



**Compliance
Engine
Difference**



Who Is NeQter Labs?

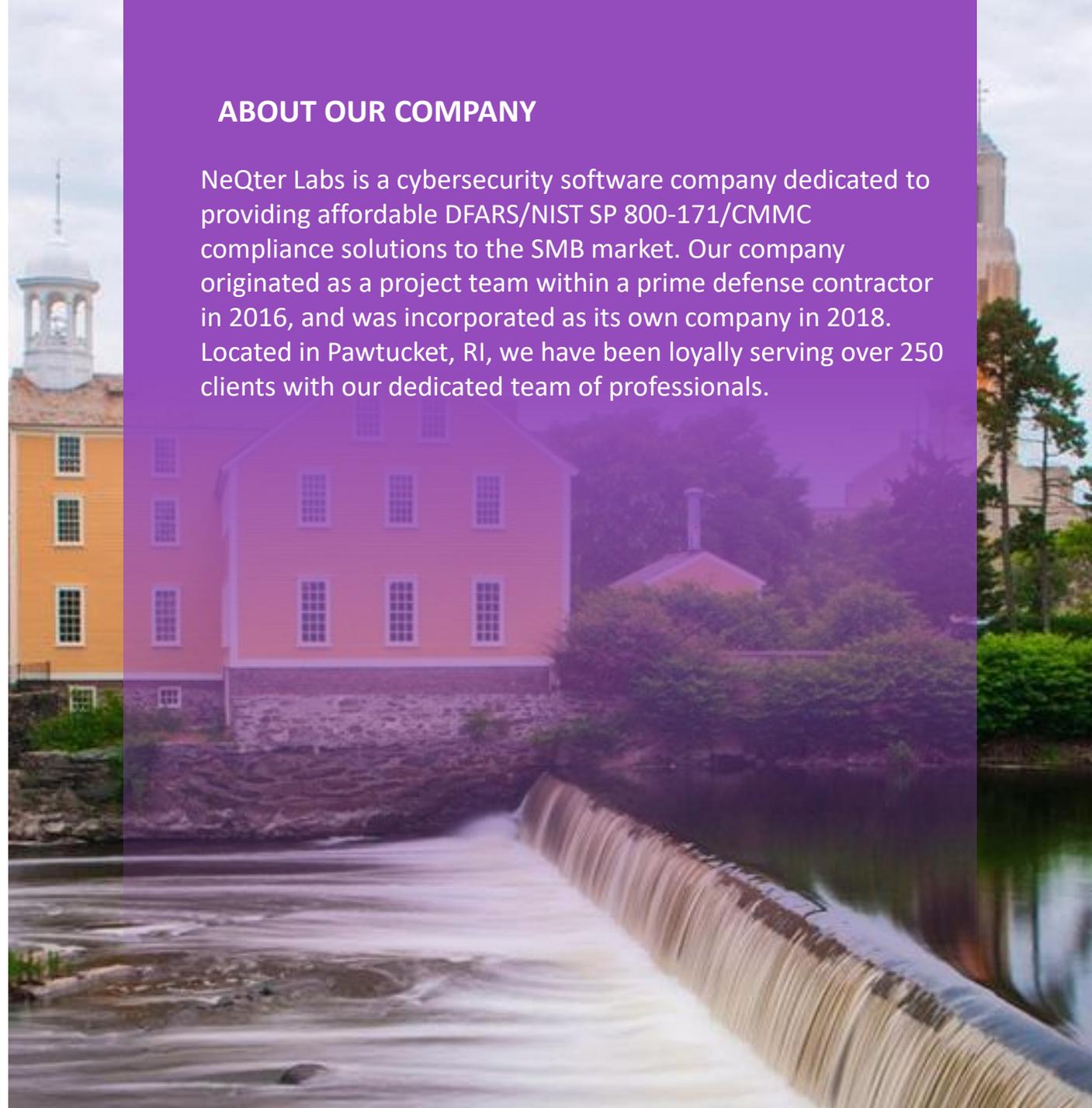
ABOUT OUR PLATFORM

The NeQter Labs Compliance Engine combines multiple tools into a single solution, providing you with a global view of your company's network. Our platform combines Security Incident Event Management (SIEM), active alerting, inventory, and vulnerability scanning. As our platform is designed for SMB, it is easy to deploy and use, with many preconfigured dashboards and alerts for established firewall, networking, and OS vendors.



