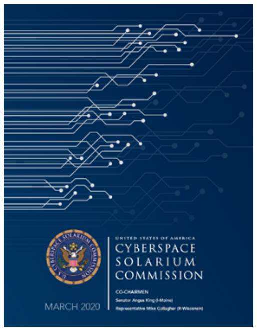
IronNet

THE U.S. CYBERSPACE SOLARIUM COMMISSION'S REPORT:

A Call to Action for Collective Defense

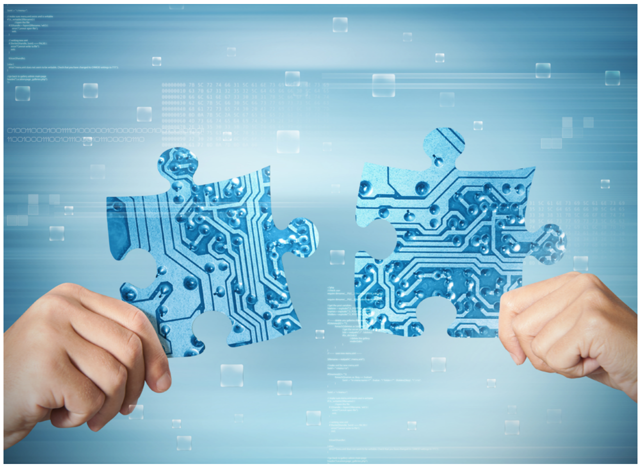
> "The U.S. government and industry … must arrive at a new social contract of shared responsibility to secure the nation in cyberspace. This 'collective defense' in cyberspace requires that the public and private sectors work from a place of truly shared situational awareness and that each leverages its unique comparative advantages for the common defense."
>
> (Cyberspace Solarium Commission Report, p. 96)


UNITED STATES OF AMERICA
CYBERSPACE
SOLARIUM
COMMISSION

CO-CHAIRMEN
Senator Angus King (I-Maine)
Representative Mike Gallagher (R-Wisconsin)

MARCH 2020

The Cyberspace Solarium Commission, created by the U.S. Congress in 2019 and made up of members of Congress and key private sector leaders and thinkers, is charged with developing a comprehensive national strategy for defending American interests and values in cyberspace.



- The Cyberspace Solarium Commission's March 2020 report reconceptualized how our nation can innovate to better defend itself in cyberspace.
- The report offers bold new ideas including planning for the continuity of the economy and strengthening key entities with direct government support.
- The report also provides actionable recommendations that Congress and the Executive Branch can move on now.
- The report's most ground-breaking aspect is its call for government and industry to adopt a strong cyber collective defense posture.
  - Collective defense is grounded in the common-sense idea that individual organizations cannot realistically be expected to effectively defend themselves against well-resourced threat actors like nation-states, major criminal organizations, and other asymmetric actors.
  - Implementing true collective defense—where organizations partner to share threat information and collaborate to defend in real-time—requires a fundamental shift in the way we think about cyber defense.

"While the U.S. government has taken a number of steps to develop situational awareness in cyberspace, there continue to be significant limitations on its ability to develop a comprehensive picture of the threat….the data or information is not routinely shared or cross-correlated at the speed and scale necessary for rapid detection and identification."

Cyberspace Solarium Commission Report, p. 101

Just as air traffic controllers can see the full radar picture in their area, if we are to truly enable cyber collective defense, we must pivot from the reactive sharing of known threats to the constant sharing of data to create a cyber common operating picture.

Such a capability will allow identification of new threats that could have escaped detection in a single environment and also provides a better understanding of campaigns being conducted across multiple organizations and sectors.

"Information sharing is an important part of public-private collaboration, but it is not an end in and of itself. It is a means of building better situational awareness of cyber threats, which can then inform the actions of both the private sector and the government."

Cyberspace Solarium Commission Report, p. 96

Building a common picture of threats is critical to collective defense because it enables the kind of real-time collaboration necessary to defend against well-resourced threat actors.

In many ways, the U.S. Cyberspace Solarium Commission's report is a wake-up call for company executives, boards of directors, and senior national security officials to come together now, crossing traditional boundaries to identify and defend against the range of threats targeting our nation.

The Collective Defense Mission Continues

> “Today, every company generally defends itself against each cyber threat on their own. While they might share some information, they also want—and need—to see the whole threat picture and collaborate in real-time to defend their critical services. Imagine how much better our defenses would be if we defended as one unit instead of many individuals. A dozen analysts collaborating on a joint set of threats can be much more productive than a single analyst at a dozen companies working in isolation. That is the true power of collective defense.“
>
> General (Ret.) Keith Alexander, Founder and Co-CEO of IronNet

IronNet is committed to answering the U.S. Cyberspace Solarium Commission’s call to action to defend companies, sectors, states, government agencies, and nations against nation-state-level cyber threats.

- IronNet’s collective defense platform allows organizations in a supply chain, industry, state, or nation to work together to identify and stop threats in real-time.
- IronNet delivers the ability for cyber defenders in multiple organizations to pool their collective knowledge and to collaborate in real-time using advanced behavioral analytics and data integrated from key cyber tools.

Operationalizing Collective Defense

COMBINING ADVANCED BEHAVIORAL THREAT ANALYSIS WITH EXISTING KNOWLEDGE

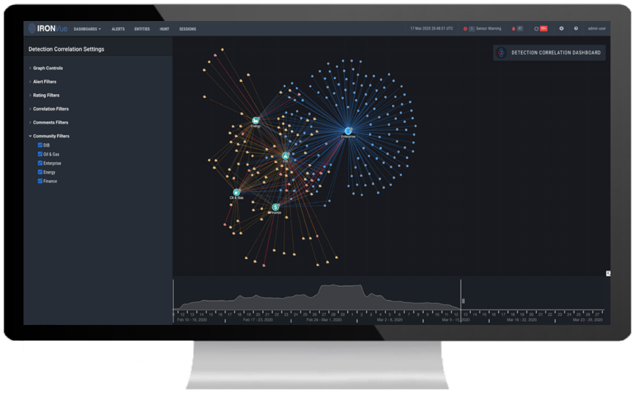
IronNet’s collective defense capability builds on our highly scalable network traffic analysis (NTA) system, IronDefense.

- This system combines data from IronNet’s core behavioral analytics with insights from our nation’s top cyber defenders as well as data from other industry-leading cyber tools and applies advanced machine learning models to help identify new and novel threats.

ANONYMIZED THREAT SHARING AND CORRELATION

- IronNet then anonymizes the threat data it gathers and correlates it across multiple organizations and sectors to create a common operating picture and help identify new threat trends.

COLLECTIVE DEFENSE IN ACTION



IronNet’s collective defense platform brings together communities to:

- Share and correlate data in real-time to accelerate threat discovery
- Collaborate to shorten triage and stop threats as they happen
- Crowdsource knowledge to prioritize resources

That is the power of collective defense.

Discover IronNet’s collective defense.