



2014 North American Perimeter Network Security Solutions in
Critical Infrastructure Entrepreneurial Company of the Year



F R O S T & S U L L I V A N



50 Years of Growth, Innovation & Leadership

Background and Company Performance

Industry Challenges

There is a growing concern in critical infrastructure industries where cybersecurity attacks are becoming more sophisticated and targeted; a prime example being the Stuxnet attack targeting Programmable Logic Controllers (PLCs). Furthermore, the hype around connecting diverse assets to bring to fruition the Internet of Things (IoT) has resulted in an influx of intelligent sensors that have their own IP addresses. While these sensors facilitate improved communication and visibility of operations, they also create multiple attack points at the facility. Although there are a number of solution offerings providing security clearances at each level (i.e. at the control layer, network layer, and application layer) the market is still in need of a solution offering that cuts across the entire spectrum of automation levels (level 0–4).

The ability to deploy an off-the-shelf offering has become imperative in this day and age where the time delay in addressing vulnerabilities could have severe repercussions. To address the skill gap between the operations group and the IT group, solution providers are required to come out with a unique solution that is easy to use, scalable to a multitude of assets and devices, reliable in complex environments, requires minimal configuration changes, delegates responsibility to the operation's personnel, and spans the entire life cycle of the devices. As specific end user verticals have regulatory mandates that drive change management, such as Chemical Facility Anti-Terrorism Standards (CFAT) for chemicals, Food and Drug Administration regulations (FDA) for food, and Environmental Protection Agency (EPA) standards for water, developing a standards-based solution offering that can be replicated across a number of applications and end user markets is a critical parameter to ensure wide-scale success.

Customer Value Excellence and Entrepreneurial Spirit

Criterion 1: Total Customer Experience

As business imperatives among diverse end users currently revolve around protection of critical infrastructure from targeted cybersecurity attacks, there is a pressing need for an out-of-the-box solution offering that reduces the attack surface and allows customers to streamline communication between protected devices.

Tempered Networks' solution offering includes three key components for implementation: a security appliance (HIPswitch™), a scalable orchestration engine (HIPswitch Conductor™) and a management console and user interface (SimpleConnect™). The unique value proposition of Tempered Networks' offering includes the creation of multiple private network environments for industrial control system devices or network devices used in the facility, where communication is isolated from the underlying network infrastructure. This defense-in-depth approach keeps the attack surface as low as possible by hiding or cloaking the protected devices and minimizing the communication between

them, in addition to enforcing additional quality constraints and rules. In contrast to competitors in this space who follow traditional approaches for network security, Tempered Networks' isolated secure communications model allows for comprehensive deployment across a gamut of applications, including industrial hardware, data centers, and historians.

Best Practices Example: The ability to create private networks across a number of applications and diverse assets has allowed Tempered Networks to gain recognition among end users in critical infrastructure industries such as oil and gas, water and waste water, manufacturing and utilities.

Criterion 2: Product/Service Value

As a result of end users looking for a product offering that allows for a sizable return on investment in the shortest possible time, it is imperative for solution providers to develop a strong product portfolio that is scalable across an array of industrial devices and assets in the automation pyramid (level 0–4). Integration and compatibility with network infrastructure is paramount in the changing landscape of connectivity.

Tempered Networks has expanded its industrial security appliances product portfolio to cater to the various levels in the automation pyramid. As traditional industrial security appliances cannot have a “one size fits all devices” for all these levels, Tempered Networks' holistic deployment model includes industrial-hardened security appliances that are appropriate for level 1 and level 2 and data-center-grade industrial security appliances that are appropriate for level 3 and level 4. Its virtual security appliances are suited for remote access and embeddable libraries that can be integrated directly into level 0 equipment, which is a clear indicator of its extended capabilities in this space. Additionally, as connectivity requirements vary at each level, its compatibility with advanced underlying network infrastructure, such as cellular wireless, will ensure that they gain more traction across critical infrastructure where assets, equipment, and devices are spread out more.

Best Practices Example: Tempered Networks' solution has a lower total cost of ownership (TCO) than competing solutions, it reduces the labor cost owing to the streamlined roles and responsibilities of the private network, and finally, it keeps the CAPEX and OPEX cost to a minimum.

Criterion 3: Service Experience

In addition to having a solution offering that is current and caters to immediate market requirements, there is a burgeoning need for solution providers to service customers in an efficient fashion. Addressing challenges, such as the skill gap within the operations group, is imperative in the current setup.

The Tempered Networks' solution allows an enterprise to provide a secure private overlay network as an internal service, where each of the private networks can be delegated to an operator who is then solely responsible for that network. As the roles and responsibilities of the network are delegated appropriately, there is minimal communication between the operations group and the information technology (IT) group during the change in

management and configuration. This service model creates an effective tool for the operations group to establish, maintain, and react suitably during the full lifecycle of connectivity of the devices. In the current landscape where operations personnel do not have the IT security expertise to set up complex networking environments, the ease-of-use with Tempered Networks' offering through its internal service for connectivity makes its service offering hard to match.

