Custom System Hardening

By

Improving Business Profitability and Efficiency®

Summer 2021

Table of Contents

1.0 Overview: Custom System Hardening

1.1 Introduction to Clarity Consulting Corporation

Clarity Consulting Corporation is uniquely built from the ground up to efficiently tackle and solve the wide array of technical, procedural and bureaucratic challenges which are inherent obstacles to effective, rapid consulting success in large-scale distributed enterprise IT network environments.

Specifically, our team has gained the following advantages from our years of domestic and international information security consulting work:

- World-class, extraordinarily skilled technical talent;
- Masterful understanding of large-scale enterprise IT networks from consulting experience gained in both governmental as well as multiple U.S. Fortune 100 mega-corporations, with our largest consulting customers to date exceeding 1 million user accounts, 100,000 servers, 50,000 routers and switches, thousands of firewalls, 70 datacenters in 15 countries, and company facilities in over 120 countries around the world;
- Unmatched experience in rapidly solving complex problems in large scale enterprise IT network environments, such as investigating and mitigating sophisticated, state-sponsored, targeted APT malware cases, and;
- Unequalled ability to rapidly reduce risk across an enterprise through our primary focus on configuration and network architectural design changes, backed by our secondary focus on the application of third-party point solutions[2].

Why is all this important? Our extensive hands-on enterprise consulting expertise gained from hundreds of consulting engagements drives our creative ingenuity and our constant development of cutting-edge, cost-effective cyber security solutions. It also inspires and powers our world-class classroom instruction expertise. For more information about the latter, see Section 3.2, *"Training"*.

1.2 Applications for our Custom System Hardening Technology

Clarity Consulting Corporation has engineered a complementary suit of custom system hardening technologies designed for use in large-scale IT enterprise networks that are adaptable to smaller IT network environments.

Our suit of custom hardening technologies provides selectable levels of cyber security assurance for legacy or stranded operating systems, applications, utilities and databases which cannot be easily or cost-affordably upgraded, migrated or replaced.

[2] Clarity Consulting is strictly vendor neutral. We do not sell third-party hardware or software solutions. However, if asked we may make recommendations of two or more roughly equivalent 3rd-party solutions along with the pros and cons of each.

2.0 How Our Technology Works

Our custom system hardening technology consists of 12 separate, independent hardening technologies which Clarity Consulting deploys separately or in combination together.

Based on our extensive system hardening experience, Clarity Consulting applies these 12 components in various combinations to match each customer's unique needs for cyber security risk reduction or risk assurance, application functionality, solution transparency, implementation costs, solution maintenance overhead, return-on-investment goals and more.

These 12 individual components of our custom system hardening service are individually discussed next.

2.1 System Isolation

The cyber security defense posture of selected portions of an enterprise IT network can often be significantly improved by *compartmentalization*, e.g. placing selected groups of systems into a state of reduced access or semi-isolation from other groups of systems or the larger IT network.

When designed and implemented optimally, compartmentalization can attain high levels of financial return-on-investment. This is not only because of its substantial real-world cyber security risk reductions, but also because of sizeable reductions in the total cost of network ownership coupled with often improved network reliability and functionality.

In short, compartmentalization can often achieve large cyber security risk reductions at a cost-benefit effectiveness ratio that can be difficult for other system hardening techniques to match.

Clarity Consulting's security team uses our substantial experience to recommend the right mixture of individual hardening techniques for each system or group of related systems which results in the maximum possible risk reductions for the least possible expenditures of capital costs and network downtime. As a side benefit, our process produces findings and recommendations that result in greater IT network performance, functionality, and reliability gains at a reduced total cost of IT network ownership, in addition to providing inherently high levels of information security risk reduction or assurance.

See Figure 1 on the next page for a representative before-and-after depiction of our system isolation tactics using the exact same physical network equipment in each case.

