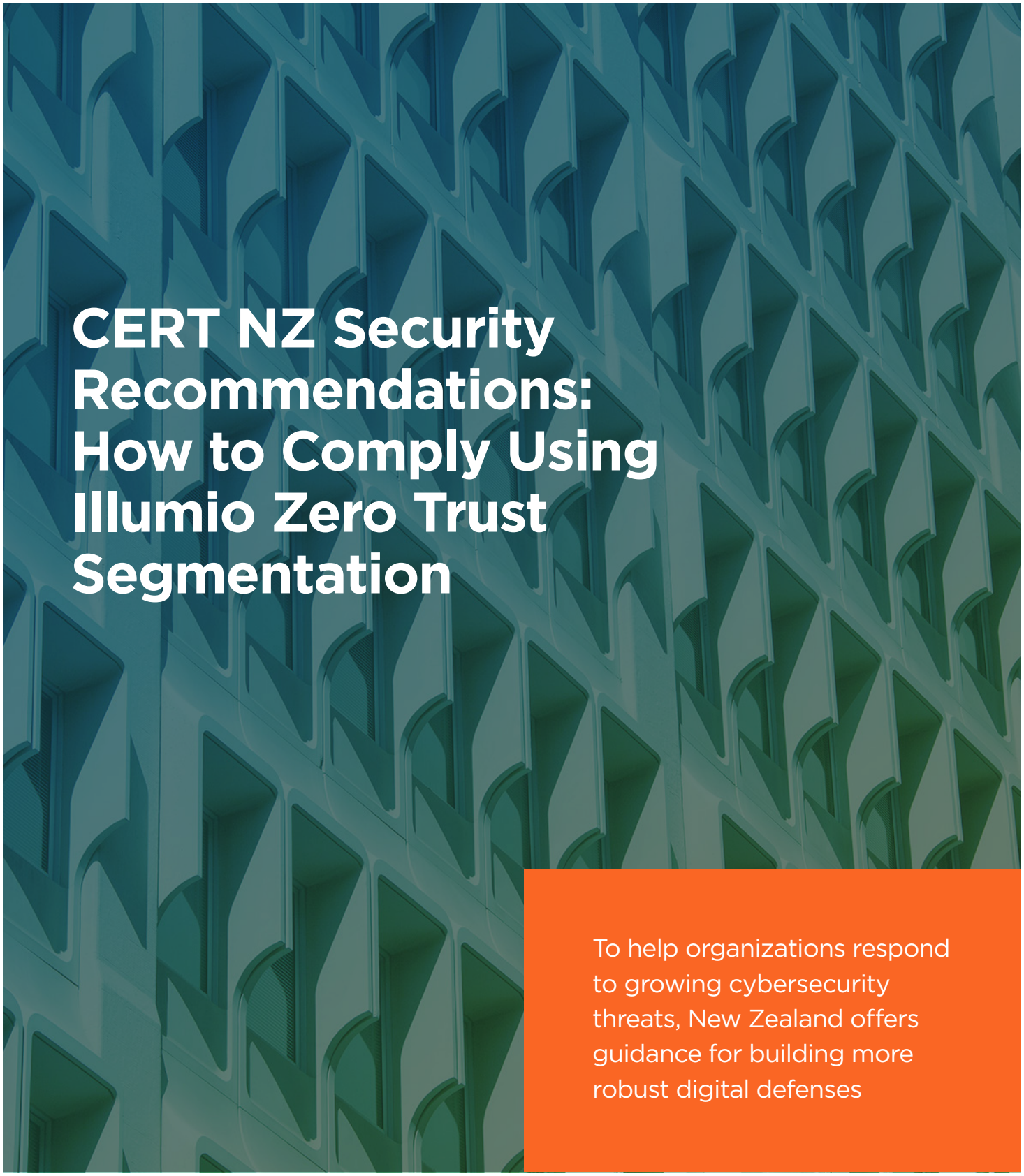
illumio

SOLUTION GUIDE



CERT NZ Security Recommendations: How to Comply Using Illumio Zero Trust Segmentation

To help organizations respond to growing cybersecurity threats, New Zealand offers guidance for building more robust digital defenses

