
Recovering from a
Ransomware Attack
How Zero Trust Network Security
Can Enable Cyber Recovery

Today's Presentation

RMI

In todays presentation we will cover…

- Current state of cyber recovery.
- A cyber-recovery solution architecture.
- Technologies available today… not futures.
- The ransomware recovery process.

-- and --

- Discuss Risk Masters' work with the Boston Global Forum.
  - The first time in history G7 nations elevated cyber security to a matter of national interest.

RMI

First… a Story.

RMI Risk Masters, Inc.

Current State

Ransomware Update

RMI

The New Jersey Cybersecurity & Communications Integration Cell (NJCCIC) provided the following update on May 27, 2016.

- The NJCCIC advises our members that paying ransom does not guarantee the decryption and restoration of data.
- Organizations can greatly reduce the likelihood of infection by ensuring employees are properly trained to identify/mitigate:
  - Social engineering attempts
  - Spear-phishing emails
  - Internet-based threats (i.e. suspect websites)
- A sound data backup strategy can mitigate the impact of a ransomware infection and successfully restore data.

What is the Current State of Cyber Recovery?

RMI

Most organizations are still develop their response capabilities.

- Little written on the topic of cyber recovery.
- Little investment has been made in cyber recovery.
- Few technology solutions offered cyber recovery.
- Few standards exist for cyber recovery.
  - NIST cybersecurity framework – February 2014.
  - First to call for recovery planning for cyberattacks.

Does NIST Deliver on Cyber Recovery?

RMI

Many organizations have not assessed their exposure.

- NIST is being used as a cyber security standard.
- However… NIST does not “raise the bar” on cyber recovery.
  - NIST focuses on traditional recovery controls.
- Cyber recovery will require new methods and solutions.

Elements of Cyber Risk Management

RMI

Cyber threats must be addressed using holistic risk management.

Your best protection against cyber attacks remains a holistic risk management approach:

- Threat Avoidance
- Operational Recovery
- Risk Transfer (e.g., insurance)

What About Operational Recovery?

RMI

Most organizations do not have formal cyber recovery plans.

- Most organizations invest in threat avoidance controls.
  - Traditional firewalls
  - Monitoring software
  - Unified Threat Management appliances
- Cyber insurance is expensive and does nothing to repair the damage caused by an attack.
- Traditional recovery planning methodologies are incomplete.

The Challenge in Avoiding Ransomware

RMI

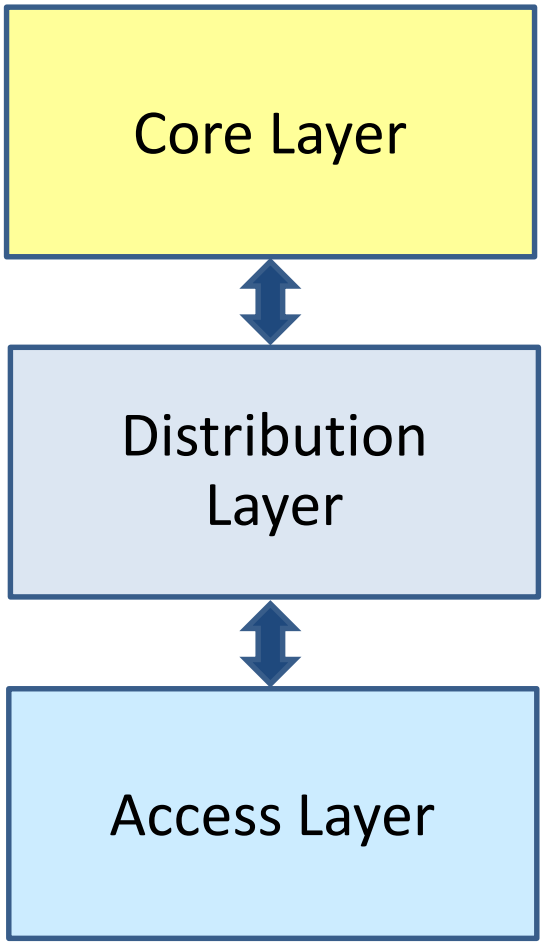
Threat Avoidance and Insurance are necessary, but insufficient.

- Latent threats increase the complexity of cyber-recovery.
  - Ransomware can lie dormant and undetected for extended periods.
  - Rolling disaster scenarios can propagate the threat to backup data.
- People are still your weakest link.
  - Monitoring of network activity is not universal
  - Password security
  - Email threats
  - Thumb drives
  - Battery backup

The Challenge in Recovering from Ransomware

RMI

Today's enterprise networks are hierarchical in structure.



- Hierarchical networks focus on perimeter (fortress/moat) security.
  - Hard on the outside… soft on inside.
  - Once on authenticated on the network you are "trusted."
- Internet applications can tunnel through traditional firewall security.

