NeQter Labs

Compliance Engine Difference
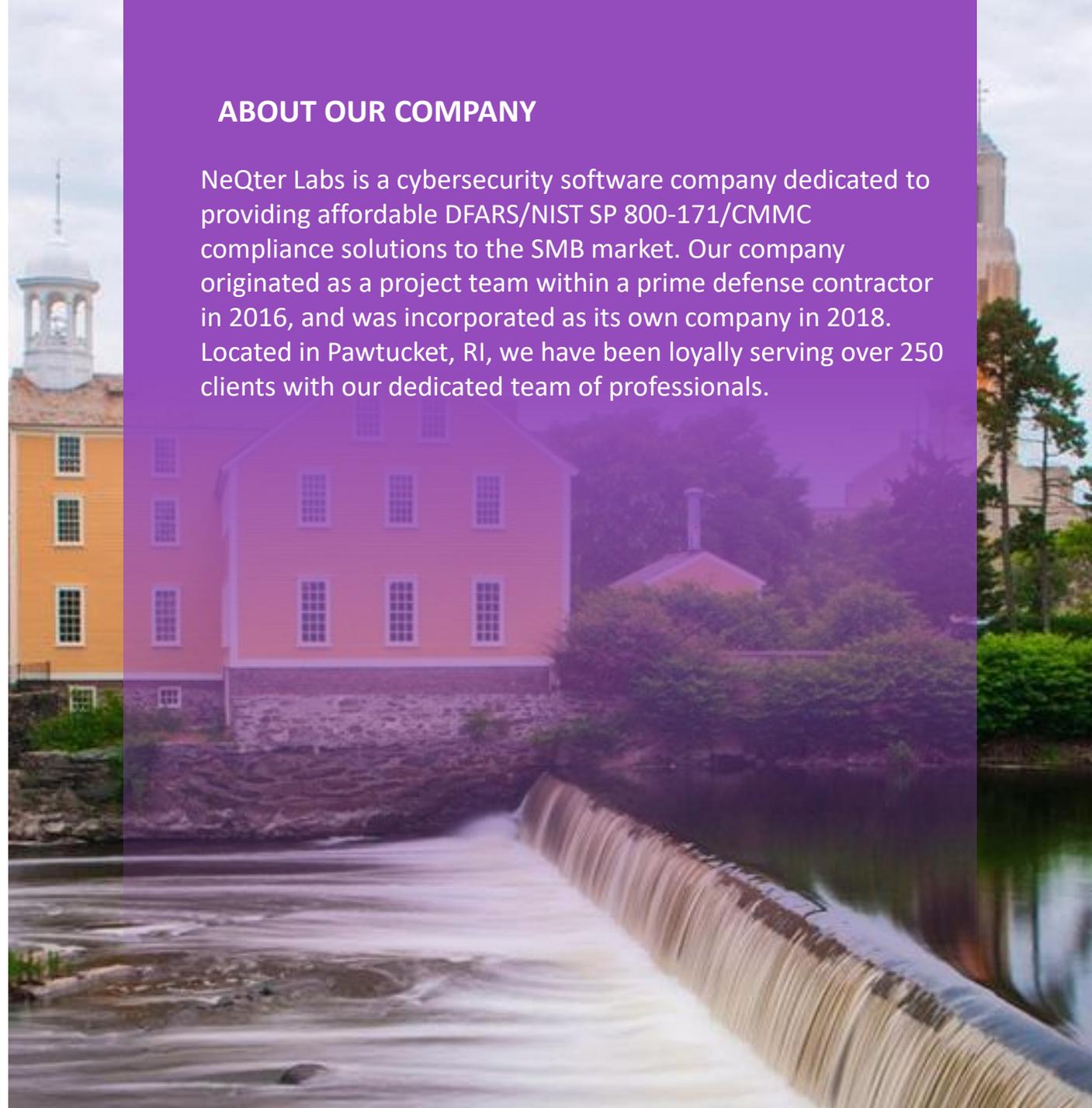
Who Is NeQter Labs?

