WHITE PAPER

Ensure Availability and Stop the ICS Cyber Kill Chain

A Non-Technical Guide to Breaking the Cyber Kill Chain to Protect Industrial Control Systems and Critical Infrastructure

BlastWave

TLDR

Critical infrastructure that provides the foundation of our public utilities, communications, transportation, and manufacturing systems enables modern society. These systems play a vital role in ensuring a nation's well-being, security, and economic prosperity.

However, critical infrastructure is under constant threat from sophisticated cyberattacks. Hackers notoriously use what is known as the Cyber Kill Chain. This is a series of steps that the bad actors follow to compromise critical infrastructure. The industrial control systems are especially hit hard, posing a significant challenge to the security and resilience of these vital systems.

By adopting advanced, non-disruptive security measures that are easy to manage and implement, organizations can strengthen their defenses against a range of cyber threats and ensure the continued operation of their critical infrastructure.

This white paper aims to educate industrial security leaders on the need to enhance critical infrastructure resilience by breaking the kill chain of cyberattacks using a modern approach to industrial security.
This paper proposes a comprehensive, simple solution ensuring security, safety, and efficiency.

CONTENTS

Secuity and Resilience are Interdependent

Ensuring the resilience of critical infrastructure is of utmost importance to both commercial enterprises and consumers alike, as it guarantees the continuous and reliable operation of vital systems and services that underpin modern society's daily functioning.

The resilience of these systems is intrinsically linked to their security, as disruptions caused by security incidents can have far-reaching consequences, ranging from financial losses and reputational damage to potential threats to public safety.

Recognizing this interconnectedness, the National Institute of Standards and Technology (NIST) has established guidelines emphasizing cyber resiliency engineering. Cyber resiliency engineering integrates systems security engineering and resilience engineering to develop reliable, secure systems capable of anticipating, withstanding, recovering from, and adapting to adverse cyber events.

Security is Key to Resilience

A key aspect of achieving resilience is implementing robust security measures that protect the infrastructure from threats and minimize the impact of incidents when they occur.

The ramifications of poor security in critical infrastructure can be severe, endangering public safety, as evidenced by disruptions to energy distribution, water treatment, or transportation systems.

Given the high stakes involved, it is essential to prioritize security as a means of bolstering resilience.

ICS Cyber Kill Chain:
What it is and How it Compromises Critical Systems

"Kill chain" is a military term that refers to a series of steps an attacker must complete to carry out an operation successfully.

In the context of cybersecurity, the cyber kill chain framework is used to describe the various stages an attacker goes through to successfully compromise a target's critical infrastructure (see **Figure 1**).

Figure 1: The Various Stages of the Kill Chain in Industrial Security Based on Lockheed Martin's Cyber Kill Chain® framework.

Examples of kill chain incidents in critical infrastructure include the Stuxnet attack on Iran's nuclear facilities, the Ukrainian power grid cyberattack, and the Triton attack on a petrochemical plant that affected numerous organizations worldwide (see **Figure 2**). These incidents demonstrate the severe consequences of a successful kill chain, ranging from operational disruptions and financial losses to threats to public safety and national security[5,6,7].

Kill Chain Incidents in the Industrial Sector

- **Stuxnet Attack:**
  Around 100,000 Infected Computers
  The Stuxnet attack infected approximately 100,000 computers by the end of 2010, with over 60% of the compromised systems located in Iran.
- **Ukrainian Power Grid Attack:**
  $2M/Transformer Needed for Repairs
  Repairing more than 40% of Ukraine's power system requires transformers that weigh hundreds of tons and carry a price tag of approximately $2 million each.
- **Triton Attack:**
  Compromised a Petrochemical Company's Network for 3 Yearss
  The Triton attack is believed to have targeted a petrochemical company's industrial control systems in 2017. However, investigations suggest that the attackers had been inside the company's corporate IT network since 2014.

Organizations can reduce the likelihood of a successful cyberattack on their critical infrastructure by identifying and addressing vulnerabilities at each stage of the kill chain. This proactive approach requires an understanding of the challenges of securing critical infrastructure.

