CYBER SECURITY
BY KORDIA

NZ'S MOST COMPREHENSIVE SECURITY SUITE

ADVISE | PROTECT | INSIGHT & RESPONSE

kordia®

CYBER SECURITY BY KORDIA

⊗ ADVISE | 🔒 PROTECT | ⚠ INSIGHT & RESPONSE

In an increasingly complex online business world that's fraught with security risks, how do you know who you can rely on to keep your business secure?

At Kordia our mission is to build connections you can trust; that make our digital world more secure, reliable and resilient. Put simply, security is part of our DNA.

Cyber-Security by Kordia combines the best people, products, services and solutions in the market to provide scaleable security solutions that enable businesses to do what they do best, without having to worry about security breaches.

WHY KORDIA?

For many organisations, outsourcing network security services appears to be a logical choice. You avoid hardware, licensing, and maintenance costs, let alone the cost and headache of trying to attract and retain specialist security staff. You also benefit from around-the-clock security monitoring and management from dedicated security experts, meaning you can free up your in-house IT staff to pursue activities core to your business objectives. Yet many business decision makers dismiss the managed security service option, fearing a loss of control and visibility over their network.

Cyber-Security by Kordia makes this decision easy, with all of the upside and none of the down. Kordia has a number of security options to suit customers of all sizes that want to outsource all, or some of their security requirements. In fact, we have New Zealand's most comprehensive cyber-security suite, so with Kordia, you know you are in good hands.

Kordia has combined industry leading security product solutions — including award-winning shielding service, RedShield, and leading independent information security consultancy, Aura Information Security — to provide a managed cyber-security portfolio specifically designed to meet the needs of New Zealand businesses.

Kordia is able to secure an enterprise's infrastructure — from desktops and web-facing assets, through the provision of perimeter security with next generation managed Firewalls, Web Application Firewalls, Content Filtering, Intrusion Prevention Services and AntiVirus scanning. And, as these are cloud-based and backed up from leading global security vendors, you can be assured they are kept up-to-date with the latest security patches and signatures.

In addition, Kordia provides and monitors security alerts, with incident handling and event analysis and incident response specifically tailored to meet the needs of enterprises wanting to manage and mitigate cyber-security risks.

Kordia has New Zealand's most comprehensive range of cyber security solutions. To help businesses understand which product or solution is best suited to their current needs, we have defined three pillars that describe the cyber-security life-cycle: **Advise**, **Protect**, and **Insight & Response**. These are underpinned by our managed security services and support functions.

INSIGHT & RESPONSE

Full visibility of your infrastructure with security alerts and response to critical threats.

ADVISE

Independent security consultancy and training to help ensure your business is secure.

PROTECT

A range of security products and services to protect your network from external threats.

1.0 ADVISE

You're about to invest time and money in making your business operations more secure. But how do you know where to focus your efforts; and how will you know if you have been successful? In addition, even with the best security products in place, the absence of an effective cyber-security policy or lack of staff training may mean that sensitive information can still be lost due to deceptive criminal behaviour or employee error. That's why you need to engage a specialist information security consultancy.
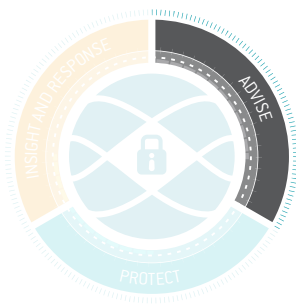
Aura Information Security Specialists

Aura Information Security is a team of highly-skilled and renowned security professionals spanning Australia and New Zealand. Aura consultants thrive on building rapport and becoming trusted advisors to our clients by maintaining impartiality and offering sound, independent security advice. Aura is a wholly owned subsidiary of Kordia.

Make Better Security Decisions

In an interconnected world, businesses rely heavily on data. Protecting this data from cyber-attacks and breaches is vital. We help you fight back and secure your future with the knowledge and support to make better security decisions.

Managed Security

Cyber-threats aren't stagnant; they're continuously evolving. Your business needs to adapt to mitigate the risk. Don't let a lack of staff or expertise hold your security efforts back. Leveraging our experts ensures the safety of your information and systems.

Design & Test

The only way to know if you're secure against an attack is to test your defences. We've got the specialist skills to identify issues and help you design a secure solution, to make sure you avoid a catastrophic breach.

Post-Attack Rapid Response

In the event of a cyber-attack, how can you get back up and running as quickly as possible? We can provide the rapid support you need and also help prevent future breaches by managing your risk and putting the right policies and governance in place.

