HIRSCHMANN
A BELDEN BRAND

White Paper

Cyber security: Simply hoping has had its day.

Prof. Dr. Tobias Heer – Senior Architect for Network Security, Hirschmann Automation and Control GmbH

Lukas Wüsteney – Architect for Industrial Networking, Hirschmann Automation and Control GmbH

Introduction

The huge number of serious cyber security incidents at flagship European businesses has led to questions being raised about security both within companies and across industry as a whole. Who can put their hand on their heart nowadays and say that their company is secure and will never experience a cyber security incident? That uncertainty now raises the question: If you can no longer be sure of your security, what can you do to respond correctly to the inevitable cyber attack, and what structural measures can be taken to cushion the blow when it arrives?
This white paper highlights the relationship between preventive measures and possible responses that can be taken and applied in industrial networks so that we don't have to keep on relying simply on hope and are better equipped to handle cyber attacks in the future.

Table of Contents

tripwire

HIRSCHMANN
A BELDEN BRAND

Be certain.
Belden.

Just a few years ago, it still seemed possible to get to grips with the issue of cyber security. A firewall, the latest patches, a virus scanner on our end systems and a VPN gateway for internal communications in our company. That was the case because the production network wasn't connected to the rest of the world, and the technology was incompatible with the tools used by attackers anyway. Such was the IT security situation for many companies. Today, serious security incidents at major companies are on the rise, sometimes resulting in losses amounting to tens of millions. Our trust in IT security has been shaken fundamentally, so much so that nowadays managers would no longer dare to say that their company was safe and couldn't be hacked. When we take a closer look at that uncertainty, however, a new area of responsibility emerges: If we assume that we will be hacked sooner or later, the question arises as to which measures and mechanisms have been put in place to handle an anticipated cyber attack adequately. This white paper explores the modern security landscape. It focuses on preventive measures and on recognizing and responding to attacks, with a view to painting a more rounded picture of the cyber security landscape of industrial systems.

Well known cyber security controls

To be prepared for an attack and to mitigate the damage or extent of that attack, we need to start with a tried and tested concept: segmenting the network infrastructure and enhancing its security. In many documented cases, automated malware and attackers were able to move through networks systematically, as they were not separated well enough, or they contained too few firewalls to properly restrict an attacker. Many systems were therefore open to further attacks or the sabotage and disruption of production lines. Today, every modern industry network should separate the IT network from the OT network, as well as any functionally independent components of the latter. The recent catastrophic effects of ransomware viruses demonstrate that most companies that were severely hit either did not have adequate segmentation, or it was ineffective.

Network segmentation follows the principle of zones and conduits. The network defines functionally independent zones which, for the most part, operate autonomously. Packet filters (e.g. firewalls or gateways) are installed between the zones (see Figure 1), which limit and monitor network traffic that still has to flow over the borders of the zone. An industry network with strong segmentation not only contains a firewall between the OT and IT networks, but also a plethora of firewalls between individual system components and machines. Soft targets (old network devices that can no longer receive patch updates or do not have adequate security features) are separated from the network using packet filters, e.g. small firewalls that conceal the full scale of potentially vulnerable interfaces from attackers.

Zoning makes it difficult for an attacker who has already infiltrated the network to move around freely. Usually, it's impossible for automated malware to infiltrate the firewalls at the zone boundaries, and it is therefore generally limited to the assets within the affected zone. That dramatically reduces damage in the event of an attack. Zoning is also a major impediment for human hackers, as only the assets within the attacker's zone are potential targets. However, a cyber attacker generally tries to move through the network (lateral movement) to gain access to other computers. In that respect the attacker depends on the existence of assets with vulnerabilities or inadequate configurations.

Zoning significantly reduces the availability of vulnerable assets and limits the impact of an attack. Large-scale epidemics of infection can therefore be prevented. Additionally, many system components retain functionality after the attack, as they

