# PRICING SHEET

## CYBER SECURITY

In 2018, NSI protected its clients by recommending measures that worked well for blocking most cyber attacks. We did things like patching, anti-virus software, and firewalls because they worked just fine. However, since hackers are getting more sophisticated and prevalent by the day, we decided it was time to upgrade our approach to protection. We researched the wide landscape of potential security partners and we landed on two top-notch companies, Continuum, and Webroot, leading cyber security technology companies who offer every distinct layer our clients could possibly need to remain safe from bad people.

## SECURITY AWARENESS TRAINING (SAT)

*Layer Goal - Prevent your staff from accidentally letting cyber criminals get in.*

Web-based lessons makes Security Awareness Training (SAT) easy to deploy, use, and manage.

Includes trainings such as phishing simulations, courses on IT and security best practices, data protection and compliance training.

SAT prepares the frontline protectors of your organization: your people.

nsi

# PRICING SHEET

CYBER SECURITY

## PROFILE AND PROTECT

*Layer Goal - Prevent cyber breaches by using advanced technologies that leverage machine learning and artificial intelligence to match the sophistication and agility of today's worst cybercriminals.*

Includes:
- Continuum's Risk Scoring and Threshold alerts
- Webroot's DNS Protection
- Webroot's SAT

### Risk Scoring and Threshold Alerts

Continuum's security experts monitor threat vector profiles, like ransomware and data theft, and these profile algorithms are updated every 5 minutes. Profiles are pitted against clients' system configurations in order to generate risk scores. When a given client's risk score surpasses suggested industry benchmarks, NSI gets alerted and this, in turn, enables NSI to adjust systems and devices to maximize protection in real time.

In short, Continuum's risk scoring keeps clients defenses as agile as hackers are.

### Webroot® DNS Protection

DNS protection is a quick and highly effective way to secure the DNS protocol connection against cyber attacks. With advanced reporting on more than 80 URL categories, NSI can tailor web usage policies to client organization's unique needs and thereby reduce the risk of breach.

nsi

# PRICING SHEET

CYBER SECURITY

## ENDPOINT PROTECTION

*Layer Goal - If a hacker manages to break in, then what? This is where endpoint protection comes in; it's a technology to identify the threat quickly and stop it. We have two options here, a best-in-class technology by Webroot, or an enterprise-level technology by Continuum that also includes SOC (Security Operations Center) support.*

### Webroot Endpoint

Unlike traditional antivirus, which only has one opportunity to detect and stop a given threat, Webroot protection works in multiple stages. First, it attempts to prevent malware from infiltrating the system. If malware does get through, Webroot protection works to stop it before it can execute. Should it execute (this might happen in cases of brand-new, never-before-seen malware), Webroot protection will journal the file's activities and undo its changes to local drives, once it's determined to be malware.

Webroot threat intelligence and BrightCloud services back all Webroot protection solutions, and are trusted by 85+ network and security vendors worldwide to enhance their own solutions. Webroot has been using machine learning to classify and categorize threats since 2007. Our advanced 6th generation machine learning architecture processes threat data sourced from
a variety of vetted sources, as well as our own real-world customers and users of our technology partners' solutions.

### Continuum's Detect & Respond Endpoint

The most complete and sophisticated solution for threat detection and attack remediation. Powered by SentinelOne, it provides SOC-supported endpoint monitoring, building on foundational security to rapidly identify and halt even the most troublesome attacks, minimizing harm and reducing risk to client environments. SentinelOne offers a $1M ransomware warranty.

nsi

# PRICING SHEET

CYBER SECURITY

## NETWORK & COMPLIANCE

*Layer Goal - If your industry has heavy compliance requirements, this solution is our most advanced and capable for meeting those types of needs.*

This is the most comprehensive solution for businesses that need to meet critical compliance requirements. It utilizes industry-leading SIEM technology to collect, analyze and correlate information from network devices, endpoint logs and threat intelligence feeds. This enables you to provide alerting, reporting and log retention for common regulatory requirements, such as daily reports and threat analysis outlines for three regulatory standards: PCI, HIPAA and NIST 800.

| | Total Care Customers | Non-Total Care Customers |
|---|---|---|
| Security Awareness Training | ✓ | *$5/user + $20/end-point* |
| Risk Scoring & DNS Protection | ✓ | |
| Endpoint Protection | *$15/user* | |
| Endpoint Protection with SOC | *$15/end-point* | *$20/end-point* |
| Network & Compliance Protection | *Assessment required* | *Assessment required* |

nsi