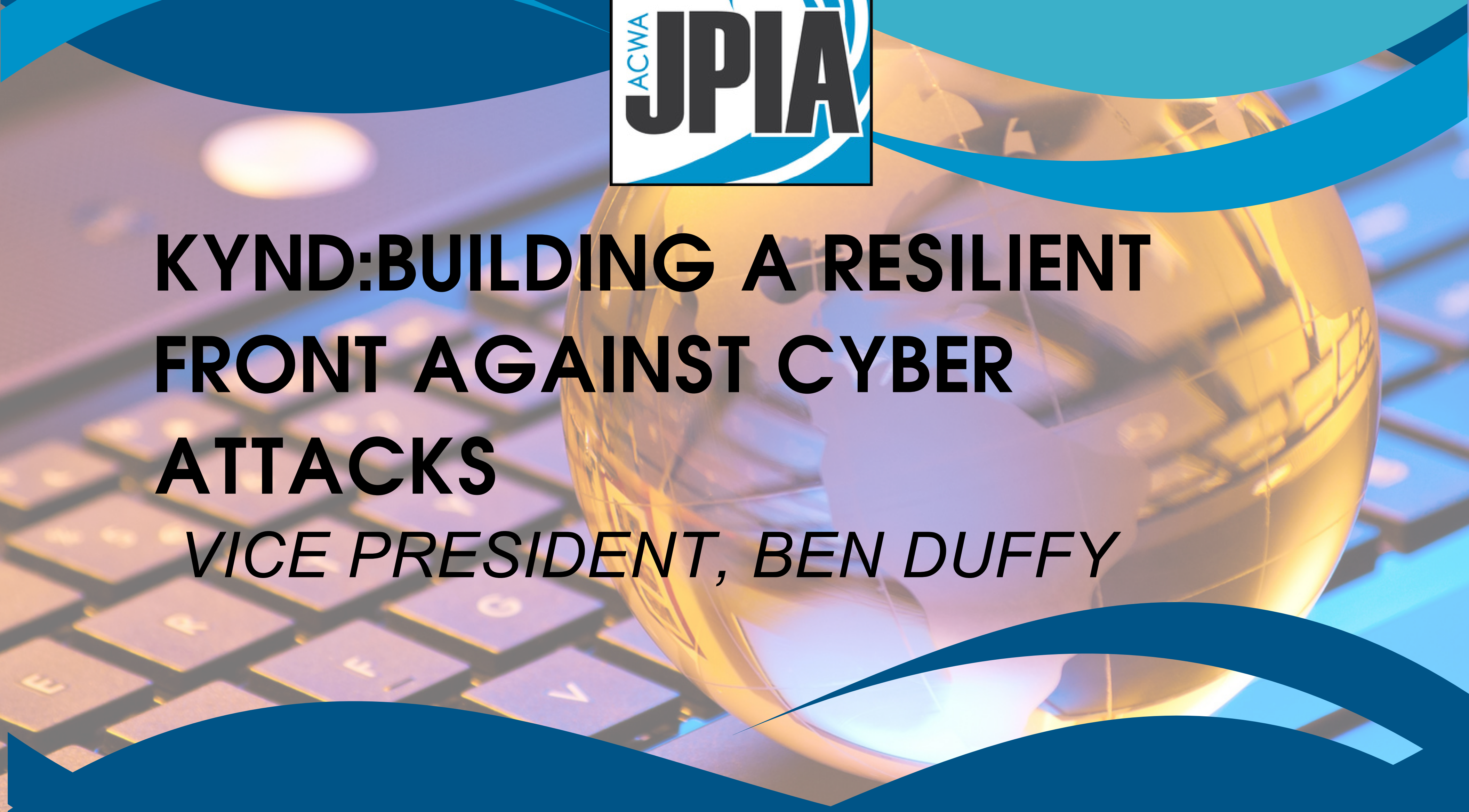


KYND:BUILDING A RESILIENT FRONT AGAINST CYBER ATTACKS

VICE PRESIDENT, BEN DUFFY

KYND

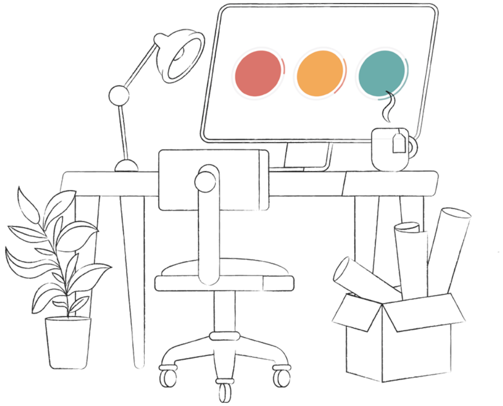
ACWA JPIA

ACWA JPIA Fall Conference

KYND Ready (Cyber Services)

KYND 28th November 2023, Palm Springs

1. Current state of the cyber market
2. Introduction to KYND
3. ACWA Cyber Risk Resilience
4. Goals & Targets
5. Q&A

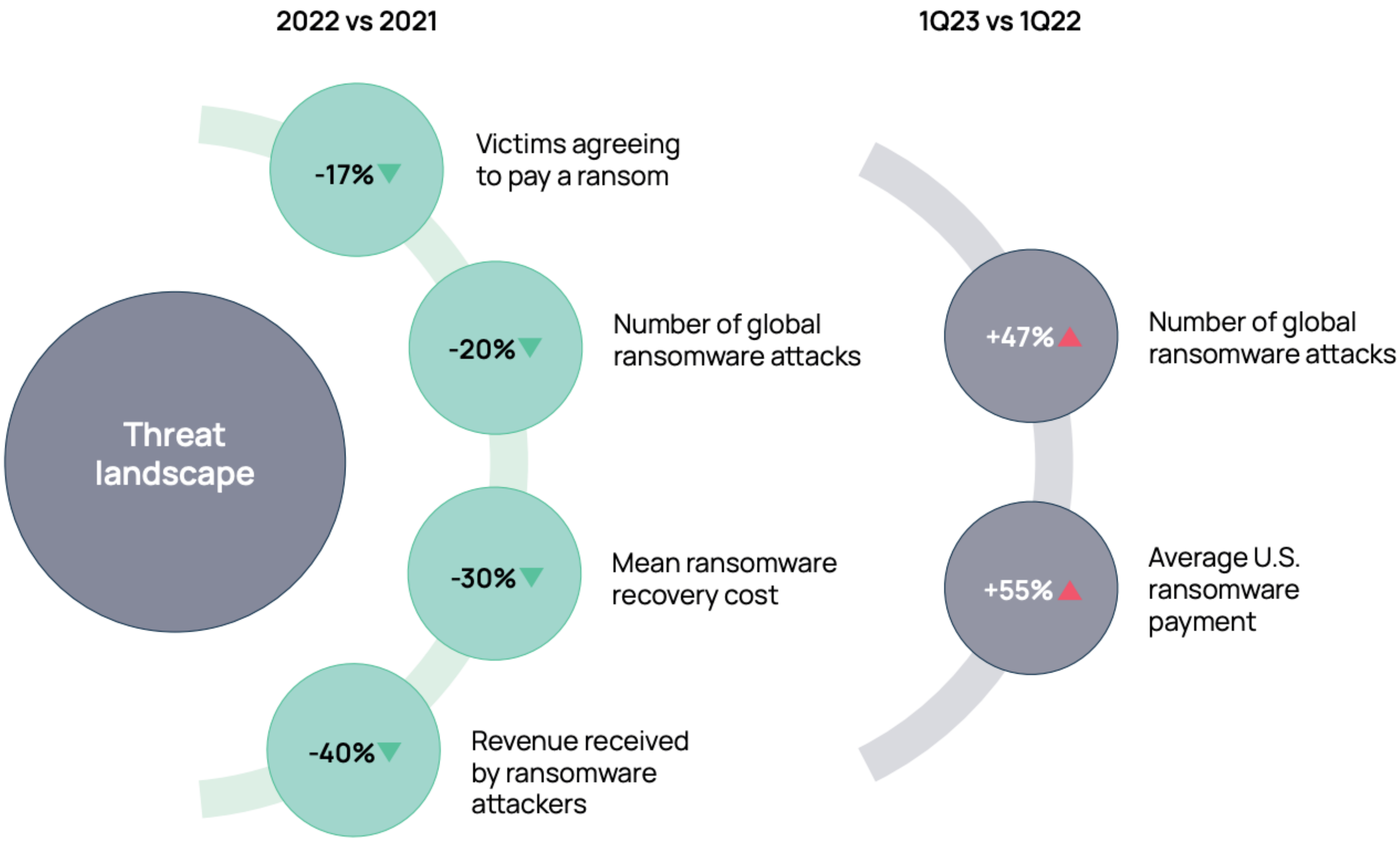


The current state of the cyber market

Following major upheaval in 2020 and 2021 caused by COVID-19 and the proliferation of ransomware, the last 18 months have represented a period of relative calm for the cyber insurance market as claims have subsided and competition has returned.

KYND

Frequency and severity of ransomware incidents



2022 vs 2021

Threat landscape

-17%▼ Victims agreeing to pay a ransom

-20%▼ Number of global ransomware attacks

-30%▼ Mean ransomware recovery cost

-40%▼ Revenue received by ransomware attackers

1Q23 vs 1Q22

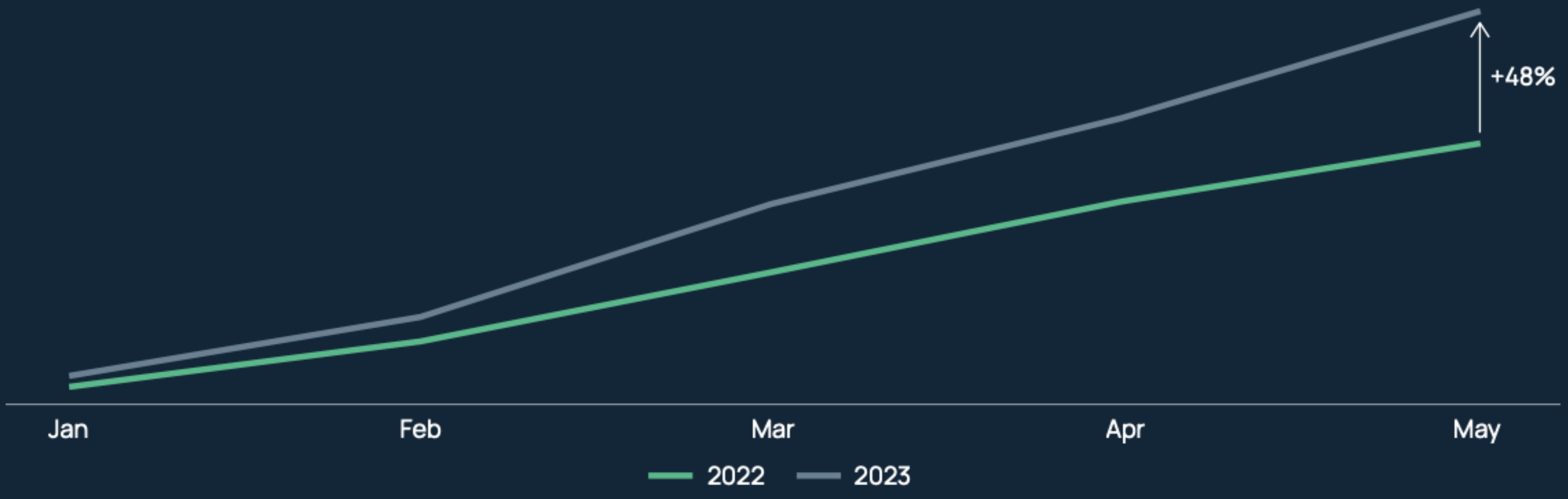
+47%▲ Number of global ransomware attacks

+55%▲ Average U.S. ransomware payment

(Source: Howden analysis using data from Coveware, SonicWall, NCC Group, Chainalysis, Sophos)

Rampant Ransomware

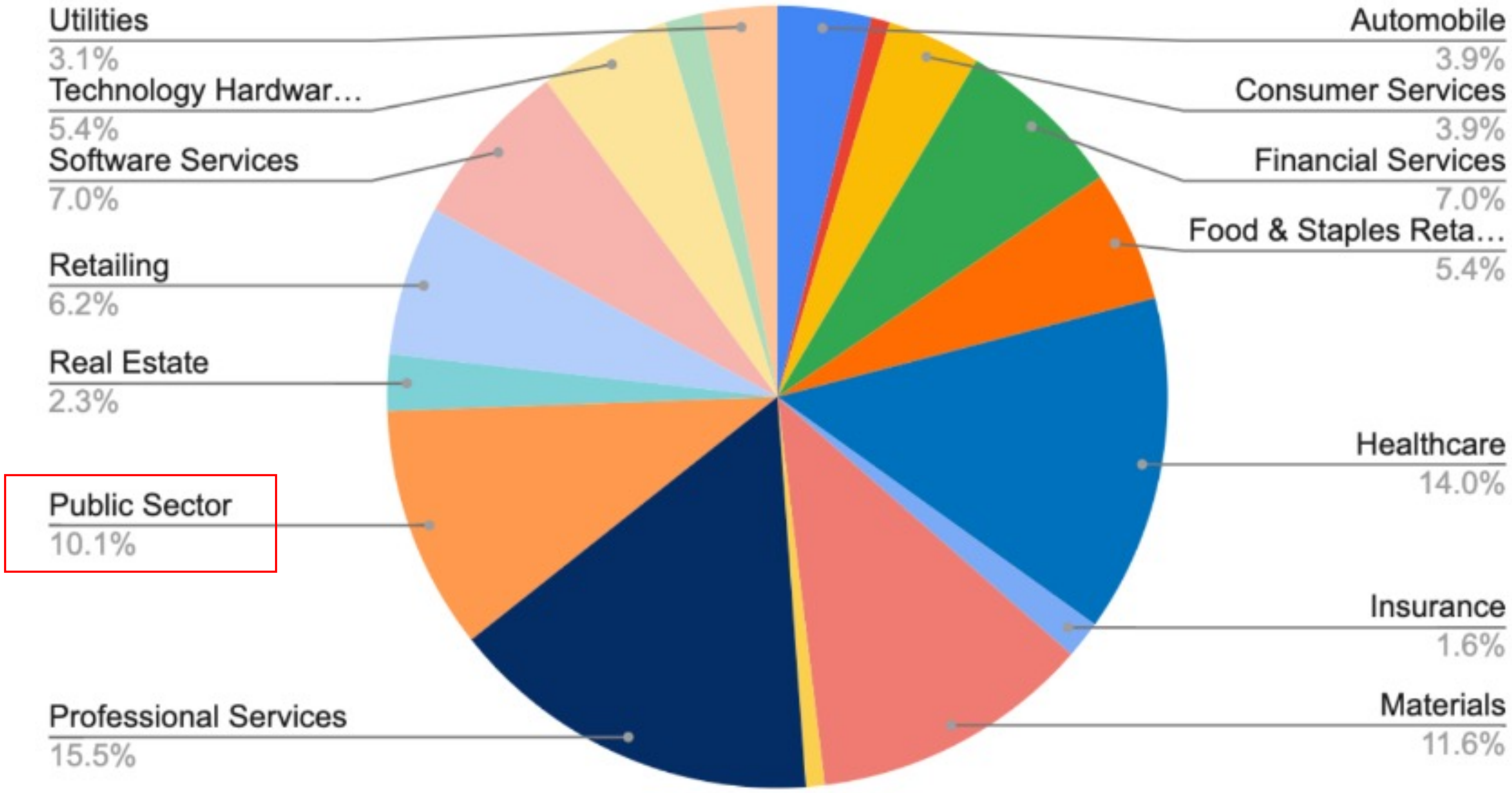
Ransomware activity up nearly 50% so far in 2023 vs 2022...