ABOUT OUR COMPANY

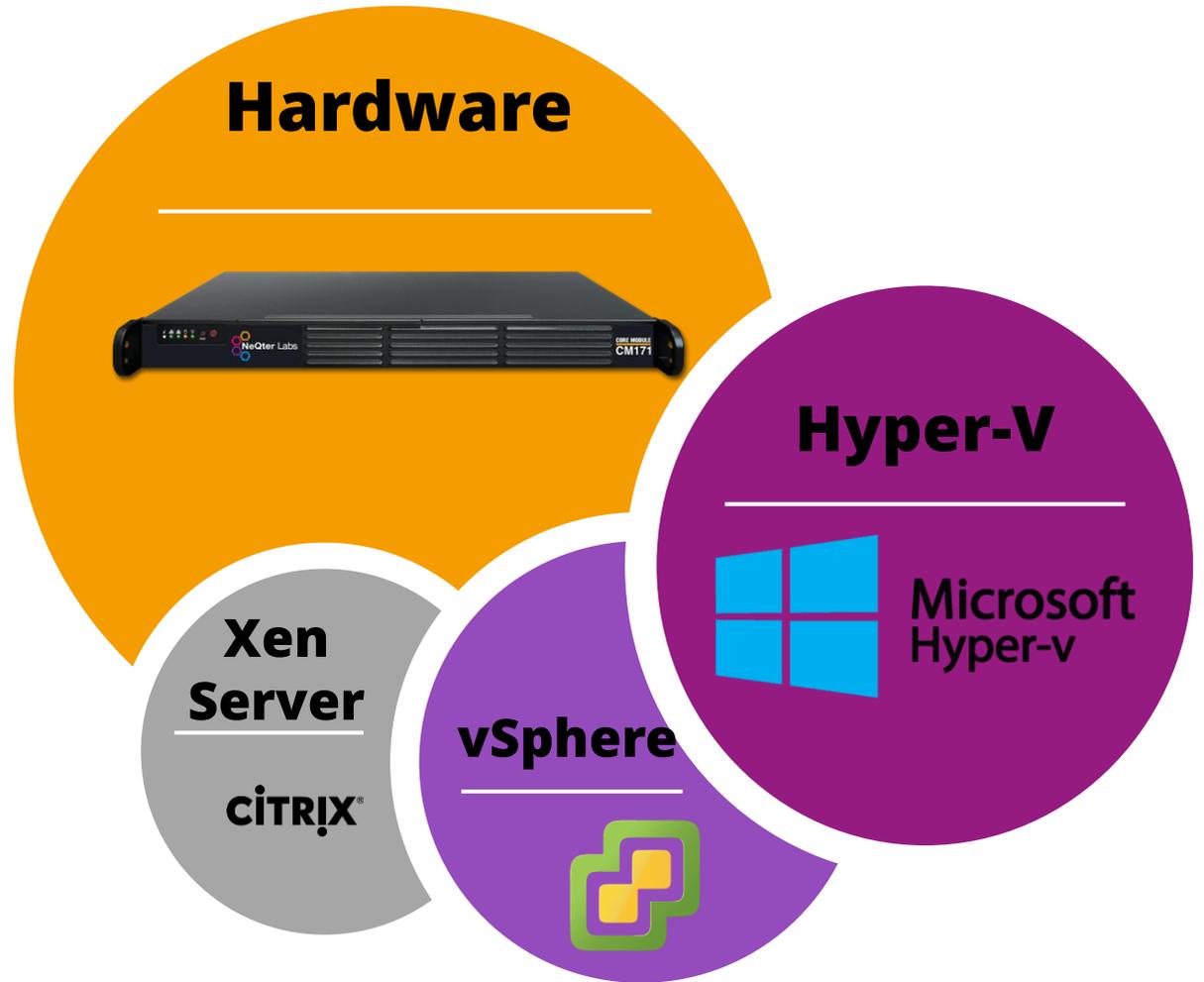
NeQter Labs is a cybersecurity software company dedicated to providing affordable DFARS/NIST SP 800-171/CMMC compliance solutions to the SMB market. Our company originated as a project team within a prime defense contractor in 2016, and was incorporated as its own company in 2018. Located in Pawtucket, RI, we have been loyally serving over 250 clients with our dedicated team of professionals.



