Building the Foundation of Security and Resilience for Your Critical Business Assets

A unified security and observability platform that enables rapid detection, investigation, response, and reporting, at scale.

splunk>

Introduction

With the increasing frequency and sophistication of cyber attacks, Australia's critical infrastructure is constantly at risk.

In 2021-22, the Australian Cyber Security Centre (ACSC) received over 76,000 cybercrime reports, equating to one report every 7 minutes — with around a quarter of attacks focused primarily on Australia's critical infrastructure and essential services.[1]

Critical infrastructure covers physical facilities, supply chains, information technologies and communication networks that if damaged or made operationally unavailable, can severely impact Australia's national security as well as the country's social and economic wellbeing.

New Critical Infrastructure reforms

To protect organisations, businesses and infrastructure, the Security of Critical Infrastructure Act (2018) has been strengthened by two legislative amendments, making it crucial that companies remain compliant. The new compliance requirements includes:

1. **A Positive Security Obligation** for reporting of critical assets and cyber incidents plus the development of a risk management program.
2. **Government Assistance Measures** for information gathering, action directions, and intervention powers.
3. **Enhanced Cyber Security Obligations** for 'Systems of National Significance'.

The reach of the Act has also been **expanded to cover 11 sectors**:

- Communications
- Data storage or processing
- Defence
- Energy
- Financial services
- Food
- Healthcare,
- Higher Education
- Space Technology
- Transport
- Water

[1] Australian Cyber Security Centre, ACSC Annual Cyber Threat Report, July 2021 to June 2022,

Key challenges to meeting the new compliance requirements

The new security reforms aim to help build a more secure and resilient infrastructure that promotes productivity and drives sustained economic growth. To avoid penalties for non-compliance, businesses need to meet timelines in developing their mitigation or risk management programs. However, there are a number of key challenges that make it difficult for organisations to comply:

- Enterprises and other large organisations can have **complex, siloed and deeply layered operations** that can impede communications and slow down decision making.
- The **lack of complete visibility across network, systems and assets** can make reporting and compliance a considerable and challenging task for many organisations.
- **No real-time data and actionable insights** can impact the speed in detecting, responding, and recovering from incidents like breaches or outages.
- Most organisations still have **legacy systems that are disjointed, inflexible and unable to scale** to meet new and changing requirements.
- **Resourcing constraints** make it difficult to find the right digital talent to effectively and intelligently manage current and ongoing workloads.
- Companies have to deal with the **additional costs to comply** with the new requirements - costs that they cannot pass on to customers.

What your organisation needs to stay secure, reliable and compliant

To achieve total compliance and maintain the security and reliability of critical assets, your business needs to not only modernise operations for improved efficiency but also gain complete visibility across systems for rapid response and reporting on incidents, at any scale.

Your organisation needs to:

Gain complete, comprehensive visibility across all critical assets and infrastructure

A complete end-to-end view of all your data across cloud, on-prem, the business edge, and Operational Technology (OT) assets, enables you to anticipate, address and resolve any issues as they arise. This also allows you to better understand how the different assets interact with each other, and act decisively to improve efficiency and productivity.

Detect, investigate and respond to incidents with real-time data

Access to real-time data and analytics helps enhance your ability to detect, investigate and respond to any security incident, at any scale. You are able to quickly identify and neutralise threats before they become significant business risks.

Consolidate data and centralise systems control

To maintain a secure and resilient infrastructure, it is important to eliminate data silos and centralise the control of systems and operations. This not only helps simplify the management of critical assets, but also allows easy access to valuable data insights, facilitates quick coordination of security investigation/response, and boosts productivity across teams and user groups.

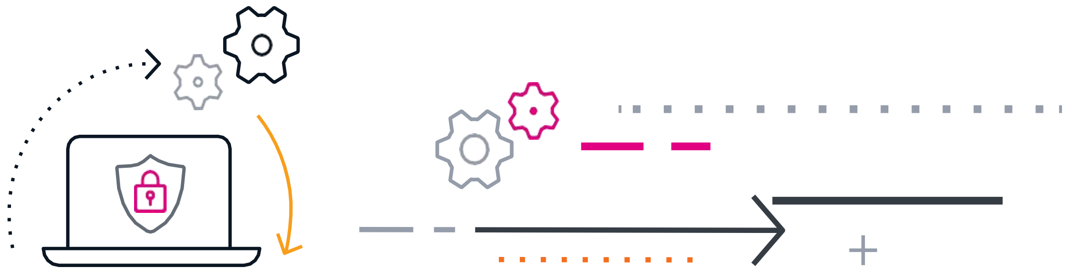
Simplify compliance and streamline reporting

Complying to the new Security of Critical Infrastructure Act requirements can be a huge and complicated task — resulting in increased operational costs, additional manpower, and even higher chances of errors in analysis and reporting. It helps to implement modern systems that can automate tasks, operationalise compliance, and simplify the audit and reporting process.