Source: Howden, NCC Group

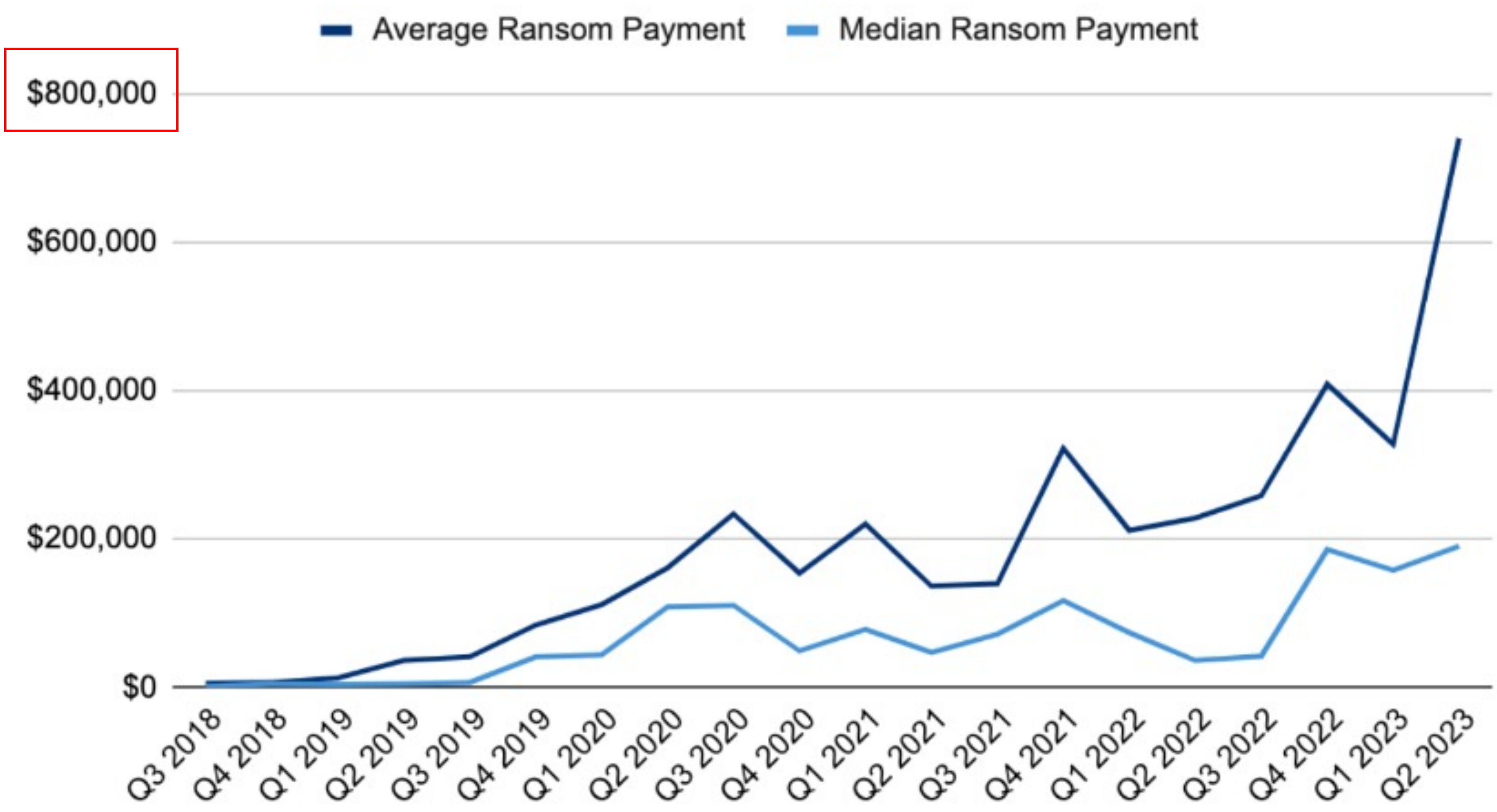
KYND

Industries impacted by Ransomware Q2, 2023



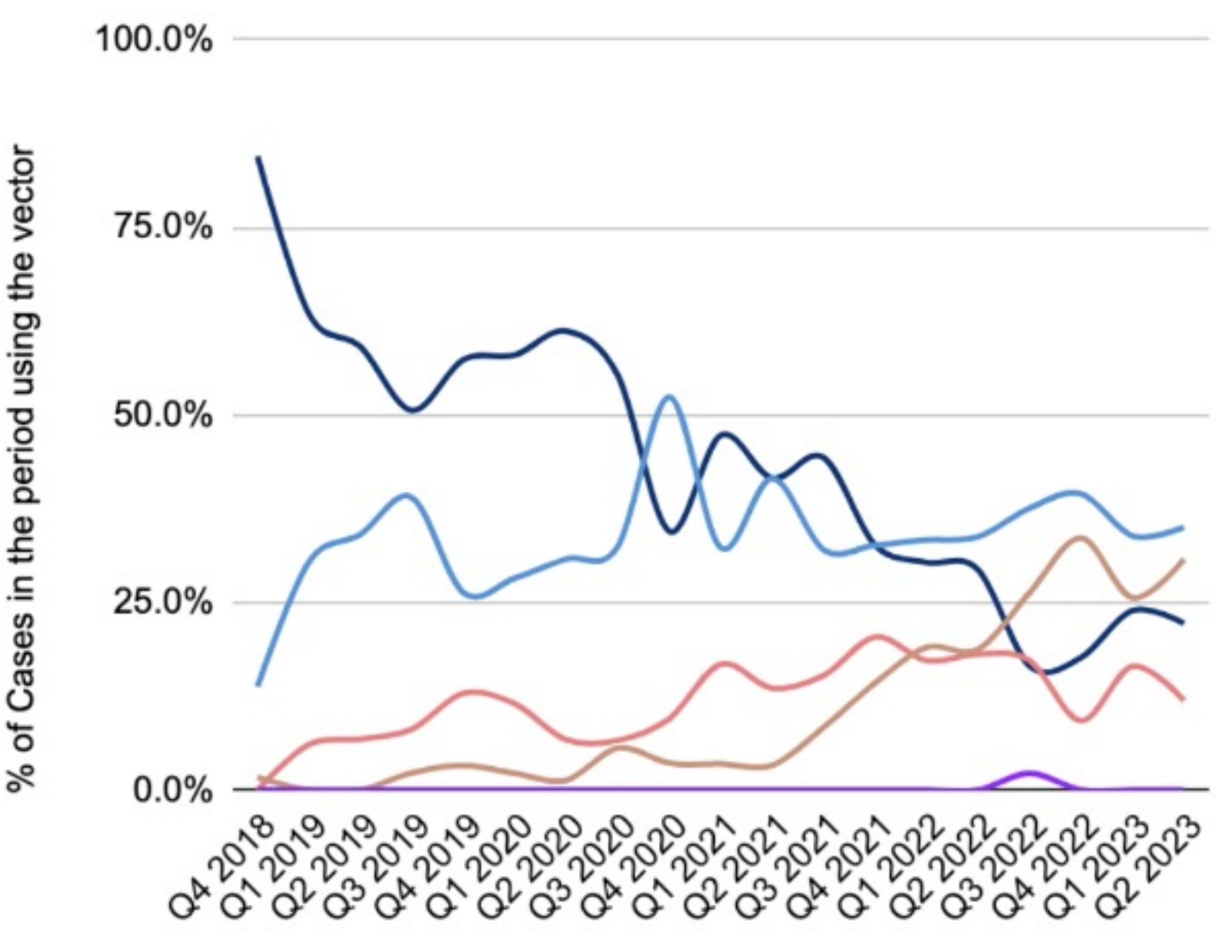
(Source: Coveware, 2023)

Ransom Payments By Quarter



(Source: Coveware, 2023)

Ransomware Attack Vectors Observed in Q2, 2023



KYND

Hello whess

Welcome to your dashboard. Here you'll find details of any cyber risk associated with your business, and some help on how to fix it.

Your cyber risk summary

128

115

1981

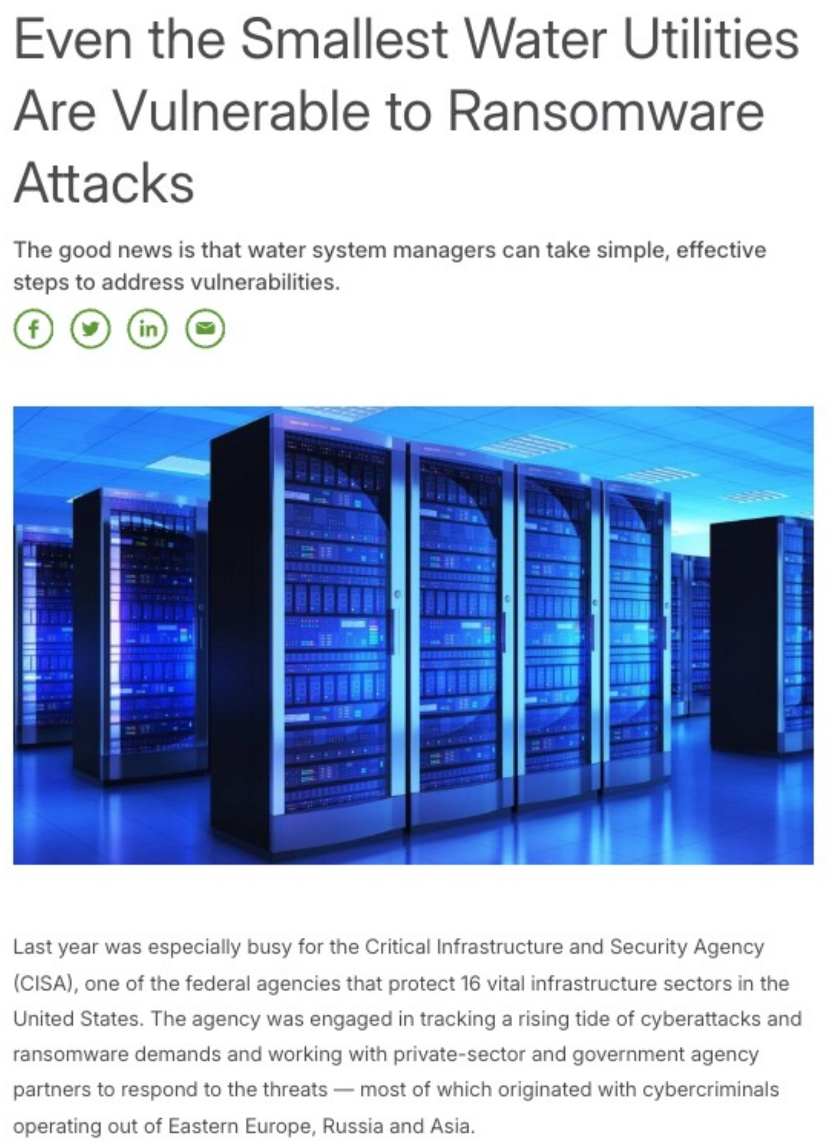
View risk report

KYND automatically scans for the above key vectors

(Source: Coveware, 2023)

What does this mean for the Cyber Insurance Market?

- The threshold for best practice keeps going up in the face of a now again, increasingly volatile threat landscape.
- To reflect this, insurance providers are increasing requirements for applicants to show their commitment to best practice.
- Insurance providers are asking for more detailed explanations and a higher standard of documentation as evidence of best practices inside organisations.
- The average cost of premiums has risen approximately 25%, with some policyholders paying over an 80% higher rate in 2022[1].
- Underwriters are adopting an “increasingly conservative approach to writing cyber cover…which could extend to the non-renewal of accounts or the reduction of limits offered.”[2]



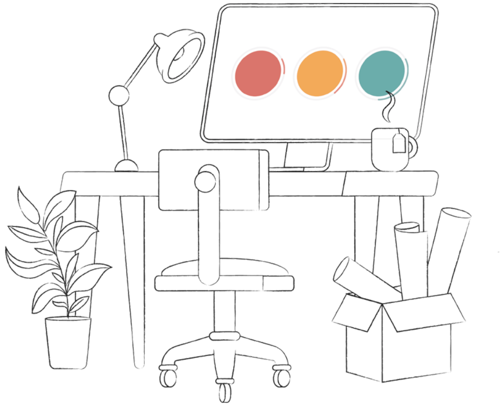
Even the Smallest Water Utilities Are Vulnerable to Ransomware Attacks

The good news is that water system managers can take simple, effective steps to address vulnerabilities.

Last year was especially busy for the Critical Infrastructure and Security Agency (CISA), one of the federal agencies that protect 16 vital infrastructure sectors in the United States. The agency was engaged in tracking a rising tide of cyberattacks and ransomware demands and working with private-sector and government agency partners to respond to the threats — most of which originated with cybercriminals operating out of Eastern Europe, Russia and Asia.

[1] AdvisorSmith.com

[2] Insurance Insider



Introduction to KYND

A new **KYND** of cyber risk management for pools…

Loss control and Improved Underwriting Performance

KYND is a new type of cyber risk management product

Pioneering cyber risk management technology that can be applied to any business. Highly accurate, quick to monitor and easy to prevent – no jargon or drama.

Who is KYND for?

KYND caters to all sizes of members. An insurance-focused ‘additive’ technology and service that helps authorities control loss and improve underwriting performance.