How is NeQter Labs delivered?

The Compliance Engine is either:

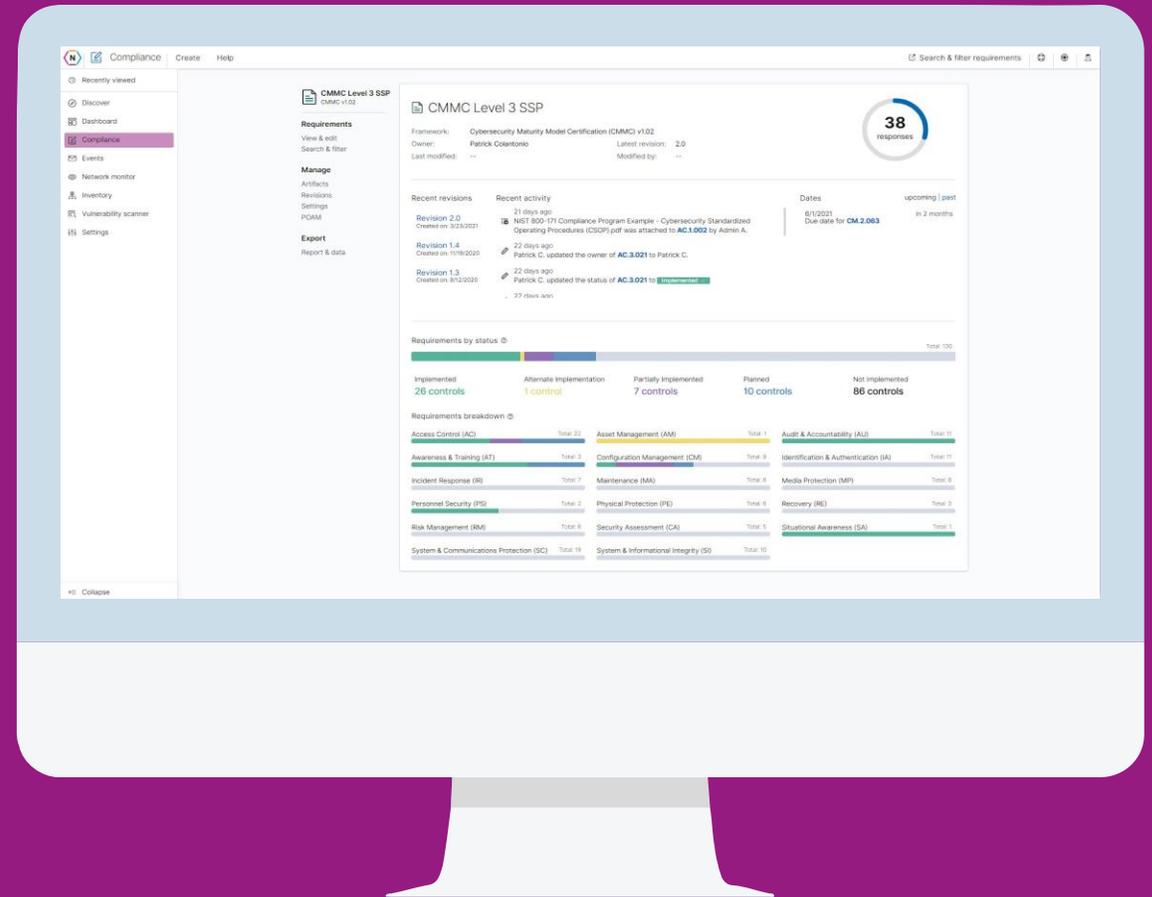
- delivered on a powerful 1U server appliance that has enterprise grade solid state storage with built-in redundancy. The hardware also offers built-in TPM encryption for securing data-at-rest, as well as 10G ports to prevent potential logging bottlenecks.
- installed as a dedicated virtual machine on supported hypervisor vendors.



