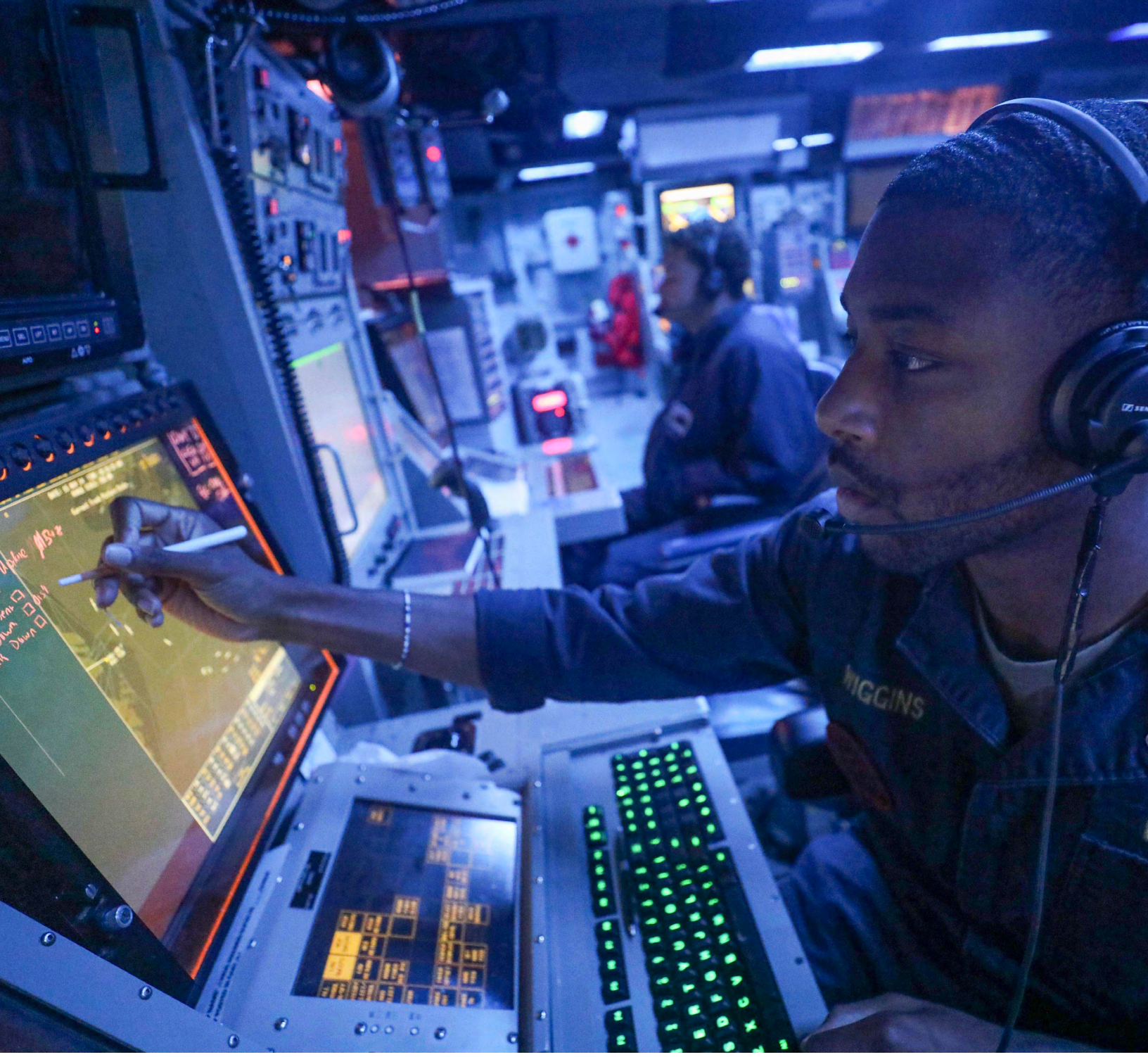


Ensuring Cybersecurity When Cloud Isn't an Option

MARKET TRENDS REPORT

govloop

CHECK POINT™
PUBLIC SECTOR

Executive Summary

For the U.S. Department of Defense, the Federal Emergency Management Administration (FEMA) and operators of critical infrastructure, cybersecurity is paramount. Yet these organizations face a significant challenge. Conventional cybersecurity depends on access to the cloud, and defense organizations and emergency responders may operate in environments where limited bandwidth strains cloud connectivity. Some military and critical-infrastructure environments are air-gapped, deliberately disconnected from the internet. In these situations, conventional cyber solutions fall short.

