Security Connected
Solution Guide

Achieve Resilient Cyber-Readiness

intel Security

Proactive Cyber-Readiness for Defense with Security Connected

Intel Security delivers an integrated security system that empowers you to prevent and respond to emerging threats. We help you resolve more threats faster and with fewer resources through stronger protection, superior detection, and rapid correction. Our trusted on-premises and cloud-enabled solutions and services help secure your enterprise against advanced attacks. Our connected architecture and centralized management reduce complexity and improve operational efficiency across your entire security infrastructure. Intel Security is committed to being your number one security partner—providing a complete set of integrated security capabilities.

Download the latest resources at mcafee.com/securityconnected.

Resilient cyber-readiness is the empirical and actionable information that allows a commander to make informed decisions rapidly.

Challenges

A security model that bridges visibility across traditional enterprise IT systems with operational systems that assess risk dynamically is necessary to assure effective military missions. Cyber-readiness incorporates speed, intelligence, and visibility and is required for resilient security.

Proactive cyber-readiness requires a complete, continuous understanding of endpoints, network, and data along with dynamic risk. A resilient cyber-readiness program encompasses IT and mission-critical data. These two disparate sources of information converge and demand exacting situational awareness that enables more informed decisions more quickly based on timely empirical data.

What's needed now are solutions that provide continuous monitoring and assessment on a large scale across a multitude of data classifications. The data collection framework needs to provide visibility across the battlefield and supporting IT networks, regardless of restriction.

Government enterprises operate across three zones: unrestricted, restricted, and operational. Unrestricted zones have a mix of enterprise applications, multiple network and Internet connectivity points, and sensitive data. Restricted zones can have several levels of restrictions and are often separated from public networks such as the Internet. They also have a mix of enterprise applications and beyond sensitive data, have top-secret data, including confidential communications, mission updates, and video. The operational zone comprises specific systems like military battle command systems. The applications used include systems designed to address logistics, law enforcement, resource planning, command and control, and intelligence. These are used for tracking supply movements to storing evidence and are generally deployed on closed operational networks.

Stakeholders are often hesitant to relinquish control over their particular environments. This results in a lack of centralization and poor situational awareness. Defense contractors develop most tactical battle command systems, and they often deploy and maintain them as well. Adding security to tactical battle command systems means a higher cost to the government.

The need for resilient cyber-readiness that operates across unrestricted, restricted, and tactical zones is clear. How else can situational awareness throughout endpoint, network, and data assets be achieved—especially if threat mitigation in one zone requires information about another zone? Defense leaders agree that a common operational picture, one that bridges visibility across traditional enterprise IT to battle command systems, is necessary and required if mission assurance to is be provided.

The Host-Based Security System (HBSS) program helps address the need for flexible, commercial-off-the-shelf (COTS) applications that can provide incident prevention, detection, and response at the host level. This includes systems such as servers, desktops, and laptops. Because of the size of many government organizations, host-based security solutions must be highly scalable and centrally manageable. In addition to providing preventative controls augmented by incident detection capabilities, they need to produce actionable alerts for rapid incident response. It is precisely these capabilities that align HBSS so tightly with resilient cyber-readiness strategies.[1]

Defense networks, especially military networks, can be very dynamic, fast-moving, and chaotic. Because of the need for rapid access to information and few barriers, security controls are often less robust than they should be. Even worse, tactical systems are generally exempt from security audits and excluded from traditional management visibility, negating the ability to truly measure risk.

Solutions

Resilient cyber-readiness is a continuous process. There is no black box that can be installed, no security service that can be utilized to achieve this goal. It is continuous awareness—understanding of what is on the network, who is on the network, and what's happening inside and outside the network.

To achieve this, there are three readiness solution requirements: continuous asset intelligence, risk assessment across IT and operational assets, and integration with computerized decision support systems. Continuous asset intelligence provides the big picture by using a framework that supports machine-to-machine data collection, comprehensive vulnerability assessments with behavior analysis, and evaluation of configuration and impact. Achieving this requires real-time discovery of assets, applications, and data. Risk assessments across IT and operational assets require local asset intelligence that is correlated with external threat intelligence feeds and automated assessments with integrated countermeasure awareness. These controls must not have a negative impact on the availability and performance of operational systems. Finally, integration with decision support systems means integration of traditional IT risk data and events with global battle command and control systems for true mission impact decision-making.

Design and Build

Multiple domains of information and an enterprise framework that supports machine-to-machine data collection must be bridged for a data strategy that is effective for resilient cyber-readiness. Within defense organizations, a security operations center framework must be built with scalable data collection capabilities. The management platforms must be interoperable, allowing integration with external intelligence and computerized decision support systems.

Discover and Understand

The foundation of situational awareness for resilient cyber-readiness is the protected environment. For the government enterprise, expanding the definition of "asset" is necessary. There must be an understanding that the asset exists if it is to be protected. The asset value must also be known. Finally, details surrounding that asset, such as vulnerabilities and security controls that are protecting it (countermeasures, policy information, and the like) are required in order to have a comprehensive understanding of the asset.

Assess and Analyze

Resilient cyber-readiness requires visibility across three key dimensions: on the network (network devices, endpoints, users, and data), inside the network (behavior), and outside the network (threat intelligence). McAfee® combines solutions for discovery, prevention, detection, response, and audit within a centralized management console enriched with threat intelligence feeds. Collectively, these solutions help detect and remediate threats sourced from inside and outside the network—even advanced stealth attacks and zero-day threats.

Improve and Measure

Improving and measuring the risk posture of the network takes situational awareness full circle. Cyber-readiness solutions must represent the risk posture at any given time. Responding to an attack in real time, based on out-of-date information could yield an undesired result. Additionally, actionable information must be based on empirical data that is as relevant as possible to achieve rapid incident response. Our centralized management and monitoring solution enables device management, threat monitoring, real-time analysis, and forensic investigation through a single pane of glass.

Best Practices Considerations

- Support large-scale data collection and machine-to-machine information exchanges for holistic analysis.
- Integrate with third-party solutions and provide centralized reporting across battlefield systems without introducing complexity, yet able to scale up to manage millions of assets.
- Leverage purpose-built solutions that operate across unrestricted, restricted, and tactical zones.
- Use a combination of dynamic risk assessment, centralization, real-time system identification, data cataloguing, and labeling of assets to build a complete situational awareness picture.
- Provide non-intrusive battle command system solutions that don't have a negative impact on availability or performance and provide dynamic risk assessment suitable for rapid decision making.
- Deploy solutions that allow for rapid expansion and incorporate models for lowering cost.
- Work with companies that have strategic relationships with defense contractors and have solutions that are integrated with military command and control systems for true battlefield situational awareness.
- Depend on solutions that have been battle-tested and proven in the rigors of recent tactical environments.

Value Drivers

Solutions for cyber-readiness not only need to provide security as a continuous process, they also need to reduce complexity and maximize return on investment. These solutions should:

- Reduce the time and resources required to assess assets, assess risk, and integrate with support systems.
- Provide scalable data collection based upon an extensible framework that doesn't require frequent re-engineering.
- Aggregate multiple decision-relevant data points to provide more exacting and timely decision making.
- Deploy quickly to support dynamic environments.

For more information about Security Connected, visit: www.mcafee.com/securityconnected.

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com

1. http://www.disa.mil/Services/Information-Assurance/HBS/HBS