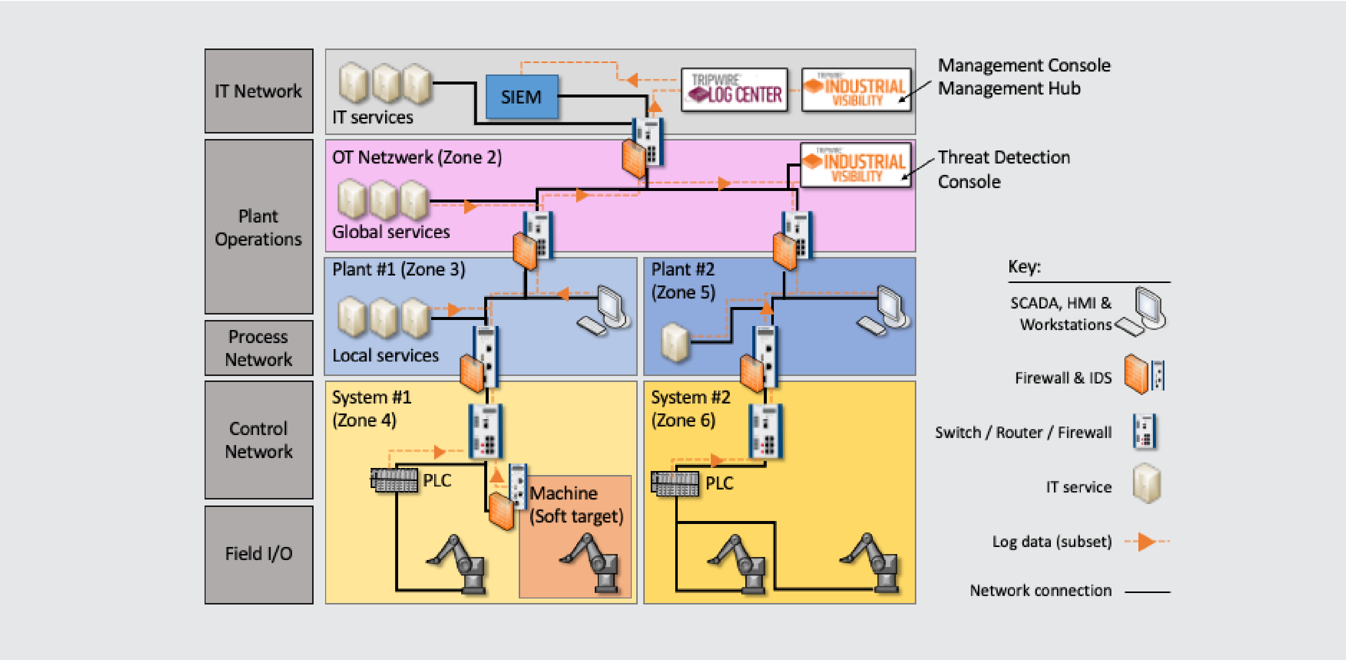

Figure 1: Network segmentation and control systems

are independent of the systems under attack. That means that outdated and unreliable measures such as paper batch cards and manual work need not be undertaken extensively in the aftermath of an attack since the attack is kept rather contained instead of widespread.

Clean-up operations after an attack are much easier if clear, effective zone boundaries have been implemented. The fewer systems an attacker can reach, the fewer forensic tasks and restoration efforts will be necessary. This is extremely costly and tedious work which could paralyze an industrial network for weeks or even months after the attack. It is a crime scene, after all, which means that all the attacker's backdoors and malware must be completely eliminated.

Automation and cyber hygiene

Generally, the first step for an attacker is to gain access to a system within the network. That can occur through infiltrating one of its own systems via an open, non-secure Ethernet port or a compromised Wi-Fi network (e.g. a microcomputer with mobile radio modem). The attacker can also gain access through a system that has been compromised with malware and infected by a download or email.

In the event of the former, it is easy to recognize that an unknown asset (that of the attacker) is present on the network. An alarm can be triggered that allows for a rapid response to this deviation from the norm (see Figure 2). However, it is much better if the asset does not gain access to the network in the first place. Protocols such as IEEE 802.1X [1] for Ethernet and WPA2-Enterprise [2] with IEEE 802.1X for Wi-Fi allow unique access credentials to be specified for each asset on the network. Each asset wishing to access the network must provide authentication before it can communicate with it. That makes it much more difficult for an attacker who has gained access to the company or production system to do the same with the network.

In reality, however, cases where industry equipment does not support authentication via 802.1X or WPA2-Enterprise continue to crop up. In such cases with wired connections, a method known as a MAC bypass must be used, whereby the asset is recognized solely by its (easy-to-forge) MAC address. Wi-Fi without IEEE 802.1X uses a WPA2 with pre-shared key, well known from home networks, where all Wi-Fi devices connected in this way share one secret key, the "Wi-Fi password".