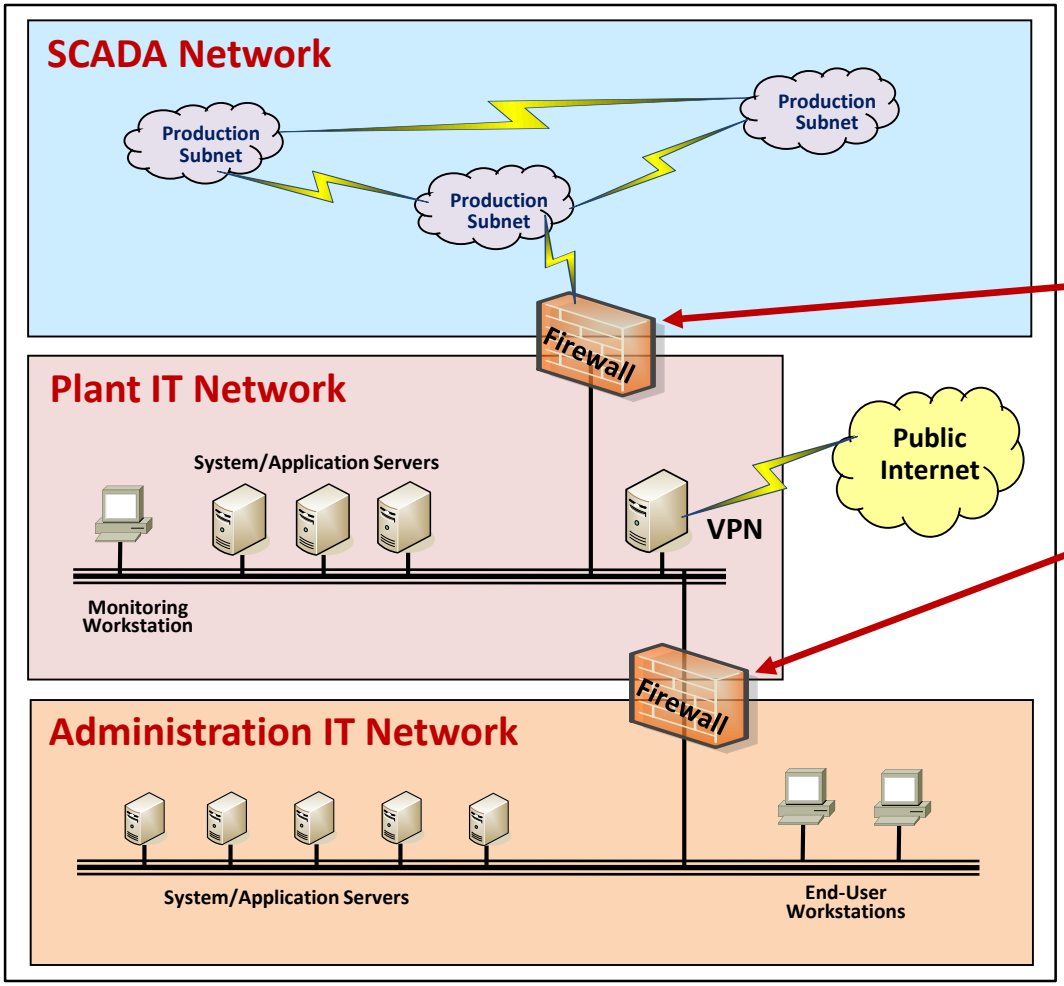
RMI Risk Masters, Inc.

Technology

Segmenting Networks Enhances Cyber Resilience

RMI

Segmentation isolates critical data and services in “Security Zones.”



- Segmenting networks enhances resilience.
- Past approaches to segmentation involved port-based firewalls.
- Firewalls and other point solutions are expensive to implement on an enterprise basis.

Segmenting Networks Using Port-Based Firewalls

RMI

Port-based firewalls can be compromised by cyber threats.

- Traditional firewalls that classify traffic by port and protocol can be bypassed by knowledgeable hackers and malware:
  - “Port hopping” to locate an open port on a device.
  - Use of SSL and SSH encryption to hide malware transmission.
  - Sneaking across “Port 80” or using non-standard ports.
- Cyber recovery requires a more reliable way of segmenting networks.