This presents significant operational risk. "There is malware out there now that can sit dormant for days, weeks, months or even years before it executes," said Joe Ford, Cyber Security Evangelist and Security Architect at Check Point Software Technologies. Imagine a sailor who goes ashore, logs in at a coffee shop, then brings that laptop back to the ship. Once at sea, the ship likely isn't updating its cybersecurity frequently — there just isn't the bandwidth available to do that. Now that malware can slip by and lie dormant, awaiting activation.

That's just one scenario in which low or no cloud connectivity imperils cyber readiness.

In disconnected and low-bandwidth environments, a new approach is needed — one that does not depend on cloud connectivity. A modernized approach will leverage artificial intelligence (AI) to keep protections current, even when cloud-based updates aren't available. Such a solution could help ensure the security of troops on the edge and ships at sea, as well as emergency responders and sensitive critical infrastructure.

184

The average number of days to identify a cyber breach, plus 63 days to contain the breach with AI, versus 239 days to identify and 85 days to contain without AI

Over 20,000

Distinct cybersecurity vulnerabilities each year in the defense industrial base

Need to Know

50+

The number of security engines powered by AI in ThreatCloud AI

86 billion

Daily transactions analyzed by Private ThreatCloud AI

Examples of AI-based Security Technologies

- Infected hosts detection
- Sandbox static analysis
- Sandbox dynamic analysis

30,000

The number of DoD cyber worker vacancies in late 2024

$1.88 million

The average savings for organizations using AI in cybersecurity

Advantages of AI in Security

AI is already used in security, and its role will continue to grow over time. Some of the benefits of AI for security include:

Automation of repetitive tasks: Cybersecurity requires a great deal of data collection, analysis, system management and other repetitive tasks that consume analysts' time and resources. AI has the potential to automate these activities, enabling security personnel to focus their efforts where they are most needed.

Improved threat detection and response: AI is ideally suited to collecting massive amounts of data, analyzing it and responding based on extracted insights. These capabilities can enhance an organization's threat detection and response by speeding and scaling the detection and response of cyberattacks, reducing the damage that attackers can do to the organization.

Enhanced situational awareness and decision-making: Often, security personnel suffer from data overload, having more information than they can effectively process and use. AI excels at data collection and processing, and the insights it provides can improve security personnel's situational awareness and ability to make data-driven decisions.

Cybersecurity When Ensured Connectivity Is Lacking

The Challenge: Cyber Without Cloud

A number of challenges can hinder effective cyber resilience in disconnected and low-bandwidth environments. Common issues include:

Architectural issues: Conventional approaches to cyber depend on access to the internet. "Most modern security solutions require cloud connectivity to pull updates and identify new threat indicators," Ford said. "You have endpoints that are connecting to a management server, which is connecting to the cloud to get that intelligence."

When cloud-connected architecture isn't an option, cyber resilience suffers. Defenders must rely on a static version of their threat detectors, leaving systems vulnerable to new and emerging threats. There's no real-time protection against zero-day threats — attacks that look to exploit previously unknown vulnerabilities.

Low connectivity: Ships at sea and disaster responders may have some internet connectivity, but not enough to support the continuous updates needed to keep cyber defenses current. They typically cannot afford to devote their limited connectivity to such tasks.

"The bandwidth they have needs to be, should be and typically is, focused on the mission at hand — not the security systems," Ford said. When FEMA or forward-deployed military units do have connectivity, they're using it to communicate requirements, doing things to address the mission, not updating security solutions to keep their systems safe.

Air-gapped environments: Classified military operations often will be air-gapped, deliberately disconnected from the internet to keep them safe from prying eyes. The same applies to critical infrastructure. "We don't connect nuclear reactors to the cloud, and for good reason," Ford said.

But without that connection to the cloud, cyber resilience can fall short. Here again, the challenge lies in keeping systems current in the face of new and emerging threats. This holds true for almost all DoD classified environments, as well as almost anyone in a forward-deployed position.

The Solution: Interconnected, AI-Informed Defenses

A modernized approach can help overcome these challenges. The characteristics of such a solution include:

Interconnectivity: For a cybersecurity solution to deliver in disconnected or bandwidth-challenged environment, the devices all need to talk to one another. "You need the endpoint devices and the network devices to have interconnectivity, everything speaking the same language," Ford said.

With strong interconnectivity, "they're actually able to update each other," he said. That empowers them to share analysis capabilities, so that as new threats emerge in the system, there's a common awareness, which in turn empowers effective response.

AI-informed defenses: But how will those devices recognize new threats, in the absence of cloud-based updates? That's where AI comes into play. In this situation, defenders can leverage AI to collect and understand data reflecting system operations, thus speeding the detection of anomalous behaviors that can be threat indicators.