In such cases, however, it is no longer possible to determine absolutely which device wants to connect to the network, which is why additional measures must be taken to maintain network hygiene (e.g. automatic processes to verify the identity of the device by means of automated login by a monitoring server). Such automatic processes are often available as a post-connect phase (see Figure 3) in modern Network Access Control (NAC) [3] solutions. If an attacker has compromised a system already within the network (e.g. via a carelessly opened email or a vulnerable network service), it is considered a legitimate network asset, meaning measures such as IEEE 802.1X and WPA2-Enterprise will be of no use (the compromised asset has its own valid network key). Additional methods must therefore be used to monitor the state and integrity of the asset. Unlike checking its identity prior to connecting an asset to the network (pre-connect check), an automated system can interact with the asset after connection (post-connect checks). This is achieved by either installing an agent (small piece of software) on the system, which can identify itself and monitor critical system properties, or by making use of an alternative solution that does not use an agent. In the latter case, a control system notifies the monitored asset (e.g. via SSH or a similar remote management protocol) and subsequently uses command-line instructions to check the state of the asset. The parameters include the state of the anti-virus system (enabled/disabled, updated virus definitions/outdated virus definitions), the state of the assets' firewall, programs started on the asset, available or non-available files and registered users.

This allows the typical behaviors of an attacker to be recognized (e.g. disabling the local anti-virus program or starting its own malware routines). Assets that are known to be insecure are subsequently removed from the network automatically. This makes it more challenging for an attacker to further infiltrate the network after it has taken control of an asset and remain hidden. It also allows for initially successful attacks to be detected and mitigated sooner. Actively monitoring the state of the assets connected to the network

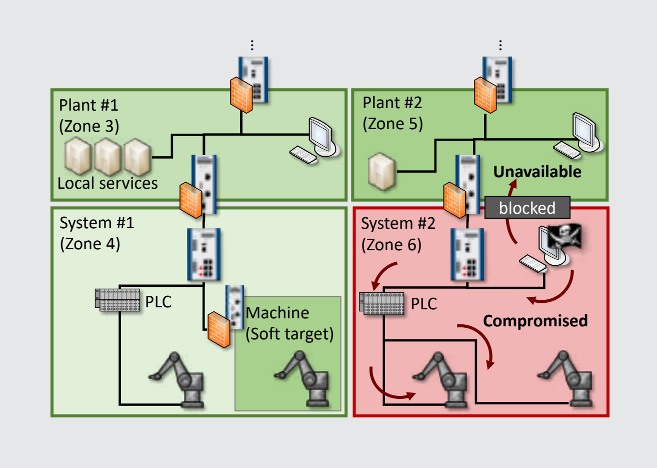

Figure 2: The attacker is limited to a single zone

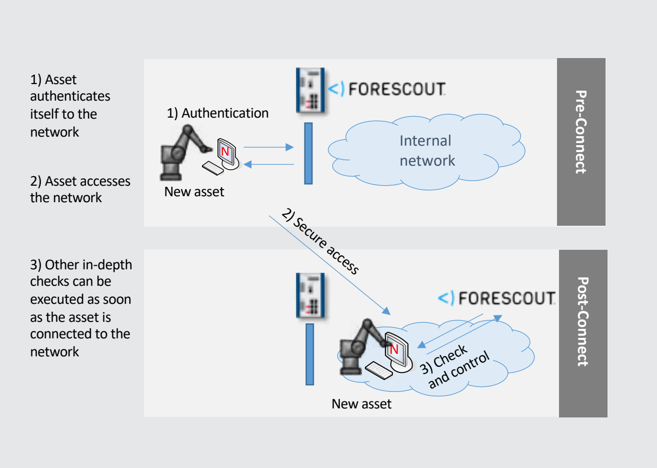
1) Asset authenticates itself to the network
2) Asset accesses the network
3) Other in-depth checks can be executed as soon as the asset is connected to the network
1) Authentication
FORESCOUT
Internal network
New asset
Pre-Connect
2) Secure access
FORESCOUT
3) Check and control
New asset
Post-Connect

Figure 3: Authorization process for assets wishing to access the network

and having effective network access control are therefore a crucial element of cyber hygiene in industrial networks.

A network access control management solution can also support asset management, in other words, all available systems and devices. The knowledge of all assets and their functions is an important basis for risk analysis prior to an attack and for deciding which response measures should or should not be taken (switch off, isolation, keep it running) in the event of an attack.

