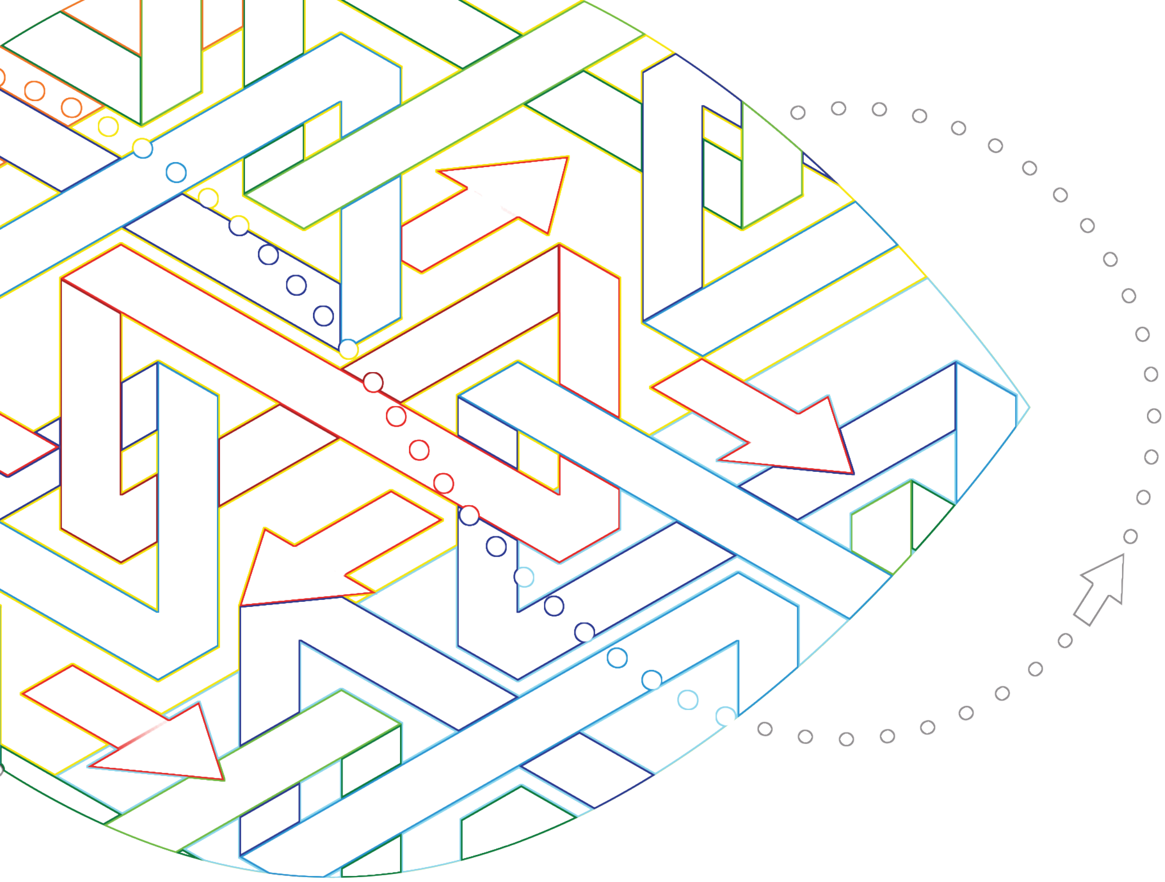
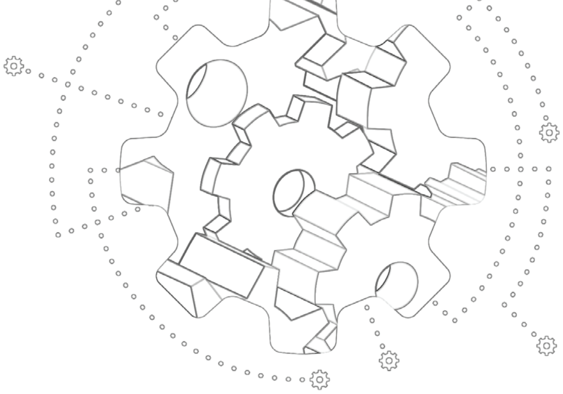


Protecting Control Networks

KEY CONSIDERATIONS FOR PROTECTION

SOURCEfire®



Whitepaper

Control networks and industrial control systems manage the generation and delivery of electricity, automate production lines, control environmental systems in large commercial buildings and hospitals and manage many other vital processes much of which is considered critical infrastructure. They also face a unique set of complications when it comes to cyber security.