“Next Generation Firewalls” Enhance Cyber Security

RMI

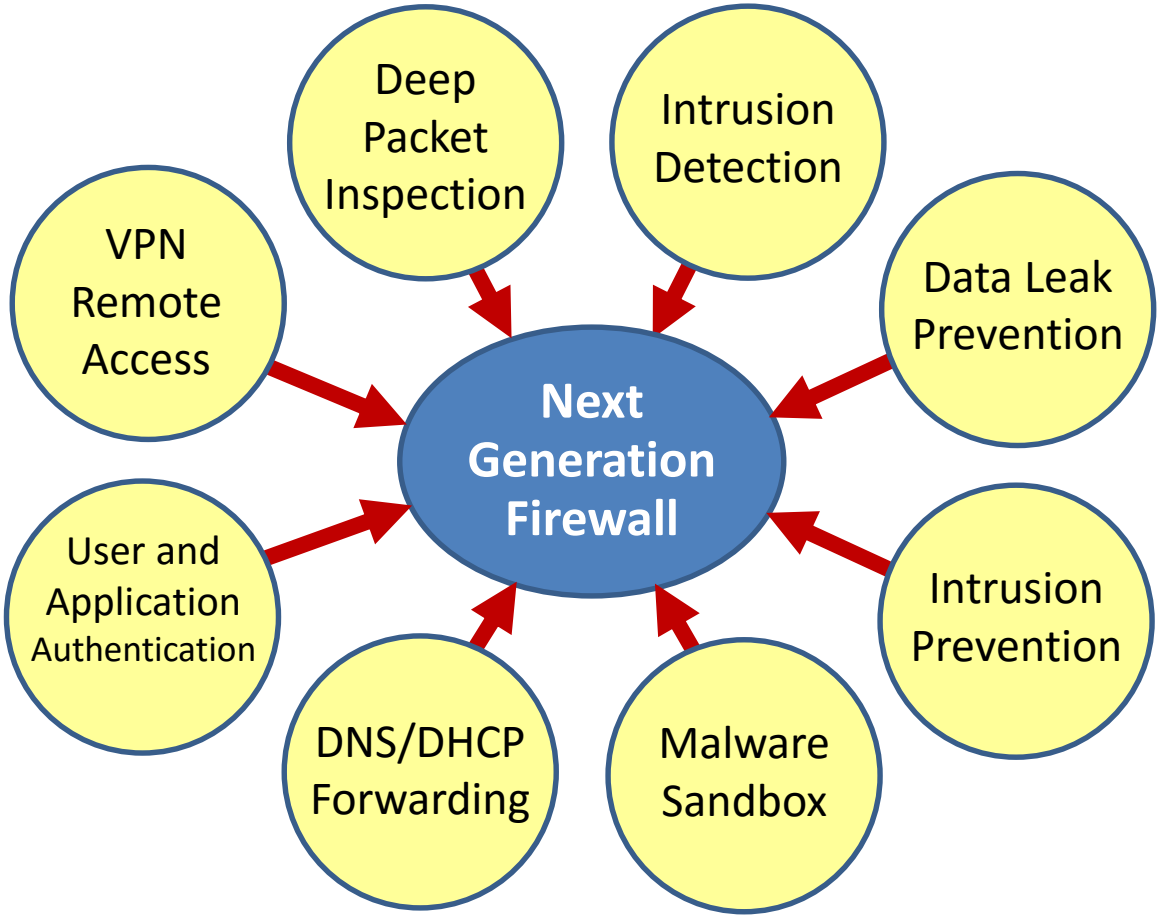
Next Generation Firewalls (NGF) enhance cyber resiliency.

- NGF’s assume all data traffic is “untrusted.”
  - Port-based data traffic is blocked.
  - Authentication elevated to application and user-ID level.
- NGF’s employ “one-pass” authentication and content scanning.
- Decrypt and scan data/content for malware signatures.
- Employ heuristics (trial and error) to identify suspect malware.
- Enforcement with rule-based access to data and applications.

Next Generation Firewall Functionality

RMI

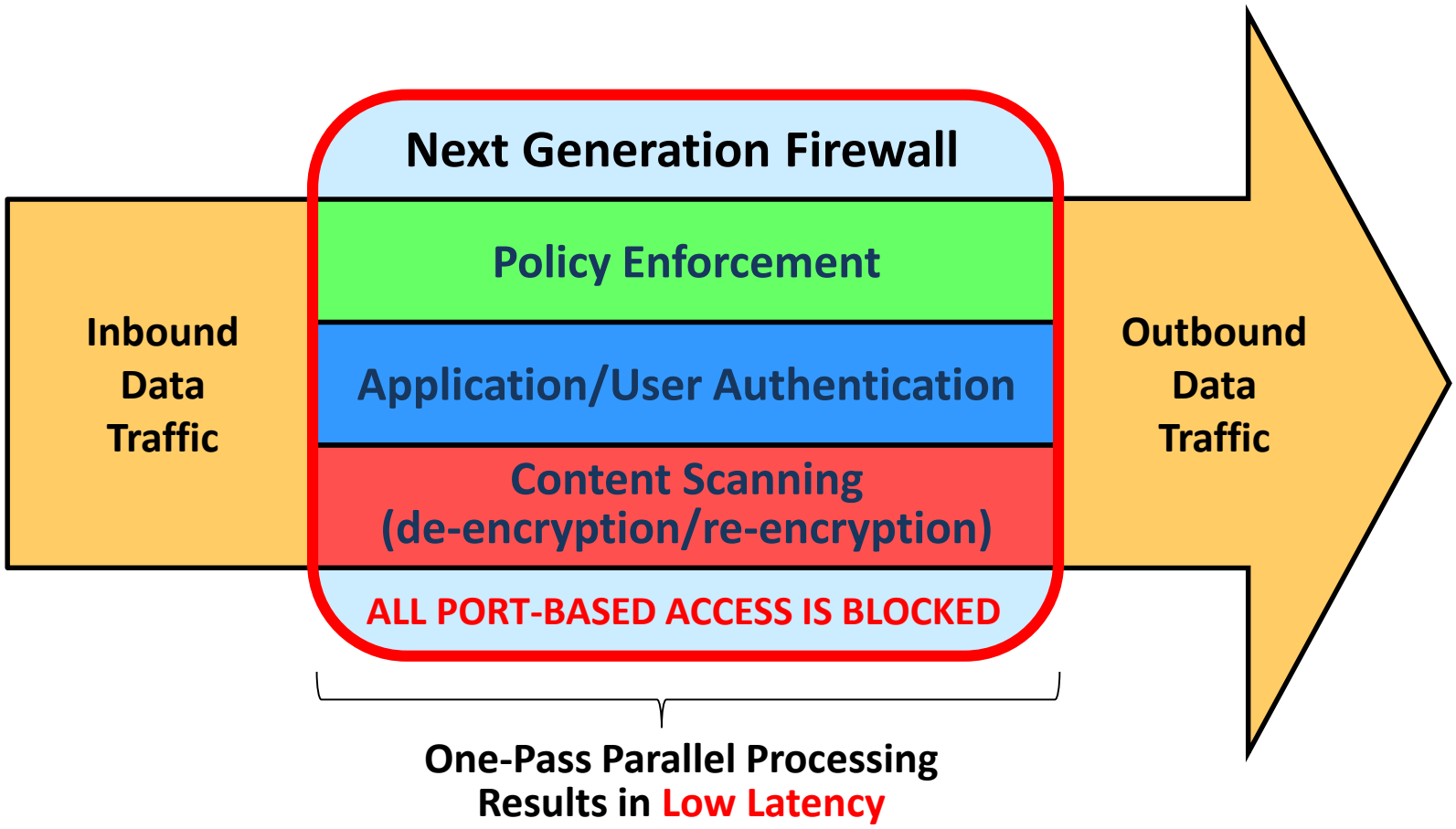
Next Generation Firewalls collapse multiple network security point solutions into a single device to enable centralized management.