Simple | Easy | Quick

Just like the product, KYND keeps things simple, easy and quick – or quite literally red, amber, green. We use a non-scoring universal traffic light system to monitor and explain cyber risk exposure – focusing on the exposures that drive losses.

115,765

Organisations within the KYND platform

50+

Insurer, Broker and Pool customers

beazley Alliant TOKIO MARINE HCC howden GLOBE UNDERWRITING TALBOT An AIG company

KYND

Our Impact

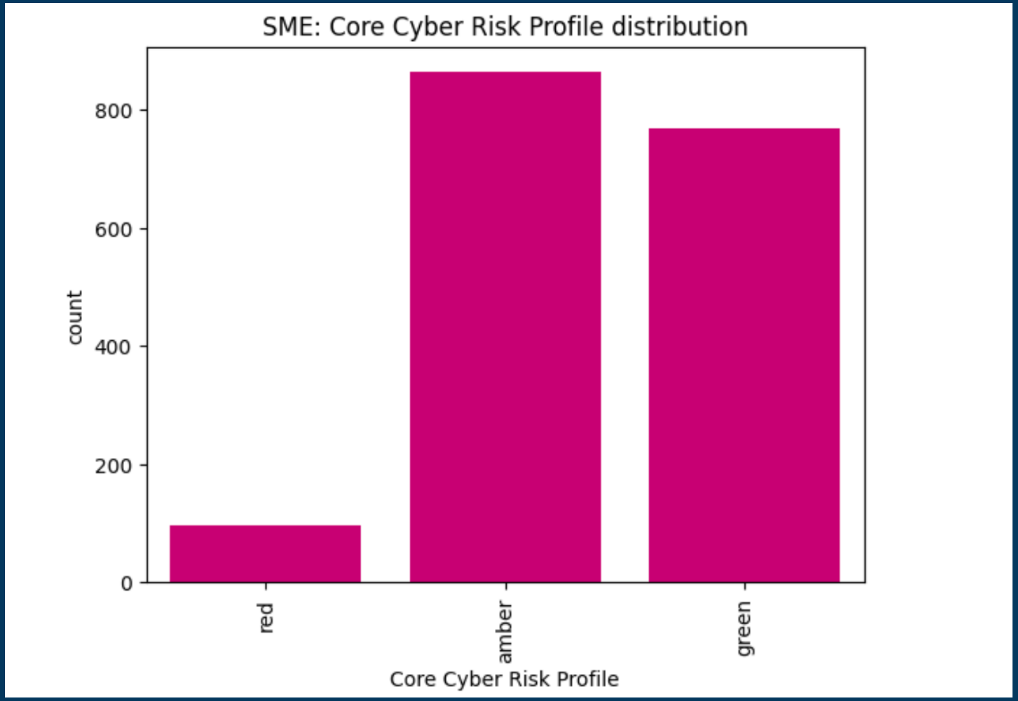
- ○ 30% reduction in ransomware claims frequency per policy and by 70% reduction by premium in 2022 – **Beazley**
- ○ KYND SIGNALS independently proven to identify proposed insureds that are 3x more likely to suffer a cyber incident - **Global Specialty Insurer (April 2023)**
- ○ Reduced cyber events, losses & claims for all clients & pools within the KYND Ready program – **Alliant**

> Due to the rapidly evolving nature of cyber threats, underwriting cyber often seems challenging. KYNDs' powerful combination of actionable cyber risk insights and expert advisory services enables Beazley underwriters to quickly and accurately obtain the right information they need to assess the risks and provide the right cover and solutions to protect businesses from cybercrime.
>
> **Paul Bantick, Global Head of Cyber and Tech / Beazley**

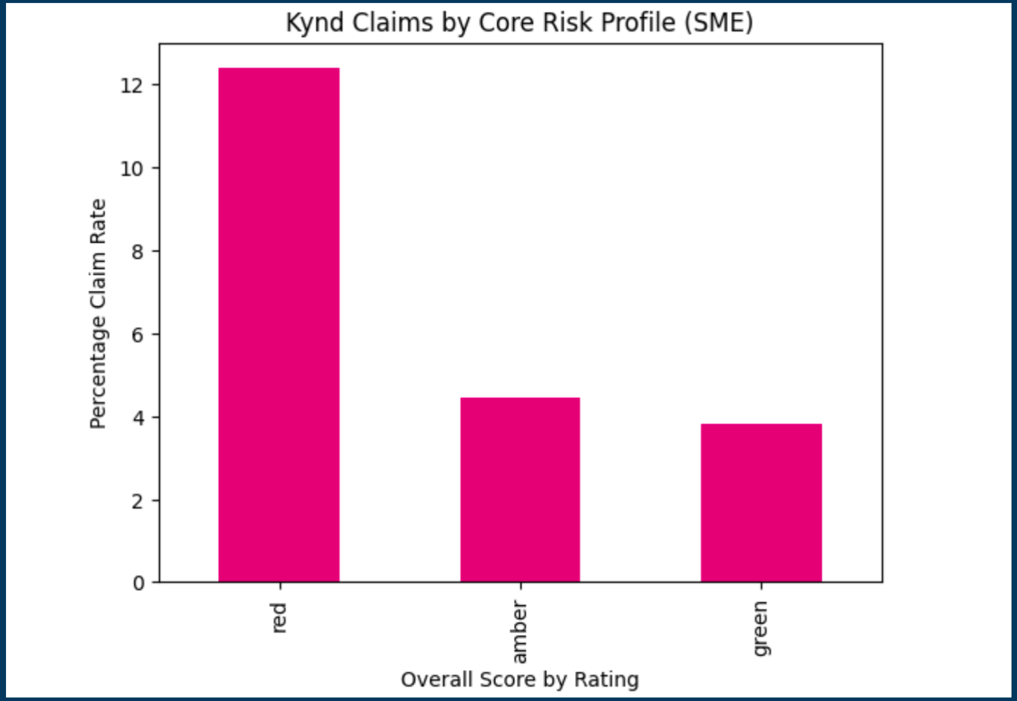
> In the hardest of hard cyber markets through 2021 and 2022 we have had a 100% success rate in securing clients the cyber insurance they need after they have been enrolled into the KYND Ready service.
>
> **David Rees, Executive Director and Head of UK Cyber / Howden**

KYND's risk analysis is proven to correlate to cyber losses

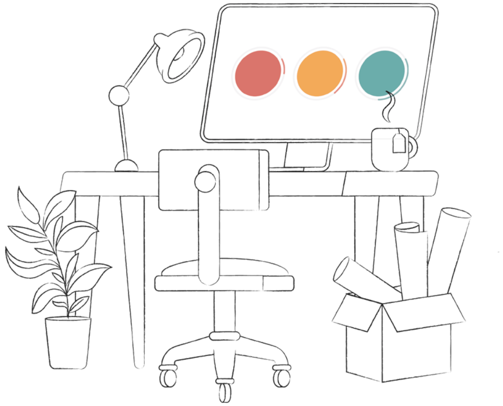
- KYND core RED profiles were 3x more likely to have suffered a loss
- Found to be predictive of claims over the prior 12 months for a sample portfolio.



Distribution of Red, Amber and Green Risk ratings within sample set.
Approx 5% of the sample were rated a core RED by KYND



Claims distribution by risk rating within sample set.
KYND core RED profiles were 3x more likely to have suffered a loss



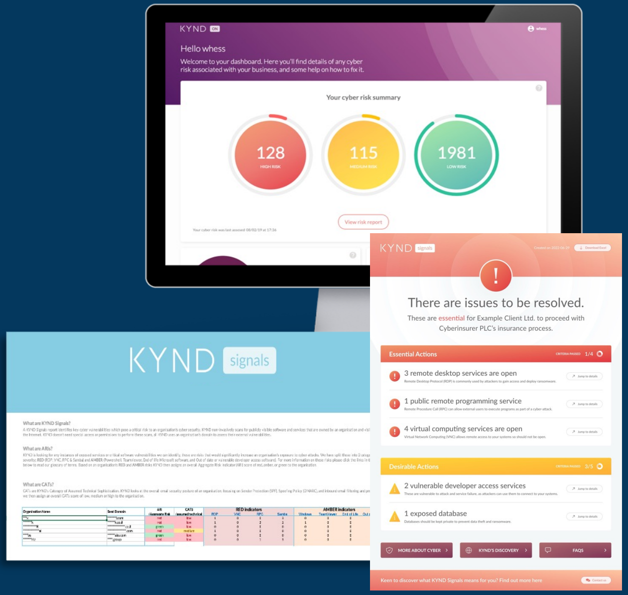
ACWA Cyber Resilience in 2024 and beyond….

KYND

ACWA JPIA

READY – ACWA PARTNERSHIP

Future Proofing your Cyber Resilience, Insurability & Underwriting Performance in 2024 and Beyond 🚀



KYND ON

Hello whess

Welcome to your dashboard. Here you'll find details of any cyber risk associated with your business, and some help on how to fix it.

Your cyber risk summary

128 HIGH RISK

115 MEDIUM RISK

1981 LOW RISK

View risk report

Your cyber risk was last assessed 08/02/19 at 17:36

KYND signals

Created on 2022-06-29

Download Excel

There are issues to be resolved.

These are essential for Example Client Ltd. to proceed with Cyberinsurer PLC's insurance process.

Essential Actions — CRITERIA PASSED 1/4

- 3 remote desktop services are open — Remote Desktop Protocol (RDP) is commonly used by attackers to gain access and deploy ransomware. — Jump to details
- 1 public remote programming service — Remote Procedure Call (RPC) can allow external users to execute programs as part of a cyber-attack. — Jump to details
- 4 virtual computing services are open — Virtual Network Computing (VNC) allows remote access to your systems so should not be open. — Jump to details

Desirable Actions — CRITERIA PASSED 3/5

- 2 vulnerable developer access services — These are vulnerable to attack and service failure, as attackers can use them to connect to your systems. — Jump to details
- 1 exposed database — Databases should be kept private to prevent data theft and ransomware. — Jump to details

MORE ABOUT CYBER | KYND'S DISCOVERY | FAQS

Keen to discover what KYND Signals means for you? Find out more here — Contact us

Cyber Risk Control Service

- Tools for members to manage their own risk
- On-going, continuous risk management - external and internal risks
- Real-time support via dedicated email and chat

Extension of ACWA's risk management practice

- Empower Risk Managers with support, data, education
- Regular check-ins & prioritized actions each month

Underwriting performance and control

- Visibility of pool's cyber exposure at any given time (in-house date)
- Understand 'themes of deficiencies' – inform cyber strategy
- Prioritised signals that enable more informed insurance decisions, T&Cs etc
- Track individual members' cyber posture between renewals.

KYND – helps members achieve long-term improvements in…

EXTERNAL VULNERABILITIES

VNC

RPC

RDP

Team Viewer

EOL

External Vulnerabilities

Dev Access & OpenSSH

Visible Databases

Samba (SMB)

Powershell

INTERNAL POSTURE

Enforce MFA & manage authentication

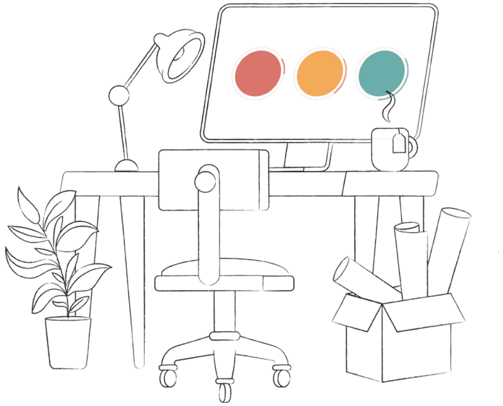
Protect networks & devices

Encrypt & restrict access to data & backups

Internal Vulnerabilities

Develop & document plans & processes

Regular & relevant training for all users



What does the service look like?

REPORT

KYND Signals Portfolio Analysis

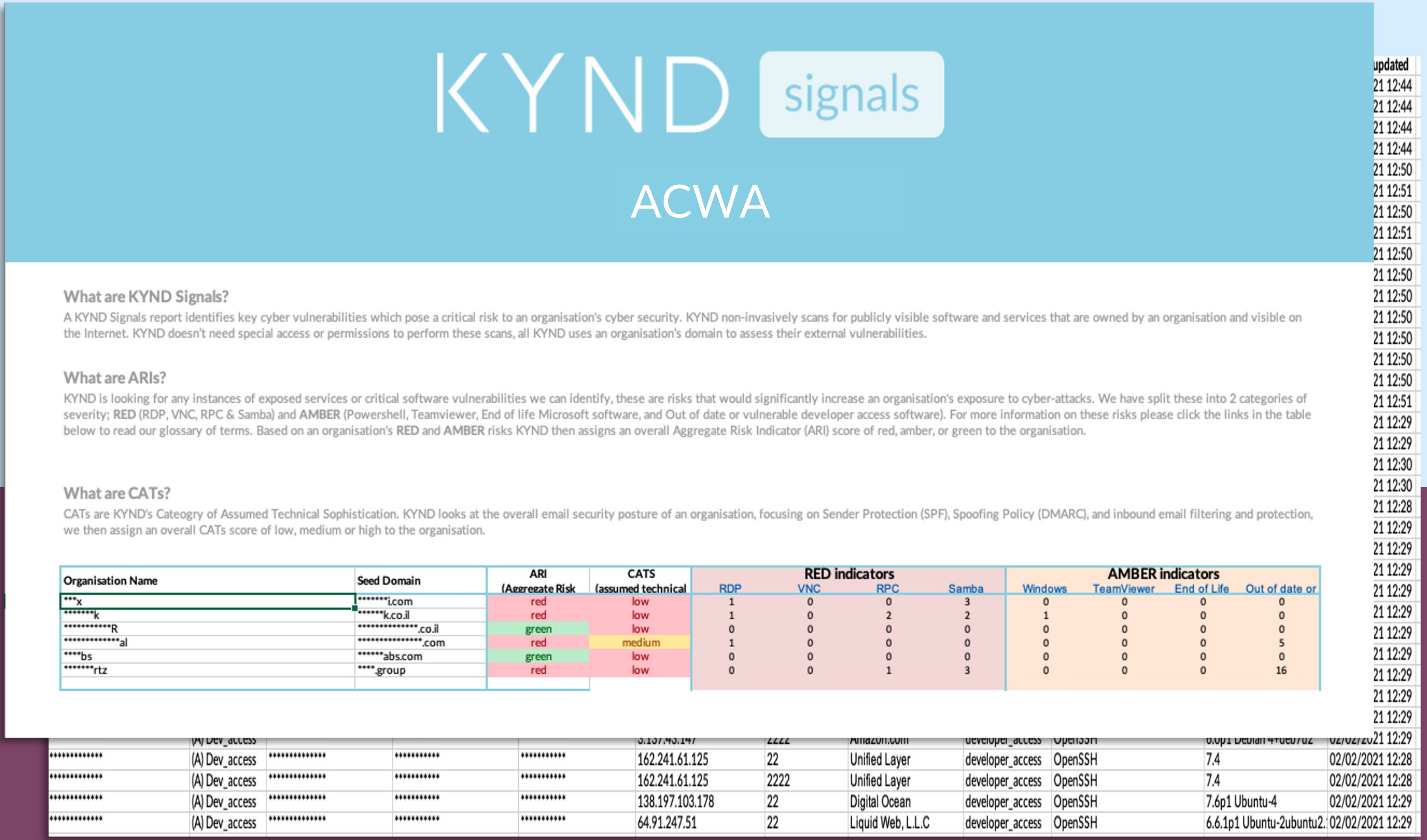
Delivered to the authority each month…

Continual ‘Top Down’ tracking…

A KYND Signals Portfolio Report will show the authority member by member where the vulnerabilities lie each month.