Detecting attacks and preparing for emergencies

It is pointless having a defense plan, if it does not include measures for detecting attacks. A technically superior attacker will otherwise be able to circumvent the defense mechanisms and move around the entire network, carrying out as many malicious activities as possible. The concept of technical superiority sounds much more sophisticated than it is in reality. The fact that in 2019 a quarter of all cyber attacks could still be attributed to the 'Wannacry' [4] ransomware that has been causing malicious activity since 2017 speaks volumes. Wannacry exploits a vulnerability for which patches, effective measures to counteract the malware, have existed since 2017. It cannot be considered high-tech when you compare the defense measures against the technical sophistication of the attacker. And with modern malware, the bar for defense is once again set much higher. Not only are more technically effective attack vectors being used, but also highly successful social engineering techniques. These exploit human vulnerabilities such as uncertainty, fear and greed.

Security Information and Event Management Systems (SIEM) are used to recognize and classify cyber attacks in log files. Today, they are standard in many office IT environments, yet they are still rare in many industrial networks. The necessity of SIEM systems in industrial networks is, however, just as important as in IT networks. This is because the technology used, and the tools and methods used by attackers are often similar or even identical.

However, by compromising devices, attackers inevitably leave behind traces. For example, telltale registry entries, attack programs and files remain, and suspicious processes have been started on the systems or system configurations such as anti-virus and firewall settings have been changed. These can all be retrieved from the event logs of the compromised devices. If you view the logs from all the assets, you will get a general picture of all the activities going on in an industrial network.

The event logs and traffic pattern analyses contain an incredible treasure trove of valuable security information. These treasure troves are often not exploited as they can be somewhat difficult to handle. For one, it is not affordable to centrally collate information from hundreds of assets without a suitable management system (log management system). The other side of the coin is that it consists of a plethora of very small pieces of information from which it is not easy to identify an attack. Staying with the treasure trove metaphor, we are dealing here with tons of 1 cent coins of which a considerable quantity has been forged. In this sense, the 'counterfeit money' is fragments of information that, although they do not belong to an attack, can still be misjudged as one. Normal system maintenance that requires starting new programs, software updates or opening network ports are examples of such activities. That means not only is there an issue with recognizing cyber security threats within the plethora of log entries, but false positives must also be avoided.

In addition to offering the potential to analyze huge quantities of log data, SIEM systems also allow for the automated recognition of attackers. These systems are known as intrusion detection systems (IDS) [3]. Not only do they analyze log data, but also network traffic between the assets in an industrial network.

Moreover, once an attack has been recognized, countermeasures are automated to mitigate it. These intrusion prevention systems (IPS) can interrupt partially successful attacks and prevent further malicious activity. They have a bad reputation in industrial systems because if they are used without consideration they can lead to breakdowns, downtime and functionality errors which are tricky to fix. This is the case even if there is no attack but harmless activity that is wrongfully classed as an attack (a false positive, in other words, the counterfeit coins in our example). This bad reputation means that IPS systems have, in the past, responded with overly aggressive blockades in the event of an attack. For security purposes, whole network segments or assets were separated from the network in the event of a (wrongfully) recognized attack. This can result in extensive functional downtime.

Today, it is possible to use IDS systems more systematically. Thus, even in the event of an attack, a control asset can continue its tasks, while the configuration interface of interest to the attacker can be separated from the network by the IPS system. Through the isolation of such components, essential assets shall continue to operate even in the event of an attack while the spread of the attack can be curtailed.

After an attack

Finally, rapid and effective responses are required in the event of a known attack. To be ready to respond to an attack, full and detailed data required for analysis must be stored in the log management system and trained employees must be available. The log management and SIEM systems mentioned previously are important here as they make information available in a format that is easy and efficient to search. That is key as a central logging system often contains gigabytes of log data, meaning that recognizing an attack (and determining which systems have been attacked) is about as straightforward as finding a needle in a haystack. On account of the enormous volume of data, the entire process is challenging from a technological perspective too.

If you establish an effective system to handle emergencies on time, you can respond rapidly in the event of an attack. Without such precautions, in the worst-case scenario there is a risk that many of the affected systems could be separated from the network for a long period of time and that log data might have to be manually copied onto USB sticks for analysis. This leads to lengthy periods of downtime and thus canceled deliveries or breaches of contract. In this respect, the procurement of a suitable system often already sees a return on investment after your organization has fended off a ransomware attack.