Challenges in Preventing the Kill Chain

The modern era presents numerous challenges for securing critical infrastructure, which arise from the evolving nature of technology, the expanding attack surface, and the growing sophistication of cyber threats.

Some of the most significant challenges faced by organizations responsible for critical infrastructure include:

Increasing Surface of Attack
The merging of IT and OT systems, the widespread use of IoT devices, and hybrid work environments create more chances for attackers to exploit weaknesses.
More Than 100 Million Connected Devices
Key sectors with over 100 million IoT devices connected presently include power generation, gas, and water and waste management[8].
Source: Statista

Human Error
Employees can unintentionally expose systems to threats by clicking on phishing links, using weakpasswords, or not updating security, while attackers may target them for system and data accessthrough manipulation tactics.
67% Failed to Comply
Almost 70% of polled employees indicated they did not completely comply with cybersecurity protocols at least on one occasion, with an approximate non-compliance rate of one in every 20 work assignments.9
Source: The Harvard Business Review

Outdated, Unfixable Systems
Critical infrastructure organizations often depend on old, unsupported systems that can't be updated to address current security risks, making them easy targets for attackers.
7 to 10 Years Old Systems Still in Operation, Creating Security Risks
Manufacturers typically offer support for legacy hardware and software for7-10 years. However, obsolete operating systems and an inability to updatevulnerable systems can create security risks for IIOT.10
Source: Security Industry Association

Inadequacies of Traditional Security
Conventional security measures like industrial firewalls, intrusion detection, and antivirus software struggle to keep pace with evolving threats, are challenging to manage, and may not protect against advanced attacks.
40% are Not Confident with Existing Solutions
The level of confidence in their company's current access security solution was low for 40% of the respondents.11
Source: Statista

Expertise Shortage
The cybersecurity field faces a significant skills gap, making it hard for organizations to maintain therequired in-house knowledge to tackle emerging threats and vulnerabilities.
59% Face Cybersecurity Challenges Due to Skills Shortage
More than half of the surveyed cyber leaders revealed they find it challenging torespond to a cybersecurity incident due to the shortage of skills within their team.12
Source: Global Cybersecurity Outlook 2022

Given these challenges, organizations require a new approach to industrial security that simplifies the processes, addresses the unique requirements of critical infrastructures, and offers effective protection against the evolving threat landscape.

A Practical Approach to Industrial Security

Organizations must embrace a more modern, simple, and comprehensive approach to industrial security to overcome the challenges of securing critical infrastructure. This new approach involves several fundamental principles and actionable steps, including:

Simplify
Gartner advises that organizations should rethink their security technology stack to better address sophisticated new threats.13

By adopting a unified security solution instead of multiple disparate ones, organizations can simplifytheir security infrastructure, minimize potential vulnerabilities, and streamline management. This approach leads to a more effective security posture, without the added complexity of managing multiple solutions such as industrial VPN routers and firewalls.

Authenticate
Restricting access to resources using identity is essential for securing critical infrastructure.

Organizations can enforce strong authentication and authorization policies by implementing a zero-trust security model, such as using a software-defined perimeter (SDP) solution with phishing-resistant multi-factor authentication (MFA), which ensures that only authorized users and devices can access sensitive systems and data.

Orchestrate
Comprehensive visibility and control over all elements of the critical infrastructure environment are crucial for maintaining a strong security posture.

Deploying robust management solutions can enable organizations to monitor and control all assets, including gateways, endpoints, users, and agents. This ensures that security policies are consistently applied and enforced.

Set Controls
To further enhance security, organizations should implement granular control measures to defineand enforce access policies for different groups, services, and proxies.

This level of control helps ensure that users and devices can only access the resources they require to perform their job functions, reducing the potential for unauthorized access and data breaches.

Cloak
Creating a virtual boundary around critical infrastructure helps hide it from potential attackers, making it more difficult for them to identify and exploit vulnerabilities.

By leveraging software-defined perimeter technology, organizations can create a virtual perimeter around their critical infrastructure, effectively "cloaking" or hiding it from outsiders and reducing the attack surface.

Organizations can utilize the latest technology to enhance their security posture by following these guidelines and easy-to-follow steps as a foundation.