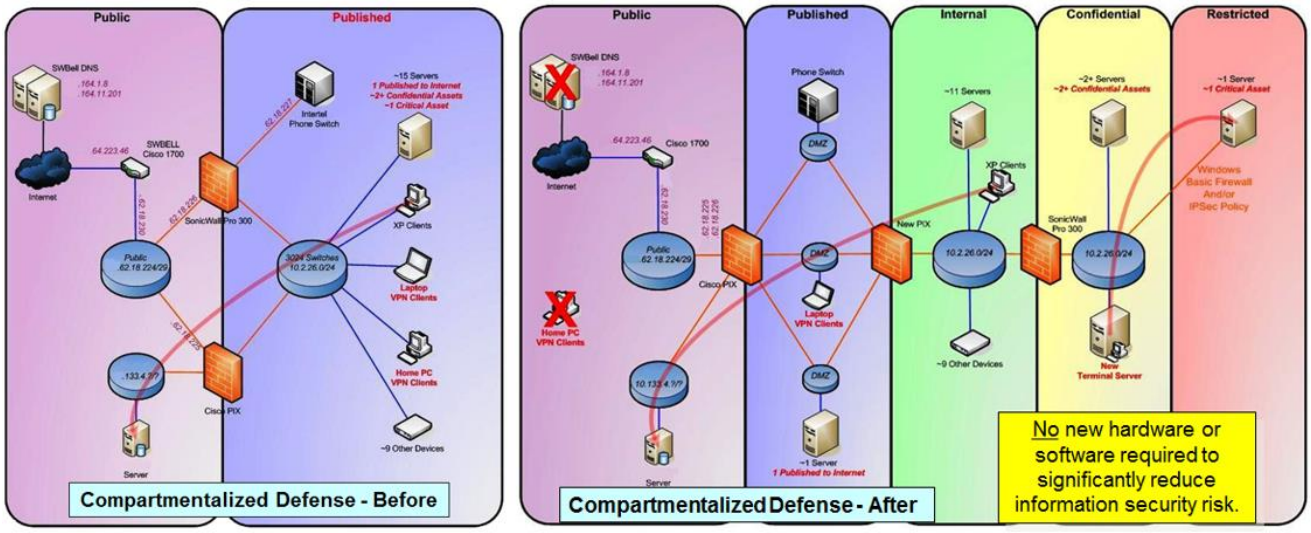


Fig. 1 – Compartmentalized Defense – Before and After

Risk Reduction:	90% on average.
Pros:	No changes of any kind to protected systems.
Cons:	Remaining risk exposure may exceed business requirements.
Capital Cost $$$:	None ($0.00) to substantial, depending on existing network.
Transparency:	No change to network functionality or end user procedures.

2.2 Traditional "Best Practices" System Hardening

Traditional best practices system hardening works by reducing the attack surface presented to potential attackers, therefore indirectly reducing a treated system's cyber security risk of compromise. Many standards have been developed by vendors and government organizations that specify these best practices, although they do not generally do not address their combined implementation and management techniques.

Because many operating systems, databases, and application types exist, appropriate system hardening techniques also vary widely. However, in general classic hardening techniques can be summarized as consisting of the following methods:

- Disable or remove unneeded services or daemons.
- Install only the bare minimum software required to perform necessary business functions, uninstalling unneeded applications.
- Keep all software up to date - install the latest security patches.
- Disable guest and other non-essential account(s).
- Ensure no unused or backdoor administrator or user account(s) exist.
- Ensure passwords are sufficiently strong and complex, and forcing password changes on a regular basis.

- Change local security policy to force all network connections to authenticate as themselves, not as guest.
- Disable all file shares unless absolutely necessary.
- Enable a host firewall.
- Verifying the configuration and effectiveness of antivirus software.

The above is not an exhaustive list; other techniques may apply and be applicable on a system-by-system basis.

Clarity Consulting applies specific elements of traditional best practices hardening techniques as applicable for each system or group of systems individually wherever doing so may cost-effectively assist each customer in achieving their unique risk reduction goals.

Risk Reduction:	35% on average.
Pros:	Rapid and inexpensive.
Cons:	Remaining risk exposure may exceed business requirements.
Capital Cost $$$:	None ($0.00) to considerable, depending on existing network.
Transparency:	No change to functionality or end user use procedures other than end user authentication improvements.

2.3 Access Control Restrictions

Access control lists, or ACLs for short, can form another layer of effective system defense if implemented properly and completely.

Clarity Consulting applies specific ACL hardening techniques as applicable for each system or group of systems individually.

Risk Reduction:	10 - 50%.
Solution Pros:	Swift and inexpensive.
Solution Cons:	Remaining risk exposure may exceed business requirements.
Capital Cost $$$:	None.
Transparency:	No changes in functionality or end user procedures.

2.4 Cryptography-Based Hardening

An extremely strong --and often extremely cost-effective-- method of indirect system "hardening" is simply to encrypt the system with one or more types of local or PKI based encryption.

Cryptography-based hardening can be an extremely difficult-to-defeat and cost-effective layer of defense against even the most advanced and sophisticated nation-state attacks[3]. Under this method, attackers which succeed in compromising a system succeed only in retrieving military-grade encrypted data which they cannot decode or use.

[3] This is provided appropriate and suitably secure and cryptography algorithm(s) are employed and their encryption keys are generated, stored, managed and used with an appropriate level of technical and administrative controls and precautions which match the desired information security assurance level.

Clarity Consulting has enormous expertise with cryptography-based hardening. In fact, this method comprises key layers of defense throughout our company's own internal defense strategy.

Clarity Consulting's security team uses our substantial experience to recommend the right mixture of specific cryptography-based hardening techniques and multi-factor authentication tactics for each system or group of related systems to obtain maximum possible risk reductions for the least possible expenditure of capital expenditure and network downtime.

Risk Reduction: 95 to 99.9%.
Solution Pros: Large risk reductions, often quickly.
Solution Cons: Complexity of solution may require new in-house administrative talent; changes to end user work procedures.
Capital Cost $$$: Minimal to modest.
Transparency: Change in end user use procedures; no change to functionality.

2.5 Application Whitelisting

Application whitelisting can reduce risk to a system by preventing the installation of unauthorized software. This enforced limitation prevents many types of hacker attacks from working at all, while making other hacker attacks more difficult.

However, application whitelisting is not a panacea, as it has no effect in preventing or slowing several entire classes of hacker attacks.