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?
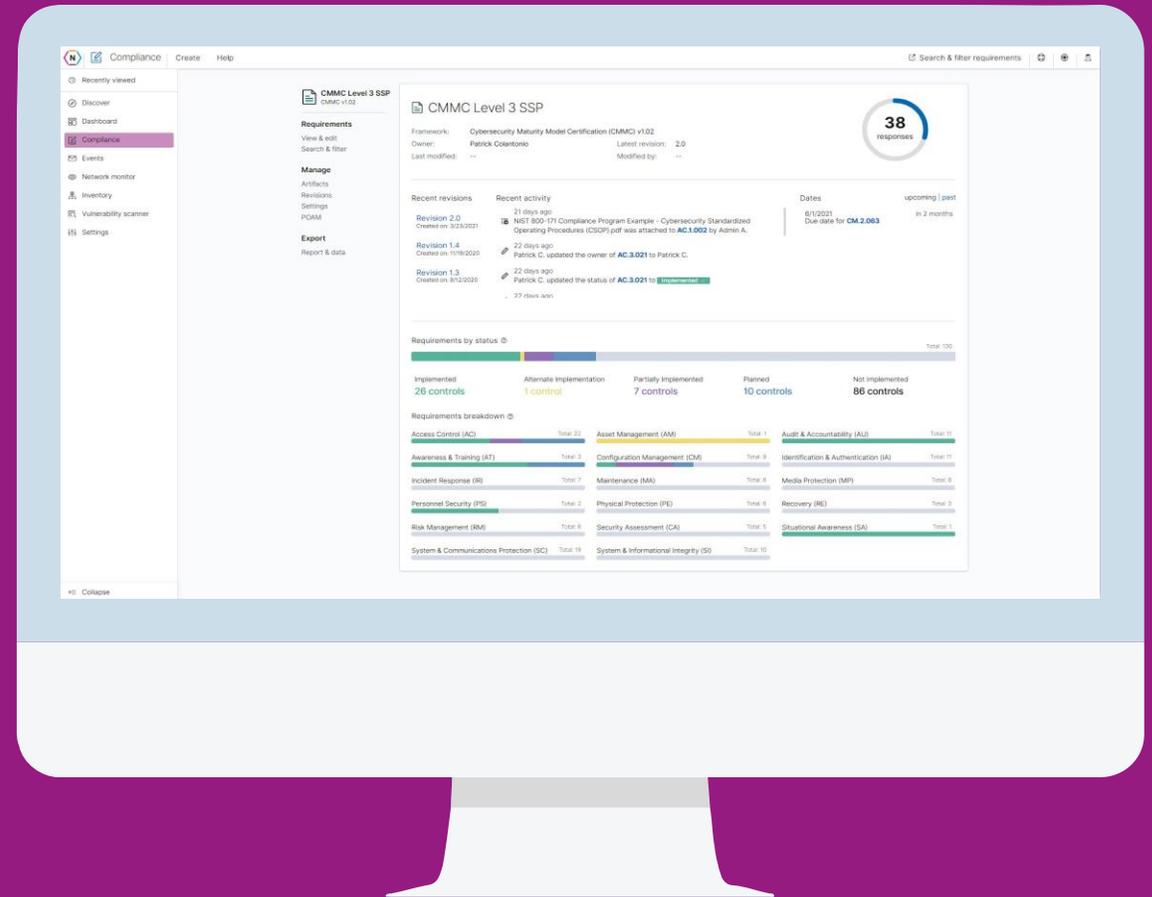
The Compliance Engine is either:

- 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.