Most ‘at-risk’ members:

Enables, data-driven risk-based conversations without unnecessary scoring.



KYND signals

ACWA

What are KYND Signals?

A KYND Signals report identifies key cyber vulnerabilities which pose a critical risk to an organisation's cyber security. KYND non-invasively scans for publicly visible software and services that are owned by an organisation and visible on the Internet. KYND doesn't need special access or permissions to perform these scans, all KYND uses an organisation's domain to assess their external vulnerabilities.

What are ARIs?

KYND is looking for any instances of exposed services or critical software vulnerabilities we can identify, these are risks that would significantly increase an organisation's exposure to cyber-attacks. We have split these into 2 categories of severity; **RED** (RDP, VNC, RPC & Samba) and **AMBER** (Powershell, Teamviewer, End of life Microsoft software, and Out of date or vulnerable developer access software). For more information on these risks please click the links in the table below to read our glossary of terms. Based on an organisation's **RED** and **AMBER** risks KYND then assigns an overall Aggregate Risk Indicator (ARI) score of red, amber, or green to the organisation.

What are CATs?

CATs are KYND's Cateogry of Assumed Technical Sophistication. KYND looks at the overall email security posture of an organisation, focusing on Sender Protection (SPF), Spoofing Policy (DMARC), and inbound email filtering and protection, we then assign an overall CATs score of low, medium or high to the organisation.

Organisation Name	Seed Domain	ARI (Aggregate Risk	CATS (assumed technical	RED indicators RDP	 VNC	 RPC	 Samba	AMBER indicators Windows	 TeamViewer	 End of Life	 Out of date or
***x	*******i.com	red	low	1	0	0	3	0	0	0	0
*******k	******k.co.il	red	low	1	0	2	2	1	0	0	0
***********R	**************.co.il	green	low	0	0	0	0	0	0	0	0
*************al	***************.com	red	medium	1	0	0	0	0	0	0	5
****bs	******abs.com	green	low	0	0	0	0	0	0	0	0
*******rtz	****.group	red	low	0	0	1	3	0	0	0	16

updated
21 12:44
21 12:44
21 12:44
21 12:44
21 12:50
21 12:51
21 12:50
21 12:51
21 12:50
21 12:50
21 12:50
21 12:50
21 12:50
21 12:50
21 12:50
21 12:51
21 12:29
21 12:29
21 12:30
21 12:30
21 12:28
21 12:29
21 12:29
21 12:29
21 12:29
21 12:29
21 12:29
21 12:29
21 12:29
21 12:29
21 12:29

	(A) Dev_access				3.137.43.147	2222	Amazon.com	developer_access	OpenSSH	6.0p1 Debian 4+deb7u2	02/02/2021 12:29
*************	(A) Dev_access	**************	***********	***********	162.241.61.125	22	Unified Layer	developer_access	OpenSSH	7.4	02/02/2021 12:28
*************	(A) Dev_access	**************	***********	***********	162.241.61.125	2222	Unified Layer	developer_access	OpenSSH	7.4	02/02/2021 12:28
*************	(A) Dev_access	**************	***********	***********	138.197.103.178	22	Digital Ocean	developer_access	OpenSSH	7.6p1 Ubuntu-4	02/02/2021 12:29
*************	(A) Dev_access	**************	***********	***********	64.91.247.51	22	Liquid Web, L.L.C	developer_access	OpenSSH	6.6.1p1 Ubuntu-2ubuntu2.	02/02/2021 12:29

REPORT

KYND Signals Report

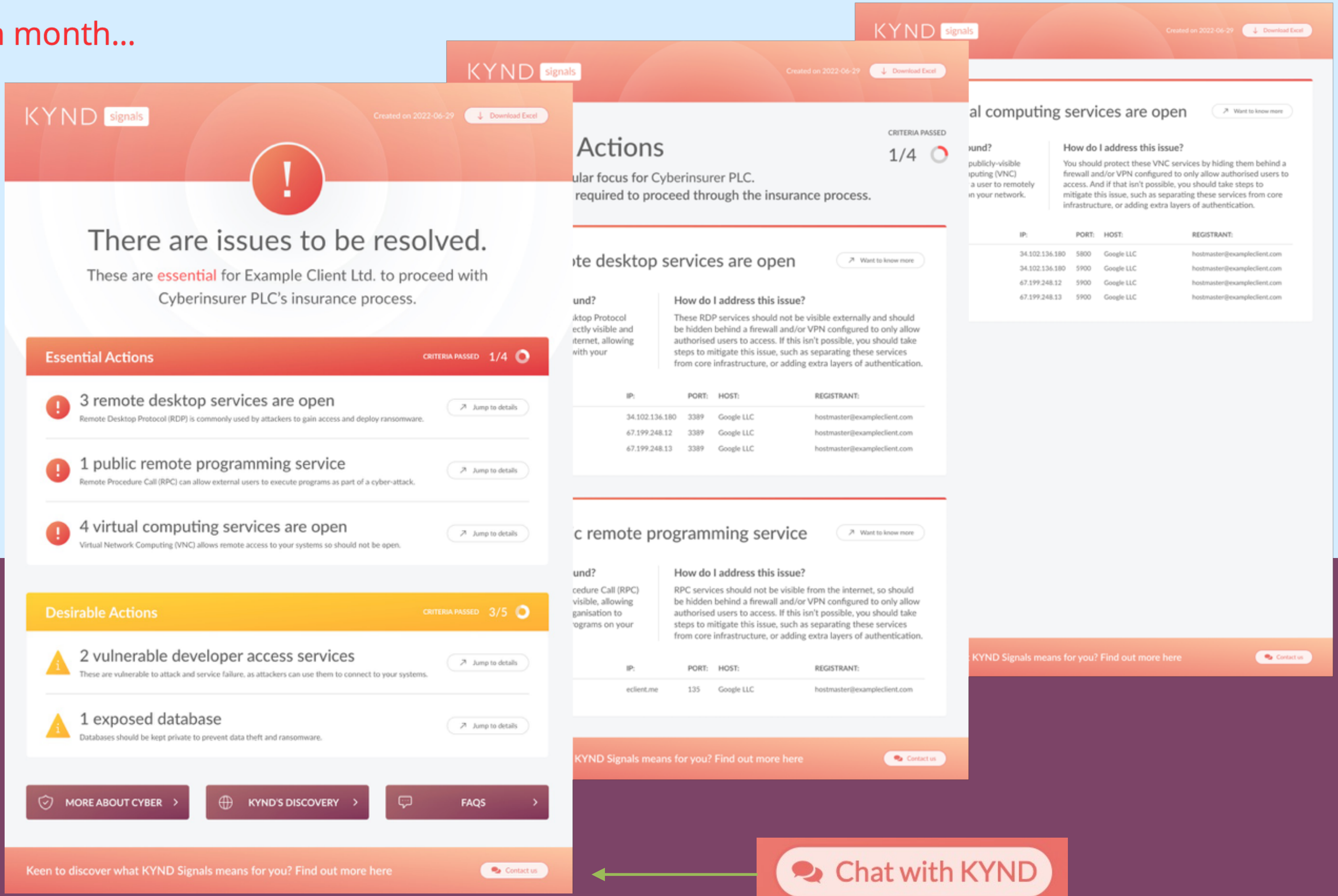
Delivered to all ‘Red’ Members each month…

Optimum results

for IT managers to simply see and manage the exposure most pressing to the insurance process.

Aligned with the vulnerabilities

that drive losses and claims. Simple presentation of risk with ‘real-time’ support.



KYND signals — Created on 2022-06-29 — Download Excel

There are issues to be resolved.

These are essential for Example Client Ltd. to proceed with Cyberinsurer PLC’s insurance process.

Essential Actions — CRITERIA PASSED 1/4

- 3 remote desktop services are open — Remote Desktop Protocol (RDP) is commonly used by attackers to gain access and deploy ransomware. — Jump to details
- 1 public remote programming service — Remote Procedure Call (RPC) can allow external users to execute programs as part of a cyber-attack. — Jump to details
- 4 virtual computing services are open — Virtual Network Computing (VNC) allows remote access to your systems so should not be open. — Jump to details

Desirable Actions — CRITERIA PASSED 3/5

- 2 vulnerable developer access services — These are vulnerable to attack and service failure, as attackers can use them to connect to your systems. — Jump to details
- 1 exposed database — Databases should be kept private to prevent data theft and ransomware. — Jump to details

MORE ABOUT CYBER › KYND’S DISCOVERY › FAQS ›

Keen to discover what KYND Signals means for you? Find out more here — Contact us

KYND signals — Created on 2022-06-29 — Download Excel

Actions — CRITERIA PASSED 1/4

ular focus for Cyberinsurer PLC.
required to proceed through the insurance process.

ote desktop services are open — Want to know more

und?
ktop Protocol
ectly visible and
ternet, allowing
with your

How do I address this issue?
These RDP services should not be visible externally and should be hidden behind a firewall and/or VPN configured to only allow authorised users to access. If this isn’t possible, you should take steps to mitigate this issue, such as separating these services from core infrastructure, or adding extra layers of authentication.

IP:	PORT:	HOST:	REGISTRANT:
34.102.136.180	3389	Google LLC	hostmaster@exampleclient.com
67.199.248.12	3389	Google LLC	hostmaster@exampleclient.com
67.199.248.13	3389	Google LLC	hostmaster@exampleclient.com

c remote programming service — Want to know more

und?
cedure Call (RPC)
visible, allowing
ganisation to
ograms on your

How do I address this issue?
RPC services should not be visible from the internet, so should be hidden behind a firewall and/or VPN configured to only allow authorised users to access. If this isn’t possible, you should take steps to mitigate this issue, such as separating these services from core infrastructure, or adding extra layers of authentication.

IP:	PORT:	HOST:	REGISTRANT:
eclient.me	135	Google LLC	hostmaster@exampleclient.com

KYND Signals means for you? Find out more here — Contact us

KYND signals — Created on 2022-06-29 — Download Excel

al computing services are open — Want to know more

ound?
publicly-visible
puting (VNC)
a user to remotely
n your network.

How do I address this issue?
You should protect these VNC services by hiding them behind a firewall and/or VPN configured to only allow authorised users to access. And if that isn’t possible, you should take steps to mitigate this issue, such as separating these services from core infrastructure, or adding extra layers of authentication.

IP:	PORT:	HOST:	REGISTRANT:
34.102.136.180	5800	Google LLC	hostmaster@exampleclient.com
34.102.136.180	5900	Google LLC	hostmaster@exampleclient.com
67.199.248.12	5900	Google LLC	hostmaster@exampleclient.com
67.199.248.13	5900	Google LLC	hostmaster@exampleclient.com

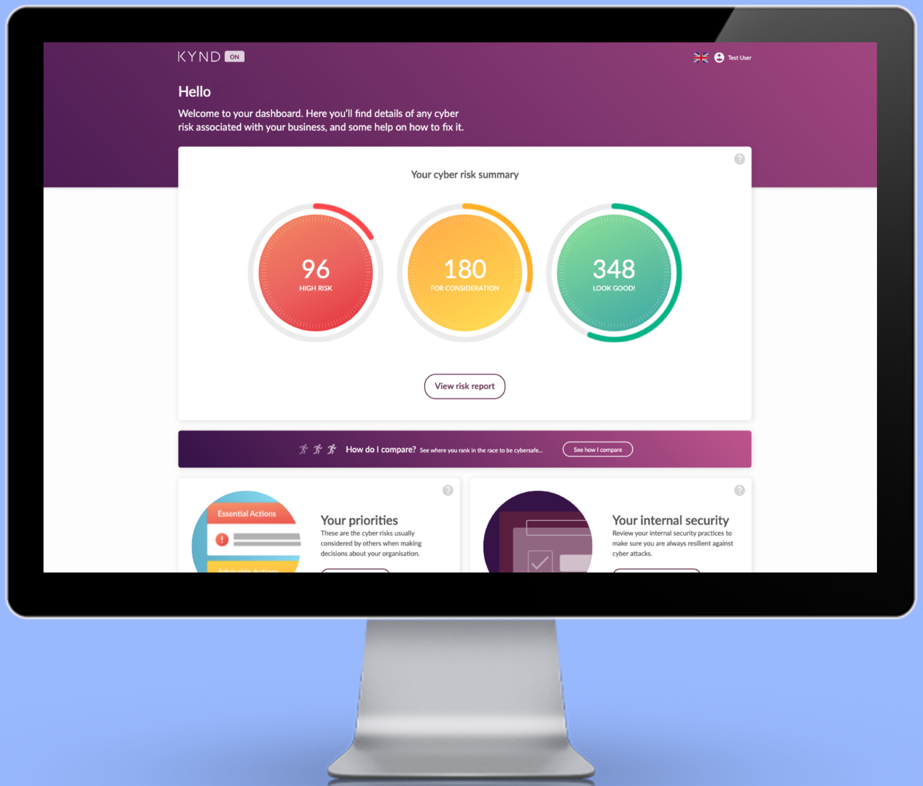
KYND Signals means for you? Find out more here — Contact us

Chat with KYND

CONTINUOUS MONITORING

KYND ON

For each member…



Hello

Welcome to your dashboard. Here you'll find details of any cyber risk associated with your business, and some help on how to fix it.

Your cyber risk summary

How do I compare? See where you rank in the race to be cybersafe...

Your priorities

These are the cyber risks usually considered by others when making decisions about your organisation.

Your internal security

Review your internal security practices to make sure you are always resilient against cyber attacks.

