Confronting AI-Powered Threats

AI-Resistant OT Cybersecurity Simplified

BlastWave

Introduction

Generative AI (GenAI) tools have fueled an alarming rise in successful attacks on critical infrastructure. These AI tools dramatically improve the quality of phishing emails and enable the fast creation of no-code hacking tools.

A report by the National Cyber Crime Security Center in the UK highlighted the uplift that AI would give hackers, especially unskilled hackers, dramatically affecting two of the biggest initial threat vectors: Phishing and Reconnaissance.

New solutions are required to cut off these attack vectors and protect critical infrastructure networks vital for a nation's operation. Existing IT solutions are too complex and expensive.

This eBook explores the new type of Operational Technology (OT) cybersecurity protection solution needed to combat the rapidly growing threat from AI-powered cybercriminals, hacktivists, hackers, bad actors, and hostile nation-states.

CONTENTS

The Evolving AI-Threat Landscape

OT Protection solutions are intended to permit only authorized users access to the critical network they protect. The existing paradigm of using Firewalls (designed for filtering network traffic) and VPNs (designed for access based on credentials) has dramatically failed to protect OT networks worldwide, as shown by the constant stream of news stories on hacks and ransomware.

New Generative AI (GenAI) tools are being created that build on the strong foundation provided by ChatGPT (like WormGPT and FraudGPT) and an ever-evolving suite of Large Language Modles (LLMs) to automate hacking attempts. The UK NCSC Impact of AI Report highlights that AI will almost certainly increase the volume and heighten the impact of cyber attacks over the next two years.

It also highlights that these threats will not be novel threats but an evolution and enhancement of existing tactics, techniques, and procedures (TTPs).

The most concerning contents of the report are the discussion of who will benefit the most from these new tools. Although highly capable nation-states and hacking groups will gain benefit from the tools, the largest benefit will be had by low-skilled hackers, which could unleash a tsunami of hacking attempts around the world.

OT cybersecurity managers looking to minimize the attack surface vulnerable to AI-powered attacks can focus today on two of the vectors identified in the report: Phishing and Reconnaissance.

	Highly capable state threat actors	Capable state actors, commercial companies selling to states, organised cyber crime groups	Less-skilled hackers-for-hire, opportunistic cyber criminals, hacktivists
Intent	High	High	Opportunistic
Capability	Highly skilled in AI and cyber, well resourced	Skilled in cyber, some resource constraints	Novice cyber skills, limited resource
Reconnaissance	**Moderate uplift**	**Moderate uplift**	Uplift
Social engineering, phishing, passwords	**Uplift**	**Uplift**	**Significant uplift (from low base)**
Tools (malware, exploits)	**Realistic possibility of uplift**	**Minimal uplift**	**Moderate uplift (from low base)**
Lateral movement	**Minimal uplift**	**Minimal uplift**	No uplift
Exfiltration	**Uplift**	**Uplift**	**Uplift**
Implications	Best placed to harness AI's potential in advanced cyber operations against networks, for example use in advanced malware generation.	Most capability uplift in reconnaissance, social engineering and exfiltration. Will proliferate AI-enabled tools to novice cyber actors.	Lower barrier to entry to effective and scalable access operations - increasing volume of successful compromise of devices and accounts.

Phishing:

Many phishing attempts today are clumsy attempts at getting you to click on a link to steal your credentials or install malware/ransomware. This will change as hackers leverage GenAI to craft better phishing emails and conduct research on targets and their business and social networks. Now, the hackers will send more effective emails, tricking the user because they use the right "voice" of the spoofed identity with customized emails per target.

Imagine a teenager who has had a bad experience with a brand. To get revenge, they want to attack a brand's manufacturing plant for revenge. They know nothing about the plant at all and they are not a hacker. So, they ask an AI to find who the critical network manager is at the plant, study their online profiles and style of writing, and then write targeted phishing emails to their employees to steal credentials. For example, social media might reveal a trip or an activity that can be referenced by email to show an intimate knowledge of the target. Then, wait for the phishing to work and proceed to the next phase of the attack, which more AI tools will power.