Hardware

Hyper-V

Microsoft Hyper-v

Xen Server

CITRIX®

vSphere
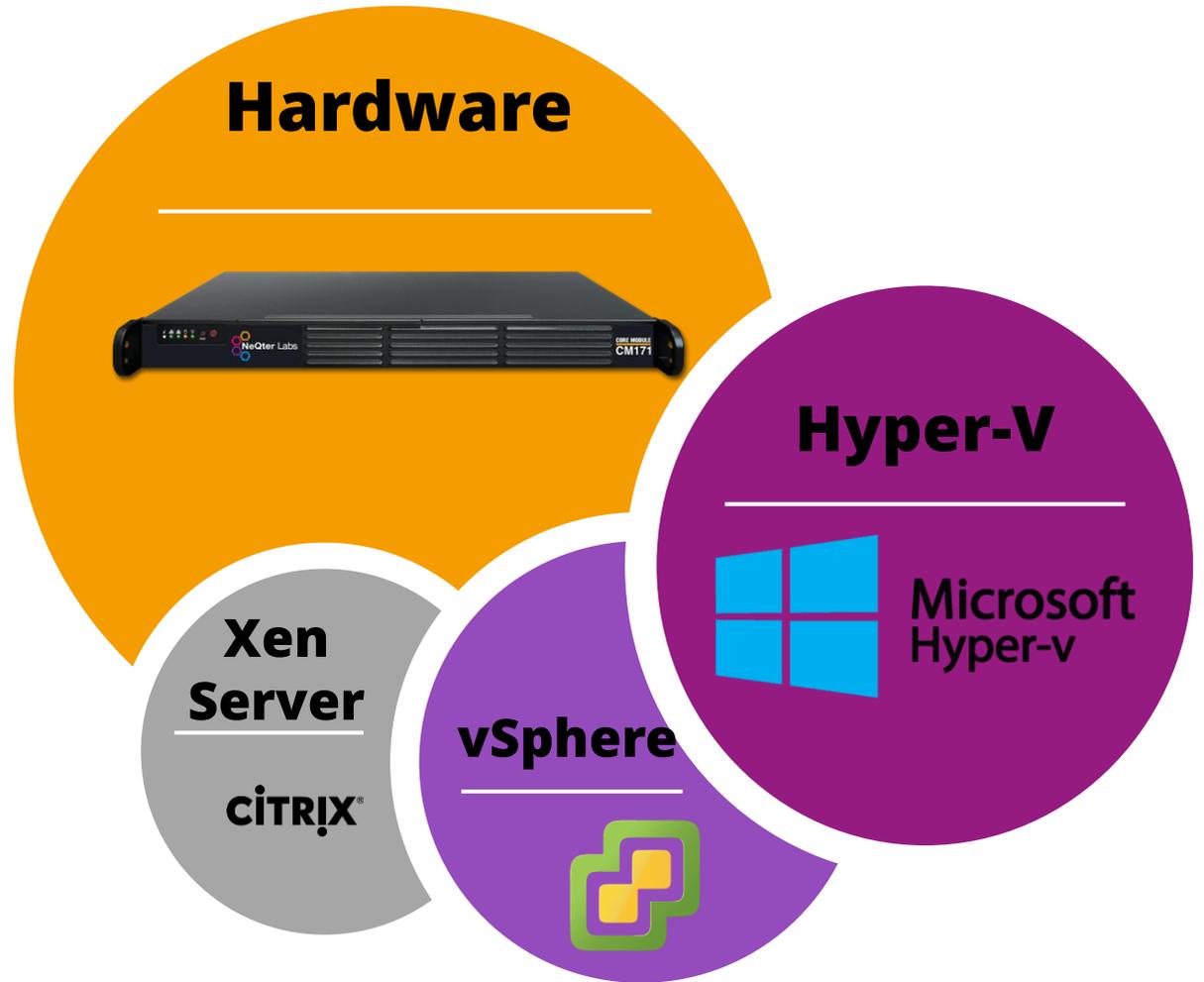
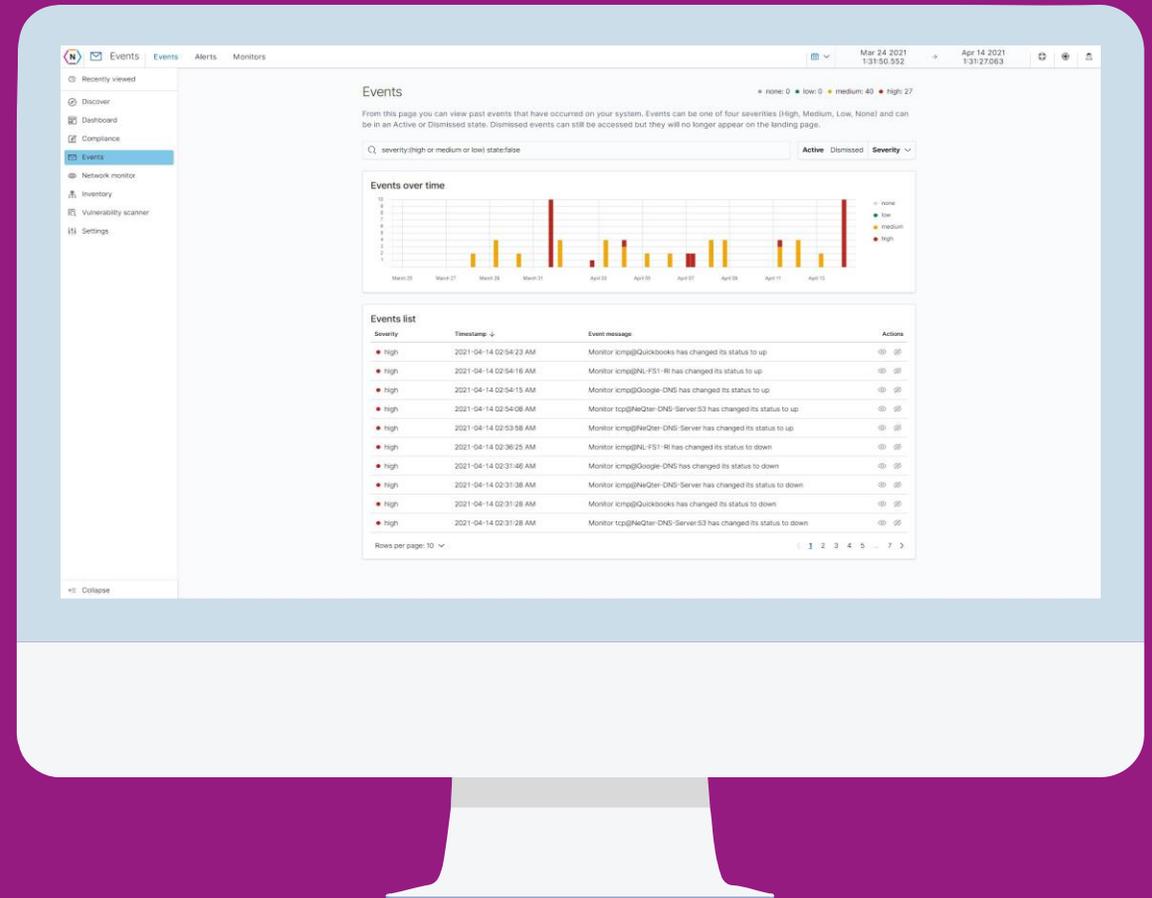# System Security Plan Builder