Best Practices Example: Its service model of delegating control of private networks to operations users and groups for greater visibility of roles and responsibilities allows for a faster response time to cybersecurity attacks on devices.

Criterion 4: Ownership Experience

End users are sometimes apprehensive to patch their industrial control systems (ICS) software because critical infrastructure environments operate 24/7. Furthermore, as they are unaware of the vulnerability of attacks, there is a significant time lag between threat identification and rectification. It is imperative for solution providers to empower the end user with proactive security control and management capabilities.

Tempered Networks' independent security layer allows the enterprise to minimize vulnerabilities caused by insider impact; where personnel in the enterprise who go into the network for an event, incident, or support situation leave those systems prone to targeted attacks. The compelling benefits of an independent security layer, between the operations devices, automation equipment, and the network infrastructure, ensures that the enterprise can manage that piece appropriately, respond to emerging threats, and be reactive to imminent vulnerabilities. Furthermore, the ability to reduce the cost of implementation change coupled with compliance with any kind of regulatory or enterprise environment enforces greater customer satisfaction and will pave the way for higher penetration across critical infrastructure industries.

Best Practices Example: Over the last year, Tempered Networks has gained significant momentum in this space, amassing approximately 15 customers and enforcing 9 live production implementations.

Criterion 5: Competitiveness

The pressing security requirements in critical infrastructure industries has resulted in a number of niche solution providers developing innovative products to ensure secure communication within the enterprise. For new entrants in this space, it is imperative to leverage their foundation capabilities to create a solution offering that is repeatable across a gamut of applications.

Tempered Networks was formed from a Boeing project that required wireless-enabled mobile robotic tools to be enabled on Industrial Control Systems (ICS). Because the prototype developed was based on standards such as the International Society of Automation (ISA), Trusted Computing Group (TCG), and Internet Engineering Task Force (IETF), Tempered Networks has leveraged its existing foundation capabilities to develop an isolated network security solution that can be replicated across diverse vertical markets. While peer solution providers focus on specific elements of the industrial

cybersecurity space such as network configuration management, network monitoring, and network communications, Tempered Networks' standards-based comprehensive solution offering is uniquely poised to cater to the advent of IoT in conjunction with the traditional industrial control systems (ICS) used in critical infrastructure industries.

Best Practices Example: As a result of Tempered Networks basing its product line on the International Society of Automation (ISA) 100.15.01 architecture, end user benefits include flexible network segmentation, no ICS configuration changes, increased reliability, and centralized management of networks.

Criterion 6: Uniqueness

While there are a number of solution providers entering into the network security space, in order to build a business case for adoption among end users, solution providers are required to understand customers' desired outcomes and exhibit unique product attributes that cater to their immediate needs.

While there are a number of solution providers that focus on IT security, Tempered Networks' focus on network security for industrial control systems (ICS) is in sync with customer-driven requirements. Its unique value proposition works in a multitude of environments, be it where the enterprise is looking to add an increase level of protection for their critical infrastructure to reduce the attack surface and to reduce the risk on the equipment, or in an environment with highly distributed assets that need to be monitored over shared network infrastructure that the enterprise does not necessarily own, which exemplifies its acute focus to serve diverse customer requirements. In addition to having a very efficient, highly reliable, scalable, and ease-to-use platform, the ability to delegate administration and the ability to be explicit about trust management are critical attributes that will allow them to become a preferred vendor of choice.

Best Practices Example: A case example to illustrate the successful implementation of Tempered Networks' solution is in a water and waste water environment, where a reputed county deployed the Tempered Networks solution to add an additional layer of security on top of the shared network infrastructure to isolate their equipment and minimize connectivity between the components.

Conclusion

Tempered Networks' solution provides end users across critical infrastructure industries a holistic solution offering to minimize targeted attacks by isolating communication between industrial control system devices in a private network from the underlying network infrastructure and further delegating that network to a specified operator. Its efficient, reliable, scalable, and ease-to-use off-the-shelf solution offering that can be applied across various automation levels (level 0-4) is expected to gain even more traction owing to the increase in the number of connected assets fueled by the IoT. Based on Frost & Sullivan's independent analysis of Perimeter Network Security Solutions in Critical Infrastructure, Tempered Networks is recognized with the 2014 North American Entrepreneurial Company of the Year Award.