System Security Plan Builder

Compliance Simplified

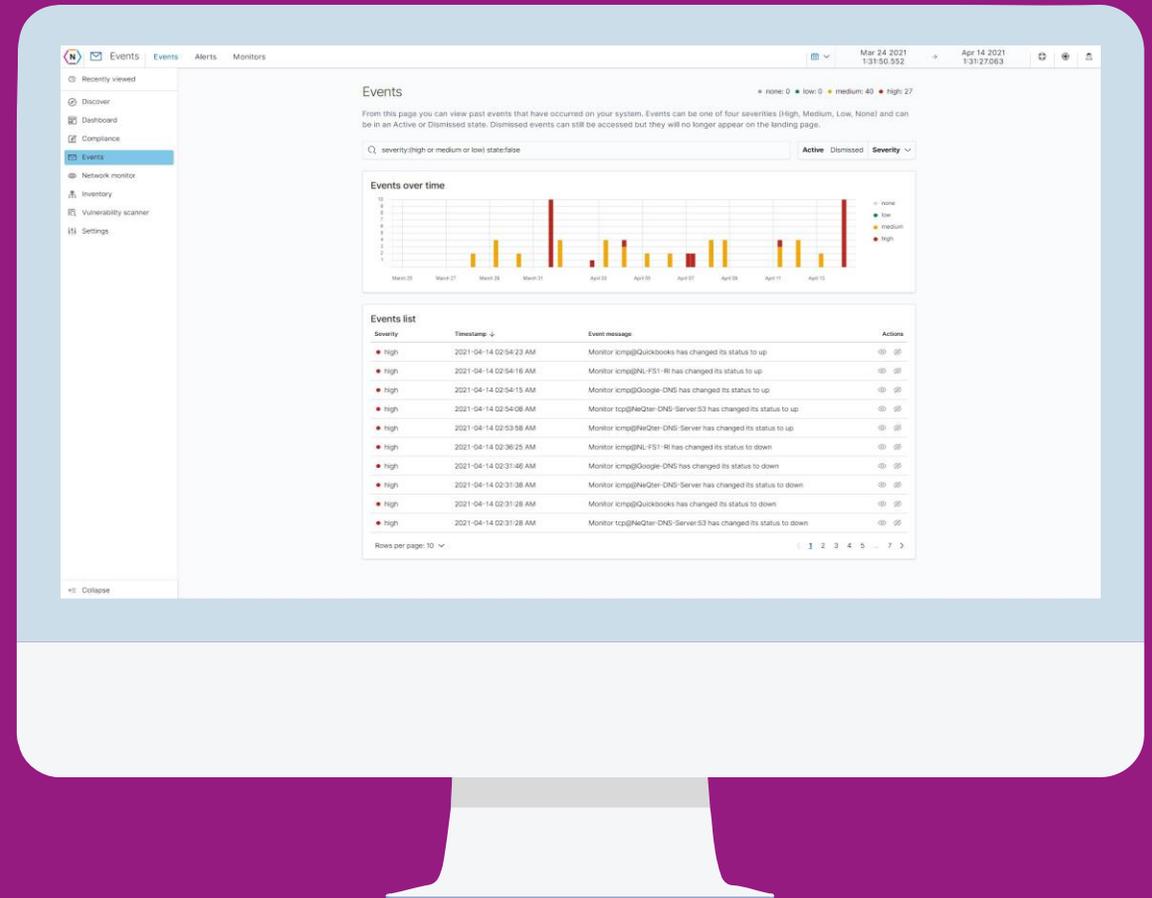
- Designed to meet requirements for DFARS, NIST SP 800-171, and CMMC
- Assists in the creation of both the System Security Plan and Plan of Action and Milestones for both NIST SP 800-171 & CMMC



Active Alerting

Receive live events and alerts in real-time

Leverage a library of pre-configured dashboards and alerts that provide you actionable data on day one.



