# CISCO ISE CYLERA



#### **Cylera and Cisco ISE Integration**

# Accelerate Network Access Control **Policy Creation**

Maximize Cisco ISE investments while improving healthcare IoT device visibility and security



## The Challenge

Network Access Control (NAC) solutions, such as Cisco ISE, are vital to ensure that only authorized devices within healthcare systems are granted access to network resources. However, in healthcare and clinical settings, most NAC solutions lack the depth of insight and context required to fully identify all healthcare IoT and connected medical devices and appropriately enforce appropriate device access control security policies.

Many healthcare IoT and connected medical devices present as undiscovered and umanaged on healthcare networks. As a result, NACs struggle to obtain and verify these types of unmanaged devices' software, firmware, and other details required to accurately enforce device access security policies.

Although NAC solutions can enable preventative protection and enforce efficient device authorization and segmentation policies, for healthcare IoT, NAC solutions require more details as to why and under what clinical conditions these systems should take specified action. This requires additional behavioral analytics, baseline device profiling, and an understanding of clinical requirements that complement existing NAC capabilities.

When factored against the range of medical device manufacturers, device and model types, specialized and proprietary protocols, and limited documentation, an integration between Cisco ISE and the Cylera platform becomes essential. The Cylera's platform's clinical risk assessment capabilities, combined with the ability to automatically create and share granular network segmentation security policies with Cisco ISE, ensures the right network access for the right devices at the right times for optimal healthcare network protection.

## The Integrated Solution

- Cylera has partnered with Cisco to deliver patented techniques and clinical context through its integration with Cisco Identity Services Engine (ISE).
- Cylera's healthcare-centric cybersecurity intelligence combines intimate knowledge of healthcare IoT device behavior. protocols, medical workflows, patient care, safety, and privacy standards with Cisco's networking and cybersecurity expertise.
- Cylera provides healthcare IT teams that administer Cisco ISE the enriched visibility and advanced capabilities required to automatically generate errorfree policies. The generated policies are seamlessly forwarded to Cisco ISE, where they are enforced automatically or after manual review. This minimizes errors and ensures consistent medical device access policy enforcement.

# **Integrated Solution Benefits**

- Enhanced Security: Cylera's detailed device profiling and risk analysis, combined with Cisco ISE's access control capabilities, strengthens the overall security posture, reduces vulnerabilities, and protects sensitive patient data.
- Improved Operational Efficiency: Automated policy creation and seamless enforcement save IT teams time and effort, allowing them to focus on strategic initiatives rather than on manual, repetitive tasks prone to human error.
- **Uninterrupted Patient Care:** With robust security and efficient operations, clinical workflows remain uninterrupted, enabling healthcare professionals to focus on delivering quality patient care.
- **Cost Savings:** By reducing the risk of cyber attacks and streamlining operations, the integration minimizes potential financial losses and optimizes resource allocation.

#### **How It Works**

Cylera's sensor is easily deployed to monitor network traffic through SPAN or tap ports on a switch. Connectivity to Cisco ISE and data sharing is through Cisco's Platform Exchange Grid (pxGrid).

- The Cylera sensor passively monitors network traffic, discovering and profiling IT, IoT, and connected medical device assets with zero disruption to patient care services and normal device operations.
- New and updated IT, IoT, and connected medical device identification data from Cylera is forwarded to Cisco ISE, updating ISE device inventory with granular device information based on a deep clinical understanding of device operational norms, workflows, and risks.
- Within Cylera, administrators can create Cisco TrustSec or dACL/SGACL policies, then automatically forward the policies to Cisco ISE.

			Summary
choose policy kind		~	KIND dACL PROFILE CANADA AND A
elect existing or create new profile		~	DEVICES 20 RULES 10
			NAC Profile Rules
create and edit rules		^	Syne New Syne New
Create egress rules:	Collapse Internal IPs to subnets:		SYNC TO NAC ON SAVE:
Collapse ports to ranges:	Require ports in rules:		OVERWRITE EXISTING
L nemit of any her 22 67 588 222		_	Delete Save
2 permit udp any host 52.100.222.39 3 permit udp any host 52.100.222.39			
4 permit udp any host 10.50.170.160			

 Once Cylea forwards the policies to Cisco ISE, the Cylera policies display in the Cisco Management Console.