Reconnaissance:

AI can also gather critical intelligence that mimics the old hacker trick of "dumpster diving." AI can be pointed at a target to determine what networking vendors they use (often available in vendor announcements, public RFP releases, etc) and if they have any known vulnerabilities. It can also create simple no-code scanning tools once the hacker is inside the network (when their phishing attack bears fruit, for example.)

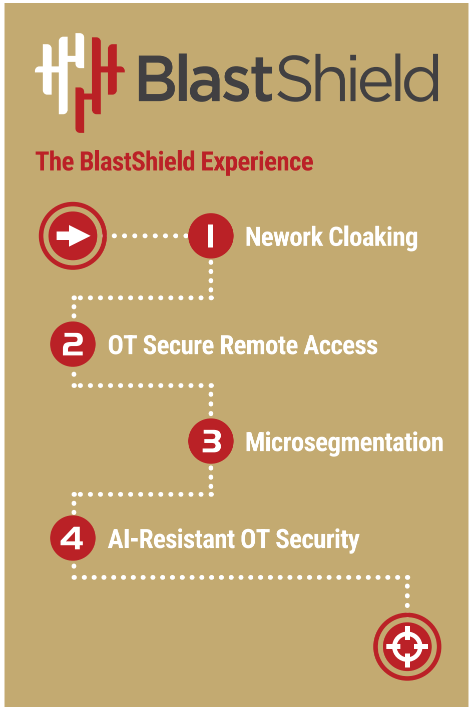
Going back to the previous example, they can also ask the AI to code some network reconnaissance and exploit tools based on the vendors that the company uses. Using these tools, they can map out the entire network and take control of multiple vulnerable systems that have not been patched by the IT or OT staff. By this time, they have access and control of enough of the network to cause severe damage (if solely focused on revenge) or to attempt to extort the brand for money (either with ransomware, threatening damage, or exfiltrating sensitive data and leaking it).

OT CyberSecurity Simplified

If the AI can’t get access to your network, then it can’t attack it.

In today’s always connected environment, many OT systems are remote-controlled and monitored, and their administrators and contractors need remote access to manage and monitor them. But you can create a Virtual Air Gap. Firewalls and VPN solutions tried (and failed) to do that, but AI can beat both because the keys to access can be stolen or hijacked.

AI can’t (yet) beat a system that does not allow internal systems internet access and when only biometric authentication can access the gateway. If you combine Network Cloaking with biometric enforced Secure Remote Access, you get something that an AI can’t see (cloaking) and can’t access (biometrics). Operational Technology networks are sometimes called “Cyber-Physical” because they combine physical systems with network technology. If you combine something physical with something cyber, you create a strong barrier to AI-powered cyber threats.


BlastShield
The BlastShield Experience
1 Nework Cloaking
2 OT Secure Remote Access
3 Microsegmentation
4 AI-Resistant OT Security

Network Cloaking

Network Cloaking proactively secures systems, making them undiscoverable to potential attackers by blocking all inbound and outbound internet access to legacy OT systems. Imagine a hacker scanning a network and finding nothing that responds.

Network cloaking, combined with Zero Trust access controls, effectively creates a “virtual air gap.” This simulates the security benefits of a physical air gap by isolating vulnerable devices from the outside world, but without the operational limitations of physical disconnection. It ensures data cannot be viewed, deleted, or changed by unauthorized entities, accessible only with validated credentials and Multi-Factor Authentication (MFA). While a physical air gap is often impracti cal in modern, connected OT environments, a virtual air gap provides the security benefits of isolation (e.g., breach containment, protection for unpatchable devices) while maintaining operational connectivity, thus bridging the traditional security-availability divide in OT.

While traditional firewalls primarily function by enforcing access control based on predefined rules, determining which specific types of traffic are permitted or denied, network cloaking alters an attacker’s perception of the network. Instead of merely filtering traffic, it actively conceals the network infrastructure itself. A cloaking system, unlike a firewall that might still present a discernible interface, does not respond to network scans, rendering the devices behind it undiscoverable and unanalyzable. This prevents the exploitation of both known and zero-day vulnerabilities.