Network monitor Hosts Monitors Refresh every 1 minutes

Recently viewed Discover Dashboard Compliance Events Network monitor Inventory Vulnerability scanner Settings

Monitors

Create new host

On this page you can view the current status of every service monitored by NeQter. Monitors that have the 'Alert' field checked will send an email to the defined recipients when its state changes

Device	Status	Name	Address	Type	Port	Interval	Alert
NL-FS1-RI	Up	Ping	nl-fs1-ri.ad.neqterlabs.com	icmp	--	@every 1s	<input checked="" type="checkbox"/>
Localhost	Up	Up status	172.16.5.100	icmp	--	@every 5s	<input checked="" type="checkbox"/>
Google-DNS	Up	Connectivity	google.com	icmp	--	@every 1s	<input checked="" type="checkbox"/>
Quickbooks	Up	Test	www.quickbooks.com	icmp	--	@every 5s	<input checked="" type="checkbox"/>
NeQter-DNS-Server	Up	DNS Server	172.16.0.100	tcp	53	@every 10s	<input checked="" type="checkbox"/>
NeQter-DNS-Server	Up	--	172.16.0.100	icmp	--	@every 10s	<input checked="" type="checkbox"/>
Internet-Connectivity	Up	--	8.8.4.4	icmp	--	@every 10s	<input checked="" type="checkbox"/>
NL-FS1-RI	Down	SMB	nl-fs1-ri.ad.neqterlabs.com	tcp	445	@every 5s	<input checked="" type="checkbox"/>
Localhost	Down	Syslog	172.16.5.100	tcp	514	@every 15s	<input checked="" type="checkbox"/>
Localhost	Down	NeQter	172.16.5.100	tcp	5000	@every 10s	<input checked="" type="checkbox"/>

Rows per page: 10 < 1 2 >

Inventory Overview All computers Inventory Configuration Manage

Recently viewed Discover Dashboard Compliance Events Network monitor Inventory Vulnerability scanner Settings

DESKTOP-KAFPIP7 XML

Administrative data

Category	Item	Value
Hardware	Connected user	SHouston
Software	OS Name	Microsoft Windows 10 Pro
Network	OS Version	10.0.18362
Devices	Architecture	x86 64 bit
Configuration	Windows user	ldepartment
Miscellaneous	Windows license	00330-80000-00000-AA895
	Windows key	VK7JG-NPHTM-C97JM-9MPGT-3V66T
	Swap	21424
	Memory	16384
	Ulid	03000200-0400-0500-0006-000700080009
	Domain	ad.neqterlabs.com
	IP address	WOL
	User agent	OCS-NG_WINDOWS_AGENT_v2.4.0.0
	Last inventory	12/22/2019 14:47:14.47:48
	Last contact	12/23/2019 10:35:10.35:44