Next Generation Firewall Performance

RMI

Next Generation Firewalls (NGF) employ one-pass high performance parallel processing that is engineered for purpose.



RMI Risk Masters, Inc.

The Solution

Cyber Resilient "Zero Trust" Network Architecture

RMI

Next Generation Firewalls enable migration from a hierarchical network to a cyber-resilient "Zero Trust" network architecture.

- Zero Trust security advanced by John Kindervag of Forrester.
- Zero Trust assumes all applications and users are "untrusted."
  - Restricted to the minimum set of resources required.
- Zero Trust should include an NGF at the center of the network.
  - NGF acts as a traffic hub.
  - NGF authenticates and scans all data packets during pass-through.
  - NGF enforces "security zones" that restrict "user" and "application" access to specific data assets.

Cyber DRaaS™ – A Solution for Cyber Recovery

RMI

Cyber DRaaS integrates the NGF with cloud-based DR backup service to enable recovery from cyberattacks.

- Cyber DRaaS employs enhanced authentication of data backup traffic under a Zero Trust network security model.
  - Authentication at the “application” and “user” level
- Creates “trusted image” backups that are used as the vehicle for post-event cyber recovery.
- Provides continuous integrity checking of trusted image backups.
- Relies on the implementation of operational processes.
  - Change Control
  - Cyber Event Monitoring
  - Computer Emergency Response Team (CERT)

Cyber DRaaS – Key Benefits

RMI

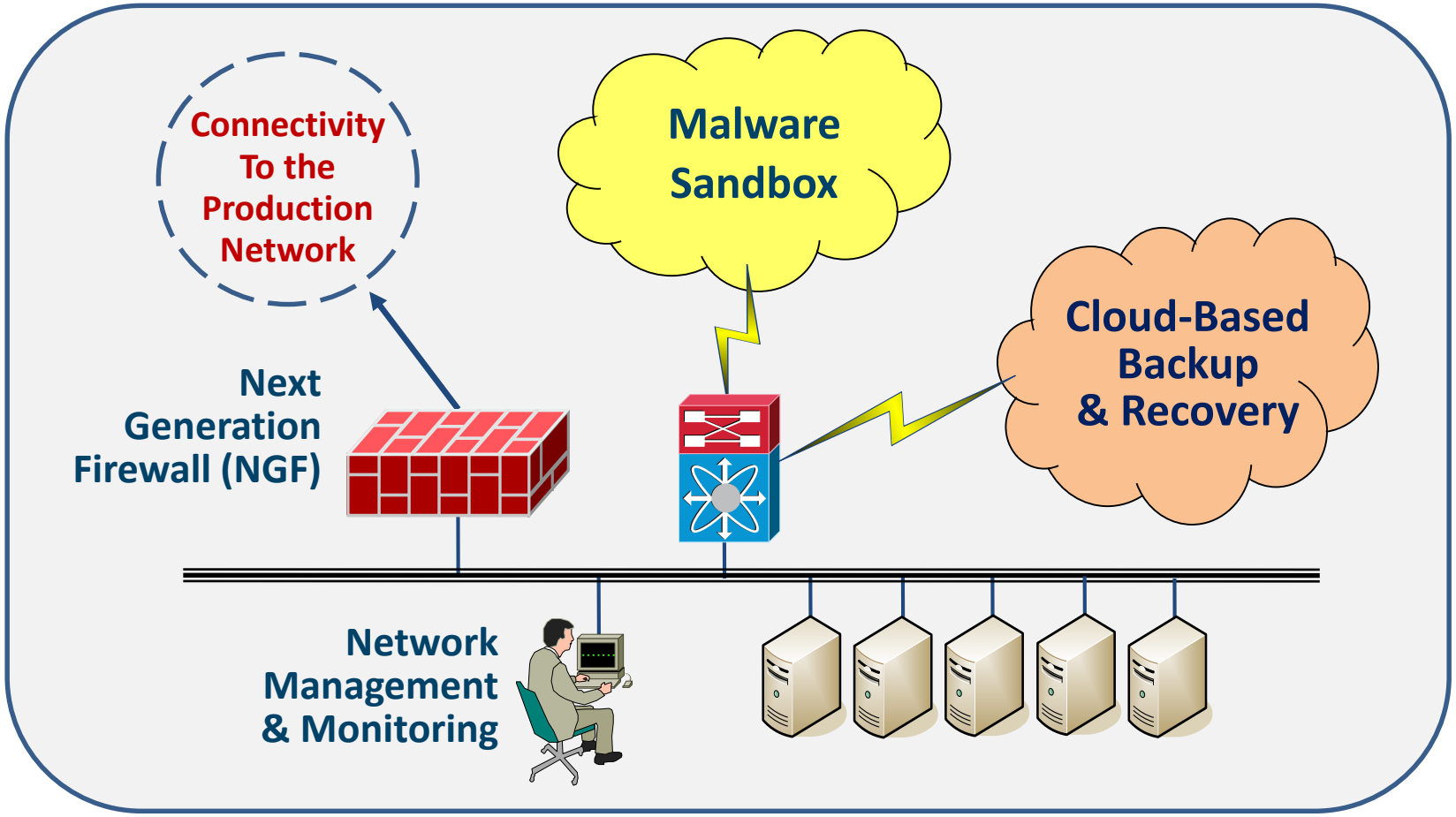
Cyber DRaaS benefits mitigate the threat from a cyber attack.