Clarity Consulting applies various application whitelisting hardening techniques for each system or group of systems individually.

Risk Reduction: 30 - 80%.
Solution Pros: Substantial risk reductions quickly for large numbers of systems.
Solution Cons: Remaining risk exposure may not meet business goals.
Capital Cost: None to Modest, depending on solution implementation.
Transparency: Potential changes to end-user network use procedures; no change to network functionality.

2.6 Network Traffic Whitelisting

An extremely interesting and effective layer of high-value cost-effective cyber security defense is Clarity Consulting's proprietary assortment of network traffic whitelisting tactics. These tactics work together in various combinations to drastically reduce risk by limiting an attacker's ability to successfully introduce exploit code to a vulnerable system.

The outcome is a system that while *technically* is just as vulnerable as before, is nevertheless enormously more secure due to an attacker's inability to successfully exploit the vulnerable system's weaknesses.

Our proprietary traffic whitelisting tactics may be deployed between separate networks or within network segments; between individual systems, or internally within a given system such as between a data repository and its operating system network stack, or combinations of these techniques.

Based on our extensive experience, Clarity Consulting applies specific mixes of network traffic whitelisting techniques for each system or group of systems on a case-by-case basis.

Risk Reduction: 90 - 100%.
Solution Pros: Ability to protect large numbers of systems at once.
Solution Cons: Remaining risk exposure may exceed business requirements.
Capital Cost $$$: Modest to considerable, depending on solution set.
Transparency: No change to functionality or end user use procedures.

2.7 Application/Library/OS Virtualization and Sandboxing

In cases where specific components are not adequately protected by one or more of the hardening techniques described previously in this brochure, internally within a given system it may be appropriate to isolate applicable portions of a sub-system away from the others or the underlying OS. Depending on which part of the software stack needs to be isolated, Clarity Consulting terms this technique *virtualization*, or sandboxing.

By utilizing a collection of third party tools, almost any part or sub-part of a given system, whether the OS itself, a single library, a layer of middleware, a specific application, or entire collections of applications can be put in a container and run separately from the remainder of the system, while still maintaining full original functionality.

This division capability also allows for expanded options where software/hardware backwards compatibility is an issue, and also provides a safe area for handling riskier tasks within a more secure host system.

Clarity Consulting uses our extensive expertise to apply various configurations and techniques as applicable to fulfil requirements for each system or a group of systems individually.

Risk Reduction: 50 - 95%.
Solution Pros: Ability to isolate and protect a single vulnerable application, without affecting the remainder of a system.
Solution Cons: Cumbersome for protecting whole systems rather than specific applications; Remaining risk exposure may exceed business requirements.
Capital Cost $$$: Minimal to modest, depending on specific solution implementation.
Transparency: Limited or no changes in functionality or end user procedures.

2.8 System Visibility and Reporting

There is an old saying in the industry that forms a key component of all cost-effective cyber security defense strategies: *"When all else fails, monitor"*.

One of the most cost-effective defenses possible is to deploy the right combination of application level and system monitoring, alerting and reporting technologies where most useful to produce early warning of anomalies and incidents.

When correctly designed and implemented, a visibility-centric defense strategy can be a surprisingly effective and practical solution to number of difficult system, database and application security hardening challenges. A partial solution depiction follows in Figure 2.

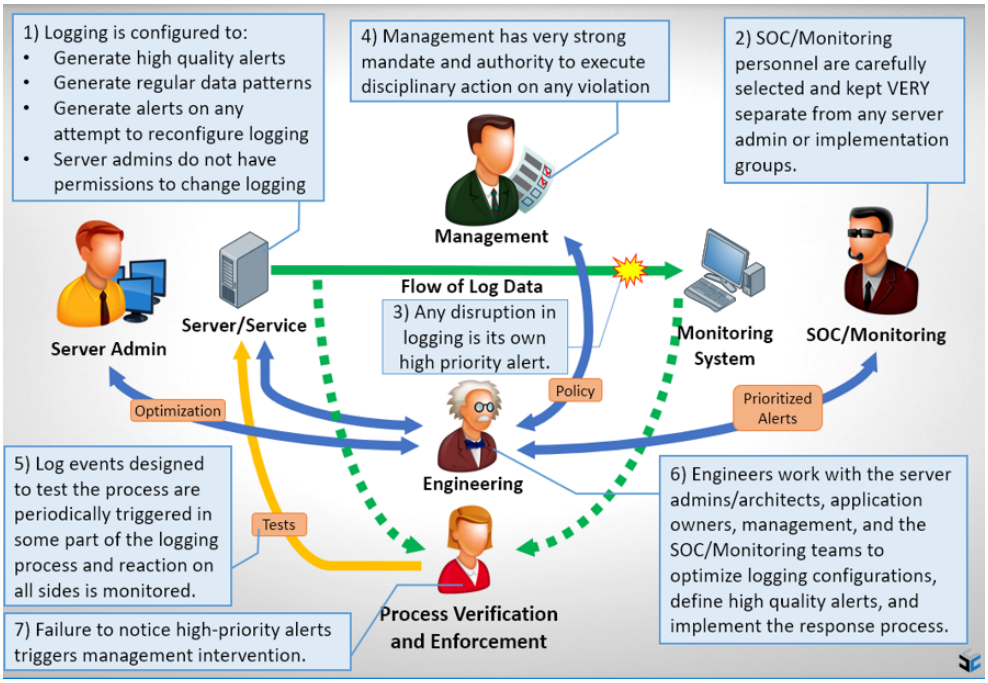


Fig. 2 – Bulletproof Monitoring Design for an Enterprise Network (Partial Solution)

Based on application and desired cyber security end goals, Clarity Consulting applies unique system alerting and reporting hardening techniques as is best applicable and useful for each system or group of systems individually.