				ty + Operations	· Policy	<ul> <li>Administratio</li> </ul>	n + Work Centers			License e	- prime		
Policy Set	a Profiling	Posture Client Provisioning	+ Policy I	Dements									
olicy S	ets + Cyl	lera Policy Set							Rese	t Policyset I	Rcoun	a Rea	-
	Status	Policy Set Name	Descri	ption	Cont	ditions			Alto	wed Protocol	is / Serv	er Sequence	
Search													
	0	Cylera Policy Set				Default Network	Access		D	fault Network /	lccess		
> Authe	ntication Pol	6cy (1)											
> Autho	rization Polis	cy - Local Exceptions											
> Autho	rization Polis	cy - Global Exceptions											
> Autho	rization Poli	cy - Global Exceptions											
> Autro	rization Poli	cy - Godell Exceptions					Results						
> Autro < Autro (*)	rization Poli rization Polic Status	cy - Guodal Exceptions cy (11) Rule Name	Con	Stors			Results Profiles		Security Groups			Hits	Acti
> Autho Autho Beach	rization Poli rization Polic Status	cy - Gaobal Exceptions cy (11) Rule Name	Con	Stons			Results Profiles		Security Groups			HIS	Acti
<ul> <li>Autho</li> <li>Autho</li> <li>Esenth</li> </ul>	rization Poli rization Poli Status	cy - Galoar Exceptions cy (11) Rule Name cylen_sgl070_bootmap_sue	Cont	Sions EndPaints cylerafe	top EQUALS	\$ cylera_sgt010	Results Profiles (+Pemblocess)		Security Groups		•	HIS	Acti
> Autho Autho Econth	rization Pole rization Pole Status ©	cy - olocar Exceptions cy (11) Rule Name cylera_sgl015_bontsrap_rule cylera_sgl015_bontsrap_rule	Cont E	<b>Stons</b> EndPoets cylenife EndPoets cylenife	NP EQUALS	\$ cylena_agt510 \$ cylena_agt5009	Results Profiles *PerniAccess *PerniAccess	*	Security Groups cylera_sg010 cylera_sg009		•	HIS 0	Acti
> Autho	rization Poli rization Poli Status @ @ @	cy-culou Exceptions gy (11) Rule Name cylera, sgl010, Jontima, Jule cylera, sgl020, Jontima, Jule cylera, sgl020, Jontima, Jule	Cont Lu Lu	Bons EndPorts cylerafe EndPorts cylerafe EndPorts cylerafe	THE EQUALS	S cylera_sg010 S cylera_sg009 S cylera_sg008	Results Profiles IPerniAccess IPerniAccess	*	Security Groups opters, sp010 opters, sp000 opters, sp000		•	HIS 0	Acti
> Autho	rization Poli rization Poli Status @ @ @	cy-cubble Exceptions gy (11) Rule Name cylera, sg009, Joethinap, sile cylera, sg009, Joethinap, sile cylera, sg009, Joethinap, sile cylera, sg007, Joethinap, sile	Contra In In	Bons EndPoets operade EndPoets operade EndPoets operade EndPoets operade	THE EQUALS	5 cylera_sg010 5 cylera_sg009 5 cylera_sg008 8 cylera_sg007	Results Profiles (*Pernikkons) (*Pernikkons) (*Pernikkons) (*Pernikkons)	*	Security Groups optex_spt010 optex_spt000 optex_spt000 optex_spt000		•	Hts 0 0 0	A09

### Summary

The Cylera and Cisco ISE integration enhances healthcare IoT and medical device security by providing enriched visibility and automated policy enforcement. Cylera profiles connected devices, sharing detailed insights with Cisco ISE to enable precise medical device identification and security management. The integration automates medical device security policy creation and deployment, reducing manual effort and minimizing errors. It also supports dynamic network segmentation, isolating devices based on risk levels and operational needs. For healthcare organizations, the integration ensures robust security, uninterrupted clinical workflows, and compliance with regulatory standards such as HIPAA and HITECH in the US, and NIS, CAF, DSPT, and GDPR in the UK. By safeguarding sensitive patient data and streamlining operations, the Cylera and Cisco partnership helps ensure secure, reliable, high-quality patient care.

Cylera provides the easiest, most accurate and extensible platform for healthcare IoT intelligence and security to optimize patient care, service availability, and cyber defenses across diverse connected medical device and healthcare environments. The Cylera platform accurately discovers, categorizes, assesses, and monitors known and unknown assets with high fidelity to deliver unparalleled asset inventory, usage telemetry, risk prioritization, analytics, and guided threat remediation. Cylera integrates with popular IT and healthcare systems to allow organizations to advance cyber program maturity, increase operational efficiency, mitigate cyber threats, and enable compliance readiness.



www.cylera.com