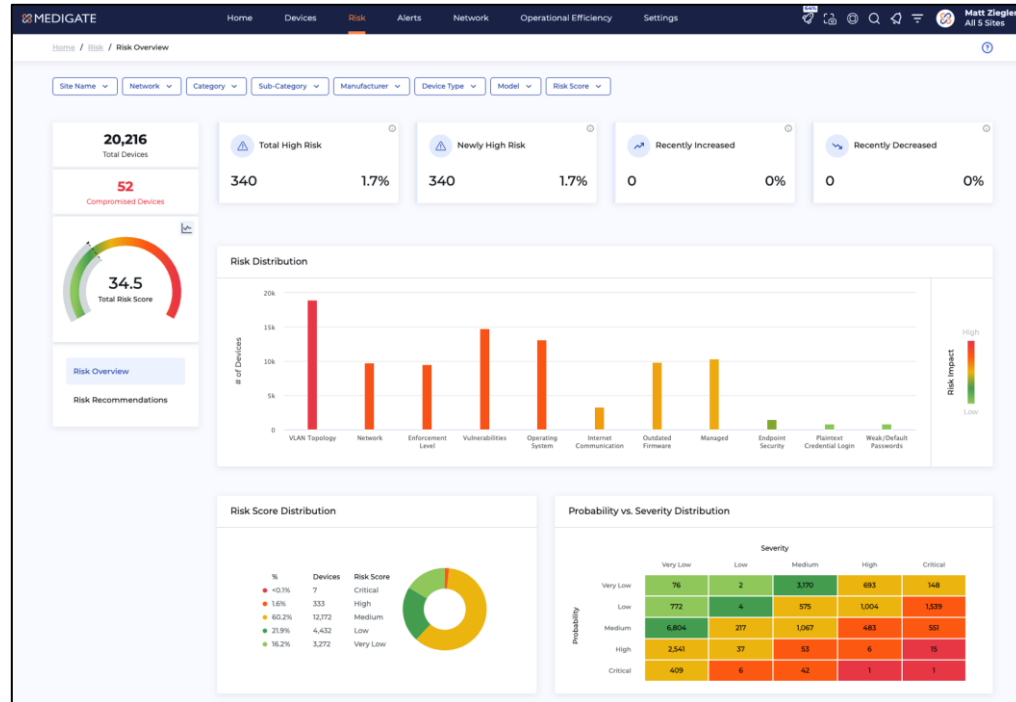
Asset Management



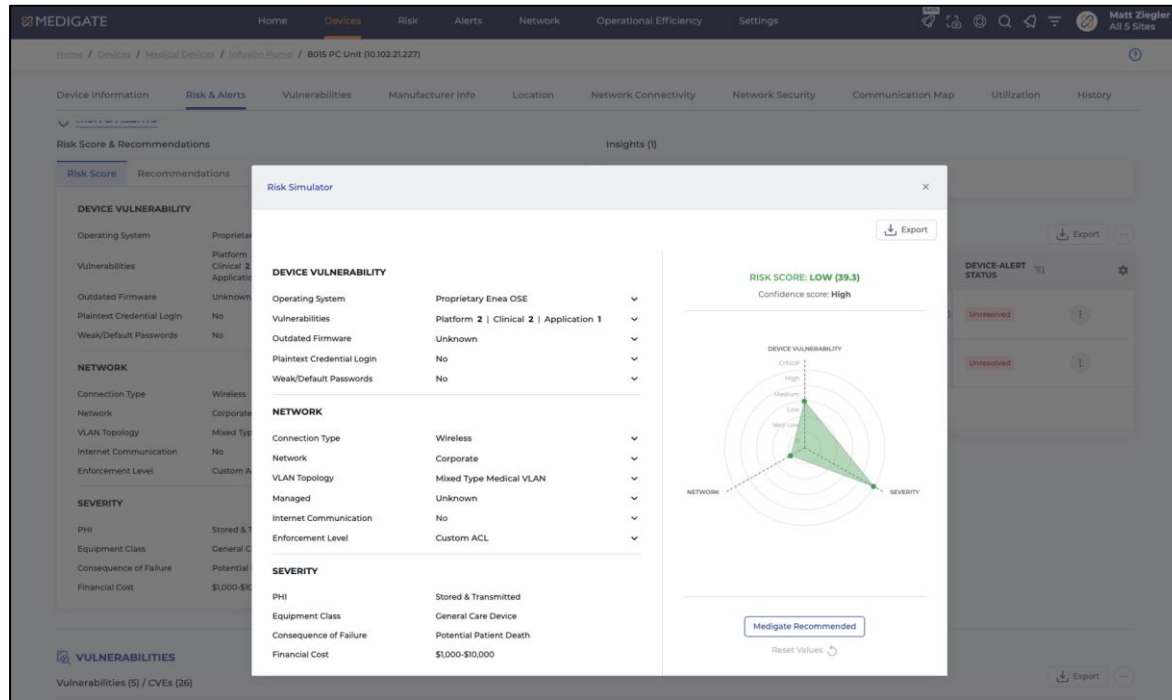
Auslastung



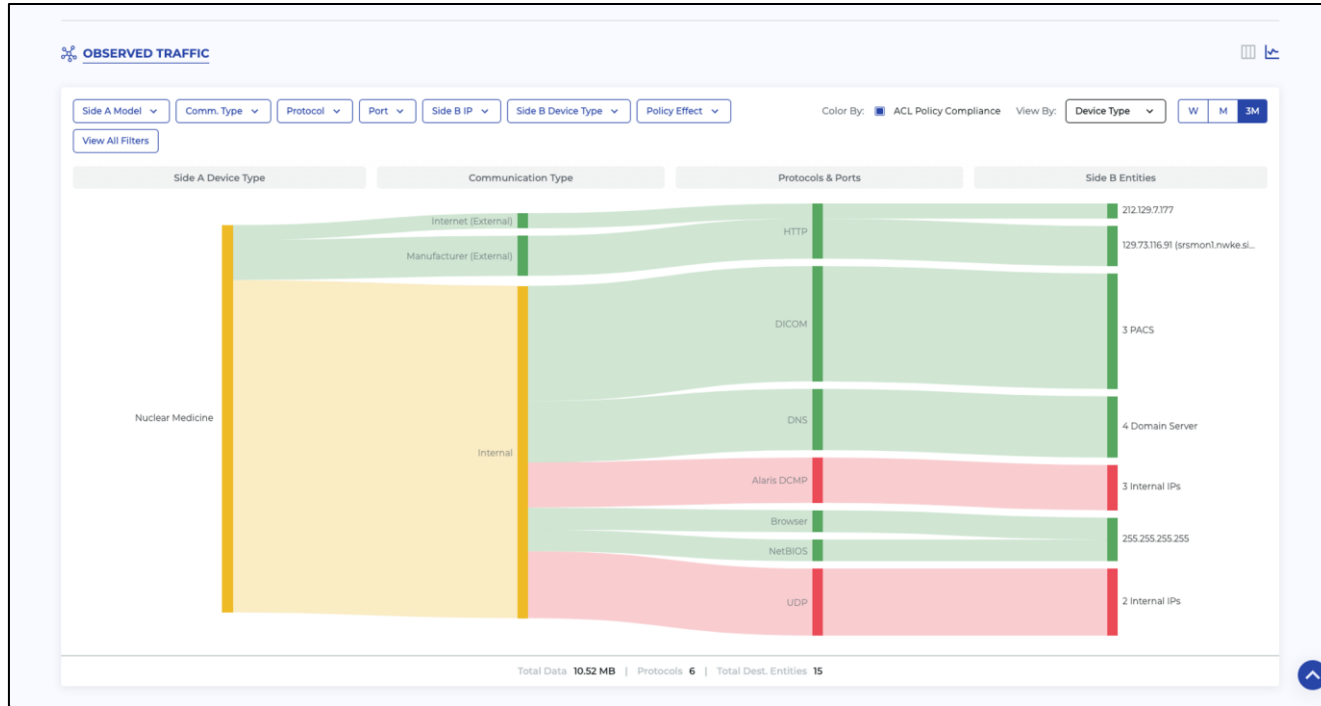
Schwachstellen- & Risikomanagement



Risikosimulationen



Überwachung - Anomalieerkennung



Sicherheitsrichtlinien

The screenshot displays the MEDIGATE ACL Enforcement interface. The top navigation bar includes links for Home, Devices, Risk, Alerts, Network (selected), Operational Efficiency, and Settings. The user is identified as Matt Ziegler, All 5 Sites.