"With AI built into that solution, it's possible to deliver real-time analysis, identifying threats as they're occurring based on the behaviors," Ford said. That accelerates detection and response, bolstering cyber protection and ensuring mission security.

Ability to operate in real time: With AI support and device interconnectivity, a modernized solution can deliver real-time cyber awareness and protection, even when systems are disconnected from the cloud, or deprived of adequate bandwidth to support frequent updates.

That's essential in today's high-stakes cyber environment. "This is something that needs to occur at the speed of the mission. It can't be something that the mission's waiting on," Ford said.

Automation also can help, taking on repetitive, time-intensive tasks, such as building out and refreshing indicators of compromise that are used to find vulnerabilities.

Best Practices

Organizations need to make thoughtful choices in selecting a cyber solution that can support the mission in disconnected and low-bandwidth environments. As a matter of best practice, IT leaders in military, emergency management and critical infrastructure need to look for solutions that can deliver ...

Compliance

In the federal space, cyber solutions need to hit a number of regulatory benchmarks in order to attain authority to operate. For example, they need to comply with NIST SP 800-53, which defines security and privacy controls for information systems and organizations.

"You need something that will check the boxes that are required for the technical security controls around both endpoint and network security," Ford said.

For military users, it makes sense to seek out solutions that are already on the Department of Defense Information Network (DoDIN) Approved Products List (APL), a list of products that meet DoD cybersecurity and interoperability requirements.

A platform for consistency and repeatability

Heterogeny often is the enemy of cybersecurity in high-stakes environments. "Navy people move from ship to ship. FEMA people move from disaster to disaster. There's a lot of mobility in the workforce associated with these types of work," Ford said.

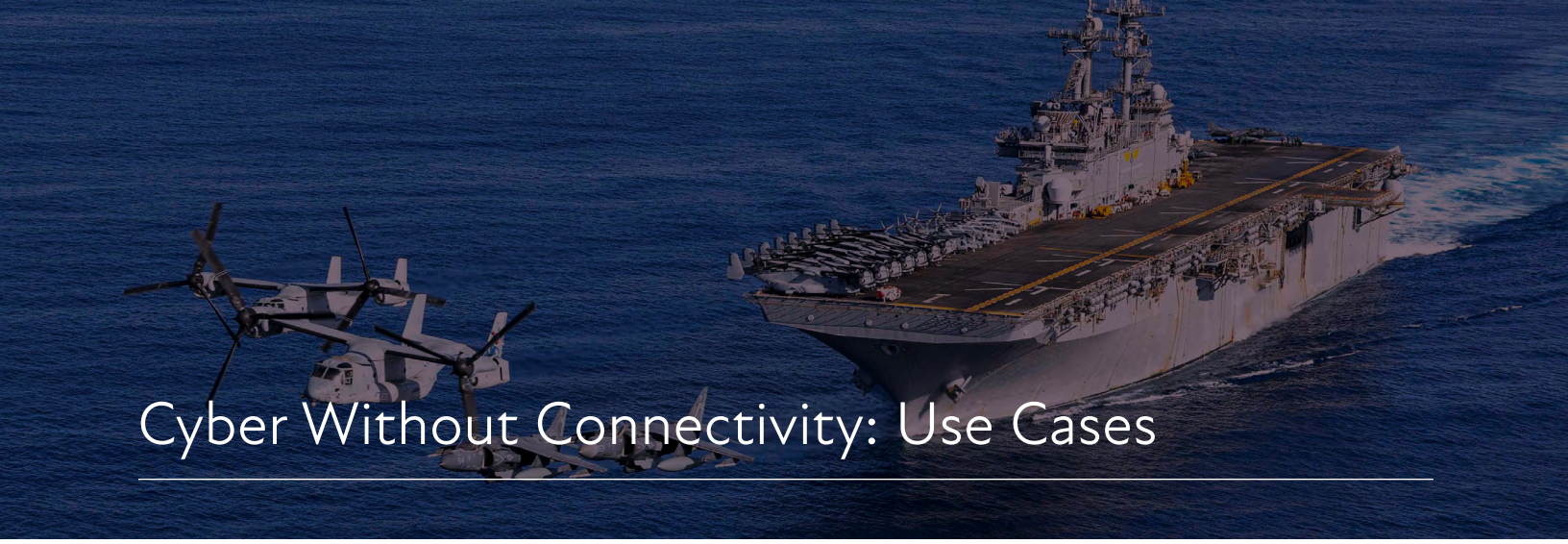
When individuals confront unfamiliar systems, there's a learning curve and potentially a lag in effective cyber defense. Ideally, "you want a system that's deployed exactly the same in every environment, so that anyone can walk in and know exactly how to operate it, and not have to be retrained and re-accredited," he said.