Contents

Illumio Zero Trust Segmentation 03

How Illumio Helps Organizations Comply With CERT NZ Recommendations 04

Complying With CERT NZ Guidelines for Ransomware Mitigation 4
Complying With CERT NZ Guidelines for Hardening RDP 4
Complying With CERT NZ Guidelines for Disabling Unused Services and Protocols 4

Implementing CERT NZ's List of Critical Security Controls 05

Mitigate Software Vulnerabilities Through Patching 5
Capture Evidence for Investigations 5
Maintain and Visualize an Asset Inventory 6
Protect Backup Data and Systems 6
Restrict Application Behavior 6
Enforce the Principle of Least Privilege 7
Implement Network Segmentation and Separation 7
Secure Automated Processes 8

Conclusion 09

Organizations of all kinds face increased threats from ransomware and other types of cyber threats. Breaches today are more catastrophic, resulting in multi-million-dollar ransoms and outages of critical infrastructure. And in most organizations, the attack surface is expanding because of proliferating endpoints, increased use of cloud services, workforces using personal devices in home offices and broader adoption of IoT devices.

CERT NZ, the national Computer Emergency Response Team (CERT) funded by the New Zealand government, is dedicated to helping organizations defend themselves against cyber threats. To support this mission, CERT NZ collects information about cyberattacks, analyzes the threat landscape in New Zealand and offers guidance that it regularly revises to address the latest threats.

Recent recommendations from CERT NZ include:

- Mitigating ransomware
- Hardening the RDP protocol which is used for lateral movement by many ransomware strains
- Shutting down unused services and protocols
- Implementing CERT NZ's annually-updated list of critical security controls which include:
    - Mitigating software vulnerabilities through patching
    - Capturing evidence for investigations
    - Maintaining and visualizing an asset inventory
    - Protecting backup data and systems
    - Restricting application behavior
    - Enforcing the principle of least privilege
    - Implementing network segmentation and separation
    - Securing automated processes

Illumio Zero Trust Segmentation

Illumio can help organizations implement security recommendations from CERT NZ, including recommendations related to network visibility, user privileges and network segmentation for preventing the spread of malware.

Illumio is a Forrester Wave™ Leader in Microsegmentation and Zero Trust eXtended Ecosystem Platforms. Illumio Zero Trust segmentation makes it easy for organizations to define and enforce micro-segmentation policies to reduce the attack surface of IT infrastructures and to block the network paths attackers rely on for breaching networks and spreading ransomware.

Using Illumio, organizations can quickly generate an application dependency map showing all the communications taking place on their network and which communication pathways are required for legitimate business. Then they can use Illumio's Policy Control Engine (PCE) to define high-level segmentation policies, such as limiting access to critical assets only to authorized users. The PCE generates detailed firewall rules enforcing these policies and pushes these rules out to the host-based firewalls built into the systems already deployed.

The result: fast, effective Zero Trust segmentation that blocks all communications that aren't explicitly allowed and the elimination of pathways that ransomware and other attacks rely on.

Here's a detailed look at how Illumio Zero Trust segmentation helps companies implement CERT NZ recommendations.

Breaches today are more catastrophic, resulting in multi-million-dollar ransoms and outages of critical infrastructure.

How Illumio Helps Organizations Comply With CERT NZ Recommendations

Complying With CERT NZ Guidelines for Ransomware Mitigation

CERT NZ advises organizations to seize "opportunities to detect, prevent, and respond to ransomware attacks before…data gets encrypted."

Illumio Zero Trust segmentation helps prevent the spread of ransomware by blocking all unauthorized traffic on a network; only explicitly-trusted traffic is allowed to pass through. Even if ransomware manages to infect a single device, it won't be able to move laterally across the network to other devices, encrypting data as it goes. Instead, Illumio segmentation policies will contain the attack on the initial device, minimizing the effect of the breach.

Illumio raises an alert when it detects software or devices attempting to send or receive unauthorized traffic. Alerts can be fed to an SIEM system for manual mitigation by SOC analysts, or they can be fed to a SOAR platform for an automated response as part of a security playbook. A single command to the lightweight Illumio agent running on the device instantly quarantines the device, containing the threat so it can be remediated by the security team.