KYND ON includes every cyber risk we can see from the outside of a member's infrastructure.

This is then delivered in a continuous monitoring fashion – alerting members of the cyber risks that could affect them all via the members' own KYND ON dashboard.

Supports regular interaction & remediation – members can track their progress and log in and interact with their risk profile at any time.

Data Breach Monitors – alerts to the leak or theft of the customer, employee or supplier data you hold.

How does the KYND ON analysis work?

KYND only needs the name of one website registered by the member to produce this full cyber risk assessment.

As part of the analysis, KYND assesses the risk factors across domain registration and email security and services, by using a simple traffic light system.

KYND's analysis is entirely non-invasive and requires no special access or involvement by the organization itself.

SERVICES

Our Cyber Services

The KYND Ready program includes several product and service components available to you to strengthen your cyber security posture.

KYND ON

Continuous Cyber Risk Management

KYND Ready Call

1-2-1 call with a cyber risk expert to review your internal processes and ask questions.

KYND Signals Report

A report that outlines Insurance specific Risk

Dedicated support

A specific email address and chat support to support members

KYND signals

Zero Day vulnerabilities

Helping ACWA and its members identify and respond to new cyber vulnerabilities that hit the headlines MOVEit, Log4Shell...

One-off analysis and continuous monitoring

For a members exposure to vulnerabilities listed and actively updated in the CISA Catalogue.

Precise notifications

KYND performs direct scans confirming specific exposure where it exists; accurate indications of susceptibility rather than speculation.

Rapid Response

New zero days added to the ACWA data feeds within 24 hours of a new vulnerability being published.

CISA Known Exploited Vulnerabilities Catalogue

In November 2021 CISA began to publish a catalogue of the most critical and actively exploited cyber security vulnerabilities and issued a binding operational directive ordering US federal agencies to address them within specific timeframes and deadlines

This catalogue is constantly updated and although not binding on non-federal agencies it provides a clear benchmark of best practice for every business.

Goals and Targets

KYND Ready

KYND

ACWA & KYND

Future Proofing your Cyber Resilience, Insurability & Underwriting Performance in 2024 and Beyond 🚀

- Reduction in external risks across members and then maintained.
- Engagement – Raising digital risk to a key priority for members and the need to change the culture around cyber – simple, achievable actions that drive members' own risk governance.
- Enhance support for members around cyber insurance applications – keep the pool ahead of more stringent underwriting requirements.
- Resource Allocation: Track '*themes of deficiencies*' in an ongoing manner – real-time data for ACWA to base cyber-related sprints and extra support (MFA, backups etc).
- Support ACWA in response to this rise in ransomware and softer insurance conditions – future-proof insurance process.

KYND

Thank You
Q&A

KYND

KYND Ready & Cyber Services

Commercial in confidence

Thank You!

If you have any questions or would like additional information please contact:

Ben Duffy, KYND
VP, Head Of North America
e: bduffy@kind.io
t: US: +1 9097675424 UK: +44 (0) 77366 50 735

RISK & INSURANCE IN THE WILDLAND-URBAN INTERFACE

ALEX TOKAR, FRANK FRIEVALT, JENNIFER JOBE, KEVIN PHILLIPS AND ADRIENNE BEATTY.

ACWA JPIA

WUI Property Mitigation Strategy: Transferable Concepts to Infrastructure

FRANK FRIEVALT, DIRECTOR

11/28/2023

LEARN BY DOING

CAL POLY

WUI Fire Institute

COLLEGE OF AGRICULTURE, FOOD & ENVIRONMENTAL SCIENCES

An Informal "WUI We" Working Together on a Path Forward:

❑ Systematic alignment of multiple stakeholders

❑ Taking coordinated and effective action to disrupt fire pathways in the WUI

❑ Facilitating visibility of effective resilience actions by WUI communities

LEARN BY DOING
CAL POLY
WUI Fire Institute
COLLEGE OF AGRICULTURE, FOOD & ENVIRONMENTAL SCIENCES

NIST
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

CALIFORNIA DEPARTMENT OF FORESTRY & FIRE PROTECTION
CAL FIRE
SINCE 1885

GORDON AND BETTY MOORE FOUNDATION

Colorado State University

WESTERN FIRE CHIEFS ASSOCIATION

CALIFORNIA FIRE CHIEFS ASSOC.
CFCA

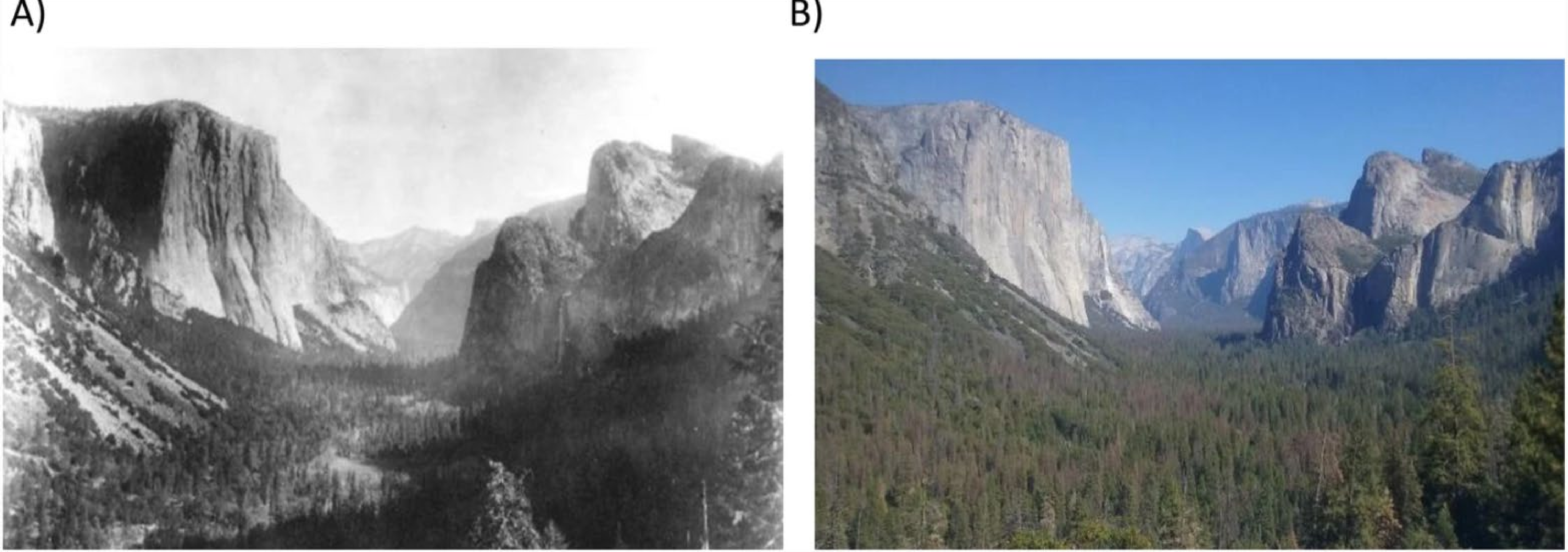
Milliman

Water Agencies & WUI Communities: Common Threats & Shared Consequences

- Environmental
  - Proximity Exposure, Surface Water, Ground Water
- Economic
  - Infrastructure, Risk Transfer, Property Tax, User Fees, GO Bond Ratings, Surge Pricing

Why Now?

- Significant Increase in Fuel Loading
- More Development in Fire Dependent Landscapes
- Increasing Vapor Pressure Deficit

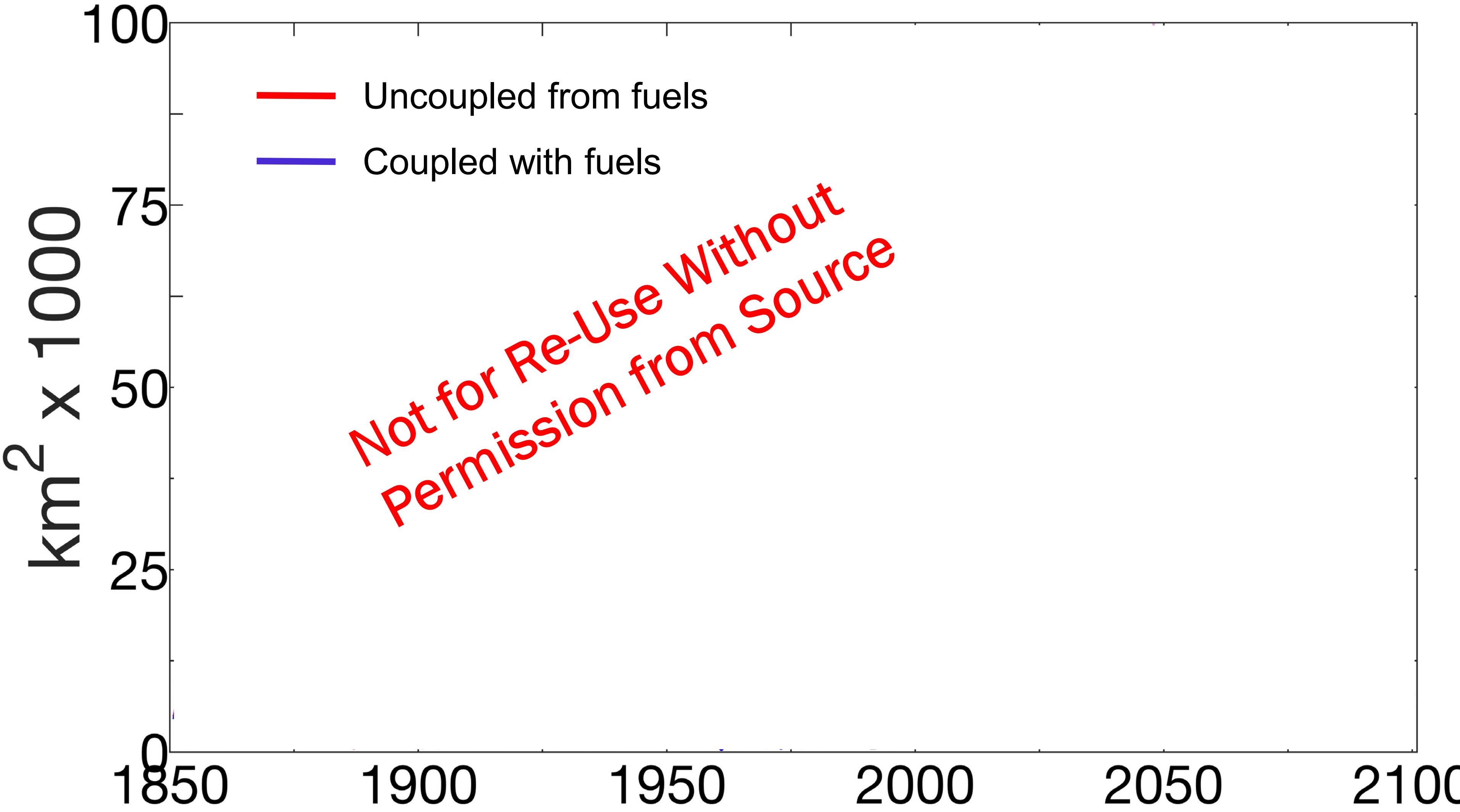


Photographs of Yosemite Valley in California from 1892 (**A**) and 2011 (**B**) show denser forest and shrub growth. Source for A: https://www.usgs.gov/news/yosemite-science , Photo B by Gabrielle Boisrame

Source: https://fireecology.springeropen.com/articles/10.1186/s42408-022-00129-4/figures/9

The Future is Frightening

Forest area burned (Middle of the road emissions scenario)



Not for Re-Use Without Permission from Source

Source: Williams, Hansen, et al. In Prep.

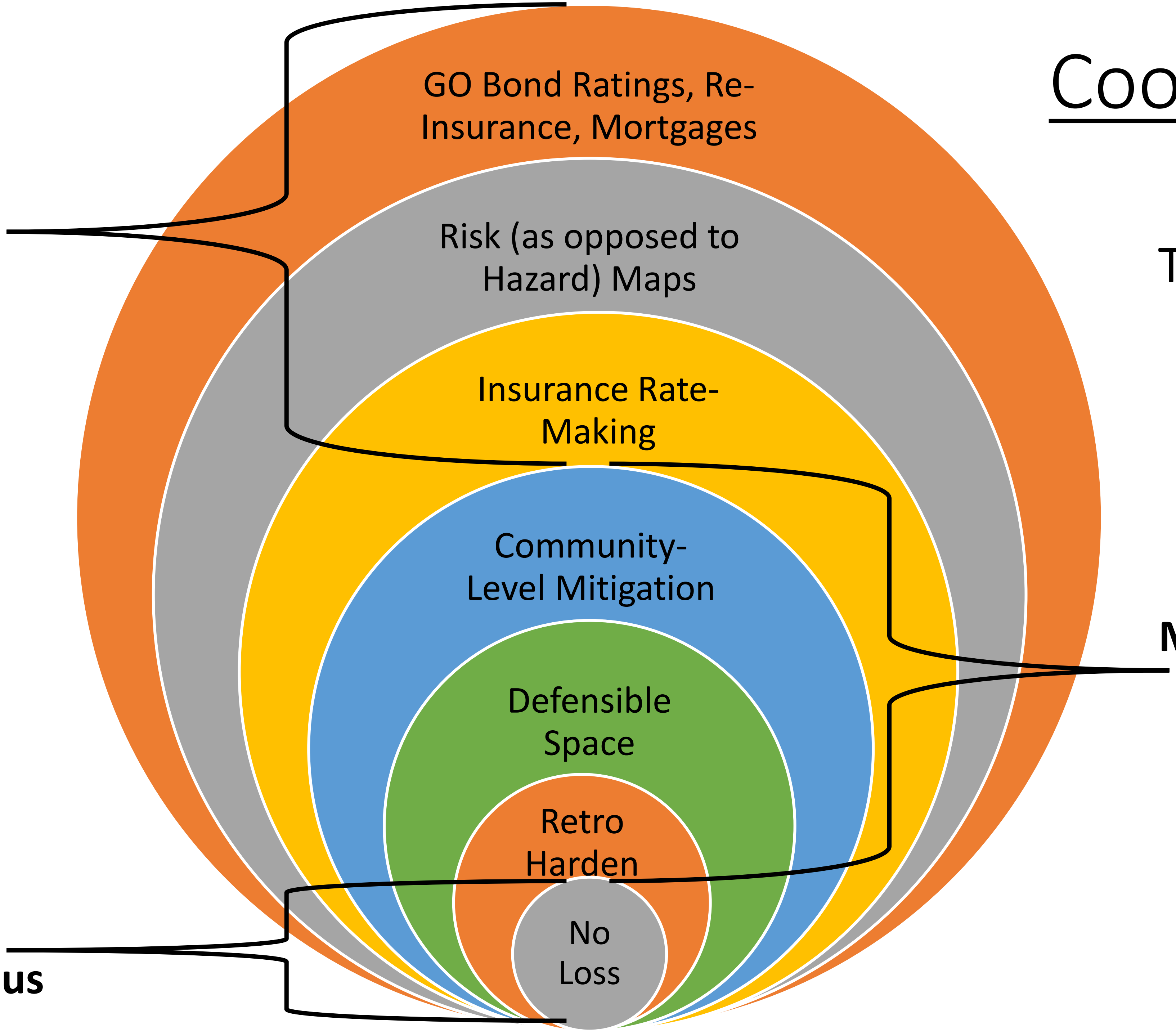
Williams, Hansen, et al. in

Disconnect in Understanding Wildfire Risk

- The “Smiths” and a “Tale of Two Inspections”
- Why legacy data and systems won’t work
- We Cannot Suppress, Regulate, or Price Our Way Out of the WUI Conundrum