Education and Training

The threats are real. We can open your organisation's eyes to the risks and why your staff should care. We show you why information security matters and how you can protect yourself and your business with effective security policies. We offer a range of training options to suit your needs; from general staff, to your software developers to company management and the board. Good security starts with employee awareness.

SOME OF THE TRAINING OPTIONS OFFERED INCLUDE:

Security Awareness - Learn how to protect yourself, your business and employees from today's threats.

Governance & Risk - Learn the fundamentals of information security governance, risk and compliance.

Secure Web Development - Learn how to design and build secure applications to OWASP standards.

Security Awareness - Learn how to protect yourself, your business and employees from today's threats using online self-paced training modules.

ISACA - ISACA certification is locally and global recognised by security and IT professionals. Aura is a certified trainer.

Good Security is a Process

Although Aura provides independent security advice, the benefit of dealing with Kordia for all your cyber-security needs is that we keep a watchful eye on your business — this means any gaps uncovered by our consultants can be fed into the products and services provided to you by Kordia to further improve your security defences.

CYBER SECURITY BY KORDIA
2.0 PROTECT
___

Imagine someone has gained access to your computer systems and refuses to give you access until you pay a ransom; or even worse someone has access to your systems and you don't even know about it. If your own commercial information, as well as that of your customers is compromised, it's a ticking time-bomb – one that could be catastrophic for your business.
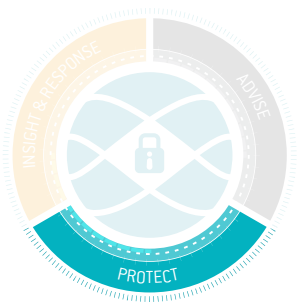
CYBER SECURITY BY KORDIA ENABLES YOU TO:
Protect your **Network** With SecureWan & Managed Firewall
Protect your **Applications** With RedShield Web-Shielding
Protect your **Data** With SecureVault Backup & Restore

SecureWan

As New Zealand's largest Telco solely focused on business customers, our approach is simple. We offer secure, simple and scalable network infrastructure, coupled with good old-fashioned one-on-one customer service. Kordia SecureWan makes it easy to add services and applications without complex network upgrades or design changes. As applications are running across a single network it is much easier to obtain network security, efficiency and diversity.

We understand that our customers' network and security needs are different; we also believe that security shouldn't be an afterthought — it should be baked in. For this reason SecureWan not only keeps business critical operations running smoothly from a connectivity point of view, each standard connection also comes with an on-site stateful Firewall. Our on-site equipment is locked down and our management systems ensure that they cannot be tampered with. A Virtual Private Network (VPN) also ensures your connections are less prone to interface or interception by 3rd parties.

We also make it easy for you to add features or security services as your needs change. We call this being 'best connected' and SecureWan ticks all these boxes and more.

SecureWan fits into the 'Protect' security pillar with all of our security services available as simple add-ons; or in some cases as discreet services.
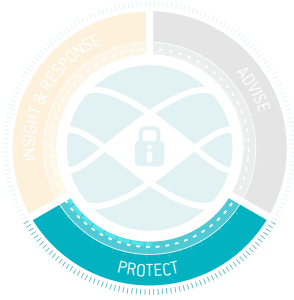
Managed Firewall

The foundation of our managed firewall service is the management portal which allows Kordia to manage all your Firewall security services from a single pane of glass. This functionality also allows customers to self-manage some, or all, their security environment without having to worry about complex development, maintenance costs or the requirement to retain highly skilled security personnel.

This environment combines the power, efficiency, and features of a public cloud, with the security, control, and performance of a dedicated private environment. Kordia's Managed Firewall Service offers the perfect solution for customers that want to outsource their network security requirements without losing visibility or control of their critical infrastructure.

SERVICE FEATURES AND OPTIONS:

Firewall Policies

Filtering rules configured on the firewall to allow/deny selected traffic to traverse between interfaces (zones).

Web Filtering

Provides control over what the user can view as well as protecting the network from internet content threats such as malicious URLs. Administrators have the flexibility to block content or to provide automated pop-up warnings to allow users to determine whether or not they should proceed.

AntiVirus (AV)

Provides protection against a variety of threats, including malicious codes (Malware), and Advanced Persistent Threats (APT). AV provides fully automated updates to ensure protection against the latest content-level threats offering you the highest level of protection.

Application Control

There are a number of reasons companies may wish to control applications such as un-approved internet applications (e.g. peer-to-peer or gaming applications consuming bandwidth). Application control allows you to block these, or limit their bandwidth to improve the performance of your business applications.