The Intersection between 360-Degree Research and Best Practices Awards

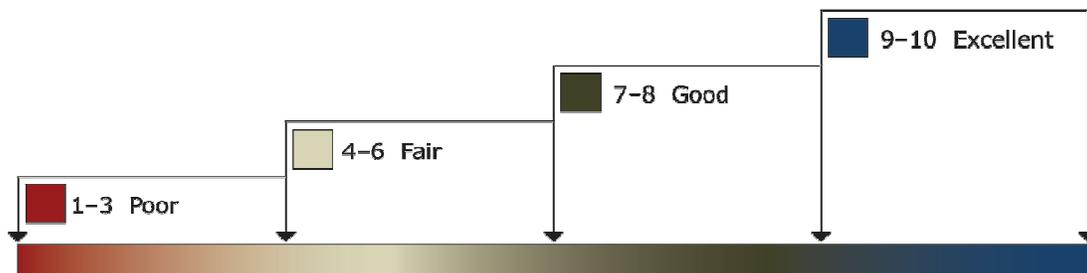
Research Methodology

Frost & Sullivan’s 360-degree research methodology represents the analytical rigor of our research process. It offers a 360-degree-view of industry challenges, trends, and issues by integrating all 7 of Frost & Sullivan’s research methodologies. Too often, companies make important growth decisions based on a narrow understanding of their environment. Successful growth strategies are founded on a thorough understanding of market, technical, economic, financial, customer, best practices, and demographic analyses. The integration of these research disciplines into the 360-degree research methodology provides an evaluation platform for benchmarking industry players and for identifying those performing at best-in-class levels.



Decision Support Scorecard and Matrix

To support its evaluation of best practices across multiple business performance categories, Frost & Sullivan employs a customized Decision Support Scorecard and Matrix. This analytical tool compares companies’ performance relative to each other. It features criteria unique to each award category and ranks importance by assigning weights to each criterion. The relative weighting reflects current market conditions and illustrates the associated importance of each criterion according to Frost & Sullivan. This tool allows our research and consulting teams to objectively analyze performance, according to each criterion, and to assign ratings on that basis. The tool follows a 10-point scale that allows for nuances in performance evaluation; ratings guidelines are illustrated below.



Best Practice Award Analysis for Tempered Networks

The Decision Support Scorecard, shown below, includes all performance criteria and illustrates the relative importance of each criterion and the ratings for each company under evaluation for the Entrepreneurial Company of the Year Award. The research team confirms the veracity of the model by ensuring that small changes to the ratings for a specific criterion do not lead to a significant change in the overall relative rankings of the companies.

Finally, to remain unbiased and to protect the interests of all organizations reviewed, we have chosen to refer to the other key players in as Company 2 and Company 3.

Decision Support Scorecard: Customer Value Excellence

<i>Measurement of 1-10 (1 = poor; 10 = excellent)</i>	Award Criteria					
	Total Customer Experience	Product/Service Value	Purchase Experience	Ownership Experience	Service Experience	Weighted Rating
Customer Value Excellence						
Relative Weight (%)	20%	20%	20%	20%	20%	100%
Tempered Networks	9	10	9	9	10	9.4
Company 2	9	9	8	9	9	8.8
Company 3	8	9	8	8	8	8.2

Criterion 1: Total Customer Experience

Requirement: Customers receive exceptional impression at every stage of the purchase cycle

Criterion 2: Product/Service Value

Requirement: Products or services offer the best value for the price, compared to similar offerings in the market

Criterion 3: Purchase Experience

Requirement: It is as simple for salespeople to sell the product or service as it is for the customer to buy the product or service

Criterion 4: Ownership Experience

Requirement: Customers are proud to own and use the company's product or service

Criterion 5: Service Experience

Requirement: Customer service is accessible, fast, and stress-free

Decision Support Scorecard: Entrepreneurial Spirit

Measurement of 1-10 (1 = poor; 10 = excellent)	Award Criteria					
Entrepreneurial Spirit	Courage	Competitiveness	Uniqueness	Blue Ocean Strategy	Persistence	Weighted Rating
Relative Weight (%)	20%	20%	20%	20%	20%	100%
Tempered Networks	9	9	10	9	9	9.2
Company 2	8	8	9	9	8	8.4
Company 3	8	8	8	8	8	8.0

Criterion 1: Courage

Requirement: A demonstrated willingness to take a leap of faith – at financial, personal, or emotional risk – to launch and sustain a new business venture

Criterion 2: Competitiveness

Requirement: Intense awareness of the competition and willingness to take steps to reduce their market share

Criterion 3: Uniqueness

Requirement: A clear understanding of customers' desired outcomes, the products that currently help them achieve those outcomes, and where key gaps may exist

Criterion 4: Blue Ocean Strategy

Requirement: Proven track record of creating new demand in an uncontested market space, rendering the competition obsolete

Criterion 5: Persistence

Requirement: A deep belief in the "rightness" of an idea, and a commitment to pursuing that idea despite resistance or naysayers

About Frost & Sullivan

Frost & Sullivan, the Growth Partnership Company, enables clients to accelerate growth and achieve best in class positions in growth, innovation and leadership. The company's Growth Partnership Service provides the CEO and the CEO's Growth Team with disciplined research and best practice models to drive the generation, evaluation and implementation of powerful growth strategies. Frost & Sullivan leverages almost 50 years of experience in partnering with Global 1000 companies, emerging businesses and the investment community from 31 offices on six continents. To join our Growth Partnership, please visit <http://www.frost.com>.