carahsoft

FORTINET FEDERAL

Key Webinar Insights:

Fortinet Federal & Garland Technology Better Together

Thank you for your interest in exploring this content.

Carahsoft is the **Trusted Government IT Solutions Provider**® supporting a broad portfolio of industry-leading technologies through GSA, DoD ESI, and a wide range of other contract vehicles.

As the **Master Government Aggregator**®, Carahsoft connects government agencies, industry partners, and technology providers to deliver innovative, mission-focused solutions.

In partnership with Fortinet Federal, we provide technology solutions that drive modernization, strengthen operations, and ensure compliance with evolving government standards.

To learn more about how Carahsoft can support your technology needs, please visit carahsoft.com

Explore More Resources:
carah.io/FortinetFederalResources

Join Events & Webinars:
carah.io/FortinetFederalEvents

Discover Technology Solutions:
carah.io/FortinetFederal

Learn About Procurement:
carah.io/FortinetFederalContracts

Connect With Our Team:
fortinetfederal@carahsoft.com
(866) 468-3868

FORTINET FEDERAL | GARLAND TECHNOLOGY See every bit, byte, and packet® | carahsoft.

Webinar Key Insights:

Fortinet Federal and Garland Technology Better Together

1) How is Zero Trust forcing the convergence of IT and OT networks?

Ben Brooks, Fortinet Federal:

"Zero Trust is continually kind of forcing this convergence of IT and OT networks. There's going to continue to be that connection, and those OT devices are very, very vulnerable to any kind of IT tool that has the ability to move laterally down to those devices and see what they can pull off of them."

2) Why are OT environments especially difficult to secure?

Ben Brooks, Fortinet Federal:

"Some of these OT devices are 30, 40 years old, especially on the DOD side, and so you can't update them. You can't add additional software updates to secure them. A lot of times, if you put anything that's security, any kind of security product down towards those tools, it will break something, and they can't withstand something that sits as a security tool in line to pull information off of it."

3) What makes monitoring DoD legacy networks uniquely challenging?

Sean Gerrity, Garland Technology:

"Most of it is on a lower speed, especially in my space in the DoD side, because we are talking about legacy networks. When we think about that, we want to make sure we have a really broad product portfolio line that is going to support that lower end traffic and all the way up into our core perspective, obviously on the data center side, where we are hitting on 100, 400 gig."

4) How do bypass taps prevent outages caused by inline tools?

Sean Gerrity, Garland Technology:

"An inline tool can become a potential single point of failure when inserted directly into the path of a critical network link. The bypass tap was developed to resolve this problem of an inline tool and eliminate the single point of failure. It maintains network uptime, eliminates maintenance windows, ensures tool configurations are working properly, and ensures that the monitoring tool only receives traffic when it is healthy."

5) Why is partnership essential for securing federal IT/OT ecosystems?

Sean Gerrity, Garland Technology:

"It really is a collective environment to secure these networks. It takes a lot of different solutions and partners to come together with a common cause for us to bring this to market and support the community. When we think about that, we spend a lot of time with our partners, whether it is Navy, Army, or Air Force, and they are really focused on these environments and how we can support their mission set."

6) Why are hardware data diodes critical in Zero Trust architectures?

Sean Gerrity, Garland Technology:

"Hardware data diodes ensure that Ethernet packets flow in one direction out of the monitoring ports without physical hardware separation. It is impossible for the traffic to flow bidirectionally, and this is hardware based so there is no software path. The traffic control is enforced at the physical hardware level, which is really important to kind of focus on in this discussion, and this is much more secure and much less expensive than a software based approach."

7) How does virtual patching work for vulnerable OT and ICS devices?

Ben Brooks, Fortinet Federal:

"We can perform virtual patching to effectively create a signature that notices that traffic. It knows that that product is blank years old, it knows the version that it is on because we are getting that extra visibility, and we can preemptively block specific kinds of traffic that might be a known threat vector for that OT or ICS device before it can be acted on."

Watch the webinar recording:

Learn More:

Fortinet Federal

(866) 468-3868

Fortinet@carahsoft.com

Garland Technology

(844) 445-5688

GarlandTech@carahsoft.com