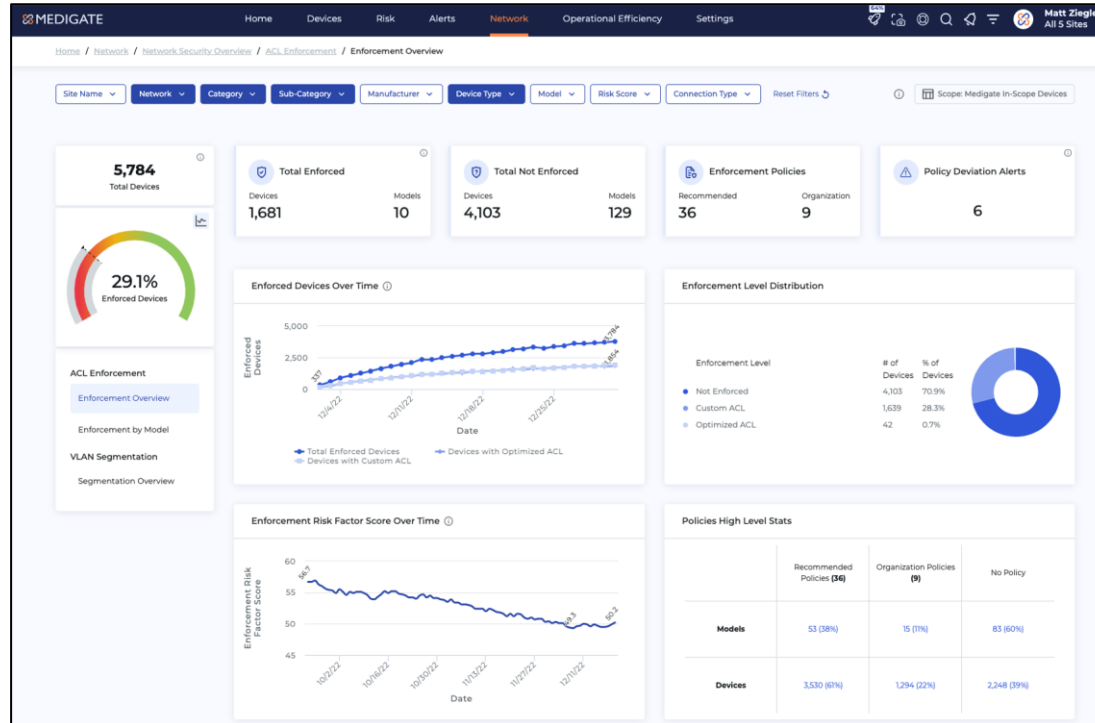
The main section is titled "MEDIGATE RECOMMENDED POLICIES" and shows a list of 38 recommended policies. The table columns are: POLICY ID, POLICY SOURCE, POLICY NAME, APPLIED MODELS, MATCHING DEVICES, POLICY RULES, and POLICY ACL. The table lists several policies, all of which are Recommendations.

A modal window titled "Policy 'Central Station - GE' - ACL" is open, showing a warning: "Alterations may be required to apply these rules to your network." The modal also displays the device type (Cisco > Wired Switch) and the HPE configuration rules:

```
1 remark Carescape ADT
2 permit tcp any any eq 11111
3
4 remark Carescape Alarm
5 permit udp any any eq 7001
6
7 remark Carescape MultiKM
8 permit tcp any any eq 5225
9 permit tcp any eq 5225 any
10
```

The modal includes a "Copy" button at the bottom right.

Vorfallsbehandlung



Integrationen

Visibility, Vulnerability Insights, and Threat Detection

Endpoint Detection



SIEM



Monitoring



Ticketing



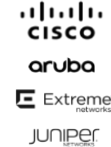
DHCP/DNS



Network Mgmt



Networking



MDM



Clinical Cyber Hygiene (CCH)

Patch Management



Vuln. Management



Network Security Management (NSM)

NAC



Firewalls



Clinical Device Efficiency (CDE)

Device Management



Clinical Eng.



Optimierungsvorschläge