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

Security Information and Event Management (SIEM)

Real Time Visualizations and Reporting

Intuitive interface allows for fluid navigation and drill down capabilities in just a few clicks.

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 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.
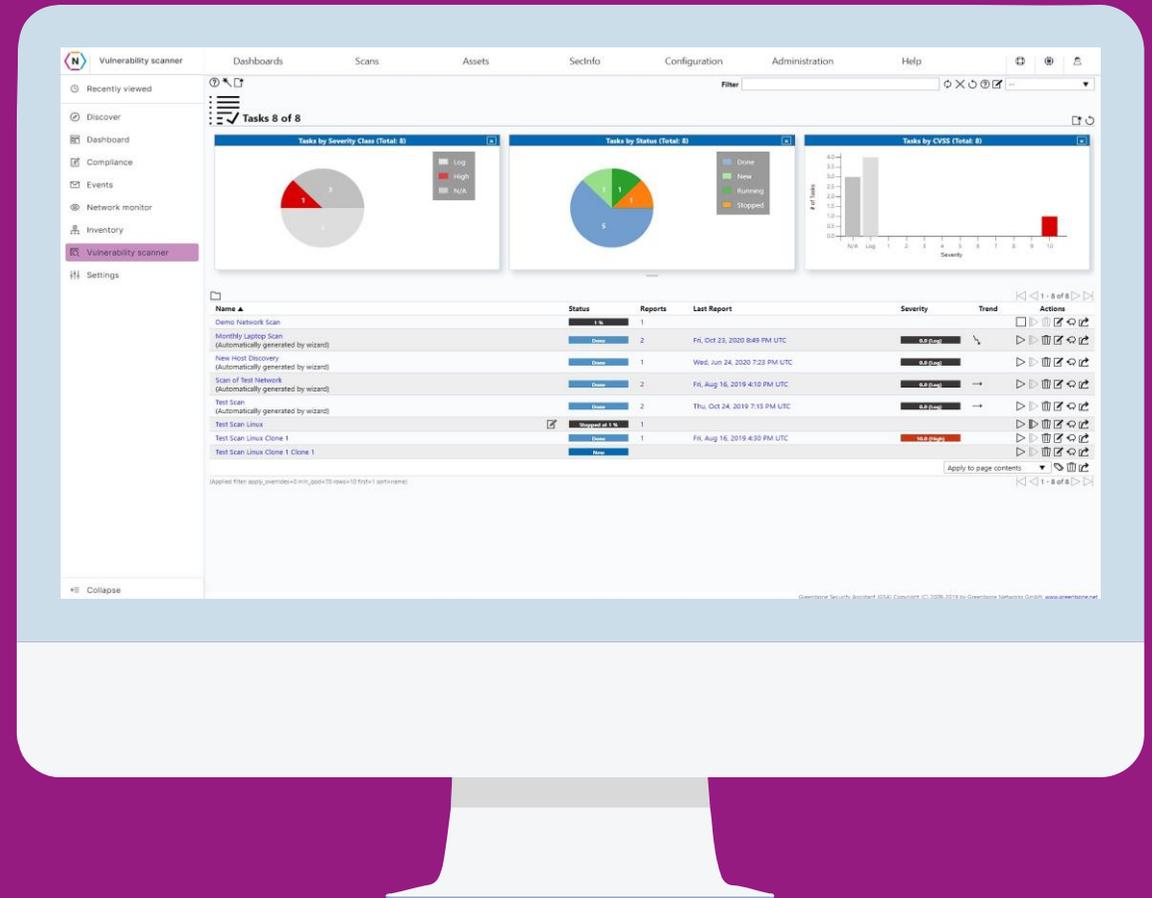
Average Hours Spent Per Week

How many hours are you spending on your toolstack?

20hrs

NeQter Labs Compliance Engine

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

5hrs

Current Solution

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

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.	▪ **$1000** installation fee ▪ **$2500** hardware purchase (VM supported) ▪ **$21,500** total cost for 3-year commitment	▪ **$1600** installation fee ▪ **$5000** hardware purchase (VM supported) ▪ **$35,400** total cost for 3-year commitment	▪ **$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