Helping you build the foundation of security and resilience for your critical business assets

Splunk's Unified Security and Observability Platform helps your organisation gain complete visibility of critical business assets, and enables rapid detection, investigation, response, and reporting, at scale. SecOps, ITOps and DevOps teams are able to work more closely together to ensure your mission-critical infrastructure stays secure, reliable and compliant.

- **End-to-end visibility across critical systems & assets:** We deliver full-stack visibility and advanced analytics to prevent issues before they impact performance — eliminating data silos to develop a more cohesive, connected and secure organisation.
- **Enhanced security to protect critical infrastructure:** Modernise your security operations and protect the business with data, analytics, automation and end-to-end integrations. We help you implement a data-driven approach to detecting, investigating and responding to threats.
- **Real-time insights to streamline compliance and reporting:** Our single, trusted platform enables you to automatically collect and process data from diverse sources, then access real-time insights to help operationalise compliance and reporting.
- **Unified security and full-stack observability platform:** Our extensible data platform with limitless applications, Machine Learning tools and customisable solutions empowers your organisation to be more secure, everywhere you operate. It allows your teams to access and search data from any source and across any device.



We’re a recognized industry leader with a world-class partner ecosystem

Splunk is a recognised leader trusted by some of the world’s biggest brands. We bring unique capabilities and unmatched breadth and depth of experience to enable true end-to-end visibility. We’re ideally placed to support your business across any industry.

Trusted by the world’s leading brands

Our depth of experience in keeping mission-critical systems secure and reliable has been gained over 20 years and is unmatched. We’ve been named by Gartner for nine consecutive years as a leader for Security Information and Event Management (SIEM).

Uniquely able to deliver a true central platform with capability across IT and OT

We empower teams like no other and help unlock the value of data while making security and compliance simpler through a single platform. Our marketplace, Splunkbase integrates with other vendor tools seamlessly and comes with over 2,400 pre-built apps.

End-to-end data visibility to ensure complete security, compliance and resilience

We give you full visibility of critical assets and unify SecOps and ITOps teams to ensure faster, more precise responses. We offer the only full-stack, analytics-powered solution able to solve problems in just seconds.

Providing world-class ecosystem to guide you through your journey

Our unique partner ecosystem brings extended expertise from large scale migrations and managing expanding environments, to scaling technologies to meet user needs. We also have a community with 13,000+ active members available to field questions, share ideas and solve problems.

“Splunk enables us to leverage a single source of truth to turn data into better, faster security decisions.”
- Md Harmizam Md Aris, Manager, IT Operations of Sapura Energy Berhad

“Splunk lets us oversee everything at one stroke and keep the company safe from any attack, wherever we’re working and under any circumstances.”
- Jonathan Pineda, Vice President, Chief Information Security Officer and Data Protection Officer, GSIS

We have completed the **Australian Information Security Registered Assessors Program (IRAP) assessment at Protected Level**. Australian government agencies can leverage the assurance of the ‘protected’ status we hold.

Our security and observability benchmarks:

- 80% reduction in alert volume
- 30 secs to complete processes that once took 30 minutes
- 2x improvement in alert fidelity
- 26% reduction in average time per incident, saving 140 hours/month.
- 30% reduction in load time.
- <2 minutes mean time
- to acknowledge.

Your partner for critical infrastructure security and resilience

Trusted by the world's leading organisations, Splunk delivers end-to-end visibility and real-time data insights to ensure your critical business assets remain secure, compliant and reliable. All in a single, unified platform.

Take the Splunk Readiness Assessment:

Our security experts will run a **1-hour workshop** with you and your team to assess your organisation's readiness to the new Security of Critical Infrastructure (SOCI) requirements.

The workshop will include a gap analysis focused on: visibility, detection, response, and reporting capabilities.

Contact us to learn more or to request the Splunk Readiness Assessment.

splunk>