Risk Reduction: 30 – 60%.
Solution Pros: Swift, substantial risk reduction over large enterprise network segments.
Solution Cons: Remaining risk exposure may exceed business requirements.
Capital Cost: Modest to considerable.
Transparency: No change in functionality or end user use procedures.

2.9 Third-Party System Lockdown Software

System lock down software can drastically reduce, or theoretically come close to eliminating, cyber security risk in vulnerable systems and applications. However, these substantial gains may come at the expense of very significant implementation and maintenance overhead costs which far exceed the cost of the software itself.

Accordingly, Clarity Consulting always seeks to reduce as much cyber security risk as possible through our other system hardening techniques before we consider the deployment of third-party system lockdown software as part of our recommended hardening solution set.

Because there are multiple conflicting claims by the respective third-party vendors, when Clarity Consulting does recommend third-party system lockdown software,

we are careful to recommend the most effective third-party system hardening software solution(s) for each unique application.

Even then, such third-party software solutions must be carefully tailored to match each intended application. Clarity Consulting provides detailed technical configuration deployment parameters for each customer system or group of systems individually as we deem best to gain the maximum cost-benefit ratio to meet the organization's cyber security requirements[4].

See figure 3 for a computer operating system architectural illustration of this class of powerful system hardening defenses.

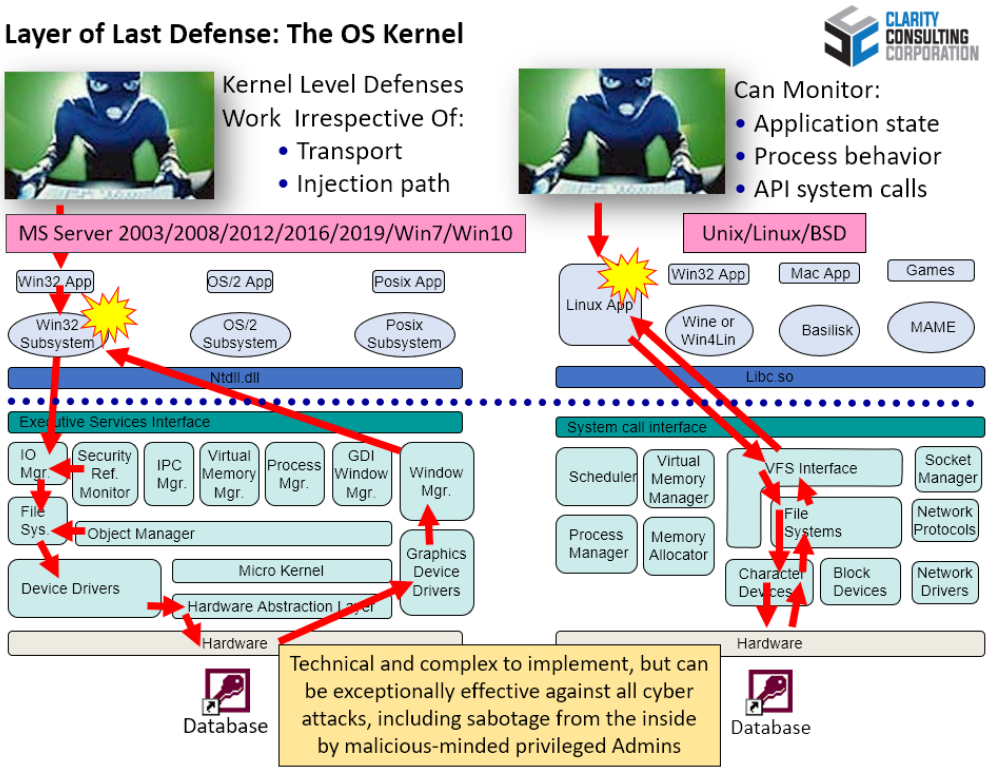


Fig. 3 – Kernel Defense Architectural Overview

Risk Reduction: 95 – 99.99%, depending upon extent of customization.
Solution Pros: Large risk reductions.
Solution Cons: Total solution expense; need for continued maintenance tweaks; difficulty of major solution changes once implemented.
Capital Cost $$$: Modest to considerable, depending on desired usage application(s) and amount of required research, configuration, and testing; cumbersome solution rollout.
Transparency: Minor or no changes in functionality or end user use procedures.

[4] Clarity Consulting recommends the use of third-party software only where combinations of other system hardening techniques in this brochure are impossible or impractical to achieve security assurance requirements.