AGENT

REGISTRY

Key name Key value

Network Monitoring & Inventory

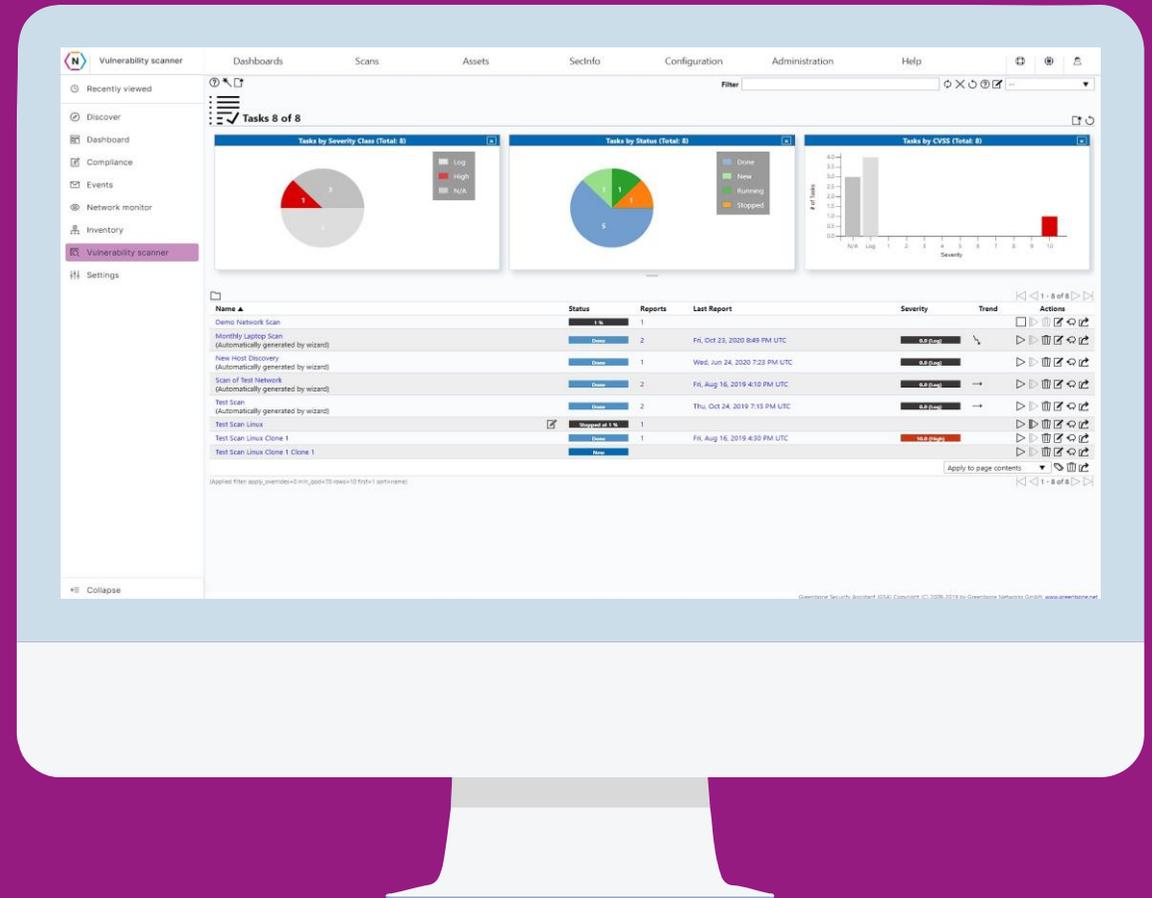
Real Time Visualizations and Reporting

- Actively tracks events generated from endpoints
- Tracks user activity on the network
- Automated baseline asset inventory

Vulnerability Scanning and Reporting

Compare against recognized vulnerability databases

Vulnerabilities are identified throughout all areas of the environment, from networking equipment to user endpoints and all connected devices.



Average Hours Spent Per Week

How many hours are you spending on your toolstack?

20hrs

Current Solution



Security Incident Event Management (SIEM), active alerting, inventory, and vulnerability scanning managed in **separate, individual platforms**.



NeQter Labs Compliance Engine

Security Incident Event Management (SIEM), active alerting, inventory, and vulnerability scanning combined into a **single platform**.

5hrs

Why NeQter Labs?

What separates NeQter Labs in this market is our expertise of DFARS, NIST and CMMC and how our application translates into these different compliance frameworks in a simple, affordable and comprehensive way for small and medium sized businesses.

Competitors include:



NeQter Labs Pricing

All future feature updates and support included.

Microbusiness	Tier 1	Tier 2	Tier 3
Contact Us	\$500/mo	\$800/mo	\$1210/mo
Under 10 assets	10 – 100 logging assets	100 – 500 logging assets	500 – 1500 logging assets
Because companies of this size do not fit into our traditional model, please feel free to contact NeQter Labs to discuss working with one of our trusted partners.	<ul style="list-style-type: none">▪ \$1000 installation fee▪ \$2500 hardware purchase (VM supported)▪ \$21,500 total cost for 3-year commitment	<ul style="list-style-type: none">▪ \$1600 installation fee▪ \$5000 hardware purchase (VM supported)▪ \$35,400 total cost for 3-year commitment	<ul style="list-style-type: none">▪ \$2420 installation fee▪ \$7500 hardware purchase (VM unsupported)▪ \$53,480 total cost for 3-year commitment

Thank you for viewing the presentation.



neqterlabs.com

(401) 608-6522

pat@neqterlabs.com