Control networks have unique cyber security requirements, so IT solutions can't be deployed interchangeably to protect the control network.

Control networks are targeted by the same modern cyber security threats that typical corporate networks face, but many industrial control systems in operation today were designed during a time when it was sufficient for networks to be physically separated ("air-gapped") from their corresponding corporate networks. Designed under a model of implied trust, it was assumed that the only way a system could be on the control network was because it was explicitly authorized to be there. Therefore, it followed that there was no reason to specifically authorize communications between systems. But amidst the sensationalism the Stuxnet worm generated for its ability to sabotage an air-gapped control network, there was an important lesson: Air gaps as a cyber security technique have run their course and are no longer effective.

At the same time, it is important to recognize that information technology (IT) security solutions in use on the corporate network can't be deployed interchangeably to protect the control network. The two management teams have different priorities. While IT is typically focused on the triad of confidentiality, integrity and availability, the control network operations technology (OT) team is focused on availability, integrity and confidentiality. When control networks fail, there are very real risks posed to human life and environmental safety. Availability and reliability are paramount and must be maintained at all times.

Another consideration is ease of use. It is not uncommon to find cyber security as one of many functions for which OT engineers are responsible. Therefore, cyber security solutions deployed in control environments must be intuitive with minimal management requirements.

The Attack Continuum and Defense in Depth

For many years, conventional wisdom focused solely on a perimeter-based defense with the mission to keep out all attackers. Little attention was paid to what happened within the walls of the enterprise, to the detriment of more than one organization. For all of the effectiveness of a good, solid wall, it only protects against certain types of attack and all it takes is one door left open – intentionally or not – to render the thickest of walls useless.

Today, the conventional wisdom is to expect a successful attack, and to design and defend your network with a defense-in-depth approach to mitigate the damage. The defense-in-depth approach is a multi-layered, multi-technology strategy to defend an organization's most critical assets as determined by asset inventories, business continuity reviews and risk analyses. Another important shift in thinking is to recognize that cyber security is not a point-in-time exercise, rather it must be thought of as a continuous process, constantly evolving. Sourcefire's strategy, therefore, focuses on the full attack continuum.

The full attack continuum can be broken into three phases – Before, During and After an attack – and each phase consists of a number of activities. For instance, the Before phase consists of activities such as the attacker surveying the targeted network and planning the attack, while the exfiltration and/or the destruction of data will, logically, occur in the During phase. What is sometimes overlooked is the After phase, when attackers can remain hidden for days, weeks or months while they complete their mission and then can establish a beachhead for subsequent attacks. But if we are to prevent history from repeating itself, thwarting attacks can't only focus on detection and blocking. Ongoing analysis after an attack is vital to mitigate damage and adapt defenses before the next attack. Sourcefire offers protection along all phases of the attack continuum through research, real-time monitoring and response, and continuous event and traffic analysis to detect new trends and evasion techniques.

Applying Cyber Security to Control Networks

Before

The adage "forewarned is forearmed" is a key tenet in Sourcefire's strategy. The Sourcefire VRT® (Vulnerability Research Team) analyzes millions of pieces of malware annually and updates rule content regularly to keep our customers up to date to defend against the latest threats. Our rule library includes ICS-specific content, and protocols such as DNP3 and Modbus are natively supported. The Sourcefire VRT may add additional protocol support, often with just a packet capture file of the protocol. Custom content may be created by our customers and by other third parties that may then be imported into our rule library regardless of whether that content was created on our commercial product or our open-source Snort® product. This flexibility makes it easy to share content within the community rather than requiring each customer to build custom content from scratch.

