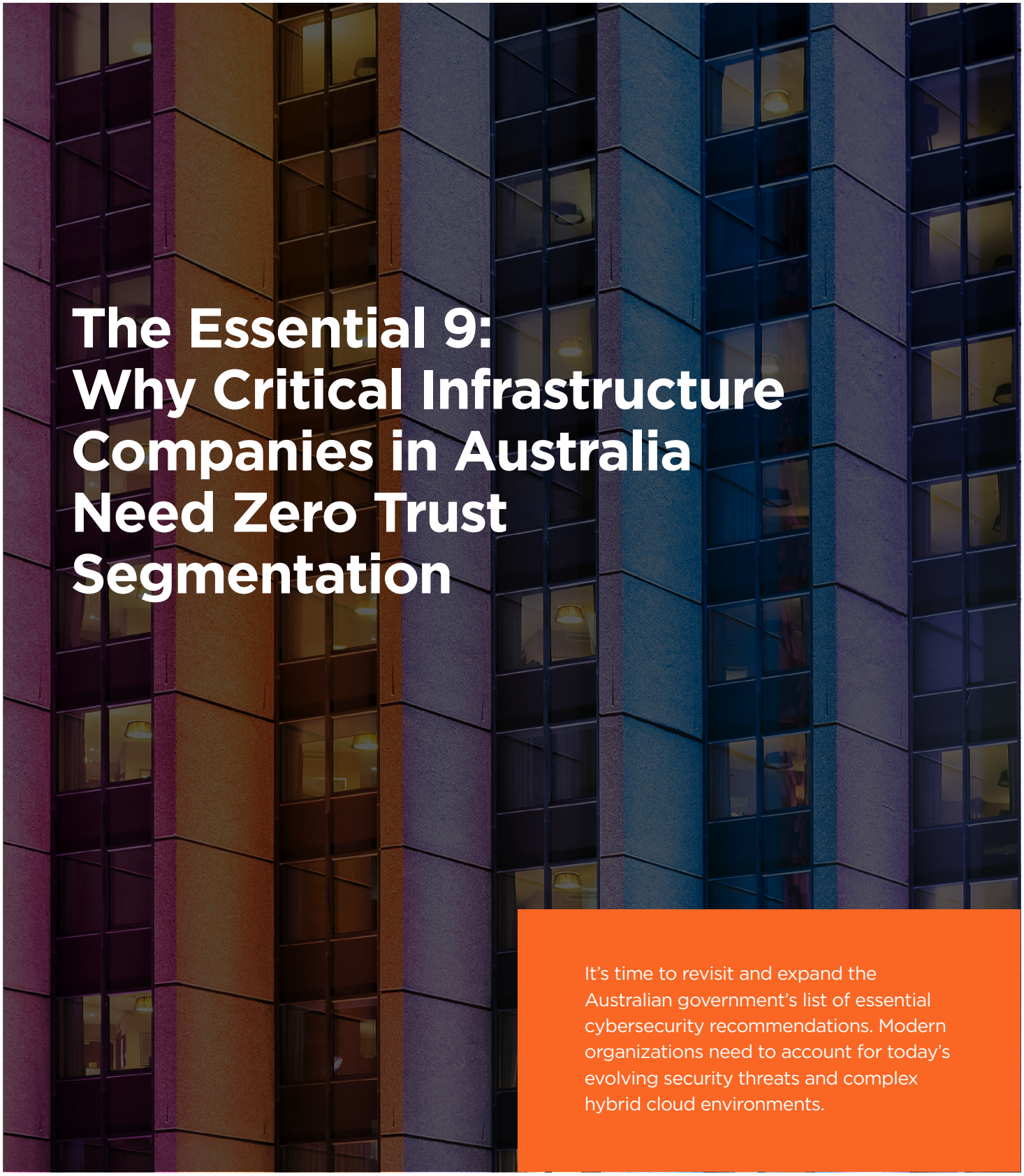
illumio

STRATEGY GUIDE



The Essential 9: Why Critical Infrastructure Companies in Australia Need Zero Trust Segmentation

It's time to revisit and expand the Australian government's list of essential cybersecurity recommendations. Modern organizations need to account for today's evolving security threats and complex hybrid cloud environments.