In addition to technical systems, the capabilities of your workers also play a decisive factor in the ability to actively fend off attacks or to restore systems afterwards. New employees should have qualifications in suitable technical fields and incident response plans must be continuously updated and properly communicated. These are important steps for a rapid and effective response in case of emergencies. Larger enterprises bundle their security competences into security operation centers (SOC). Additionally, advance contact should be made with specialized service providers to ensure additional support with incident response expertise in the event of an attack. Emergency drills are also essential. They are the most definite way to ensure that the defense team is one step ahead of the attacker. A learning-by-doing approach is always the worst solution for incident response. This is because the availability of production and company secrets, and not least personal data and even employee integrity are at stake. Statutory provisions regarding response times argue in favor of a team that is skilled in handling cyber incidents. For incidents where customer or employee data is affected, a notification period of 72 hours applies in Europe. For companies classed as critical infrastructure, the Federal Information Security contact persons must be notified immediately, without undue delay in many countries. Considering these tight timelines and the working hours of employees (a weekend has 56 hours), businesses often have no choice but to have IT security experts on site to handle emergencies.

Other measures and outlook

In addition to the security measures described above, other actions can be taken, and although they are mainly preventive, they can also significantly reduce the likelihood of an attack or infection by automated malware in the long term. Figure 4 gives an overview of practical ways to improve the security of a business and production network.

Furthermore, it is essential to foster a thorough awareness and provide full training to the entire workforce in order to prevent attacks that use social engineering techniques such as phishing, deception, and baiting. It is important to provide training for less IT-oriented workers in administration and production if they have access to computer systems. This is because attackers often target less technically experienced employees for their first attack.

The technical solutions described above are offered by different companies. Belden [5] offers turnkey solutions for network, log management and SIEM systems. It provides industrial network assets such as firewalls, switches, routers and access points from Hirschmann Automation & Control GmbH [6] and security solutions from its sister company Tripwire, Inc. [7]. In close partnership with Forescout Technologies Inc. [8], the market leader for network access control solutions, Belden is a one-stop shop for powerful NAC systems including thorough pre- and post-connect checks and asset management for industrial systems.