Cyber security is not a point-in-time exercise. It is a continuous process requiring preparation, analysis and intelligent response – Before, During and After an attack.

To put this research to use, you first have to know what it is you're protecting and where it is, but that isn't as easy as it may seem in a control network. Industrial control systems such as remote terminal units (RTUs) and programmable logic controllers (PLCs) are typically built to perform a very specific task and many run proprietary operating systems with the minimum amount of processing power and memory. Therefore, even the most basic discovery methods, such as a ping sweep, could quite conceivably take these industrial control systems down. Sourcefire is able to passively profile control networks without being inline. This means that we will not introduce communications latencies between control systems, and we do not need to aggressively scan the control network. Baselines of behavior and communications patterns may then be established in whitelists where only anomalous traffic is inspected and approved communications are allowed to flow freely as is commonly desired in control networks.

Commercial operating systems such as Microsoft Windows XP have made inroads into the control systems world over the last few years particularly with human-machine interface (HMI) systems and historians. The use of commercial operating systems has provided a benefit to manufacturers in that they do not need to devote the development effort that had gone toward proprietary operating systems, and asset owners enjoy the benefit of increased interoperability between vendors' equipment. This also means that these control systems face increased security vulnerabilities due to the complexity of the operating system code base. That interconnectivity, itself, creates another attack vector. Although commercial vendors regularly release security patches, patching systems in a control network is not the same as patching systems in an IT network. Control system patching cycles are a great deal longer and require extensive testing in order to protect reliability of the control network. Sourcefire provides compensating controls and increased security focus on these systems while they are unpatched and vulnerable.

During

A nation-state probes your corporate network looking for access to your control network; a smartphone is plugged into a management system to recharge the battery and malware is released onto the network; a new device in a substation begins communicating with a management system, which in turn begins communicating with other systems it hadn't communicated with previously; a teen hacker uses a specialized search engine to find a system that was inadvertently connected to the Internet and tries a brute force attack to take control of the system.

Attacks can be swift and blatant, or they can be slow and subtle. They can be direct, or an unknowing middleman can facilitate them. Attacks may endanger physical safety just as much as they endanger network reliability.

Sourcefire monitors your perimeter and your internal network for attacks, anomalous behavior, role violations, advanced malware, and so on, from a single appliance platform. Appliances are available as hardware or virtual appliances. Endpoints and mobile devices may also be monitored for advanced malware. You determine which capabilities you wish to enable based upon your requirements, budget and timelines without adding additional hardware and you can evolve your deployment over time. When anomalies, policy violations and/or indicators of compromise are detected, Sourcefire can respond in an alert-only mode or automatically take action to contain the threat upon detection. The choice is yours. You also have the control to set response policies based upon network segment such that response on vital segments requires human approval before execution. All monitoring, reporting and management are performed through a single, central console.

After

It has been said that no plan survives contact with the enemy. The reality is that attackers' tactics evolve quickly and our defenses must keep pace just as quickly. What may appear innocuous today may be later discovered to have been a cleverly disguised attack. How does one defend vulnerabilities that are not yet known? Sourcefire's threat-centric approach to security includes a continuous capability, always analyzing event and network data searching for patterns and anomalies. When discovered, our Retrospective Security capability determines the source and scope of compromise, contains the outbreak and remediates the malware. With this intelligence you can update protections to minimize the chance of reinfection.

Conclusion

Air gaps are no longer insurance against intrusion and the increased connectivity that brings operational efficiencies to control networks has also brought a host of vulnerabilities and an increased attack surface. While these threats are like those faced by corporate IT networks, the unique requirements of control networks means cyber security solutions are not one-size-fits-all. Sourcefire understands this and helps protect control networks with an advanced cyber security portfolio to remediate threats before, during and after an attack without sacrificing reliability.

6.13 | REV1B