Coordinated Policy:

The WUI issue viewed as a Nested Policy Construct



Risk Policy Focus

GO Bond Ratings, Re-Insurance, Mortgages

Risk (as opposed to Hazard) Maps

Insurance Rate-Making

Mitigation Policy Focus

Community-Level Mitigation

Defensible Space

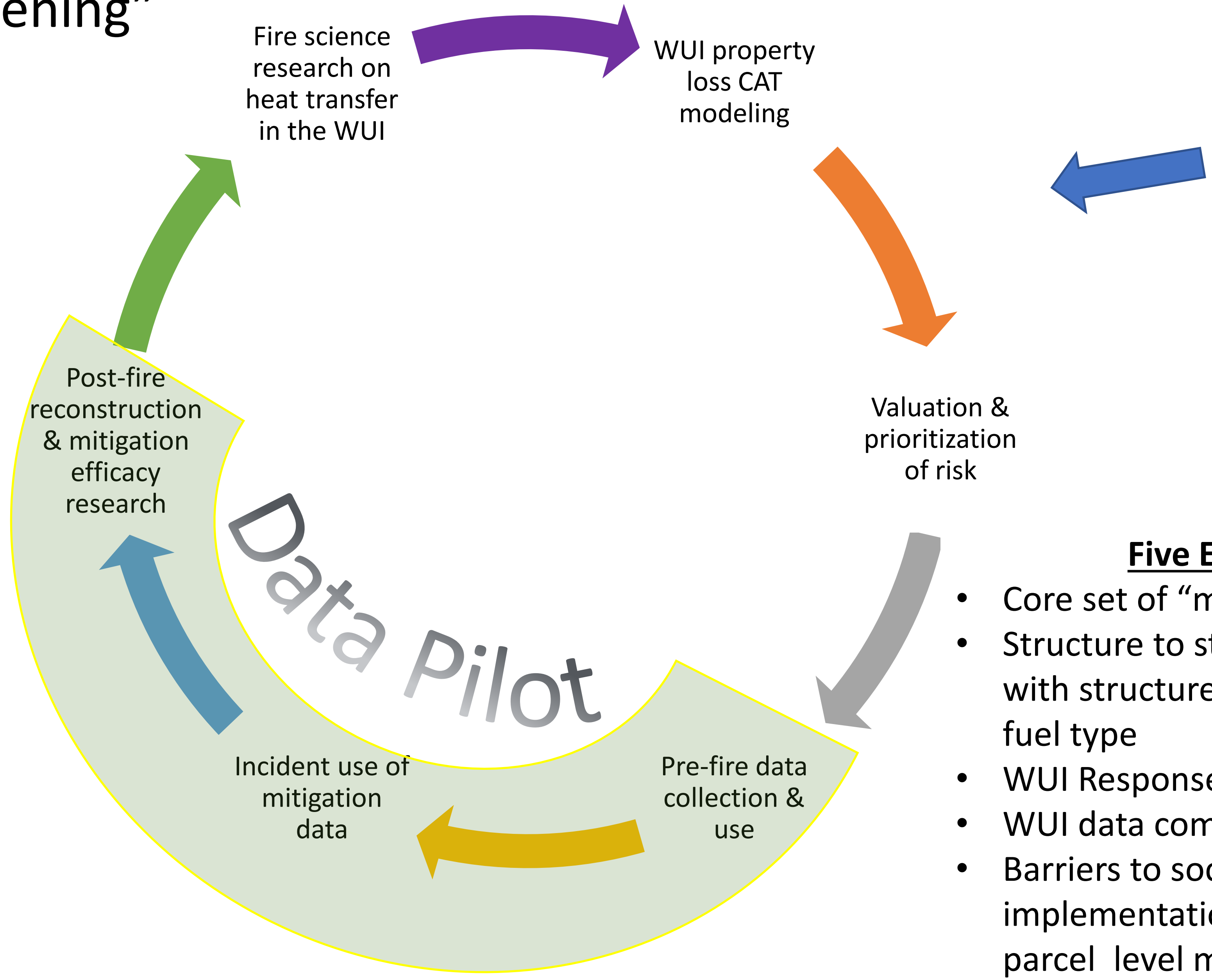
Retro Harden

Policy Outcome Focus

No Loss

CAL POLY
WUI Fire Institute
COLLEGE OF AGRICULTURE, FOOD
& ENVIRONMENTAL SCIENCES

Ideal State for Sustained WUI Mitigation from "The Convening"

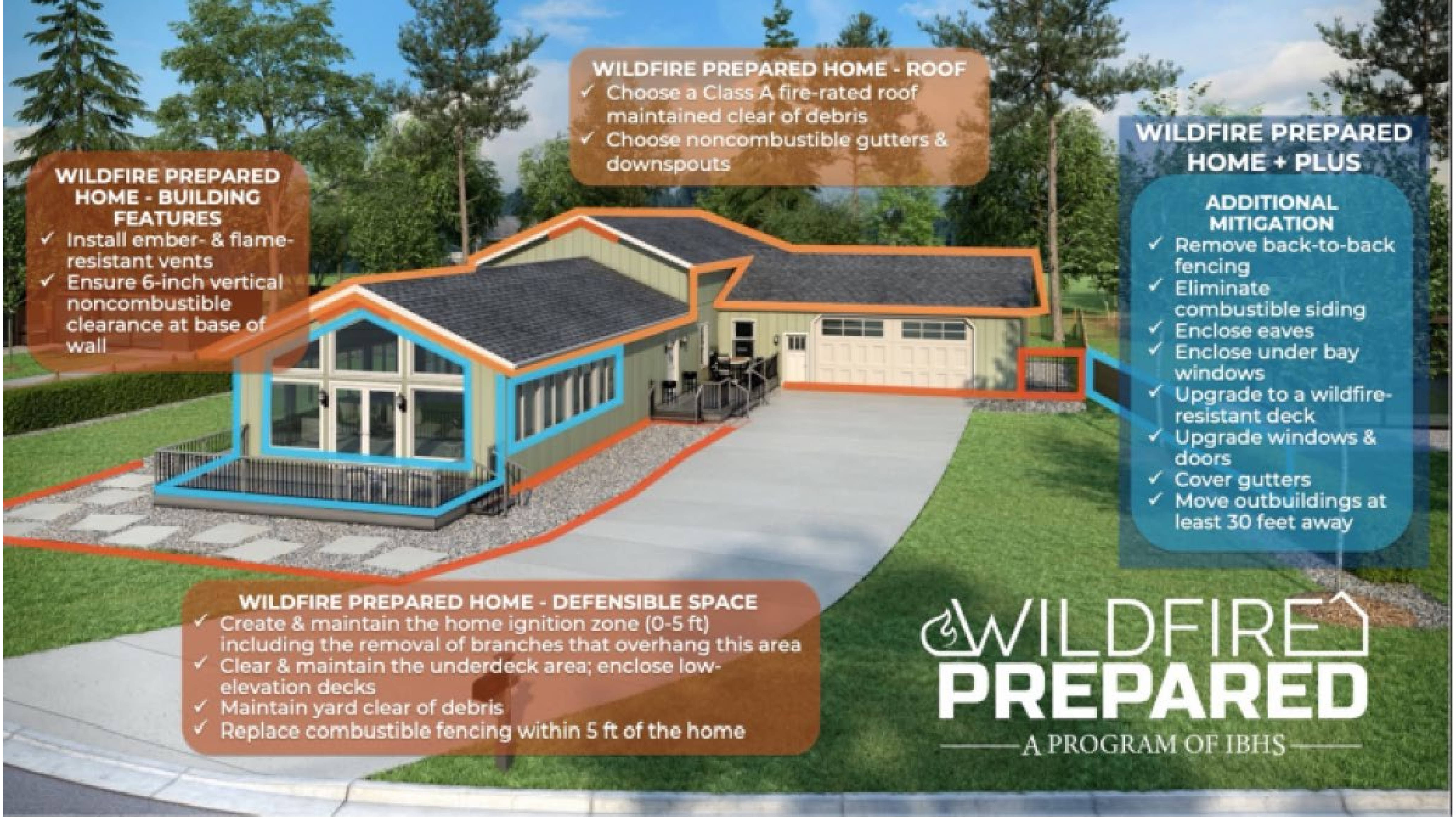

Fire science research on heat transfer in the WUI
WUI property loss CAT modeling
Valuation & prioritization of risk
Pre-fire data collection & use
Incident use of mitigation data
Post-fire reconstruction & mitigation efficacy research
Data Pilot

Five Enabling Tasks:

- Core set of "mitigations-that-matter"
- Structure to structure spread modeling with structures as a new and distinct fuel type
- WUI Response rating
- WUI data commons
- Barriers to social support for implementation and maintenance of parcel level mitigations

CAL POLY
WUI Fire Institute
COLLEGE OF AGRICULTURE, FOOD & ENVIRONMENTAL SCIENCES

Mitigations-That-Matter; Parcel-Level



WILDFIRE PREPARED HOME - ROOF

- ✓ Choose a Class A fire-rated roof maintained clear of debris
- ✓ Choose noncombustible gutters & downspouts

WILDFIRE PREPARED HOME - BUILDING FEATURES

- ✓ Install ember- & flame-resistant vents
- ✓ Ensure 6-inch vertical noncombustible clearance at base of wall

WILDFIRE PREPARED HOME + PLUS

ADDITIONAL MITIGATION

- ✓ Remove back-to-back fencing
- ✓ Eliminate combustible siding
- ✓ Enclose eaves
- ✓ Enclose under bay windows
- ✓ Upgrade to a wildfire-resistant deck
- ✓ Upgrade windows & doors
- ✓ Cover gutters
- ✓ Move outbuildings at least 30 feet away

WILDFIRE PREPARED HOME - DEFENSIBLE SPACE

- ✓ Create & maintain the home ignition zone (0-5 ft) including the removal of branches that overhang this area
- ✓ Clear & maintain the underdeck area; enclose low-elevation decks
- ✓ Maintain yard clear of debris
- ✓ Replace combustible fencing within 5 ft of the home