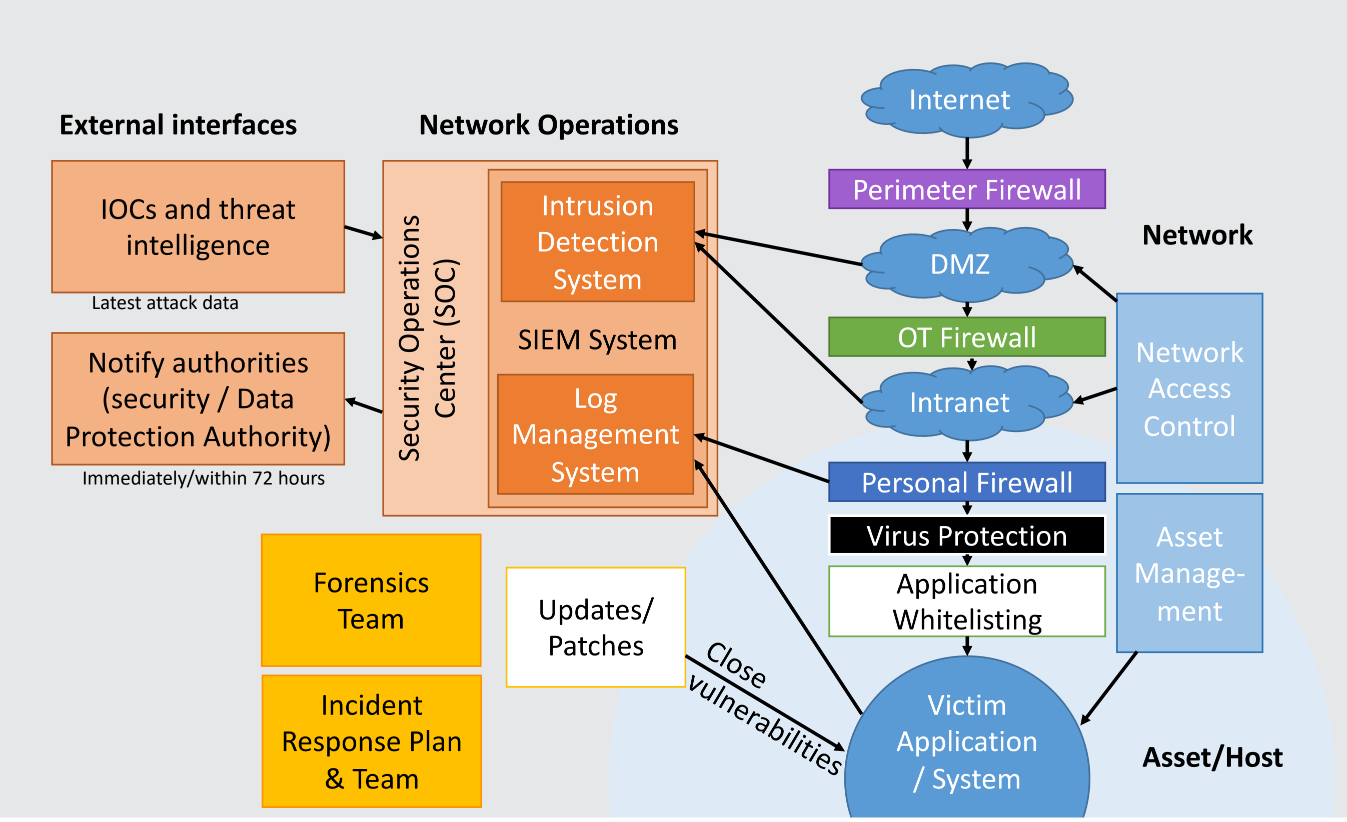

Figure 4: Summary of different measures to prevent, detect and respond to cyber attacks

References

[1] 802.1X-2010 - IEEE Standard for Local and metropolitan area networks--Port-Based Network Access Control, https://standards.ieee.org/standard/802_1X-2010.html

[2] 802.11i-2004 - IEEE Standard for information technology-Telecommunications and information exchange between systems, https://standards.ieee.org/standard/802_11i-2004.html

[3 Monitoring Industrial Control Systems to Improve Operations and Security, https://www.forescout.com/company/resources/monitoring-industrial-control-systems-to-improve-operations-and-security/

[4] Ransomware reloaded: Wannacry verursacht immer noch Schäden in Milliardenhöhe, https://t3n.de/news/ransomware-reloaded-wannacry-1240246/

[5] Belden, Inc. Website, https://www.belden.com/

[6] Hirschmann Automation & Control GmbH Website, https://hirschmann.com/

[7] Tripwire, Inc. Website, https://www.tripwire.com/

[8] Forescout Technologies, Inc. Website, https://www.forescout.com/

Always Stay Ahead with Belden

In a highly competitive environment, it is crucial to have reliable partners who add value to your business. When it comes to signal transmissions, Belden is the No. 1 solutions provider. We know your business and want to understand your specific challenges and goals to show how effective signal transmission solutions can push you ahead of the competition.

By combining the strengths of our leading brands, Belden, GarrettCom, Hirschmann, Lumberg Automation, Tofino Security and Tripwire, we are able to offer the integrated solution you need. Today, it may be a single cable, switch or connector, to solve a specific issue; tomorrow, it can be a complex range of integrated applications, systems and solutions. With the rise in smart, connected devices brought on by the Industrial Internet of Things (IIoT), together, we can make sure your infrastructure is ready to handle and make sense of the influx of data. Transform your business now with instant access to information, and make your vision a reality. Visit info.belden.com/iiot. to learn more.

About Belden

Belden Inc., a global leader in high quality, end-to-end signal transmission solutions, delivers a comprehensive product portfolio designed to meet the mission-critical network infrastructure needs of industrial, enterprise and broadcast markets. With innovative solutions targeted at reliable and secure transmission of rapidly growing amounts of data, audio and video needed for today’s applications, Belden is at the center of the global transformation to a connected world. Founded in 1902, the company is headquartered in St. Louis, USA, and has manufacturing capabilities in North and South America, Europe and Asia.

About ForeScout

For more than 2,900 enterprises in over 80 countries, ForeScout network access control solutions provide intelligent, cost-effective network access control that meet the highest standards for security and regulatory compliance as well as ease of use and deployment.

The ForeScout platform is sold as either a virtual or physical appliance that deploys within your existing infrastructure and typically requires no changes to your network configuration. It installs out-of-band, avoiding latency or issues related to the potential for network failure, and can be centrally administered to dynamically manage up to two million endpoints from one Enterprise Manager console.

For more information, visit us at www.belden.com and follow us on **Linkedin** and **Facebook**.