- Directly addresses the need for a viable and workable approach to cyber recovery from ransomeware.
- Solution options include deployment within a hierarchical network or in a Zero Trust network.
- Eliminates the need for an “air-gap” that physically separates the production network from a cyber-backup network.
- Reduces recovery time from a cyber-attack.
  - Simplifies the recovery process.
  - Enables early recognition of an attack.
- Demonstrates due diligence on the part of corporate officers and directors by effectively mitigating a known risk.

Cyber DRaaS™ Data Center Architecture

RMI

Cyber DRaaS integrates the Next Generation Firewall with cloud based DR to protect trusted backups from cyber attack.



Cyber DRaaS™ – Technology Components

RMI

Cyber DRaaS incorporates the following enabling technologies.

Cloud Backup & Recovery	• Manages backup/restore process for trusted images. • Integrity checking of trusted image backups. • Data compression and deduplication.
Next Generation Firewall	• Policy enforcement at application/user level (not port). • Content scanning for malware signatures. • High performance single-pass software engine.
Network Management	• Enterprise-level policy management across firewalls. • Visibility into user/application traffic on the network. • Tools enabling immediate investigation of malware.
Malware Sandbox	• Malware redirection to virtualized sandbox. • Monitoring of malicious network behaviors. • New malware discoveries generate new signatures.

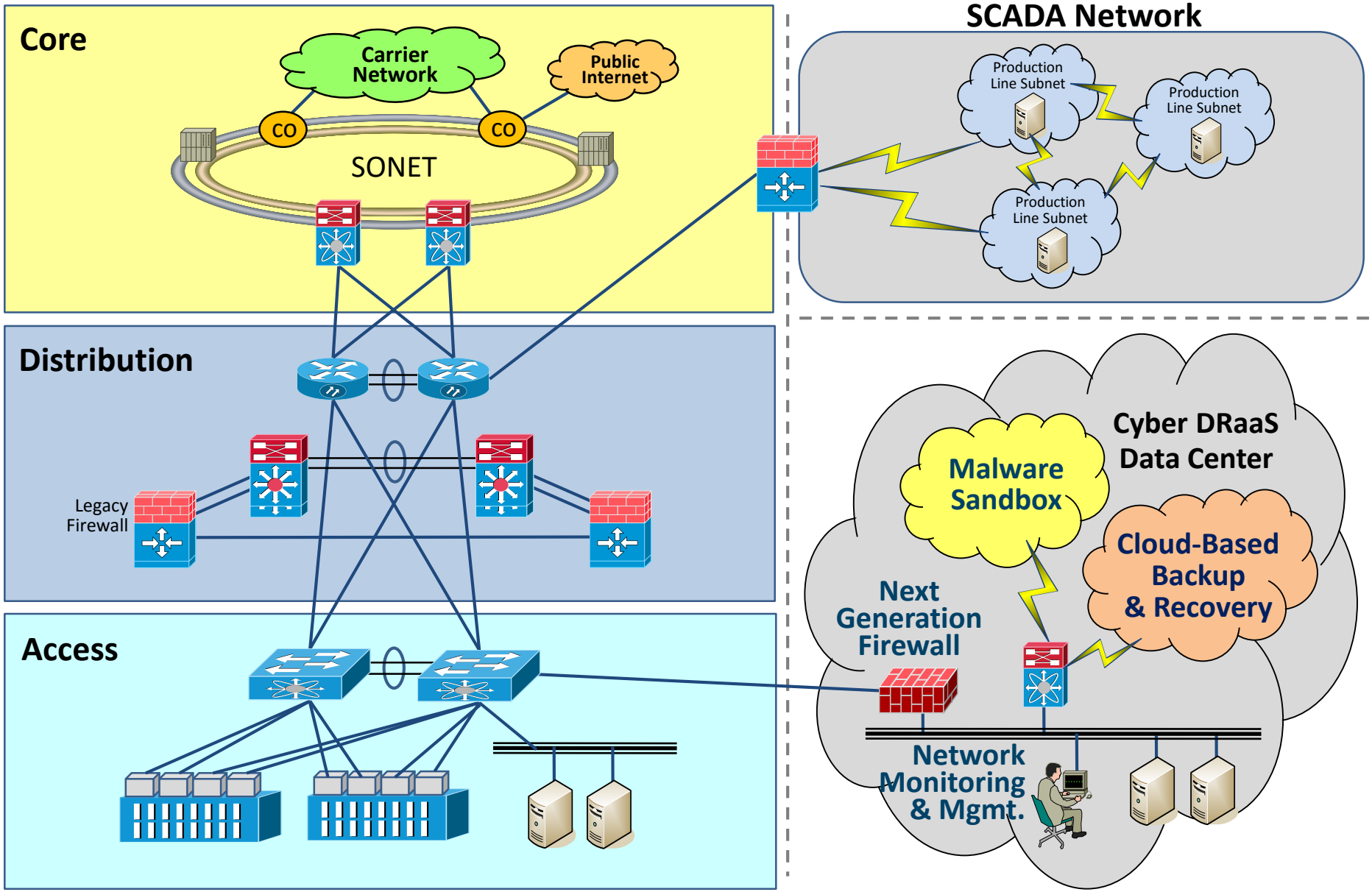
Deploying Cyber DRaaS in a Hierarchical Network

