A CYBER 1 Company

# Managed

## Services

While the importance of cybersecurity in today's business environment is getting more advanced, businesses are having to deal with new challenges in order to stay ahead of cybercriminals and amongst these are increasingly tight budgets and a lack of skills. Some businesses are lacking in service providers that can offer the skills and services needed to complement their strengths and alleviate their weaknesses. **With 20 years' worth of experience and highly skilled teams of specialists, DRS provides services designed to give tailormade solutions to the client's needs providing the best in information security.**

Managed Services offered include:


- Network Access Control (pg 2)
- IDP/IDS Systems (pg 3)
- Security Incident & Event Monitoring (pg 4)
- Managed email gateways (pg 5)
- Managed web gateways (pg 6)
- VPN (pg 7)
- Firewall configuration management (pg 8)
- Patch Management (pg 9)

drs
A CYBER 1 Company

A CYBER 1 Company

# Network

## Access Control (NAC)

Network access control systems keep rogue or compromised devices off of business networks. The main benefit of NAC solutions is to prevent end-stations that lack antivirus, patches, or host intrusion prevention software from accessing the network and placing other computers at risk of cross-contamination of computer worms.

- **Mitigation of non-zero-day attacks**
- **Authorization, Authentication and Accounting of network connections.**
- **Encryption of traffic to the wireless and wired network using protocols.**
- **Role-based controls of user, device, application and security.**
- **Automation with other tools to define network role based on other information such as known vulnerabilities, jailbreak status etc.**
- **Policy enforcement**
- **NAC solutions allow network operators to define policies, such as the types of computers or roles of users allowed to access areas of the network, and enforce them in switches, routers, and network middleboxes.**
- **Identity and access management.**

A CYBER 1 Company

# Intrusion

## Protection and Detection Systems (IDP/IDS)

DRS provides a fully managed, 24/7 service that uses network-based intrusion detection and prevention systems to protect networks from attack and misuse.

### KEY BENEFITS:

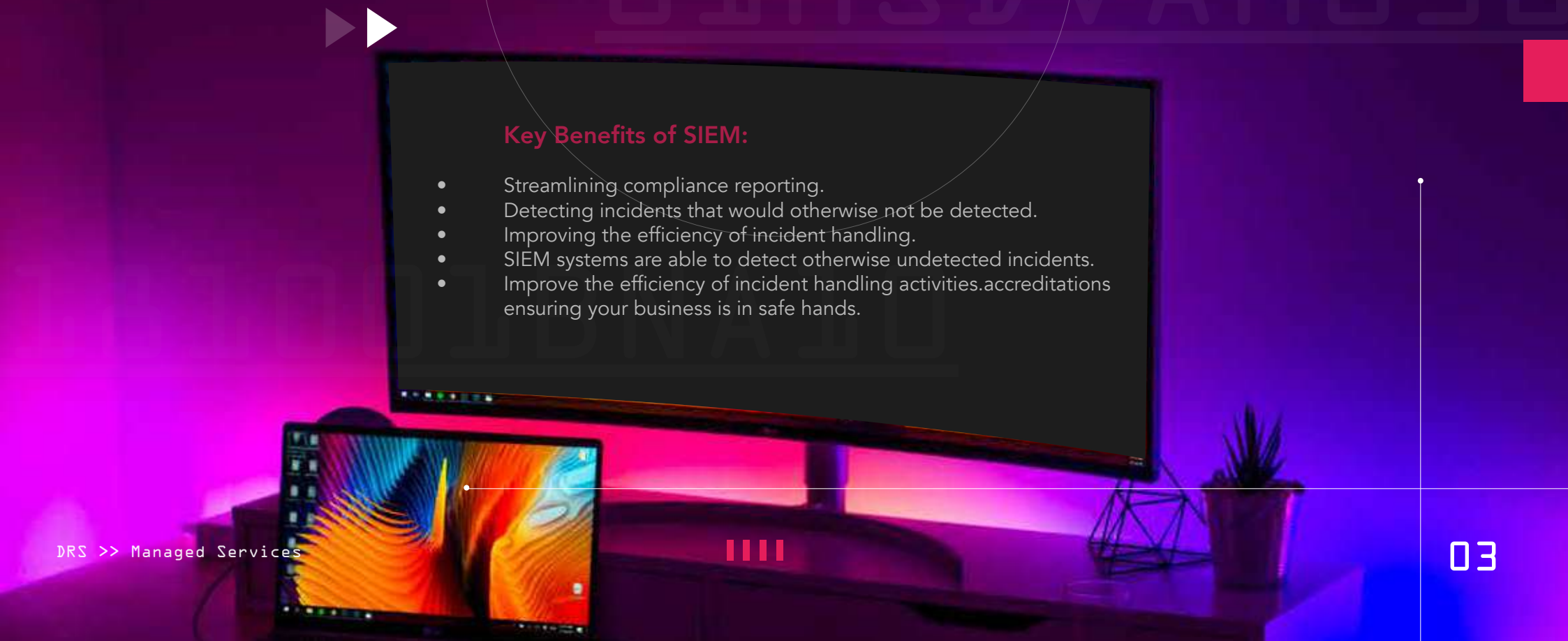
- **Reduce risk:** Expert Intrusion protection and detection systems configured for your business. DRS further provides management and monitoring with immediate response to any issues lowering the risk of business disruption.
- **Protect your brand:** Continuous proactive IDP/IDS monitoring helps safeguard your business against attacks – protecting revenues, customer loyalty and brand reputation.
- **Focus on your business:** By entrusting security to experts with over 25 years' experience, your overstretched technical staff can focus on your core business.
- **Access to scarce expertise:** The DRS team is security-cleared and have the highest industry accreditations ensuring your business is in safe hands.