2.10 The Multi-Factor Defense Framework® (MFDF)

Clarity Consulting's Multi-Factor Defense Framework® (MFDF)[5] technical cyber security risk reduction methodology allows corporations and government agencies to achieve very high levels of predictable and reliable cyber security assurance.

MFDF works by improving the United States Department of Defense's Defense-in-Depth ("layered defense") model, which acts as the foundational basis for all cyber security defenses in this country in both government and commercial IT networks. Unfortunately, Clarity Consulting believes the layered defense model is badly flawed not just in its typical implementation, but in its very design principal itself. Its two critical flaws are outlined in Figure 4 following.

The United States Department of Defense's Defense-in-Depth model ("layered defense") has two critical flaws, namely:

1. It fails to provide a method to determine *how many* layers must be used to reliably achieve a desired level of cyber security protection. This results in under-application and over-application of cyber security defenses.

2. It fails to specify the *composition* of the layers. This results in gaps and duplications of functional effort which undermine the model's real-world practical strength.

Fig. 4 – Critical flaws in the widely used "Layered Defense" model

Substantial improvement to this model is needed. Clarity Consulting Corporation has done this. This improved model is called the Multi-Factor Defense Framework® (MFDF).

MFDF specifies that for each broad category of cyberattack being defended against, each defensive layer must use a completely separate, independent defense of an entirely different type of defense principle than is used by any other layer in the stack.

Each such defensive layer in MFDF is termed a *factor*, solely and only for distinguishment purposes from the term "*layer*" in the DOD's Defense-In-Depth model. The number of factors of protection that are needed is directly determined by the required information assurance classification level. MFDF enables a comprehensive

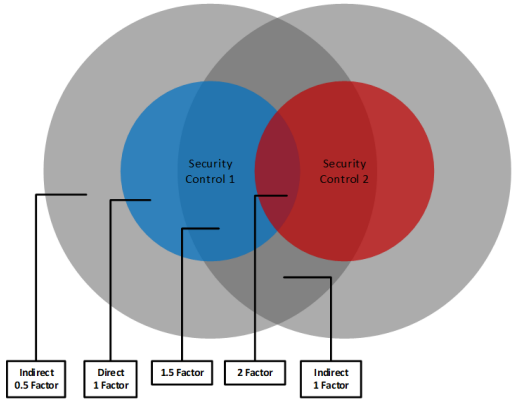


Fig. 5 – MFDF compounds defense effectiveness

[5] The Multi-Factor Defense Framework® is a registered trademark of Clarity Consulting Corporation.

understanding of the realistic ability of an existing or planned system, sub-system, application, or component to withstand real world attacks.

At a technical level, our MFDF model works by layering non-arbitrary numbers of independent and separate technical defenses to achieve compliance with the required information assurance level for each unique protected asset.

The MFDF model specifies the use of defense factors in a specific quantity and manner in order to take advantage of the **significant compounding effect of cyber security defense effectiveness** that is created between the primary and secondary areas of a given control's defense capabilities. Further, the MFDF framework configures the primary and secondary capabilities of multiple factors of technical controls to provide exceptionally high levels of cyber security assurance that are easily adjustable to varying business requirements and cyber security classification requirements. See Figure 5 on the prior page for a visual depiction.

This compounding effect results in large gains in real-world cyber security effectiveness, accomplished at times through major technical IT network changes but more often through what at first glance appears to be seemingly small or even insignificant technical IT network changes.

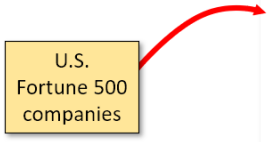
Just two factors of MFDF protection represent an enormous yet readily attainable increase in real-world cyber security assurance for commercial enterprise IT networks, while three factors of MFDF protection are represent the same practical increase for many U.S. government networks.

This is because in practical reality, it is very difficult for even for the most sophisticated and advanced nation-state attackers on the planet to successfully exploit vulnerability risk gaps at three (3) factors of MFDF protection. Yet MFDF is capable of far exceeding three (3) factors of protection.

See Figure 6 and Figure 7 following for more information.

Number of Required Factors	Defense Level
0.5	Home computers, as commonly used in the United States.
1	Corporate computers as normally "secured" by the Fortune 500.
2	Corporate computers secured to very high practical levels of information assurance.
3	Suitable for U.S. Government Secret classified information.
4	Suitable for U.S. Government Top Secret classified information.
5	Theoretical attacks become difficult to even conceive, never mind implement.

Fig. 6 – Number of MFDF factors of protection required to achieve a given level of information assurance



Number of Factors	Odds of Defeating Attacker	Odds of Attacker Success
0	0%	100%
0.5	55%	45%
1	80%	20%
1.5	91%	9%
2	96%	4%
2.5	98%	2%
3	99%	1%
3.5	100%	0%
4	100%	0%

Fig. 7 – Odds of hacker success and scale of breach decline proportionately

Risk Reduction: 0 – 100%, depending upon extent of MFDF application.
Solution Pros: Large risk reductions using existing network equipment
Solution Cons:
Capital Cost $$$: Modest to considerable, depending on the desired level of information assurance.
Transparency: Minor or no changes in functionality or end user use procedures.