RMI

Cyber DRaaS deployed on its own subnet in a Hierarchical Network.

- The Data Center sits inside its own subnet created by a Next Generation Firewall.
- Only authorized users and applications permitted to backup copies of trusted images into the cloud.
- Malware sandbox enables suspect malware to be analyzed.
- Hash totaling monitors any changes to backups in the cloud.

Example — Fortress/Moat Network Incorporating the Cyber DRaaS™ Cloud



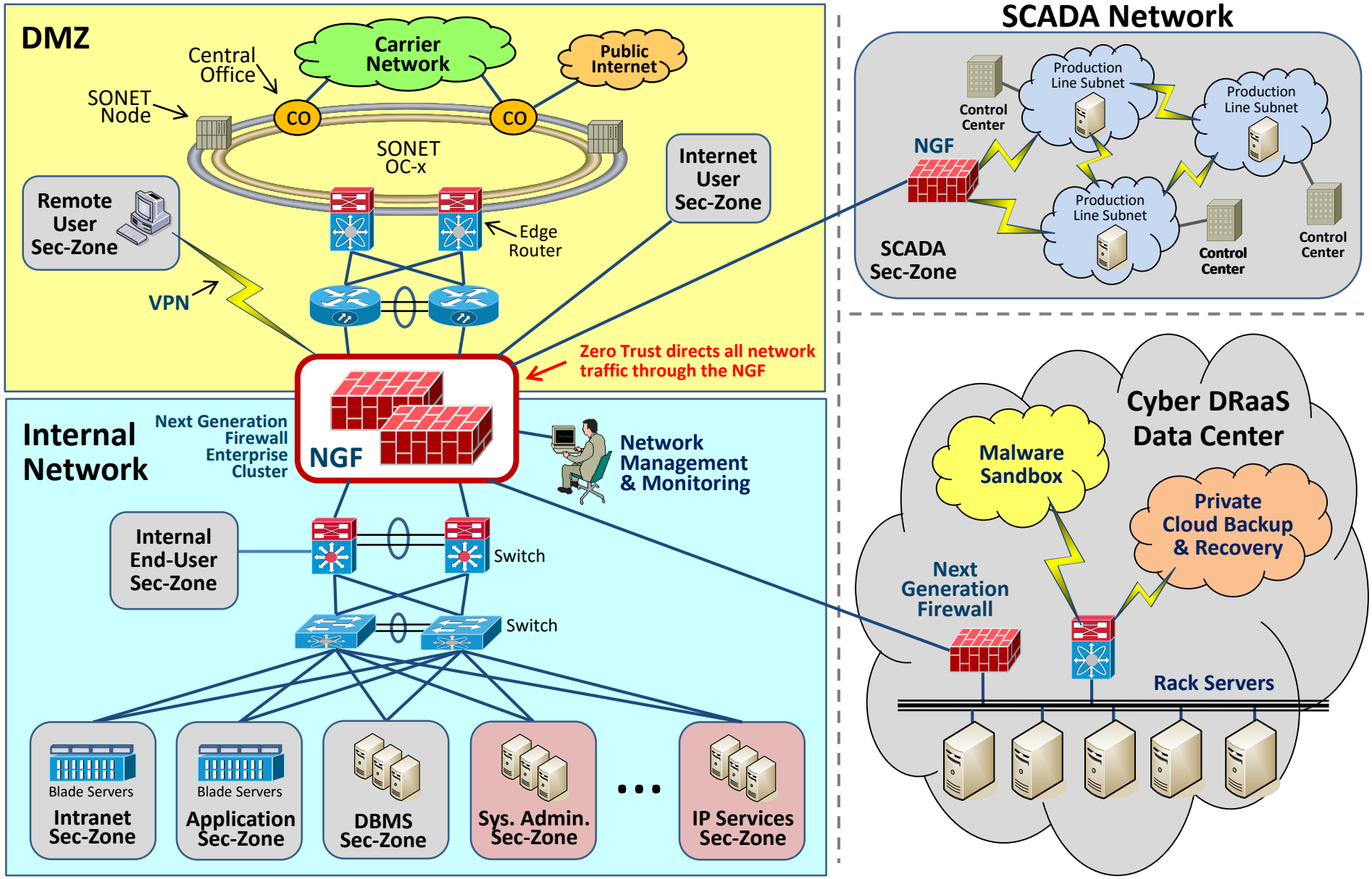
Deploying Cyber DRaaS in a Zero Trust Network