Complying With CERT NZ Guidelines for Hardening RDP

Microsoft designed the Remote Desktop Protocol (RDP) to provide users with a way of giving help desk agents access to their devices for troubleshooting. In many organizations, the protocol is enabled on all Windows devices by default. Unfortunately, RDP has become a convenient, unguarded highway attackers can use to rapidly spread malware. Common malware strains such as SamSam use RDP to traverse the network. In fact, so many malware strains use this protocol that some studies rank it as the most popular intrusion vector for attacks.

CERT NZ recommends that organizations harden their RDP configurations to reduce the chance of attackers taking advantage of this protocol. They recommend that RDP servers "only allow access from specific sources." They also recommend that RDP servers enforce multi-factor authentication (MFA), run Network Level Authentication (NLA) to guard against the BlueKeep vulnerability and enforce session timeouts so that authorized sessions don't last indefinitely, giving attackers more time to take advantage of an established, trusted connection.

Illumio application dependency maps and vulnerability maps make it easy for security teams to see where RDP is being used in the organization. Teams can then define policies limiting or forbidding the use of RDP and instantly enforce those policies by pushing them out to host-based firewalls on devices. Illumio can also raise alerts when it detects suspicious RDP traffic appearing on the network.

Complying With CERT NZ Guidelines for Disabling Unused Services and Protocols

According to CERT NZ, "All unnecessary and unused services and ports [should be] disabled." Organizations should have "a complete view of which protocols and services are used in your environment and why they are necessary" and be "aware of changes to the services, ports, and protocols in use."

Illumio provides comprehensive visibility into traffic flows with port, protocol and process information. Also, a summary of how Illumio provides controls for limiting traffic to only approved protocols and raises alerts upon detecting unauthorized traffic.

Using Illumio, security teams can easily identify which devices are supporting services and protocols not needed for authorized operations. Security teams can then shut down those services and protocols and enforce policies forbidding their use.

Implementing CERT NZ's List of Critical Security Controls

Illumio helps organizations comply with the majority of CERT NZ's 2022 list of Security Controls, including critical controls for monitoring traffic, reducing the attack surface, and curtailing lateral movement by attackers.

Illumio helps organizations implement the following security controls.

Mitigate Software Vulnerabilities Through Patching

CERT NZ recommends that organizations patch their software and systems in a timely manner. Attackers regularly take advantage of unpatched vulnerabilities to break into systems. In fact, 60% of data breaches involve a vulnerability that was published but not patched in time.

By establishing a rigorous and timely patching practice, teams can close the door on this type of attack.

CERT NZ notes that "attackers take advantage of the interconnectedness to join multiple vulnerabilities together to get into business systems." They add that organizations should "understand which systems or components are directly or indirectly impacted — including the systems that the vulnerable systems communicate with."

Illumio gives security teams live visibility into all traffic flows, including flows involving vulnerable IT assets. Using this visibility, security teams can prioritize patches based on how exposed various applications and systems are to threats. They can also use segmentation to restrict traffic to and from vulnerable systems in cases where patches cannot be deployed quickly or where patches aren't yet available because the threat is from a recently-discovered Zero Day attack.

60% of data breaches involve a vulnerability that was published but not patched in time.

Capture Evidence for Investigations

CERT NZ recommends that organizations implement centralized logging, including "logging for events that are business critical or involve sensitive data." Security teams need to be vigilant not just about traffic but also unexpected changes to security configurations. "You need to know when there's suspicious traffic on your web application, or when security configurations that rarely change are modified," CERT NZ notes. Security teams will also want to know when protocols are used inappropriately, such as when an employee's device uses the RDP protocol to connect to something other than an authorized RDP server.

Illumio continuously monitors traffic among all devices. If offers Common Criteria-certified logging as well as an auditable events framework. Using context-rich traffic data from Illumio, IT teams can audit systems, conduct threat hunting and forensic investigations, and collect information for automated responses from telemetry about all connections within the environment that they wouldn't have had before.