2.11 Absolute Security for Classified Environments

For customers with absolute information security assurance requirements, Clarity Consulting delivers. Clarity Consulting personnel have extensive experience designing sophisticated cyber security defenses at the Top Secret/SCI level for national security and defense environments.

Unprotected, vulnerable systems which cannot be air-gapped yet require bi-directional, two-way connections to the Internet or networks of lower classification levels face especially daunting challenges from sophisticated state-sponsored attacks. For customers with absolute cyber security assurance needs despite challenging operational environments, Clarity Consulting can design and implement absolute levels of information assurance protection for vulnerable systems without touching or altering these systems in any way. Protected systems electronically cannot be compromised, and remain immune from sophisticated attackers on an indefinite basis, without needing software or hardware maintenance or updates of any kind.

Protected systems can send and receive full network communications via a bi-directional, two-way network connection, while permanently withstanding sustained and sophisticated targeted attacks by the most advanced nation-state adversaries on the planet. **No changes or modifications whatsoever of any kind are made to the protected systems themselves**, and no maintenance of any kind is needed to maintain absolute information assurance indefinitely.

Our technology works by normalizing network traffic using a proprietary innovation which prevents even sophisticated attacks, including zero-day buffer-overrun exploits, from altering or blocking the sanitizing mechanism. Without modification of the protected systems or applications of any kind, the vulnerable machines on the back side of the sanitizing mechanism receive and send normalized incoming network traffic, eliminating all risk exposure to zero -- despite the sophistication, intensity and source of the incoming attacks, including whether known or unknown attacks.

The key to our system its proprietary sanitizing mechanism. First, our proprietary sanitizing mechanism employs rigid *known secure* code structures to eliminate the possibility of coding vulnerabilities. Secondly --and more relevantly-- its inherent architectural design structure itself assures that even *if* any vulnerabilities were ever discovered, their exploitation would be electronically (physically) impossible. Its inherent fundamental design architecture itself eliminates all attack surface. This eliminates the possibility of even an *attempt* at exploitation, irrespective of the technical sophistication of even the most advanced nation-state attackers.

Risk Reduction:	100% risk reduction – ZERO risk of compromise, indefinitely.
Solution Pros:	Absolute security for highly classified systems in a bi-directional, two-way connection configuration, **without** using one-way data gates, **without** requiring any change to protected systems, and **without** maintenance updates, security patches or support.
Solution Cons:	Significantly slowed network traffic may limit or cripple some applications.
Capital Cost $$$:	High ($100,000 – $150,000)
Transparency:	No change of any kind to functionality or end-user usage procedures, other than dramatically slower inbound and outbound network communications.

2.12 Constant Guardian® - Next-Generation System Hardening Technology

This is an introduction to Clarity Consulting's Logic Chain Stateful Activity Whitelist technology which is marketed under the name Constant Guardian®.

Constant Guardian® was created[6] as a powerful new response to the challenge of securing industrial process control facilities (SCADA/DCS) and other closed-looped applications from sophisticated, targeted cyber-attacks, including by state-sponsored advanced persistent threat (APT) malware.

Fig. 8 – Industrial Process Control HMIs

Value Proposition

The value proposition of Clarity Consulting's patented *Constant Guardian®* technology is its ability to provide Retroactive Cyber Security™

[6] Constant Guardian® is a registered trademark of Clarity Consulting Corporation.

to a high degree of cyber security assurance (**>= 98%**), *without* needing software or hardware changes of any kind to the facility equipment or network segments being protected.

No other technology in the world comes even remotely close to making such claims, never mind succeeds in even halfway actually doing so.

Patent & Ownership

U.S. Patent No. 9,245,147 was issued for our Constant Guardian® technology on January 26, 2016. Clarity Consulting's Chief Technology Officer Paul Williams, one of the two inventors listed on this patent, is the lead inventor who originally conceived this technology.

The initial release of our Constant Guardian® technology is aimed at industrial process control facilities, while upcoming adaptions will target large-scale enterprise IT networks, electric smart devices and grids, and embedded hardware chip applications. Additionally, Clarity Consulting has designed an adaptation for large-scale enterprise IT networks as well.

Detailed Technical Claims

Here are eight specific, detailed technical claims that Clarity Consulting makes for our Constant Guardian® technology. Our technology is:

1. Is 100% backwards compatible with existing industrial process control facilities, without modifications to the equipment being protected of any kind. No software is installed, and no configuration changes are made whatsoever. Does not require facility human machine interfaces (HMIs) to be touched. Specifically, HMIs may remain unpatched; configured with short insecure common passwords (or no passwords); screen consoles may remain unlocked as always; USB ports may remain active for use with memory sticks; and anti-virus software may remain badly out of date -- or not even installed at all.

2. Blocks sophisticated malware that is undetected by anti-virus software, Intrusion Detection Systems (IDS) or other existing technologies on the marketplace today. This even includes brand-new malware brought into the facility on a memory stick and directly introduced into an HMI.

3. Blocks sophisticated network-based cyber-attacks originating from both inside and from outside of protected facilities. This even includes sustained attacks from the inside conducted by knowledgeable personnel armed with full administrative access to everything. No signature updates are utilized for this capability (our device does not use pattern matching technology).