Stop the Kill Chain Using BlastShield:
A Practical Industrial Security Solution

BlastShield™ is the only peer-to-peer software-defined perimeter (SDP) security solution for operational technology. BlastShield provides a powerful and effective means of protecting critical infrastructure.

Built on the principles of zero-trust security, BlastShield offers a comprehensive approach to industrial security that simplifies the process, enhances resilience, and ensures operational efficiency (see **Figures 3**, **4**, and **5**).

Figure 4: Simplifying Industrial Security with BlastShield

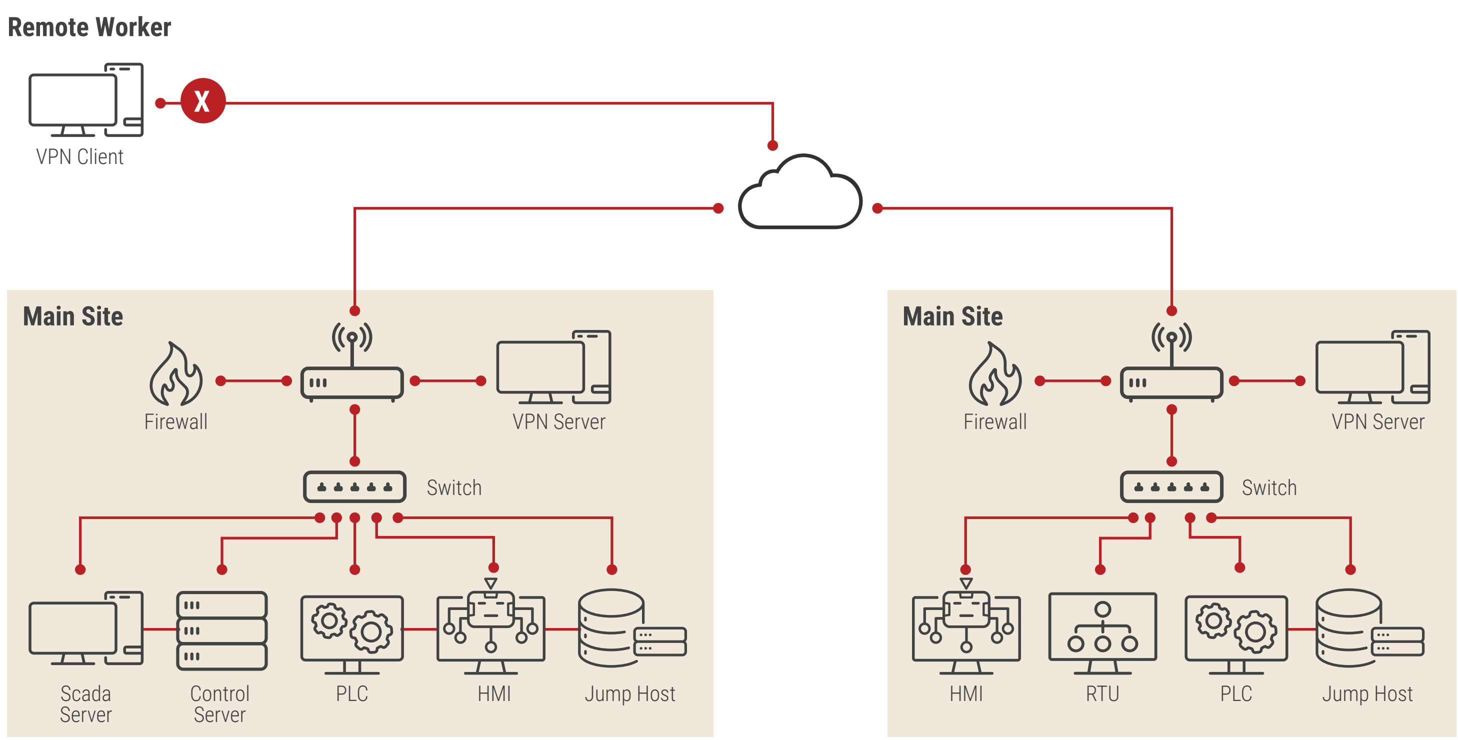


Figure 4: Simplifying Industrial Security with BlastShield

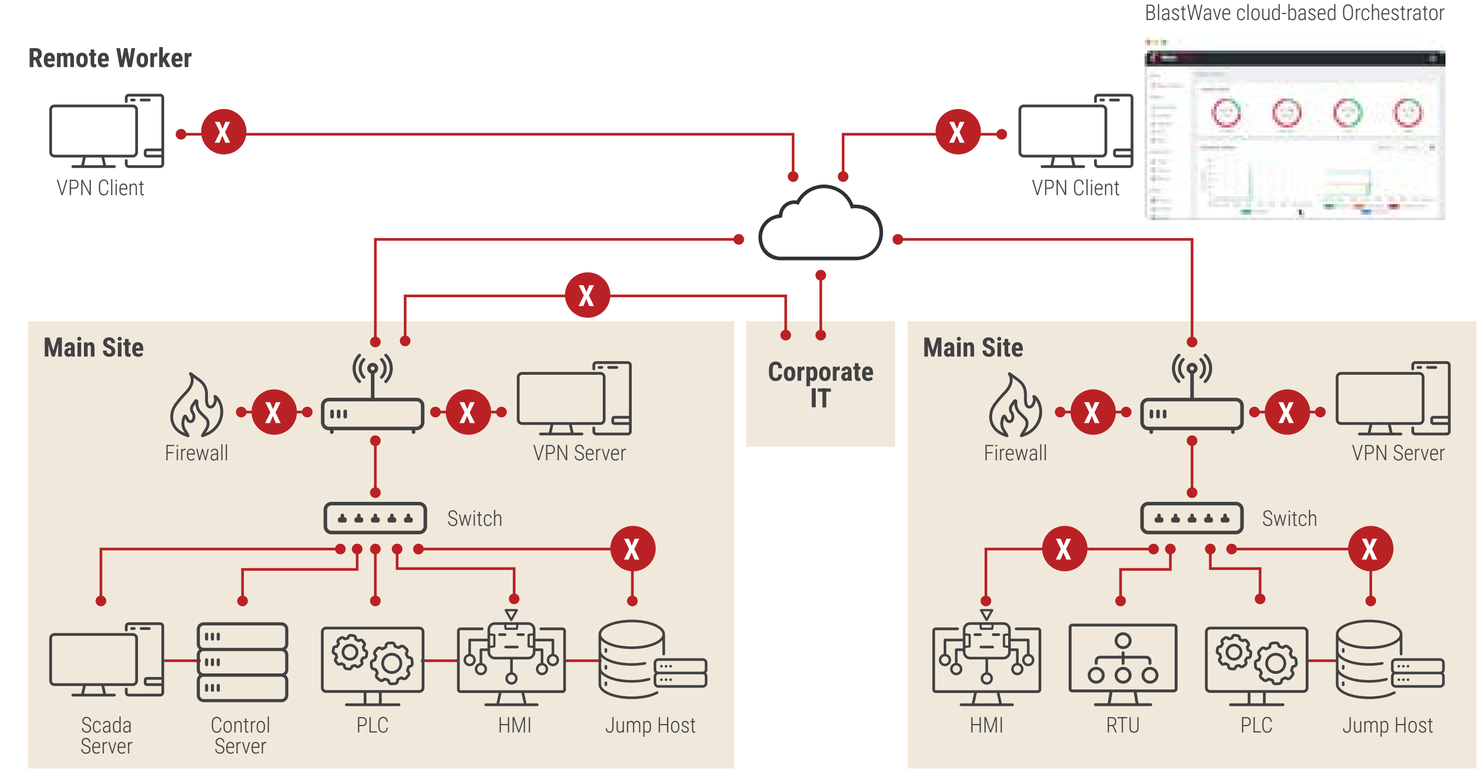
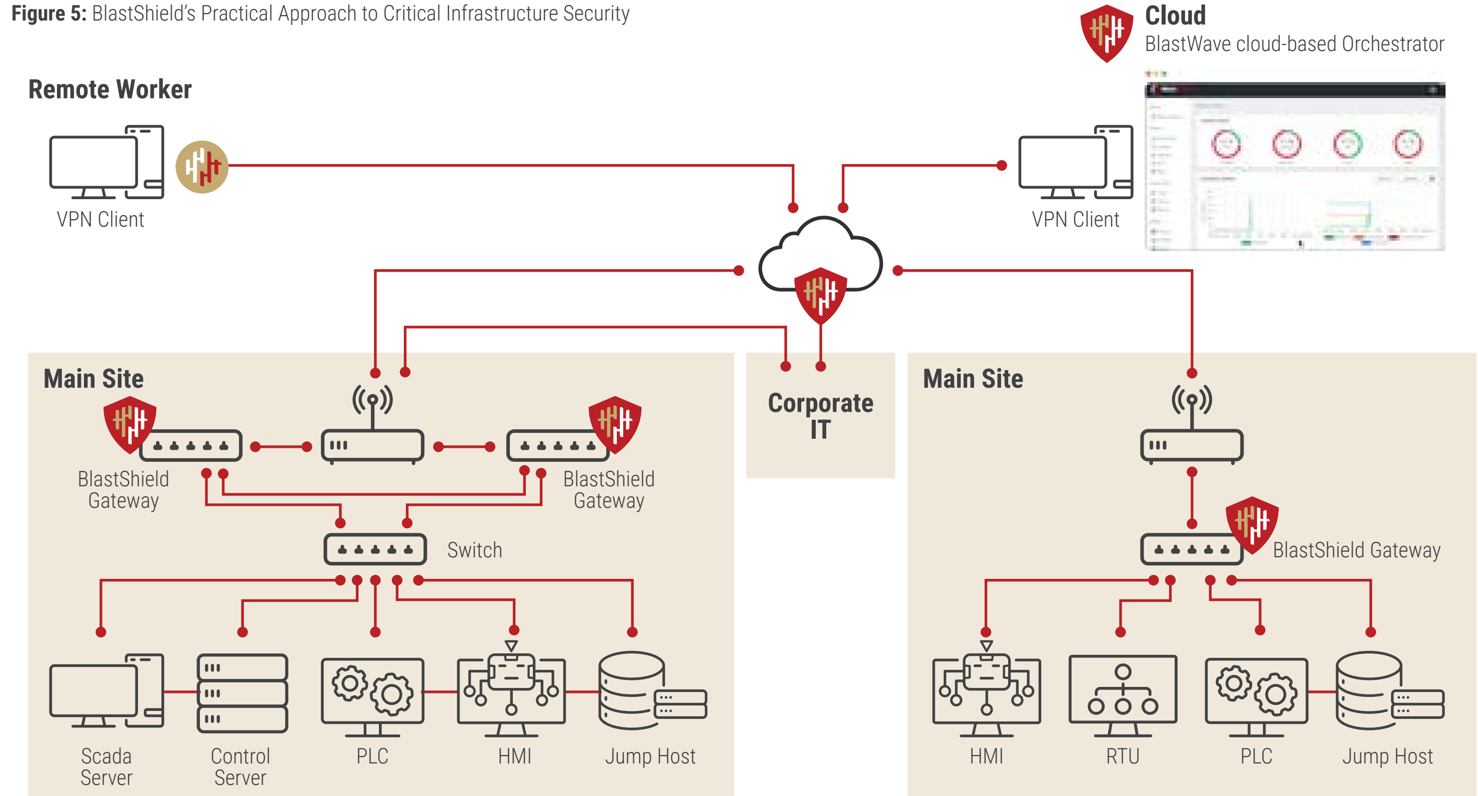


