Security

technology
unscrambled

solutions Device
confidential control networks threats
internet connections inappropriate
malicious
systems computers data Anti-virus installed
policies malware DLP Prevention
patch Web management rules information
detect authentication regulations
Private content Content AV Encryption protection firewall
criteria
secure strategy blocks security
access vulnerabilities email risk loss file
intrusion private
Application
viruses incidents Detection
Email token Software Control password running
encrypted
compliancy
VPN defence prevention devices monitor detection
attacks Intrusion network code
Network Data breaches Virtual

Contents

Foreword	2
Security Components Defined - Firewall	3
Encryption	4
Authentication	5
Virtual Private Network (VPN)	6
Intrusion Prevention and Detection	7
Email Content Control	8
Web Content Control	9
Anti-virus Software	10
Device Control/Application Control Software	11
Data Loss Prevention	12
Patch Management	13
Risk Management	14
Compliancy Software	15
Creating Strong, Hacker-proof Passwords	16
Conclusion	17
Tek Response Acquires Presence Ltd	18
Talk to us about your security/IT Strategy	19

Foreword

In June 2011, a US study by the Ponemon Institute, found that 90% of 583 businesses interviewed had been hit by at least one IT security breach in the past 12 months, with 59%, citing two or more breaches in that period.

Protecting your business against the risk of viruses, unauthorised data access, uncontrolled e-mail correspondence, data manipulation and misuse of access to the internet requires, as a minimum, a solid, integrated security strategy that addresses both internal and external threats. This does not guarantee 100% protection but is a significant step towards fending security threats.

Furthermore, as cyber criminals enhance their reach, the need for a solid strategy becomes increasingly important. We have all witnessed high profile cases of data breaches and targeted attacks.

With the move towards cloud computing and data-centre adoption, the way IT infrastructure is deployed is changing. This too, introduces a host of new risks and security considerations.

With a growing trend of a remote workforce, in addition to the increasing number of employees using personal devices at work, the need to protect data to adapt to the changing landscape brings about additional security challenges. Sensitive data, previously protected behind a firewall, is now being accessed remotely and ported onto external storage devices which are open to an increasing range of security breaches.

The internal activity of employees needs to be monitored and policed. Threats to your organisation will exist within your own boundaries. What policies have you implemented to ensure your systems are not being compromised? How do you manage the process of system updates to ensure you are protected from the latest security exploit?

This security edition of Technology Unscrambled identifies and defines key security components. It lets you consider whether you are adequately protected.

Security Components Defined

Firewall

When connecting computers to the internet they potentially become visible to all other internet users. A firewall sits between the internet and your computers and allows or blocks connections with other computers based on your predetermined rules – blocking connections that do not meet the specified security criteria. A firewall is considered a first line of defence in protecting private information.

BARRACUDA NETWORKS   Check Point SOFTWARE TECHNOLOGIES LTD.   CISCO   JUNIPER NETWORKS   SONICWALL   STONESOFT   WatchGuard

Security

Encryption

Information transported over networks is at risk of being misdirected or monitored. This risk has significantly risen with the ever-increasing popularity of wireless networks.

With a multitude of portable devices now available, the potential of data falling into the wrong hands also increases. Protecting your confidential, private and sensitive data is vital, particularly with regards to avoiding breaches in Data Protection laws.

For greater security, data can be encrypted. Encryption software ensures that only the people who are supposed to read your data can; data is translated into code. To read an encrypted file, you must be able to decrypt it using a key or password.

Check Point SOFTWARE TECHNOLOGIES LTD.

KANGURU Solutions

Lumension IT Secured. Success Optimized.

McAfee

SOPHOS

Symantec.

Authentication

In the majority of cases, authentication consists of a user name and a password, i.e. is the individual who he/she claims to be?!

Two-factor authentication provides improved security - it requires the user to meet two authentication criteria: a user name/password combination and a token or certificate, known as *something you have, something you know*.