Intrusion Prevention System (IPS)

IPS uses a number of techniques to provide protection. These include: protocol decoders that detect suspicious, non-conforming sessions that resemble known attacks or are non-compliant to standard implementations and pattern signature matching against known threats. In addition IPS uses Denial of Service policies to protect the firewall against overloading. Custom signatures can also be created to protect against unusual, specialised or unknown attacks.

Remote Access (SSL VPN)

Provides your remote users with secure access to the corporate network.

Virtual Security Engineers (VSE)

Conduct regular reviews with the customer that may include the development and presentation of customised reports, review of anomalous behaviour; and the review of security policy and firewall logs to ensure continual optimal performance of the service. Resulting service changes are generally included in the service fee. Customers will also have ability to submit change requests and seek support directly with our VSEs, rather than through our Network Operations Centre, in relation to Firewall support.
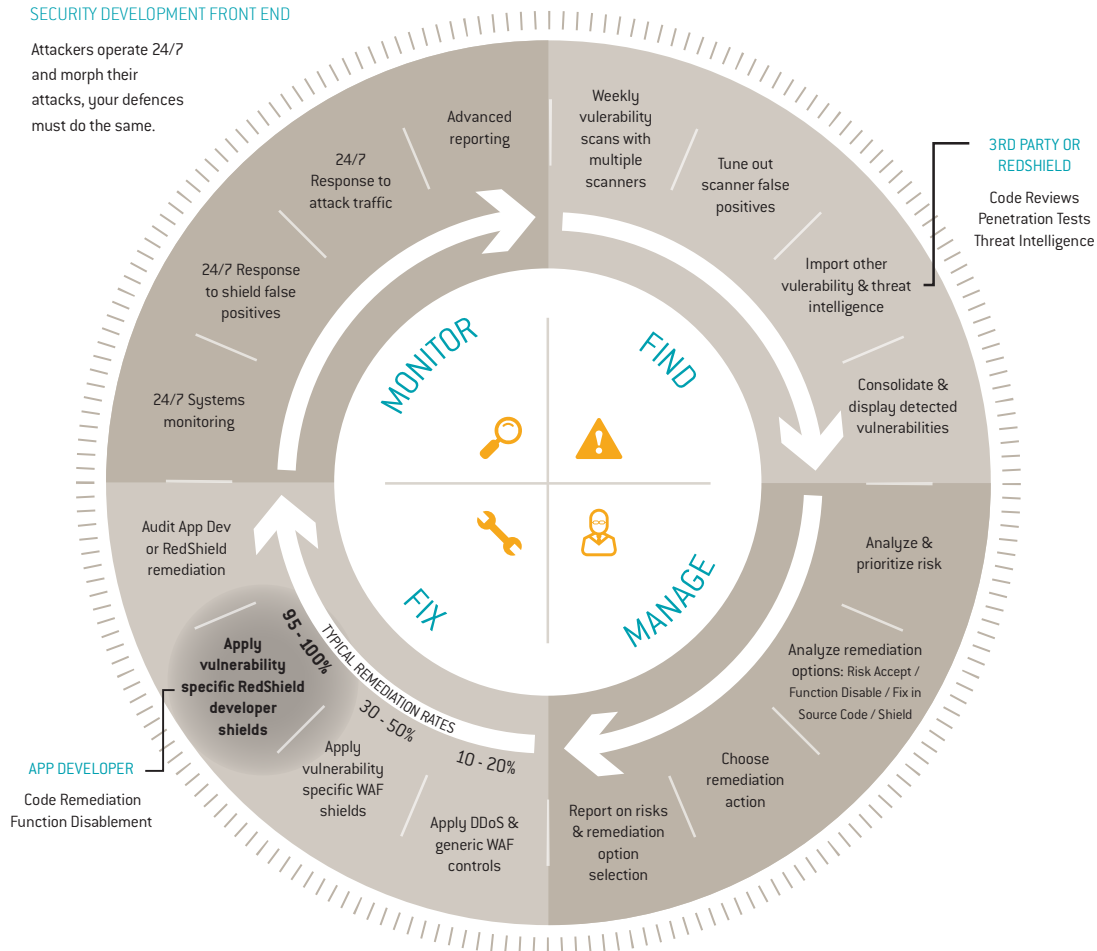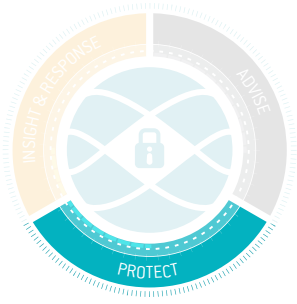
RedShield

With dozens of new web application vulnerabilities and exposures being announced daily, either you fix your web site and application weaknesses; or you risk being exploited. Finding your vulnerabilities is key, but with limited budget or resource, how can you do this regularly; let alone prioritise, fix and monitor?