In addition, Illumio raises early warning alerts for traffic-based indications of compromise, such as traffic flows that violate policies or that attempt to establish inappropriate network connections.

Maintain and Visualize an Asset Inventory

CERT NZ recommends that organizations engage in asset lifecycle management. "Keep your view of your environment accurate and up-to-date," they advise. IT teams should promptly remove decommissioned assets from the environment. If they cannot remove an asset right away, they should restrict its access to reduce the risk of it being compromised. They should also "limit the devices which can connect to and from the [decommissioned] system."

Illumio's application dependency mapping shows all software and devices active in an organization's IT environment, providing a comprehensive view of assets to be managed. IT teams can use Illumio to monitor workloads as assets are added, moved, repurposed, scaled or decommissioned. They can also use Illumio to isolate unsupported assets and to restrict access to legacy systems still running vulnerable software. And Illumio CloudSecure, Illumio's solution for building and orchestrating dynamic cloud workload policies at scale, maintains a live, accurate inventory of all cloud objects in all accounts across an organization's multi-cloud ecosystem. CloudSecure also maintains the context and relationships that cloud-based objects have with one another and with on-premise workloads.

Protect Backup Data and Systems

CERT NZ recommends that organizations implement and test backups. Backups are only useful if they can be trusted; overwriting corrupted data with other corrupted backup data containing malware doesn't serve any purpose at all. Backups "need to be protected from unauthorized access," says CERT NZ. By securing backups, IT organizations can ensure that backup data is ready should damaged or lost data ever need to be restored.

Illumio helps with backup management in three ways:

- It provides visibility into backup infrastructure, just as it provides visibility into the IT environment overall. Security teams can confirm that access to backup systems is restricted only to authorized parties.
- Illumio Zero Trust segmentation protects backups from ransomware and other attacks. Segmentation policies block attackers from reaching backup systems using the ports and protocols commonly used for attacks.
- By reducing the attack surface overall and blocking lateral movement by attackers across the IT environment, Illumio reduces the scope of any backup that needs to be deployed following an attack. Illumio constrains attacks to a single device or, at most, a few devices, reducing the amount of backup data that needs to be retrieved and put to use.

Restrict Application Behavior

CERT NZ recommends that organizations implement application controls, allowing only authorized applications to run. One of the goals of this recommendation is to "prevent malicious software from running." IT organizations should determine which devices are running which applications. They should "determine which devices to cover first. These should be higher risk devices." A device can be riskier if it supports a mission-critical operation or if it's susceptible to vulnerabilities associated with ransomware or other dangerous attacks.

Illumio provides visibility into all applications and devices. It enforces segmentation policies that allow only authorized traffic to flow to and from applications.

Illumio also provides risk-scoring that helps security teams prioritize application patching and provisioning activities. Security teams can use

the Illumio Vulnerability Exposure Score (VES) to understand the relative risk of all applications and devices in their environment. The Illumio VES combines industry-standard vulnerability scoring measurements such as the Common Vulnerability Scoring System (CVSS) with context from an organization's unique environment. The VES helps security professionals prioritize security controls to minimize the impact of vulnerabilities on the attack surface.

Enforce the Principle of Least Privilege

CERT NZ recommends that IT organizations grant users the least amount of access privileges needed for doing their jobs. Enforcing the principle of least privilege prevents users from accidentally misconfiguring applications or devices or exposing mission-critical assets to attack. It also minimizes the damage attackers can do should they succeed in taking over an account.

Attackers will find it difficult to engage in lateral movement across a network if the accounts they take over can connect only to a few applications and resources. IT organizations should "justify any administrative access" they grant to users or processes. To ensure that access privileges are accurately aligned with job functions, the organization should monitor and analyze user activity and application traffic.

Illumio is a leader in Zero Trust solutions for enterprises, providing a scalable, flexible and responsible solution for enforcing access policies that deny access by default and grant only the privileges necessary for work. Illumio makes it easy to enforce least privilege network connections between users and systems as well as between systems and systems.

In addition, Illumio provides live visualizations of access activity across the organization, including access to cloud resources and devices at remote locations. Using this visibility, security teams can tailor access privileges based on user identities, user AD group memberships and job functions, reducing privileges to the least needed for supporting operations.