OT Secure Remote Access

OT Secure Remote Access must evolve beyond the username/password paradigm to resist AI-powered attacks. Rather than granting access to a network simply because of the IP range you are coming from (like a firewall) or the credentials you present (like a VPN), your identity is your key with BlastShield.

Strong OT Secure Remote Access begins with biometrics-enabled Multi-Factor Authentication (MFA), a phishing-resistant method that today's AI cannot yet hack. A BlastShield client can be installed on any OS, and the Mobile Authenticator is deployed on a mobile device with Biometrics (Apple or Android). When the Client attempts to authenticate, it presents a QR code to be scanned by the Mobile Authenticator, completing the biometric authentication and validating the remote user.

Once a user is authenticated, peer-to-peer encrypted tunnels are set up between the client and any deployed gateways or host agents. These tunnels are cryptographically separated and protected with AES-256.

BlastShield™ is a transformative solution for OT Secure Remote Access, delivering a superior user experience with ironclad security. BlastShield™'s secure remote access capabilities are essential across various industries, each with unique challenges and requirements. BlastShield connects not only users but tens of thousands of OT systems and devices that may be geographically dispersed and require secure connectivity.

Microsegmentation

Think of network segmentation like building fences inside your factory. It separates different parts of your OT network so a problem in one area can't spread to others. Microsegmentation takes it further, putting fences around individual machines or systems. This limits the damage a hacker can do and keeps your critical operations running smoothly. AI-powered systems can't freely move around the network if it is segmented properly.

BlastShield™ exceeds traditional segmentation by advancing the concept of microsegmentation as a superior security alternative. Unlike broad segmentation strategies, BlastShield's microsegmentation allows for incredibly detailed control, segmenting networks down to the level of individual devices, systems, protocols, or users.

By isolating network segments, BlastShield effectively prevents the lateral movement of threats within the network, a critical defense mechanism against external and internal threats. BlastShield™ policy changes take effect in real-time, facilitating dynamic and flexible policy enforcement during emergencies or administration changes. Unlike many solutions that use ACLs and VLANs, microsegmentation scales effortlessly to large OT environments.

With its detailed segmentation capabilities, BlastShield™ aids in compliance with stringent regulatory standards, offering necessary tools to protect sensitive data and ensure privacy. BlastShield's microsegmentation solution is innovative, future-ready network security.

Preventing The Terminator

It isn't likely that SkyNet or an actual Terminator will come any time soon to attack your OT network. However, the quality and frequency of attacks will grow dramatically over the next few years. A 2024 report by Slashnet showed that malicious phishing emails increased by 4,154% since the launch of ChatGPT.

A different perspective is needed when looking at Critical Infrastructure and OT cybersecurity challenges. A famous entertainer once said, "Just when they think they have all the answers, I change the questions." The essence of this quote is that we need to challenge assumptions that we hold and maintain the initiative over attackers rather than simply reacting. Cybersecurity history tells us that some things will never change:

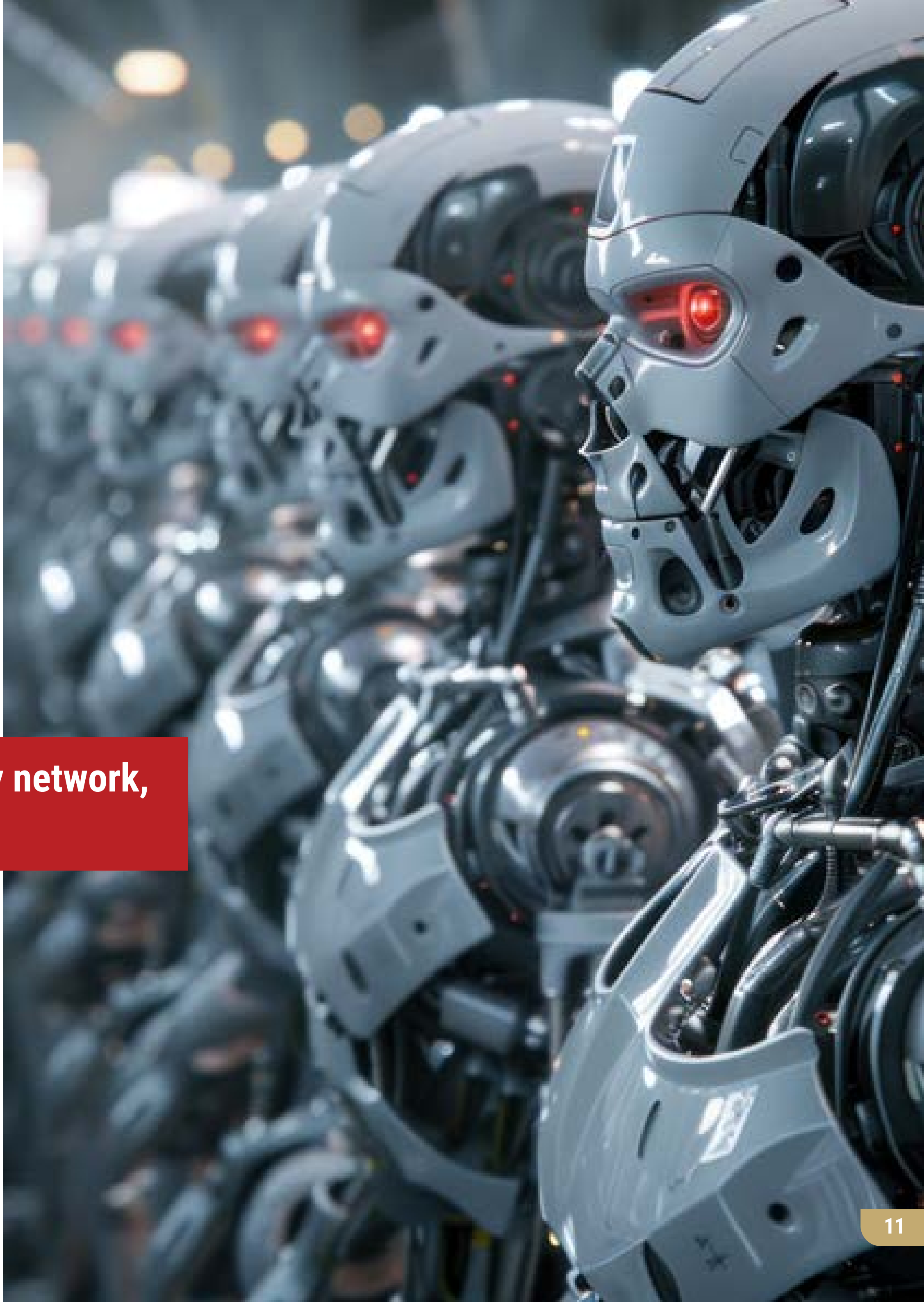
1. **Software will always have vulnerabilities:** Every system has weak points.
2. **Legacy OT systems can't always be patched:** OT systems can last for decades, not 3-5 years, like many IT systems.
3. **Human Error is unavoidable:** Misconfigurations, phishing, malware, and many other attack vectors simply cannot be blocked no matter how many firewalls you put in your network.

If we hold these three truths as selfevident, many current security strategies echo the strategies of the Dutch Boy and the Dike – keep putting your fingers in to plug the holes and hope that more don't occur.

"What if?" is the question we need to ask ourselves.
What if the hackers could not discover the OT systems and devices hidden behind a gateway? What if your access used biometrics, not passwords, and your mobile device's security certificate, just like Apple Pay? What if peer-to-peer encrypted tunnels secured all connections, and no lateral movement was allowed, even on a Layer 2 network?

So what should the new question be?
What if I could protect my network, not just react to attacks?
Cybersecurity for Critical Infrastructure is all about breaking the kill chain – and breaking multiple links, not just one. If you want to change the game and protect your OT network, explore Blastwave's Network Cloaking technology and get a demo.

What if I could protect my network, not just react to attacks?



BlastWave's OT Protection Solution

BlastWave delivers a comprehensive Zero Trust Network Protection solution to provide the best possible outcome for OT environments. With a unique combination of network cloaking, secure remote access, and software-defined microsegmentation, we minimize the attack surface, eliminate passwords, and enable segmentation without network downtime.

To learn more, come to
www.blastwave.com

v20250627

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