Contents

Expanding Security Recommendations to Address Today's Cybersecurity Threats

Over the past decade, the Australian government has issued many cybersecurity recommendations to help companies better defend against increasingly virulent cyber threats.[1] Central to those recommendations are the Essential 8 guidelines issued in 2017 and updated periodically since.[2] These eight recommendations, which evolved from the widely touted "Top 4 Controls" of the Australian Signals Directorate, are intended to provide an essential but manageable list of security practices for protecting "Microsoft Windows-based Internet-connected networks."

But today's IT infrastructures are more varied and complex than the Windows-based networks of the past. Today's security practices need to account for Linux servers, cloud services, mobile devices, work-from-anywhere practices, IoT devices, operational technology (OT) devices and more. At the same time, cybercriminals and nation-states are continuing to evolve their tactics. Their methods, especially ransomware attacks, are becoming more costly and damaging.

To address these evolving challenges, we at Illumio believe it's time to revisit and expand the Australian government's list of essential cybersecurity recommendations. Specifically, we think there is a case for Zero Trust Segmentation to be included among the Australian government's list of essential security practices.

Zero Trust Segmentation is an access control model that gives attackers little or no ability to traverse a network, even if they compromise an endpoint like a laptop or server. By enforcing strict networking controls and blocking unauthorized traffic, Zero Trust Segmentation leaves attackers nowhere to go. They can't spread malware or hunt for data to steal.

There are signs that the Australian government agrees with our viewpoint on the importance of Zero Trust Segmentation. In February 2022, a security alert jointly issued by the Australian government, U.K. government and U.S. Cybersecurity and Infrastructure Security Agency (CISA) featured network segmentation prominently among its list of recommendations.[3]

Even if Zero Trust Segmentation isn't officially added to the Australian government's list of essential strategies anytime soon, there are good reasons for critical infrastructure organizations in Australia to treat it as though it has been. However, the advisory stops short of saying Zero Trust Segmentation. As a result, many organizations will continue to wrestle with old approaches to segmentation or do nothing as they don't believe it's practical.

To understand the importance of Zero Trust Segmentation, let's review the security landscape for critical infrastructure organizations today, and the recommendations the Australian government has issued so far in response. Then, let's examine how Zero Trust Segmentation complements Australia's regulations and recommendations by providing a critical missing piece in any organization's defense against ransomware and other forms of attack.

Zero Trust Segmentation is an access control model that gives attackers little or no ability to traverse a network, even if they compromise an endpoint like a laptop or server.

The Threat Landscape for Critical Infrastructure Organizations in Australia

Cyber threats, including ransomware attacks, are increasing in Australia as they are in much of the world. Over 2020 and 2021, reports of cybercrime in Australia rose 13%.[4] Self-reported losses from cybercrime exceeded $33 billion Australian dollars.

About 25% of attacks were against critical infrastructure, which the Australian government defines as critical assets in areas of banking, broadcasting, domain name systems, electricity, financial market infrastructure, food and grocery, freight and freight services, gas, insurance, liquid fuel and superannuation.[5] Cybercrime on critical infrastructure included an attack against a Victoria public health facility that resulted in a ransom payment of over $11 million in bitcoin and an attack against JBS Meat Packing that affected the company's plants in both the U.S. and Australia.[6]

While in other countries attackers are shifting from "big game" targets to small and mid-sized businesses, they are attacking Australian organizations of all sizes, according to the recent security alert jointly issued in February 2022 by Australia, the U.S. and the U.K.[7]

The alert notes that ransomware attacks are increasing in frequency. They're also broadening their targets to include cloud services and MSA organizations, giving attackers new vectors for reaching multiple organizations at once. Critical infrastructure companies face threats from all parts of their networks. How can new security regulations, security tools and best practices help?

> Nearly 25% of cyberattacks in Australia were against critical infrastructure.

Australian Cybersecurity Regulations and Recommendations

In response to cyberattacks such as ransomware, intrusions from foreign intelligence services, business email compromise (BEC) campaigns, damage from malicious insiders and other threats, the Australian Cyber Security Centre (ACSC) issued a document called *Strategies to Mitigate Cyber Security Incidents*.[8] This document, first issued in 2010 and updated as recently as 2017, lists many security best practices, eight of which it identifies as essential:

- Application control that prevents the execution of unapproved applications and installers
- Patching applications to fix known vulnerabilities
- Configuring Microsoft Office macro settings to prevent automatic execution of malicious scripts
- Hardening user applications such as web browsers so they don't run dangerous plug-ins
- Restricting administrative privileges
- Patching operating systems
- Requiring multi-factor authentication
- Regular backups of data and configuration settings

These are all common-sense recommendations. But they're far from easy to implement.