Illumio is a leader in Zero Trust Segmentation for enterprises, providing a scalable, flexible and responsible solution.

Implement Network Segmentation and Separation

CERT NZ recommends that organizations segment their networks, breaking large networks into smaller network segments separated through access controls and preventing unfettered access among systems and devices. They note that network segmentation "allows your organization to set more granular security controls on the smaller networks that have critical data or systems. Without effective network segmentation, attackers can move around your network and gain access to additional systems. Implementing network controls limits an attacker's access once they enter your network." CERT NZ recommends the use of "host based firewalls" for implementing segmentation, giving every workload its own perimeter and leveraging features that already exist in operating systems rather than adding custom, proprietary applications that require their own maintenance and coordination.

Illumio provides a network segmentation solution that organizations can deploy within days or even hours, providing sweeping protection against lateral movement and other communications that attackers rely on to infiltrate and spread across networks. Illumio does this without requiring the deployment of cumbersome network appliances or forcing network teams to devise labyrinthine firewall rules to segment applications and user traffic across environments. Instead, Illumio makes use of the host-based firewalls already installed on devices — just as CERT NZ recommends.

Illumio also provides a Policy Compute Engine that automatically translates high-level policies, such as limiting the communications allowed for a business-critical web application, into detailed host-

based firewall rules that run on software built into a device's operating system. Rules can be tailored to account for different user roles, applications, environments (e.g., test vs. production), and locations (e.g., headquarters vs. a satellite office).

Secure Automated Processes

CERT NZ recommends that organizations set secure defaults for macros, since attackers often take advantage of macros like Office 365 macros to execute malicious code. That's excellent advice, but the principle can be applied more broadly: secure all automated processes, especially those involved in critical operations such as ecommerce, finance, manufacturing and CI/CD pipelines. By breaking into automated processes, attackers can slip past many security watchpoints and gain access to critical assets. And by breaking into CI/CD pipelines and code repositories, they can embed malware that ends up running as trusted software in production environments. A single breach can become a thousand breaches when compromised software is deployed in production.

Illumio helps secure automated processes in several ways:

- Illumio's Zero Trust segmentation curtails attackers' movements on a network, making it far less likely they they'll be able to reach any valuable IT assets in the first place.
- Illumio's traffic monitoring reveals suspicious traffic that might be an indication of compromise (IoC). By flagging traffic that violates Zero Trust policies, Illumio gives SOC analysts an opportunity to stop an attack before it spreads.
- By embedding an Illumio Virtual Enforcement Node (VEN) in software builds, DevSecOps teams can ensure that code, once deployed in any environment, enforces Zero Trust segmentation policies to guard against attacks. Even if a component (such as a Log4j component) does turn out to be vulnerable to compromise, Illumio's built-in segmentation controls can prevent the application from communicating in dangerous ways.

Conclusion

Cyber threats will continue to increase against organizations, taking advantage of their expanded attack surfaces and unaddressed vulnerabilities. CERT NZ's recommendations provide up-to-date guidance for defending against these attacks and minimizing their impact when they occur.

Illumio offers comprehensive visibility into traffic flows, including protocol and port usage, and makes it easy to define and enforce precise Zero Trust segmentation policies. As a result, Illumio provides essential security controls for complying with CERT NZ recommendations and defending distributed IT infrastructures against ransomware and other dangerous cyber threats.

Want to learn more about how Illumio can help your organization build its cyber resilience and respond to new cybersecurity mandates?

Visit www.illumio.com to learn more or email us at contact us_APAC@illumio.com to speak with our security experts.

About Illumio

Illumio, the pioneer and market leader of Zero Trust Segmentation, prevents breaches from becoming cyber disasters. Illumio protects critical applications and valuable digital assets with proven segmentation technology purpose-built for the Zero Trust security model. Illumio ransomware mitigation and segmentation solutions help you see risks, isolate attacks and secure data across cloud-native apps, hybrid and multi-clouds, data centers, and endpoints, enabling the world's leading organizations to strengthen their cyber resilience and reduce risk.