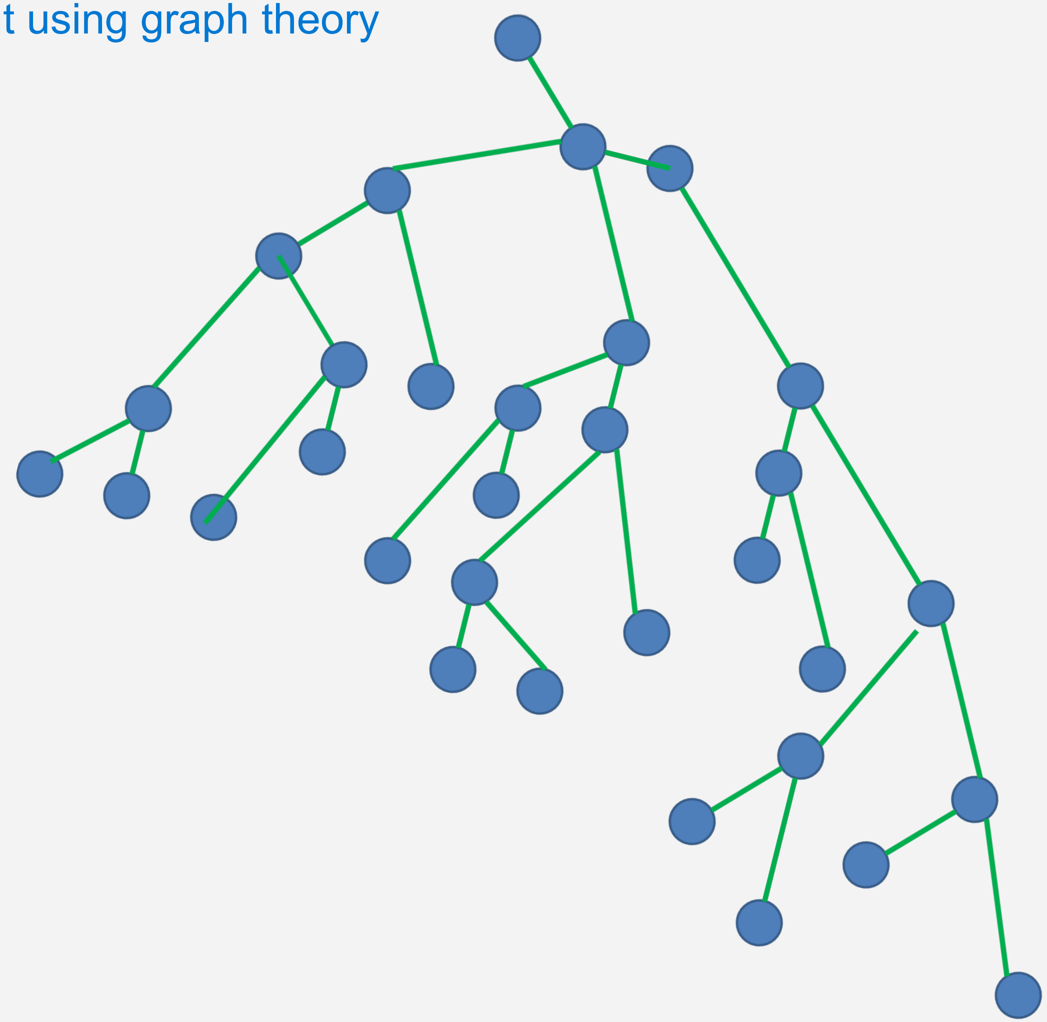
WILDFIRE PREPARED

A PROGRAM OF IBHS

Structure-to-Structure Spread Modeling

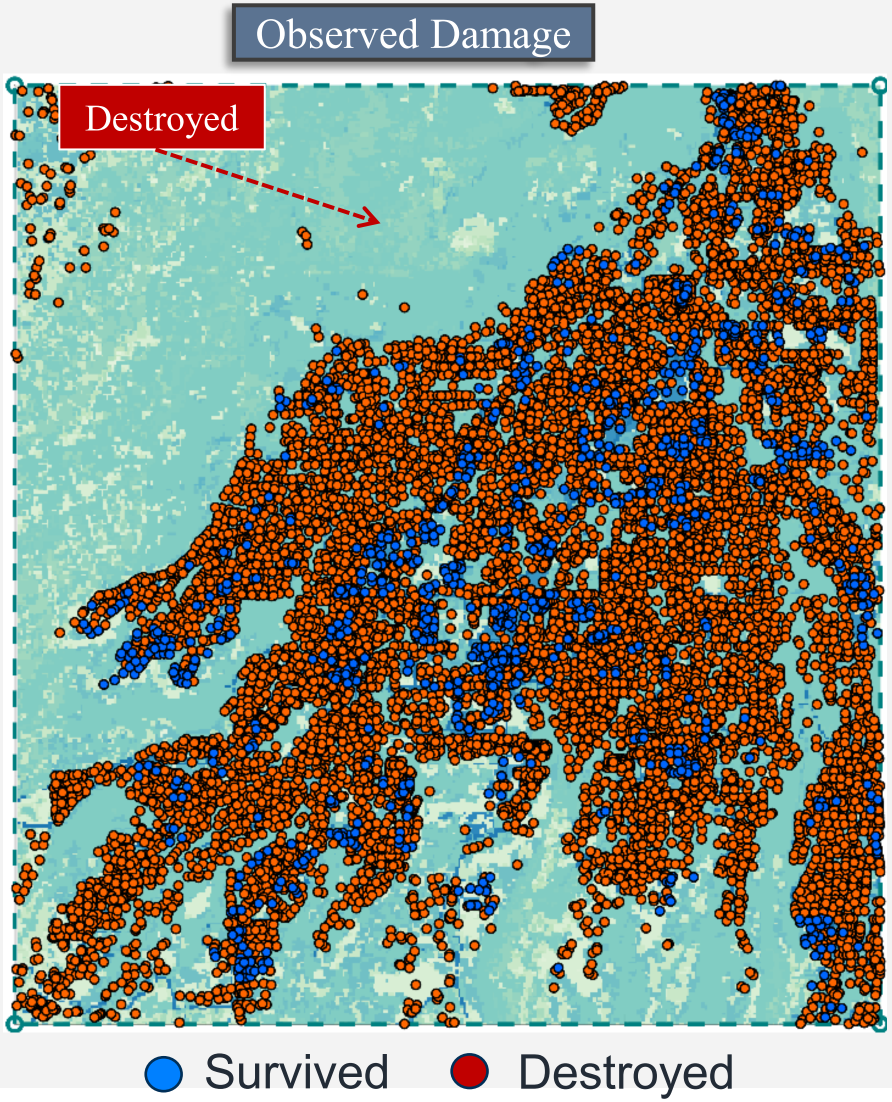
Fire spread modeling in the built environment

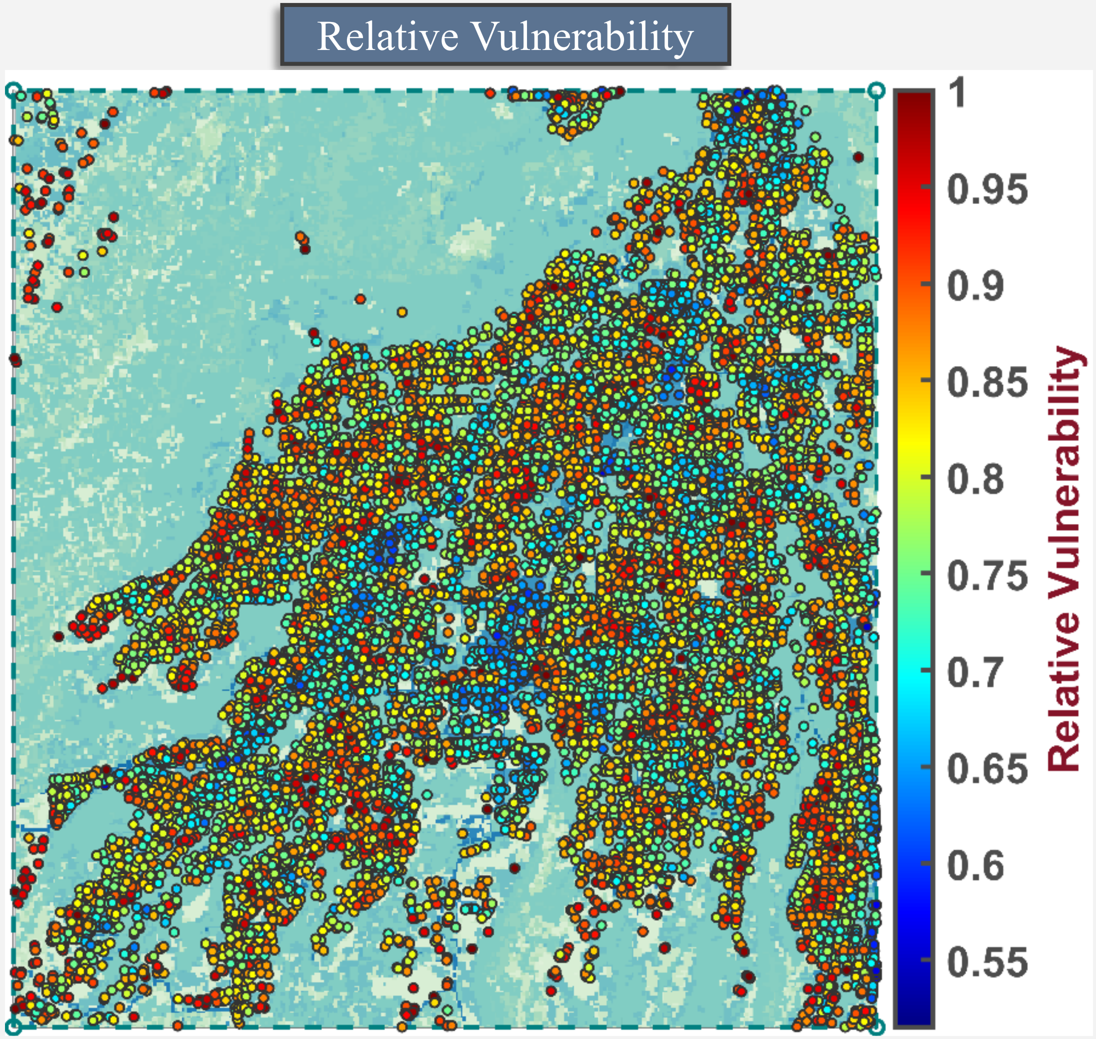
Understand structure to structure spread within the built environment using graph theory



Milliman

Damage Assessment – 2018 Camp Fire





Chulahwat et al. (2022) ***Sci. Rep.***

WUI Response Rating

WUI Response Rating; Capability & Availability by Type - Simplified

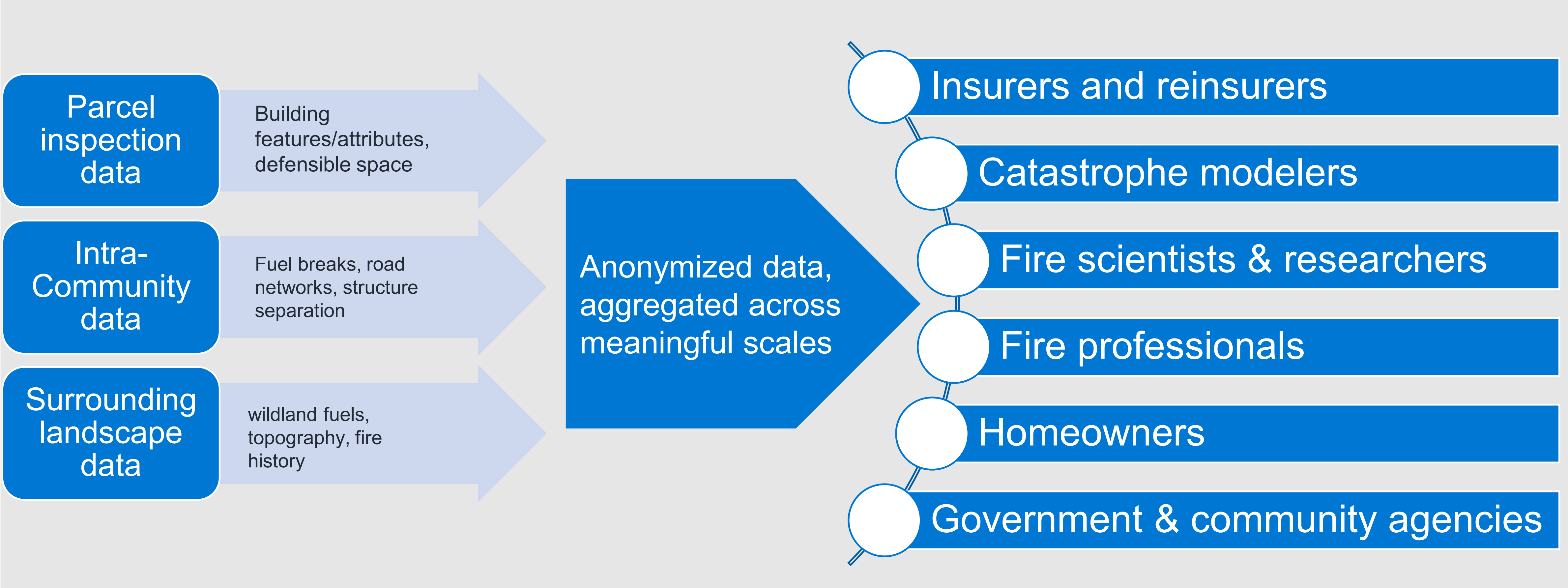
Resource Categories & Type	Capability			Capacity		
	Vegetation to Vegetation	Vegetation to Structure	Structure to Structure	Vegetation to Vegetation	Vegetation to Structure	Structure to Structure
Rolling Stock	.5	1	1.5	2	4	6
Hand Crews	1.5	.7	0	6	2	0
Aircraft	3	2	0	1	0	0
Agency Aid Agreement Type Factor	Recognizes the (in)efficiencies of coordination among resource types when single, several, or numerous agencies are responding together.					

LEARN BY DOING CAL POLY WUI Fire Institute COLLEGE OF AGRICULTURE, FOOD & ENVIRONMENTAL SCIENCES

WUI Data Commons

Wildfire Open Data Commons

Provides all stakeholders well-rounded views of risk



Parcel inspection data

Building features/attributes, defensible space

Intra-Community data

Fuel breaks, road networks, structure separation

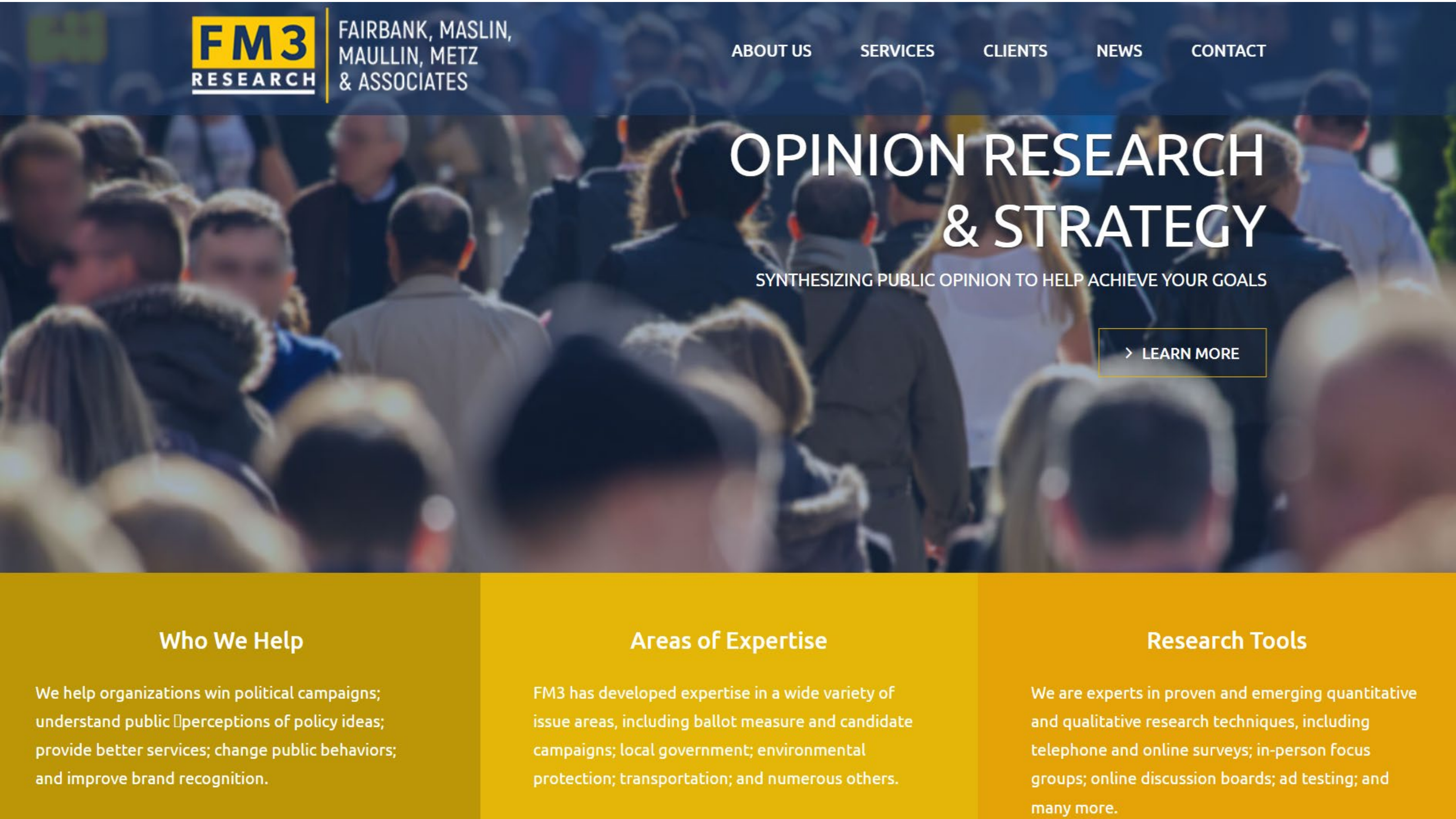
Surrounding landscape data

wildland fuels, topography, fire history

Anonymized data, aggregated across meaningful scales

- Insurers and reinsurers
- Catastrophe modelers
- Fire scientists & researchers
- Fire professionals
- Homeowners
- Government & community agencies

Social Barriers to Implementation & Maintenance of Parcel & Community Mitigations at Scale



OPINION RESEARCH & STRATEGY

SYNTHESIZING PUBLIC OPINION TO HELP ACHIEVE YOUR GOALS

Who We Help

We help organizations win political campaigns; understand public perceptions of policy ideas; provide better services; change public behaviors; and improve brand recognition.