It's worth noting that the ACSC document does list network segmentation as an excellent strategy. Why is network segmentation rated only "excellent" instead of "essential?" One reason could be that the strategy document estimated that implementing network segmentation would be highly difficult.

A decade ago, when many network segmentation products attempted to implement segmentation using network gear rather than host-based firewalls, it was indeed costly and complex. And the results lacked scalability or flexibility. Those old products could segment a few hundred or thousand endpoints, not the hundreds of thousands that can be segmented today using the right technology.

The objections to network segmentation from 2017 and earlier are no longer valid, and the success that attackers have achieved on networks lacking network segmentation speaks for itself.

> "Network segmentation can help prevent the spread of ransomware by controlling traffic flows between — and access to — various subnetworks and by restricting adversary lateral movement."
>
> **A U.S., U.K. and Australian security alert**

In any case, even in 2012, the ACSC did think that network segmentation merited its own list of recommendations. It issued a strategy document called *Implementing Network Segmentation and Segregation*, noting that these strategies were "highly effective" at limiting the impact of an intrusion.[9]

Fast forward to now. Ransomware attacks against critical infrastructure organizations are on the rise. Attackers have managed to paralyze a critical gas pipeline in the U.S. and meat packing operations in the U.S. and Australia. The commonplace defenses aren't working.

Consequently, in February 2022, Australia, the U.S. and the U.K. issued Alert (AA22-040A) warning of "an increase in sophisticated, high-impact ransomware incidents against critical infrastructure organizations globally."[10] The alert includes recommendations for improving cybersecurity, beginning with network segmentation. The alert notes:

> "Network segmentation can help prevent the spread of ransomware by controlling traffic flows between — and access to — various subnetworks and by restricting adversary lateral movement. Organizations with an international footprint should be aware that connectivity between their overseas arms can expand their threat surface; these organizations should implement network segmentation between international divisions where appropriate. For example, the ACSC has observed ransomware and data theft incidents in which Australian divisions of multinational companies were impacted by ransomware incidents affecting assets maintained and hosted by offshore divisions (outside their control)."

Attackers can't paralyze critical infrastructure without spreading across a network first. Network segmentation prevents that spread from taking place. That's why Australia, the U.S. and the U.K. began their recommendations for cyber defense with network segmentation.

What do CISOs and IT teams need to know about network segmentation before they implement it? And of the various ways of implementing network segmentation, which way is best suited for today's highly distributed, technologically heterogeneous IT infrastructures?

Attackers can't paralyze critical infrastructure without spreading across a network first. Segmentation prevents that from taking place.

Network Segmentation: A Closer Look

Network segmentation defined

Network segmentation is the practice of blocking off systems from other systems on the network using access controls enforced by the systems themselves or by other IT devices under the control of the security team. The goal of network segmentation is to prevent lateral movement; that is, to prevent attackers who gain access to one system from moving freely to other systems as part of their attack.

Network segmentation isolates systems. An attacker might gain access to a single endpoint — a laptop that they infect with ransomware, for example — but they won't be able to move laterally across the network to other systems and spread malware. This is because network segmentation controls will block them, preventing access to specific network ports, IP addresses and protocols.

For example, many types of ransomware rely on remote desktop protocol (RDP), originally designed to provide help desk agents with remote access to a system for troubleshooting. By blocking this protocol by default, network segmentation can prevent many types of ransomware from spreading. Even if attackers manage to infect a single endpoint such as a laptop, they'll find themselves trapped there, as though they had broken into a building but found themselves locked in the room they broke into.

Network-based segmentation vs. host-based segmentation

There are various ways of implementing network segmentation. Some companies try configuring their network switches and routers and perimeter firewalls to implement network segmentation controls.

Implementing segmentation with network gear typically leads to two problems. First, it's very difficult to translate high-level policies into detailed networking rules on switches, routers and firewalls. For example, it's nearly impossible to create a practical networking rule based on a high-level policy that a web application should have network access only to the services it needs to perform its intended functions. Inevitably, rules programmed into network gear end up being too strict or too lax. As a result, either application functionality or security resilience suffers.

The second problem is a lack of precision. With thousands or tens of thousands of endpoints on a network, it's difficult to enforce endpoint-specific controls from network gear and perimeter firewalls.

A better solution is to implement network segmentation on individual endpoints themselves. This approach takes advantage of the host-based firewalls built into endpoints such as laptops and servers.