4. Detects accidental operator errors and omissions.

5. Detects operator sabotage attempts, including attacks from the inside using privileged administrator accounts.

6. Detects many hardware and software malfunctions in the early stages of failure.

7. Does not use signatures or behavioral analysis (does not need regular updates or Internet access to work[7]).

8. Our technology solution cannot be targeted, subverted, negated or bypassed by hackers, no matter how skilled they may be. This is because our device operates in what may be thought of as an "offline" mode in which the device is not plugged into the network, has no IP address and is not addressable. Instead, our innovation runs off a core switch span port (or hardware tap) receiving trunked data.

How Our Constant Guardian® Technology Works

Our Constant Guardian® solution isn't an improvement of any existing cyber security technology on the market today. Rather, Constant Guardian® is a completely new type or *category* of cyber security defense. It utilizes a new and vastly different operating principal than any cyber defense that has ever existed in the industry before.

Constant Guardian® is a powerful solution that works by tracking the operational states (logic transitions) of facility equipment and devices in order to provide reliable protection against otherwise invisible, unknown brand-new attacks and malware as well as all existing attacks and malware.

In short, our Constant Guardian® solution addresses all this and more by asking the following question:

> *How can a system be protected from all possible internal and external threats without impacting performance or losing its effectiveness over time as new cyber threats evolve?*

We found the answer to be surprisingly simple:

> *Don't look for what's wrong and assume everything else is right; instead, look for what's right and assume everything else is wrong.*

This powerful defense principal is known as "whitelisting." It is incredibly effective when applied as a part of our Constant Guardian® network equipment state-watching approach to facility logic states. Until now, whitelists have been lists of acceptable actions, data, or other qualifiers that a given system was permitted to perform regardless of the larger context of how, when why, and where (as applicable) the system actually did same. For these reasons, classic whitelists need to be overly broad in order to allow the system to function. While better than nothing, classic whitelists are easily abused or bypassed.

Constant Guardian® solves this problem by applying whitelists to nearly any closed-loop facility operations, IT network environment, system, application or protocol type. It even lends itself well to data analytics, where tracking a logical flow or cycle in a body of data is a desirable outcome.

[7] Threat intrusion/aberration detection systems such as network intrusion detection systems, antivirus software and others) use regularly updated signature or behavior indicators as their primary detection methods. However, these detection methods have numerous flaws including lag between real-world attacks and their detection, limited scalability, high false negative rate, and a requirement for constant signature/behavioral updates.

Detection by Indirect Deductive Analytics

In a major enhancement to our original patent filing, the second generation of our Constant Guardian® works equally well with proprietary undocumented protocols and end-to-end encrypted protocols as it does with traditional open-standards, unencrypted protocols.

The second generation of our Constant Guardian® technology is able to derive facility operational state logic chains from both open-standards unencrypted protocols as well as indirectly by deductive data mining analytical extrapolation of network traffic which is unrelated to application layer protocols (such as ever-present ARP, DNS and more).

For example, our original first-generation technology cannot work on networks where the relevant IT network traffic is encrypted by SSL/TLS or VPN encryption or where the relevant network traffic is proprietary or undecipherable. In contrast, our second-generation technology Constant Guardian® readily works in such environments, even though it cannot understand (decipher) the encrypted or unreadable application layer protocols or network traffic.

Because both generations of our Constant Guardian® technology work by identifying disruptions of expected logic chain sequences rather than by detection of signatures, aberrant commands, or aberrant behavior, it is exceptionally difficult for attackers to devise even conceptual ways of avoiding detection by our Constant Guardian® solution.

Enormous Scale

In another substantial improvement, the second generation of our Constant Guardian® technology is able to utilize IT network traffic from multiple large-scale distributed enterprise networks simultaneously, allowing it scale to protect millions of devices per each customer solution deployment.

In contrast, our first-generation technology is unable to support anything other than relatively small LAN networks containing less than 1,024 devices in total.

Under Development Now

Constant Guardian® is in development currently and has already passed many technical hurdles in its adaption for protecting high-value industrial process control networks.

Constant Guardian® Risk Reduction

A look at the cyber security risk reduction benefits of Constant Guardian® follows.

Risk Reduction:	Risk reduction of 98% or better.
Solution Pros:	Extremely high levels of cyber security without requiring changes of any kind to protected systems; defeats all existing and new hacker attacks, defeats all existing and new malware, whether known or unknown; defeats employee insider threats including by privileged system admins; detects and prevents operator errors and

	omissions; detects and prevents many IT network and application functional errors.
Solution Cons:	Significant up-front modeling of permissible environment operations is required; Needs extensive testing before being placed in production service.
Capital Cost:	High ($250,000 – $750,000).
Transparency:	No change of any kind to industrial process control network or equipment functionality or end-user usage work procedures.

3.0 Ongoing Support, Training & Solution Pricing

3.1 Post Engagement Ongoing Support

After our custom system hardening deployment consulting process has been completed, Clarity Consulting's optionally offered ongoing monitoring and consulting support is designed to maintain your IT network's new elevated cyber security level if and where needed and give you continued peace of mind as new attacks emerge over time.