RMI

Cyber DRaaS deployed in its own security zone on Zero Trust network.

- Zero Trust network organizes all network traffic around a centralized NGF cluster.
  - All data traffic is authenticated and scanned for malware.
  - Encrypted content is decrypted and scanned.
- The Data Center sits in its own security zone.
- Only authorized users and applications permitted to backup copies of trusted images into the cloud.
- Malware sandbox enables suspect malware to be analyzed.
- Hash totaling monitors any changes to backups in the cloud.

Example — "Zero Trust" Network Incorporating the Cyber DRaaS™ Data Cloud



Cyber DRaaS – Risk Management Limitations

RMI

Cyber DRaaS does have certain security limitations.

- Cyber DRaaS cannot stop a disgruntled employee.
  - Malware introduced using a privileged account.
  - Staff having access to both production data center and cloud backup.
- Full Cyber DRaaS implementation requires network re-architecture.
- Cyber DRaaS may not identify malware introduced by vendors.
  - Microcode.
  - Supply chain or other manufacturing source.

Cyber Resilience - Advanced Recovery Solutions

RMI

Cyber DRaaS delivers a family of advanced strategy options that will mitigate cyber recovery risk.

Solution Options	Network Architecture	Firewall Technology	CERT Team & Plan	Enterprise Data Traffic Monitoring	Automated DR Backup Scanning	Integrated Malware Quarantine	DR Data Integrity Checks	Cyber Recovery Risk Level
Traditional Disaster Recovery	Flat or Hierarchical	Not Applicable	NO	NO	NO	NO	NO	HIGH
Cyber DRaaS Air-Gap	Flat or Hierarchical	Legacy (Optional)	YES	NO	Limited	NO	Optional	MODERATE to HIGH
Cyber DRaaS Hierarchical	Flat or Hierarchical	Next Generation	YES	NO	YES	YES	YES	LOW to MODERATE
Cyber DRaaS Zero Trust	Zero Trust	Next Generation	YES	YES	YES	YES	YES	LOW

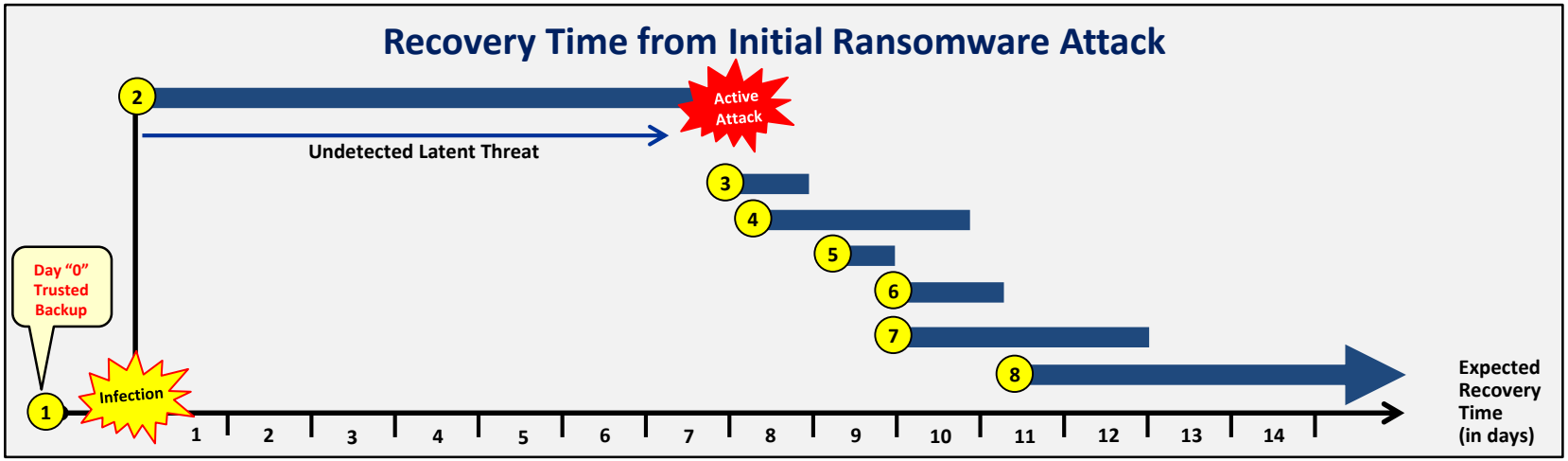
KEY: ——— = Solutions Employing Zero Trust Architecture

RMI Risk Masters, Inc.