Areas of Expertise

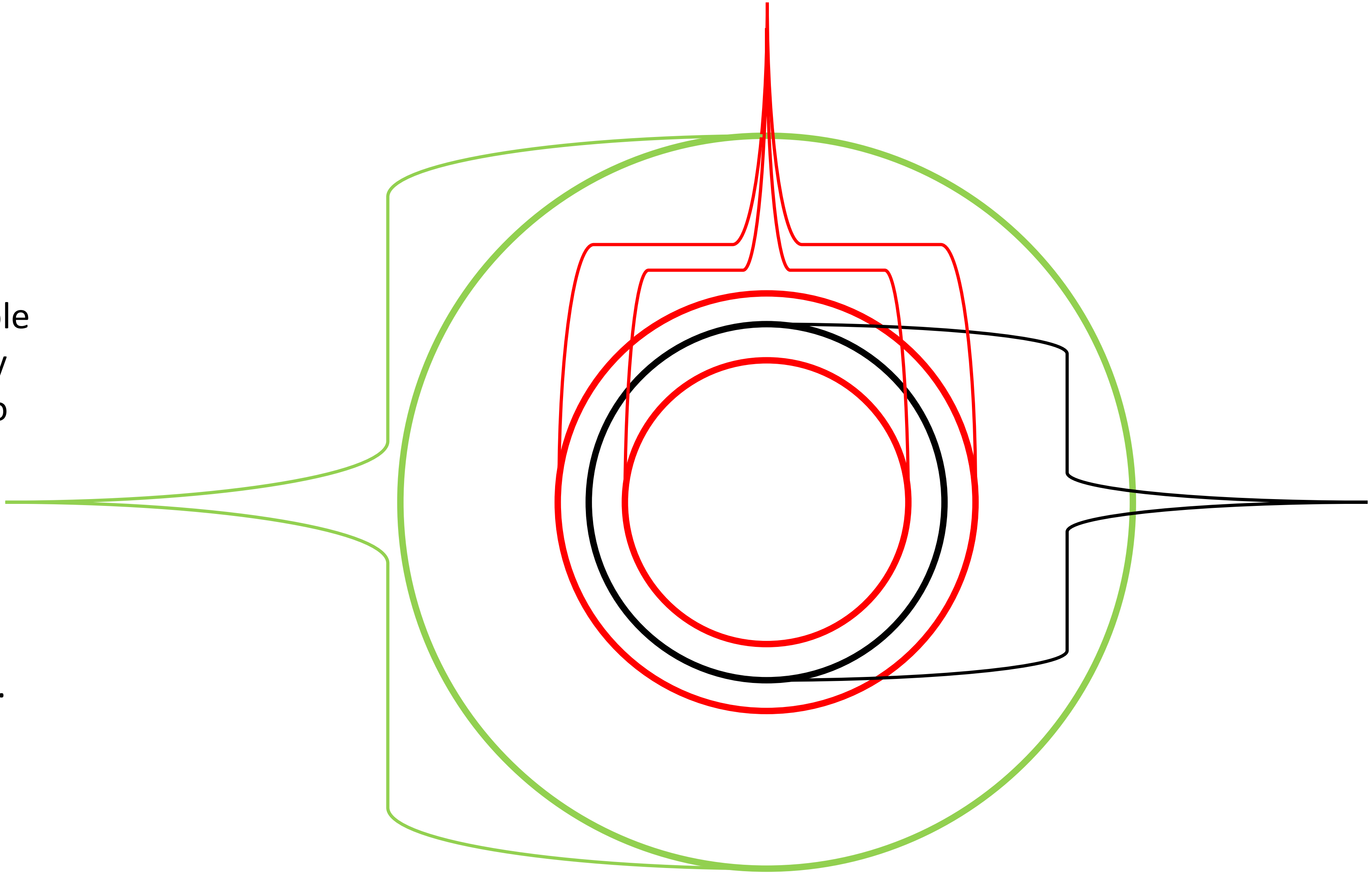
FM3 has developed expertise in a wide variety of issue areas, including ballot measure and candidate campaigns; local government; environmental protection; transportation; and numerous others.

Research Tools

We are experts in proven and emerging quantitative and qualitative research techniques, including telephone and online surveys; in-person focus groups; online discussion boards; ad testing; and many more.

WUI Fire Pathway Taxonomy

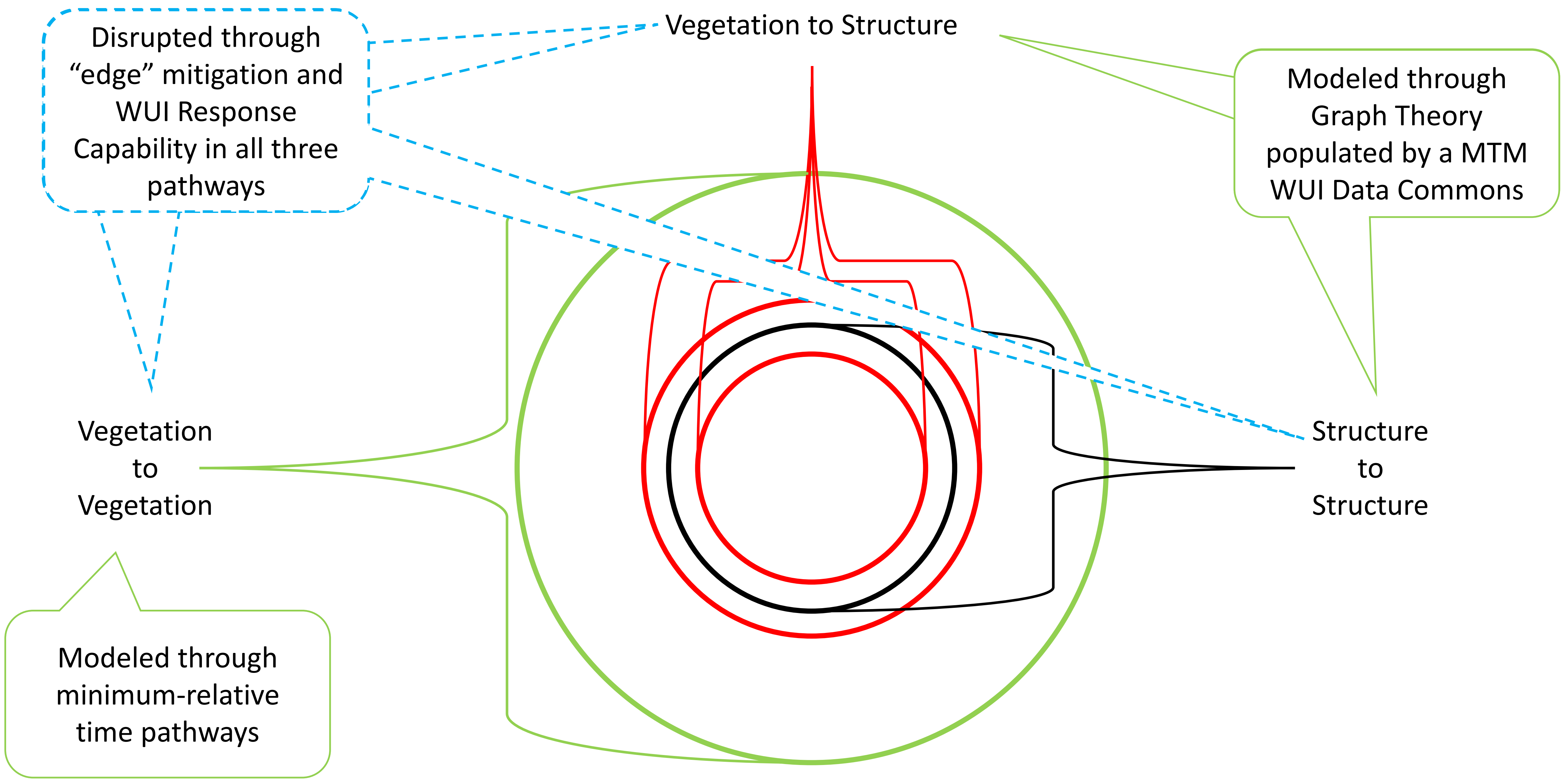
“Interface” = band within 100’ of WUI Community boundary to 2nd layer of structures with SSD < 70’



“Most Probable Fire Pathway SOI” = 1/2 to 1/4 mile of interface in vegetation landscapes capable of carrying fire.

“WUI Community” = ≥ 100 structures where 50% or more have SSD < 70’

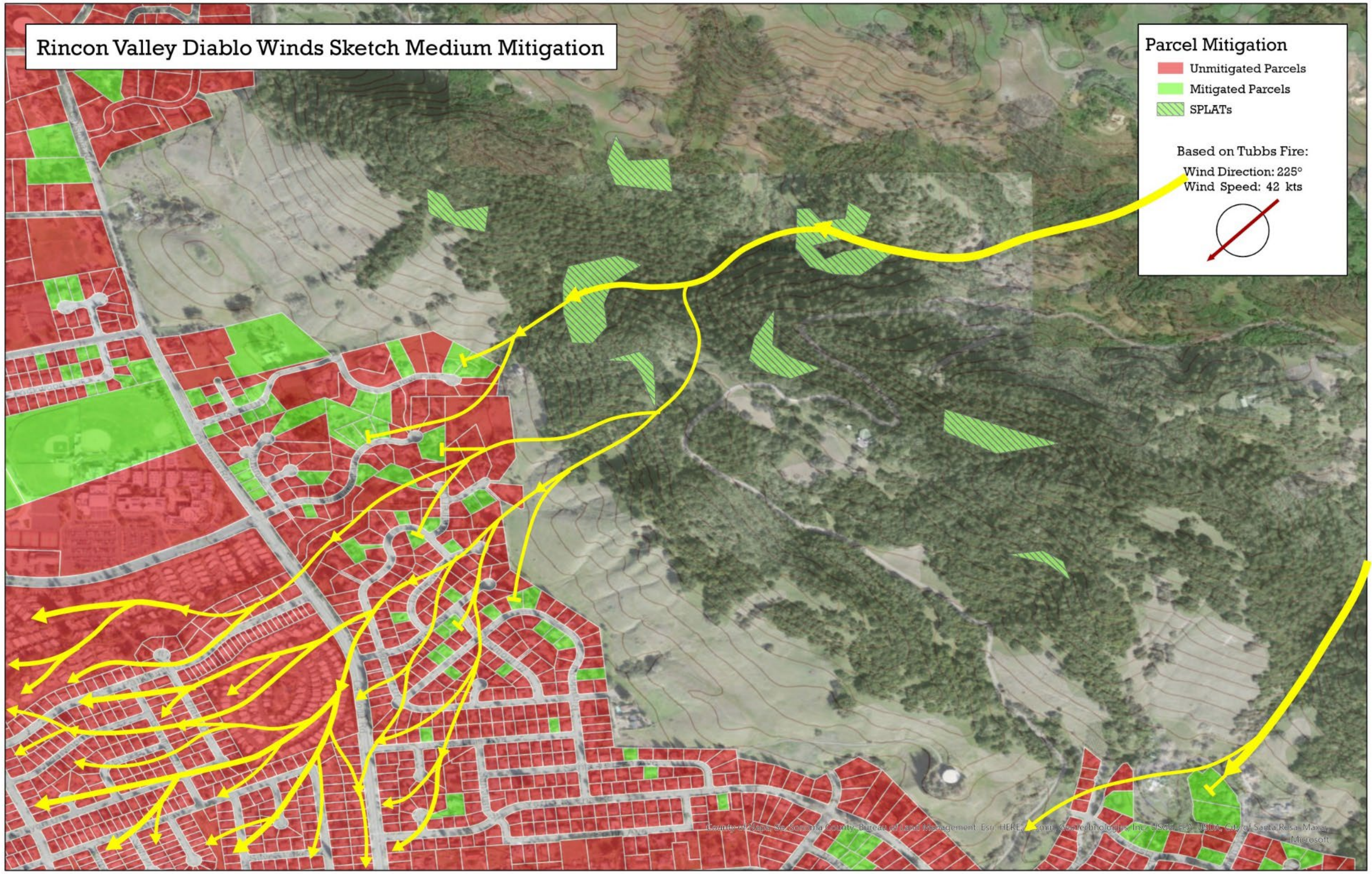
CAL POLY
WUI Fire Institute
COLLEGE OF AGRICULTURE, FOOD
& ENVIRONMENTAL SCIENCES


Disrupted through “edge” mitigation and WUI Response Capability in all three pathways
Vegetation to Structure
Modeled through Graph Theory populated by a MTM WUI Data Commons
Vegetation to Vegetation
Structure to Structure
Modeled through minimum-relative time pathways

WUI Fire Pathway Disruption

CAL POLY
WUI Fire Institute
COLLEGE OF AGRICULTURE, FOOD & ENVIRONMENTAL SCIENCES

Fire pathways into community


Rincon Valley Diablo Winds Sketch Medium Mitigation
Parcel Mitigation
🟥 Unmitigated Parcels
🟩 Mitigated Parcels
▨ SPLATs
Based on Tubbs Fire:
Wind Direction: 225°
Wind Speed: 42 kts
County of Napa, Sa, Sonoma County, Bureau of Land Management, Esri, HERE, Garmin, Geotechnologies, Inc., USGS, EPA, USDA, City of Santa Rosa, Maxar, Microsoft

“Cliffs Notes”

Who	What	When	Where	How

In Closing….

- We’re at the end of the beginning; time to stop admiring the problem and start solving it.
- Environmental and economic calamities have arrived without our permission; move with appropriate urgency.
- Water agencies and WUI Communities share common threats and consequences.