"If someone trains on a platform, then anytime they run into that same platform, they will know what to do. They don't have to be retrained," he said. "When a sailor comes to a new ship, they don't have to spend 90 or 120 days getting up to speed. They can be up and operating in 24 hours."

State-of-the-art technology

An effective solution will bring state-of-the-art technology to environments where cloud connectivity isn't readily available. "In the critical environments, whether it's a ship or a nuclear reactor during a disaster response, we can't be using legacy approaches," Ford said.

"Systems that were designed 10 years ago cannot be expected to actually protect against modern threats," he said. A modernized solution "needs to be keep up with zero-day threats, and that requires state-of-the-art technology."



Cyber Without Connectivity: Use Cases

To understand where and how a modernized, platform-based solution can support government cybersecurity in low-connectivity and disconnected environments, it's helpful to consider a few specific use cases.

Navy ships: On ships, low connectivity is a given. Most don't have high-speed internet and some never will: You're never going to get robust connectivity on a submarine.

"The threats change every day, and they need a means to address that. They need AI in order to grow and change, to detect those zero-day threats over time," he said. With a modernized approach, updates are inherent in the system, so it's possible to keep current on changing threats without having to constantly recertify the technology.

Forward-deployed units/FEMA field operations: For forward-deployed units and FEMA, these same low-bandwidth limitations are compounded by form-factor considerations. For the sake of mobility, "being able to deploy a solution that is only a box or two becomes important," Ford said.

A modernized solution "will deliver the AI needed to provide modern threat prevention in that disconnected or limited-connectivity environment, without having to have a bring along a whole data center," he said.

Critical infrastructure: Bad actors are always looking to exploit cyber-protection gaps in critical infrastructure. "For energy companies, especially the ones that run nuclear, those environments are not connected to the internet," Ford said. "But they still need to provide a high level of security, and they do compliance levels they have to meet."

HOW CHECK POINT HELPS

Check Point products help ensure cyber resilience in bandwidth-constrained and disconnected environments.

"Check Point Harmony Endpoint provides full endpoint security for user endpoints, along with full disk encryption, malware, data loss prevention, connected devices, USB protection," Ford said. A comprehensive and consolidated solution, it delivers endpoint protection at the highest level, helping organizations avoid security breaches and data compromises.

Check Point Quantum Firewall delivers the AI-powered security that organizations need to keep one step ahead. Miercom Enterprise and Hybrid Mesh Firewall Benchmark 2025 reports the tool is 99.9 percent effective in threat prevention, outpacing any other solution in the market.

Behind the scenes, both systems use the AI engine Check Point Private Threat Cloud in place of the cloud. "It integrates threat detection down into an appliance, providing the same threat cloud capabilities that we have in the cloud, in disconnected environments," Ford said.

Learn more: www.checkpoint.com

Conclusion

Conventional wisdom holds that you can't have effective cybersecurity without cloud connectivity. But for military users, emergency responders and critical-infrastructure operators, cloud isn't always an option. They may need to air-gap, for security reasons, or they may lack sufficient bandwidth to support cloud-based cyber defenses.

For these users, a modernized cyber platform can deliver enterprise-class security even in the absence of robust cloud connectivity. Rather than rely on updates in the cloud, such a solution taps the power of AI to analyze activity, highlighting areas of emerging concern in real time.

Such an approach can help to contain zero-day threats even when cloud connectivity isn't available, thus ensuring the security of systems and networks in support of mission-critical operations. At a time when cyberattacks are on the rise, and IT teams often are stretched thin, AI and automation can deliver true cyber resiliency in even the most constrained environments.

ABOUT

CHECK POINT™
PUBLIC SECTOR

Check Point is a leading cybersecurity innovator, using AI to autonomously predict and prevent attacks across networks, clouds, endpoints, and devices for the public sector. It delivers an AI-powered, cloud-based cybersecurity platform with 99.9% malware blocking, 99.7% phishing prevention, and 98% defense against critical intrusions.

Learn more at www.checkpoint.com.

govloop

GovLoop's mission is to "connect government to improve government." We aim to inspire public-sector professionals by serving as the knowledge network for government. GovLoop connects more than 300,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to connect and improve government.

For more information about this report, please reach out to info@govloop.com.

1152 15th St. NW Suite 800
Washington, DC 20005

P: (202) 407-7421 | F: (202) 407-7501

www.govloop.com
@GovLoop