Taking a host-based approach offers these advantages:

- **Direct, simplified control**
  It's easier to enforce security rules for hybrid cloud and client endpoints like laptops on endpoints themselves rather than on network devices like routers and firewalls or through necessarily limited native-cloud controls. Network firewall rules are overly complex as it is, making it difficult to implement access controls that, for instance, differentiate a manager from a subordinate in a particular department.
- **Network segmentation that works everywhere**
  Enforcing segmentation rules on endpoints themselves is much more practical now that so many employee endpoints are used in remote locations like home offices. If an employee isn't on an internal network, internal network devices can't enforce segmentation rules. Host-based segmentation enforces segmentation policies wherever an endpoint happens to be.
- **Pinpoint accuracy for rapidly isolating threats**
  Security teams can use an endpoint's host-based firewall to isolate the endpoint if they suspect it has been compromised. Because the firewall is on the endpoint itself, it isolates only the affected network, not the whole LAN or VLAN to which the endpoint is connected. Security teams don't have to risk misconfiguring firewalls as they rush to isolate an endpoint or, once an incident is resolved, to restore its connectivity.

If an employee isn't on an internal network, internal network devices can't enforce segmentation rules. Host-based segmentation enforces segmentation policies wherever an endpoint happens to be.

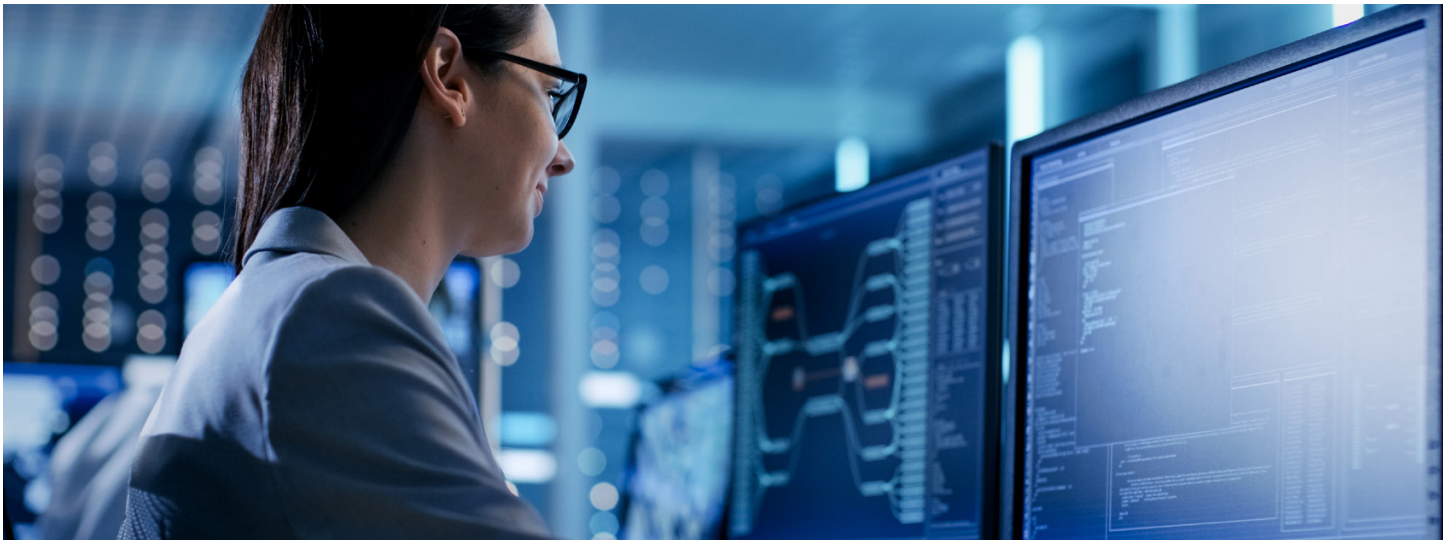
Illumio for Zero Trust Segmentation

Without requiring new appliances or performance-slowing software, Illumio helps organizations implement the network segmentation practices recommended by the ACSC. Specifically, Illumio helps organizations:

- **Segment each host**
  The ACSC's guidelines call for segmenting each host and network at the lowest possible level. Illumio uses host-based firewalls to enforce network segmentation at the lowest level without modifying operating systems.
- **Apply the principles of least privilege**
  Endorsing Zero Trust Segmentation, the guidelines direct organizations to allow hosts, services and networks to communicate only with other hosts, services and networks if absolutely necessary. Illumio's Zero Trust solution does exactly this.
- **Segmenting hosts and networks based on business sensitivity**
  Illumio makes it easy to isolate critical hosts and networks without requiring complicated programming of firewall rules. IT teams can define network policies based on business requirements. Illumio translates those policies into segmentation rules.
- **Identify, authenticate and authorize all access**
  Illumio's application dependency map shows all communications between systems, so administrators can detect unauthorized access, adjust access rules accordingly, and further protect systems through segmentation.
- **Require explicit approval for network access**
  The guidelines call for implementing a list of approved, rather than unapproved, traffic. Illumio makes it easy to rapidly implement Zero Trust Segmentation that automatically blocks all traffic not explicitly allowed — the basis for any Zero Trust strategy.

To deliver this protection, Illumio translates high-level data security and privacy policies into host-based firewall rules that can be enforced by every system in the organization, whether on-premises, in the cloud or at the network edge.

> Illumio makes it easy to rapidly implement Zero Trust Segmentation that automatically blocks all traffic not explicitly allowed.



Conclusion

Cyberattacks have been remarkably successful lately. Attackers have shut down critical infrastructure. They've reaped tens of millions of dollars from ransomware attacks. And they've turned extortion into such a predictable business model that many ransomware gangs now operate customer service centers for quickly negotiating settlements and processing ransomware payments.

Critical infrastructure organizations need to respond. That response needs to include the hardening of IT infrastructures, applying every practical strategy to prevent attackers from breaching a network and limiting their movement if an isolated breach occurs.

Because Zero Trust Segmentation prevents attackers from moving across any network — local or remote — it deserves to be on any list of essential cybersecurity strategies.

Facing growing threats from cybercriminals, nation-states and malicious insiders, Australian critical infrastructure organizations would do well to take a cue from the Australian government's recent alert and treat network segmentation as an essential strategy — a necessary addition to the list we should now think of as the Essential 9.

Zero Trust Segmentation needs to be on any list of essential cybersecurity strategies.

Stopping Cyber Disasters — That's What We Do

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

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

illumio

Endnotes

[1] *Strategies to Mitigate Cyber Security Incidents*, Australian Cyber Security Centre, https://www.cyber.gov.au/acsc/view-all-content/strategies-to-mitigate-cyber-security-incidents (Last updated: February 2017)

[2] *Essential Eight Maturity Model*, Australian Cyber Security Centre, https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-maturity-model (Last updated: October 2021)

[3] *Alert (AA22-040A): 2021 Trends Show Increased Globalized Threat of Ransomware*, Cybersecurity & Infrastructure Security Agency, February 10, 2022, https://www.cisa.gov/uscert/ncas/alerts/aa22-040a

[4] *Australia joins US and UK to warn of 2021 Ransomware trends*, Australian Cyber Security Centre, February 10, 2022, https://www.cyber.gov.au/acsc/view-all-content/news/australia-joins-us-and-uk-warn-2021-ransomware-trends

[5] *Engagement on critical infrastructure reforms*, Australian Government, Department of Home Affairs, https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/protecting-our-critical-infrastructure-reforms-engagement (Last updated: 8 April 2022)

[6] *"Significant threat": Cyber attacks increasingly targeting Australia's critical infrastructure*, The Guardian, Daniel Hurst, September 13, 2021, https://www.theguardian.com/technology/2021/sep/15/significant-threat-cyber-attacks-increasingly-targeting-australias-critical-infrastructure

[7] *Alert (AA22-040A): 2021 Trends Show Increased Globalized Threat of Ransomware*, Cybersecurity & Infrastructure Security Agency, February 10, 2022, https://www.cisa.gov/uscert/ncas/alerts/aa22-040a

[8] *Strategies to Mitigate Cyber Security Incidents*, Australian Cyber Security Centre, https://www.cyber.gov.au/acsc/view-all-content/strategies-to-mitigate-cyber-security-incidents (Last updated: February 2017)

[9] *Implementing Network Segmentation and Segregation*, Australian Cyber Security Centre, https://www.cyber.gov.au/acsc/view-all-content/publications/implementing-network-segmentation-and-segregation (Last updated: October 2021)

[10] *Alert (AA22-040A): 2021 Trends Show Increased Globalized Threat of Ransomware*, Cybersecurity & Infrastructure Security Agency, February 10, 2022, https://www.cisa.gov/uscert/ncas/alerts/aa22-040a

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 see risk, 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 resiliency and reduce risk.