RedShield is an award-winning business whose innovative approach to security is re-defining the concept of WAFs and website shielding. Not only does RedShield provide DDoS and common web vulnerability protection via our base WAF features, it is the world's first cloud WAF to be targeting 100% vulnerability mitigation through unique advanced shields, with the ability to customise and tune per application.

A CONTINUOUS WEB APPLICATION SECURITY DEVELOPMENT FRONT END

Attackers operate 24/7 and morph their attacks, your defences must do the same.

Advanced reporting

24/7 Response to attack traffic

24/7 Response to shield false positives

24/7 Systems monitoring

Audit App Dev or RedShield remediation

Weekly vulerability scans with multiple scanners

Tune out scanner false positives

Import other vulerability & threat intelligence

3RD PARTY OR REDSHIELD
Code Reviews
Penetration Tests
Threat Intelligence

Consolidate & display detected vulnerabilities

Analyze & prioritize risk

Analyze remediation options: Risk Accept / Function Disable / Fix in Source Code / Shield

Choose remediation action

Report on risks & remediation option selection

Apply DDoS & generic WAF controls

Apply vulnerability specific WAF shields

Apply vulnerability specific RedShield developer shields

APP DEVELOPER
Code Remediation
Function Disablement

TYPICAL REMEDIATION RATES
95 - 100%
30 - 50%
10 - 20%

MONITOR

FIND

FIX

MANAGE

REDSHIELD

SecureVault Backup & Restore

Backup and restore your critical data in a highly secure environment with ease. Immediate recovery ensures business continuity in the event of data loss – whether it be due to system failure or criminal activity.

Using the concept of 'incremental forever', stored data continually updated and is optimised for your network with data deduplication and compression – this includes common file elimination across all machines and incremental backups, transmitting only changes made on backed-up files.

In the event of a major IT disaster, data can also be restored by copying your data to a removable disc drive and physically delivering it to the new site. This can be arranged with Kordia and would typically occur during a complete local IT failure, or if the local site needs to be moved.

CYBER SECURITY BY KORDIA
3.0 INSIGHT & RESPONSE

———

You are the person responsible for ensuring your company's network and information is secure. So, how secure is it? In today's world, it's not a matter of *if* your security systems will be breached, but *when*. Kordia helps businesses ensure they have the systems and policies in place to not only keep the bad guys out, but also rapidly identify a breach and take immediate action to minimise the damage.

Unified Security Management

When it comes to cyber-security, prevention is no longer enough. Ongoing monitoring inside your network is required to enable early identification of a breach. Our goal is to provide an integrated threat detection and compliance management solution, which is then powered by up-to-the-minute threat intelligence from AlienVault Labs and their Open Threat Exchange. This enables collaborative defence with actionable community-powered threat data.

The result is a powerful solution that delivers on its promise of complete security visibility.

The Unified Security Management platform provides five essential security capabilities in a single console, giving you everything you need to identify and manage both compliance and threats. This is underpinned by our 24/7 Security Operations Centre (SOC) providing incident handling, security advice and response assistance if required.

SERVICE FEATURES AND OPTIONS:

🔑 Asset Discovery

Find all assets and vulnerabilities on your network before a hacker does.

- Active Network Scanning
- Passive Network Monitoring
- Asset Inventory
- Software Inventory

🖥 Behavioural Monitoring

Identify suspicious behaviour and potentially compromised systems

- Netflow Analysis
- Service Availability Monitoring
- Full packet capture

🩺 Vulnerability Assessment

Identify systems on your network that are vulnerable to exploits

- Network Vulnerability Testing
- Continuous Vulnerability Monitoring

⚠ SIEM Security Intelligence

Correlate and analyse security event data from across your network

- Log Management
- Event Correlation
- Incident Response
- Reporting and Alarms

🕵 Intrusion Detection

Detect malicious traffic on your network

- Network IDS
- Host IDS
- File Integrity Monitoring

🏢 Security Operations Centre

Security experts to provide incident handling and advice

- Security Alert Analysts
- Security Assurance Analysts

CYBER SECURITY
BY KORDIA

NZ'S MOST COMPREHENSIVE SECURITY SUITE

ADVISE | PROTECT | INSIGHT & RESPONSE

Visit www.kordia.co.nz
call your Account Manager
or phone 0800 kordia

kordia®

FORTINET

REDSHiELD

ALiEN VAULT

aura
INFORMATION SECURITY