Recovery Process

Traditional Response to a Ransomware Attack

Illustration assumes a malware attack with presence latent for seven (7) days.

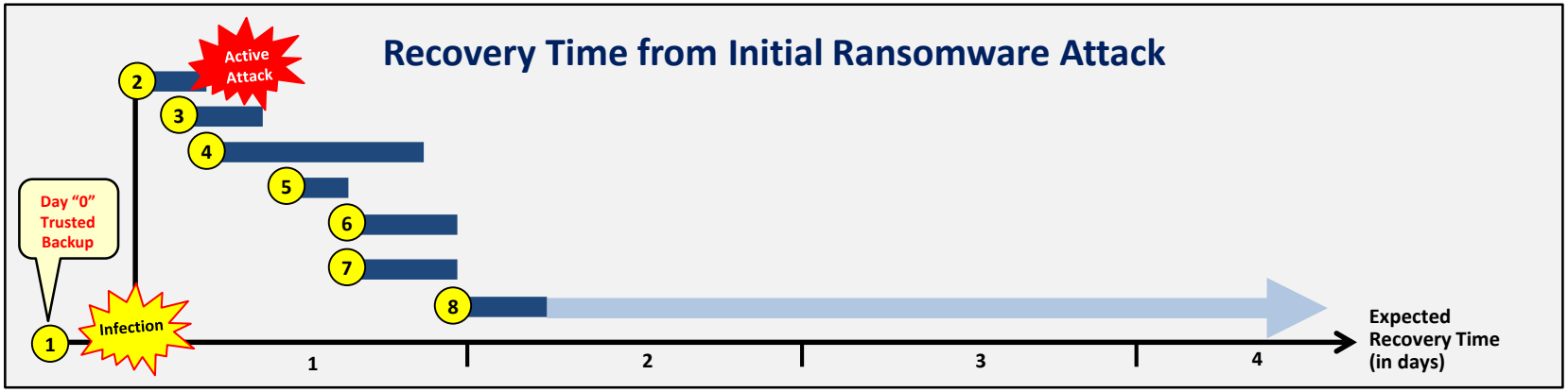


1. IT has established an isolated network using a traditional firewall to resist external intrusion.
2. Ransomware sits in a latent state while expanding the scope of encryption. Data corruption may manifest itself for days, weeks or even months after the initial infection.
3. Assemble CERT Team and manage crisis communications.
4. Engage third-party expertise to assist in damage assessment, containment and recovery.
5. Determine which strain of ransomware has infected information systems.
6. Scan image backups chronologically backward in order to identify a "trusted images".
7. Define tactical response clean, restore or rebuild based on nature/scope of infection.
8. Execute tactical response to clean, restore or rebuild servers and data.

For Illustrative Purposes Only

Cyber DRaaS Response to a Ransomware Attack

Recovery Time Drastically Reduced by Early Detection and Network Segmentation.



1. Establish a zero trust network with visibility into application and user activity on each network segment.
2. Network monitoring identifies intrusion and proactively contains infection in a malware sandbox.
3. Assemble CERT Team and manage crisis communications.
4. Engage third-party expertise to assist in damage assessment, containment and recovery.
5. Determine which strain of ransomware has infected information systems.
6. Scan image backups chronologically backward in order to identify a "trusted images".
7. Define tactical response clean, restore or rebuild based on nature/scope of infection.
8. Execute tactical response to clean, restore or rebuild servers and data.

For Illustrative Purposes Only

Cyber DRaaS Enables Ransomware Recovery

RMI

Cyber DRaaS changes traditional recovery with the following:

- Early detection and behavioral analysis.
- Proactive containment employing malware “sandbox”.
- Dynamic expansion of malware signatures.
- Trusted images that are validated and ready for restore.
- CERT Team trained and response ready.

Your Next Steps

RMI

Key steps in mitigating risk of Ransomware.

- Review current network segmentation architecture.
- Assess your ransomware prevention/recovery strategy.
- Implement a Cyber DRaaS Data solution.
  - IMPORTANT: Change monitoring of “trusted images.”
- Develop an competent CERT organization to drive cyber recovery.
  - Clearly define roles and responsibilities
  - Engage qualified third-parties for specialized expertise.
- Create a post-attack computer emergency recovery plan.

For Further Information

RMI Risk Masters International, LLC

10 Hannah Drive
Dayton, NJ 08810
(732) 261-9555
erbeck@riskmastersintl.com

Eric A. Beck
Principal

RMI Risk Masters International, LLC

234 Engle Street
Tenafly, NJ 07670
(201) 803-1536
acytryn@riskmastersintl.com

Allan Cytryn
Principal

Thank you for your attention.