Clarity Consulting has developed a hardware appliance which is the cornerstone of our ability to provide near-immediate, high-quality "onsite" support at virtually any time needed. Our appliance is protected by strong system level and network communications encryption and can only connect via VPN to Clarity Consulting's secure systems alone and to no other Internet destination.

Our appliance stores a large number of security tools, allowing us to perform ongoing routine technical monitoring and use of proprietary analysis techniques to rapidly and reliably detect a wide range of technical and procedural problems before they can spread widely or cause significant damage.

Additionally, as a standard part of our optional ongoing support package, we provide a fixed number of monthly consulting hours per month. These hours may be used for any purpose of the customer's choice, including solution support, new solution research, or for any of Clarity Consulting's consulting services and educational training classes including those not listed in this brochure.

3.2 Training

Clarity Consulting offers comprehensive training classes for much of what we do as a consulting team, including our Custom System Hardening consulting service.

Unlike other cyber security companies, Clarity Consulting does not teach your experts using teachers who aren't subject-matter experts in their respective fields of instruction. Nor do we teach your experts using subject matter experts who aren't natural, gifted teachers.

Uncanny insight. Unparalleled expertise. You get all this and more with Clarity Consulting cutting edge information security training classes.

When you need cutting edge expertise, natural teaching ability and state-of-the art instruction material combined into a single integrated package, you need Clarity Consulting Corporation.

A significant distinguishing trait of our classroom instruction is our reliance on real world expertise. First, our instructors have many years of personal hands-on consulting expertise across a wide array of customer consulting projects for government and commercial customers. Secondly, our acclaimed, animated classroom training material is based exclusively on hundreds of real-world enterprise consulting engagements and cybercrime investigations which were personally worked by the same Clarity Consulting instructors which teach our classes.

Our emphasis on hands on, real-world expertise sets Clarity Consulting apart from our competitors, who typically base their material around hypothetical examples created for their classes. Our extensive use of actual case history dissections both holds our student's attention and commands their respect. It also is a reflection of the real-life expertise that our class instructors personally have exhibited for years as professional consultants and instructors for the Clarity Consulting security team.

Add it up and it is no wonder that our classroom educational approach is recognized for its ability to convey and explain complex security technology concepts to our students in an understandable and actionable manner across a wide range of student experience and competency levels.

For more information, contact us using Section 4.0, *"Clarity Consulting Contact Information"*.

3.3 Questions and Answers

1. **Question:** What applications will a Clarity Consulting custom-hardened system no longer support, or what network services will it no longer be able to offer?

   Answer: Your network will continue to support the same applications and services as it ran or offered before, without noticeable change, depending on the specific mix of solutions that Clarity Consulting implements in close collaboration with your team. Refer to our list of hardening options in this brochure for details about the various trade-off solution benefits and deficiencies that will be exhaustively considered as part of the design and deployment hardening consulting service that we provide your firm.

2. **Question:** What differences will there be in my operational processes and practices, before and after Clarity Consulting's hardening implementation?

   Answer: The before and after differences could range from no impact at all, to a very significant impact. Consult our list of hardening options for additional details

3. **Question:** For organizations which use extensively use the cloud as an extension or as major component of their IT services, what will be the effect of using our hardening services?

   Answer: There will be no functional impact, unless your information security assurance needs specifically require our hardening option #10 (Absolute Security for Classified Environments) is a part of the unique solution set that we devise for you.

3.4 Pricing

Clarity Consulting's consulting charge is determined by the required number of *solution sets*, and not by the size of the network or by the number of machines or applications which need protection[8]. We define a "set" to be any group of computers

[8] Excludes our Constant Guardian® technology, which requires unique custom development and testing specific to each usage application.

or applications that need the same combination of system hardening protection methods.

As an example, an IT network consisting of 10,000 total systems may include only relatively small number of vulnerable legacy hardware and software which cannot be easily upgraded or replaced. This may look like the following:

Set		Required Protection
1		90 Windows Server 2019
1		75 Red Hat Linux servers
1		5 legacy Windows Server 2012
1		300 legacy Windows XP workstations/laptops
1		50 legacy Windows 7 machines running an insecure old Java applet
1		1,500 Mobil devices
1		7,975 Windows 10 workstations/laptops/tablets

7	**=**	**Quantity of technology "sets" which require a custom-engineering system hardening solution for pricing purposes.**

Accordingly, in this example our consulting fees would be based on seven (7) solution sets, not on the 10,000 total systems comprising the enterprise.

Our fees additionally vary the system type(s), application type(s), system usage(s), and required/desired information assurance level(s).

For a price quote, contact Clarity Consulting (next page).

4.0 Clarity Consulting Contact Information

To schedule a custom system hardening consulting session or a system hardening class for your organization, or to ask questions about any of the information contained in this brochure, contact us today.

For More Information or a Price Quote, Contact:

Clarity Consulting Corporation

Web: www.theclaritycorp.com
Email: info@theclaritycorp.com
Phone: 281-719-9345
USA/International: +1-281-719-9345