Figure 5: BlastShield's Practical Approach to Critical Infrastructure Security



BlastShield makes it easy for trusted users to access the company's network while making it hard for unauthorized or suspicious people or malware to get into the network. BlastShield also offers a single interface to manage all industrial systems and applications in a practical manner and hide them from attackers.

How to Use BlastShield to Stop the Cyber Kill Chain: A Step-By-Step Guide

BlastShield's simplicity and practicality make it a top choice for organizations seeking comprehensive security solutions for their critical infrastructure.

Here are the easy steps to deploy BlastShield::

1 **Step 1**
Download the Mobile Authenticator app and the Desktop Client.

2 **Step 2**
Register with your BlastShield™ Network.

3 **Step 3**
Connect to your BlastShield™ network and open your Orchestrator.

4 **Step 4**
Install BlastShield™ Agents on Windows, Linux and macOS to protect hosts.

5 **Step 5**
Install BlastShield™ Gateways to protect your devices.

6 **Step 6**
Add new users to your protected network.

This streamlined approach to security management saves time and resources while ensuring comprehensive protection for critical infrastructure.

Protect Legacy Infrastructructure and Critical Assets with BlastShield

By adopting BlastShield, organizations can effectively address the challenges they face, simplify their security stack, and enhance their systems' resilience and operational efficiency. In doing so, they can better protect their critical assets and the communities they serve from the ever-evolving threat landscape.

Protects Legacy Control Systems
BlastShield offers a robust security solution specifically designed to protect aging and unpatchable legacy industrial systems, addressing a significant challenge faced by many critical infrastructure organizations.

Simple SCADA and ICS Security
By focusing on simplicity and effectiveness, BlastShield provides comprehensive protection for industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems, disrupting the kill chain of cyberattacks and preventing threats before they can cause damage.

Significantly Reduces Security Costs
BlastShield helps organizations cut security costs by up to 70% streamlining the security stack and consolidating various security technologies into a single, unified solution.

Prevents Attacks Before They Happen
BlastShield enforces a proactive approach to security by implementing phishing-resistant multi-factor authentication (MFA) and mutual authentication, cloaking devices to make them undiscoverable on the network, and protecting critical assets and legacy infrastructure to stop lateral attacks.

Simplifies the OT Security Stack
BlastShield replaces multiple traditional security technologies, such as VPNs, firewalls, and access control lists (ACLs), simplifying the security stack and making it easier to manage and maintain.

Unintrusive Implementation
Organizations can easily integrate BlastShield into their existing infrastructure without experiencing significant downtime or workflow interruptions.

Moreover, BlastShield is designed for easy installation on Windows; Debian, ARM, and RPM based Linux distributions; and macOS, ensuring compatibility with various systems and devices used in critical infrastructure environments.

BlastWave

Conclusion

As we move towards an increasingly digital and interconnected future, it is crucial for organizations responsible for critical infrastructure to prioritize security and resilience.

By adopting innovative security solutions like BlastShield, these organizations can ensure the continuous and reliable operation of vital systems and services, safeguarding our communities, and fostering a more secure and resilient future.

BlastShield offers a powerful and practical solution for organizations seeking to enhance the resilience and security of their critical infrastructure. By leveraging software-defined perimeter technology and embracing the principles of zero-trust security, BlastShield provides a simple, effective, and cost-efficient way to protect critical systems and disrupt the kill chain of cyberattacks.

Call to Action

We invite Manufacturing CISOs and CIOs to explore how BlastWave can revolutionize their OT cybersecurity posture and help achieve strategic operational and financial goals. Take the next step towards a more secure and resilient future:

Discover the Technology:
Visit the BlastWave website at **www.blastwave.com** to download detailed technical whitepapers on BlastShield's Zero Trust capabilities and OT-specific solutions.

Assess Your Needs:
Request a personalized assessment to understand how BlastWave's network cloaking, secure remote access, and microsegmentation can address specific cybersecurity challenges within your manufacturing operations.

See it in Action: Schedule a live demonstration to witness firsthand how BlastShield™ makes OT assets invisible, provides phishing-resistant access, and prevents lateral movement within industrial networks.

Begin Your Zero Trust Journey: Protect Your Critical OT Infrastructure Quickly and Cost-Effectively. Explore options to trial BlastShield™ and experience its ease of deployment and powerful protection capabilities.

v20250904

About BlastWave

BlastWave securely connects Industrial Control Systems, Operational Technology, and Critical Infrastructure networks with Zero Trust Protection and delivers industrial-grade cybersecurity with consumer-grade ease-of-use. Visit **www.blastwave.com** to learn more.

BlastWave

1045 Hutchinson Ave.
Palo Alto, CA 94301 USA
T: +1 650 206 8499