A CYBER 1 Company

# Security Incident

## and Event Monitoring (SIEM)

Security incident and event management (SIEM) is the process of identifying, monitoring, recording and analyzing security events or incidents within a real-time IT environment. It provides a comprehensive and centralized view of the security scenario of an IT infrastructure.



### Key Benefits of SIEM:

- Streamlining compliance reporting.
- Detecting incidents that would otherwise not be detected.
- Improving the efficiency of incident handling.
- SIEM systems are able to detect otherwise undetected incidents.
- Improve the efficiency of incident handling activities.accreditations ensuring your business is in safe hands.

A CYBER 1 Company

# Managed

## Email Gateway

DRS ensures that your email gateway technologies are monitored and managed effectively, to provide continued protection from information leakage and from viruses, trojans, spyware, and malicious code distributed via email.

- Offers inbound and outbound data filtering and leak prevention
- Shields Against email-borne threats.
- Prevents threats from affecting the network as a whole.
- Ensures continuous email availability.
- Safeguards sensitive data from falling into the wrong hands.
- Simplifies email security.
- Improves PoPI and GDPR compliance

# Managed

## Web Gateway

DRS' managed web gateway ensures that your web gateway technologies are monitored and managed effectively, to provide continuous protection from information leakage and from viruses, trojans, spyware and malicious code distributed through the web.

### Benefits of a Managed Web Gateway:

- **Productivity** – Web filtering can allow an organization to address excessive use of non-work websites by either preventing or limiting access to services such as social networking, online auctions, online gambling etc.
- **Minimizing liability** – Companies should take all reasonable steps to protect themselves and their staff from liability. Limiting access to potentially offensive or illegal material online will limit the chances of internal and internal legal issues for the business.
- **Network and bandwidth management** – Web filtering and monitoring helps organizations understand the types of sites and content that is accessed at the workplace and at what time, helping with capacity planning and highlighting areas for further investigation in the case of casual browsing or upsurges in traffic x-around key events such as the Olympics, FIFA World Cup, major news events and other video-heavyvcontent events.
- **Data security** – Web filtering delivers an essential layer of protection from malware, phishing and other online scams long before client computers and end-users would be exposed to them.

A CYBER 1 Company

# VPN

"Next-generation VPN solutions from DRS fulfil any organisation's remote access requirements."

Remote access is essential to optimising productivity in all spheres of business. However, new privacy laws aimed at the protection of personal information are forcing organisations to seriously rethink the way in which their staff access intellectual property remotely. By adding security and privacy to private and public networks such as WiFi Hotspots and the Internet, a Virtual Private Network (VPN) enables staff to access internal resources in a safe and secure way, from any location.

VPN solutions from DRS: DRS's industry-leading next-generation VPN solutions fulfil any organisation's remote access requirements. Our dedicated SSL VPN solutions cater to PCs and mobile devices, using advanced encryption protocols and secure tunnelling techniques to encapsulate all online data transfers.

## Our VPN solutions include:

- Client-less Access (VPN portal-published resources)
- Group Policy Integration (Active Directory and LDAP)
- Strong Authentication (two factor, PKI, SAML 2.0, Digital Certificates)
- Host Checker (Security Policy enforcement)
- Virtual Desktop Access
- Mobile Client support
- Mobile Device Management (MDM)
- Universal Client
- Layer 3 SSL VPN
- Application VPN
- Tunnel Encryption SSL V3 and TLS support


# Firewall

configuration management

"Optimised security starts with firewall configuration management."

Firewall configuration management systems provide visibility and analysis of all changes being made to a network security infrastructure, on-premise and in the cloud. Keeping track of administrative changes to security infrastructure is essential to the change management process as well as maintaining a secure environment. This, in turn, will help identify and rectify malicious activity and human error within an enterprise network.

Firewall configuration management solutions from DRS:

DRS provides comprehensive firewall and security policy management solutions that offer a simplified view of security policies across multiple vendors. This ensures that firewall and security policies are optimised to enable business agility, while meeting the most stringent security and compliance requirements.

## Our firewall configuration management solutions include:

- Centralised policy management
- Network topology maps
- Reporting on the difference between any two running configuration changes
- Firewall rule and object usage reporting
- Real-time configuration change alerts
- Compliance reporting
- Automated change management systems
- Cloud and on-premises security infrastructure support

A CYBER 1 Company

# Patch
## management

"Patch Management is a critical component when it comes to securing your environment"

Modern operating systems and application software contain millions of lines of code, with the software under constant scrutiny by threat actors looking for a weakness, a vulnerability that can be exploited. If left unchecked, these weaknesses would leave your network vulnerable to malware and other cyber threats.

Patch management allows for the timeous updating of software within an environment. This serves to close security holes created by non-secure software development practices, as well as add value from the extra functionality enabled by the ongoing development of the software.

### Patch management solutions from DRS:

With the best patch management tools at our disposal, DRS will not only deploy the right patch management systems for your environment but will also ensure that you have the best patch management coverage possible for your environment.

With extensive knowledge of industry standards and best practices around patch management, DRS provides the tools and expertise to assist in high-level vulnerability and configuration remediation. Our solutions make patching a streamlined and efficient process. We secure your environment using the latest technologies to effectively identify and remediate any operating system or application vulnerabilities discovered on your network.