This strong/two-factor authentication approach, provides more than a simple static password (username/password approach). Via the security token/certificate, the password typically changes every 30 seconds; so even if it becomes known, it quickly becomes useless.

ACTIVIDENTITY part of HID Global

CRYPTOCARD experts in authentication.

RSA SECURITY

VASCO THE AUTHENTICATION COMPANY

Security

Barracuda Networks

Check Point Software Technologies Ltd.

Cisco

Juniper Networks

SonicWall

Stonesoft

WatchGuard

Virtual Private Network (VPN)

A VPN (Virtual Private Network) offers a secure and reliable way to share information across public computer networks, such as the internet. Data is encrypted before being passed over the public network hence the term ‘virtual private network’.

There are different types of VPNs, including:

Site-to-site: connects a network consisting of many users/devices to another similar network.

Client-to-site: connects a single user device to a network, e.g. home user accessing HQ.

SSL VPN: enables the user to access resources on a network through a web browser.

Security

Intrusion Prevention and Detection System (IPDS)

Intrusion Prevention and Detection is the process of performing intrusion detection and attempting to stop detected possible incidents. Intrusion detection and prevention systems (IDPS) are primarily focused on identifying possible incidents, logging information about them, attempting to stop them, and reporting them to security administrators.

Barracuda Networks Check Point Software Technologies Ltd. Cisco Juniper Networks SonicWall StoneSoft WatchGuard

Barracuda Networks

Blue Coat

Clear Swift

Kaspersky lab

McAfee

Sophos

Symantec

Trend Micro

websense
ESSENTIAL INFORMATION PROTECTION™

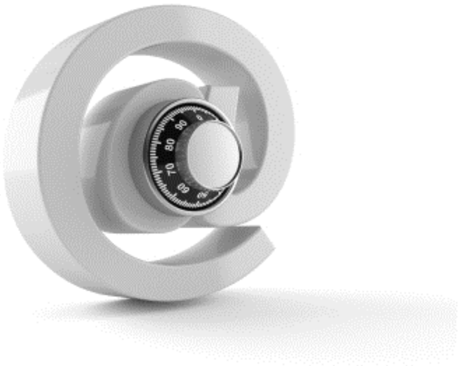
Email Content Control

Email Content Control scans all incoming and outgoing emails to detect (and then control) any inappropriate, malicious or confidential content.

Email content security solutions use multiple anti-virus engines, exploit detection, HTML threats engine, and content and attachment checking to scan incoming and outgoing email for spam, viruses, exploits and attacks.

This helps to ensure:

- confidential, sensitive and proprietary material is blocked from leaving your organisation
- inappropriate content does not reach your network
- email misuse is reduced within your organisation.



Security

technology unscrambled

BARRACUDA NETWORKS

Blue Coat

CLEAR SWIFT

KASPERSKY lab

McAfee

SOPHOS

Symantec.

TREND MICRO

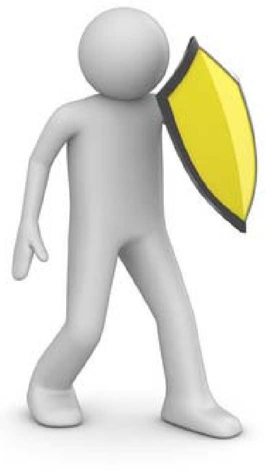
websense ESSENTIAL INFORMATION PROTECTION™

Web Content Control

Web Content Control blocks access to harmful and inappropriate website material which may contain phishing/pharming attacks, malware, or inappropriately deemed content.

Web page content is analysed and a block placed or alert given based on pre-defined rules. Different filters can be applied to different users to create the rules, in addition to restricting access to specific web pages, regardless of filter type.

Reporting facilities can provide the breadth and depth of web-based user activities on your network (e.g. time/date, username, PC domain, sites visited, bandwidth used). This detailed insight can assist with preventing infections of your network, as well as identifying misuse of employees' time and company resources.



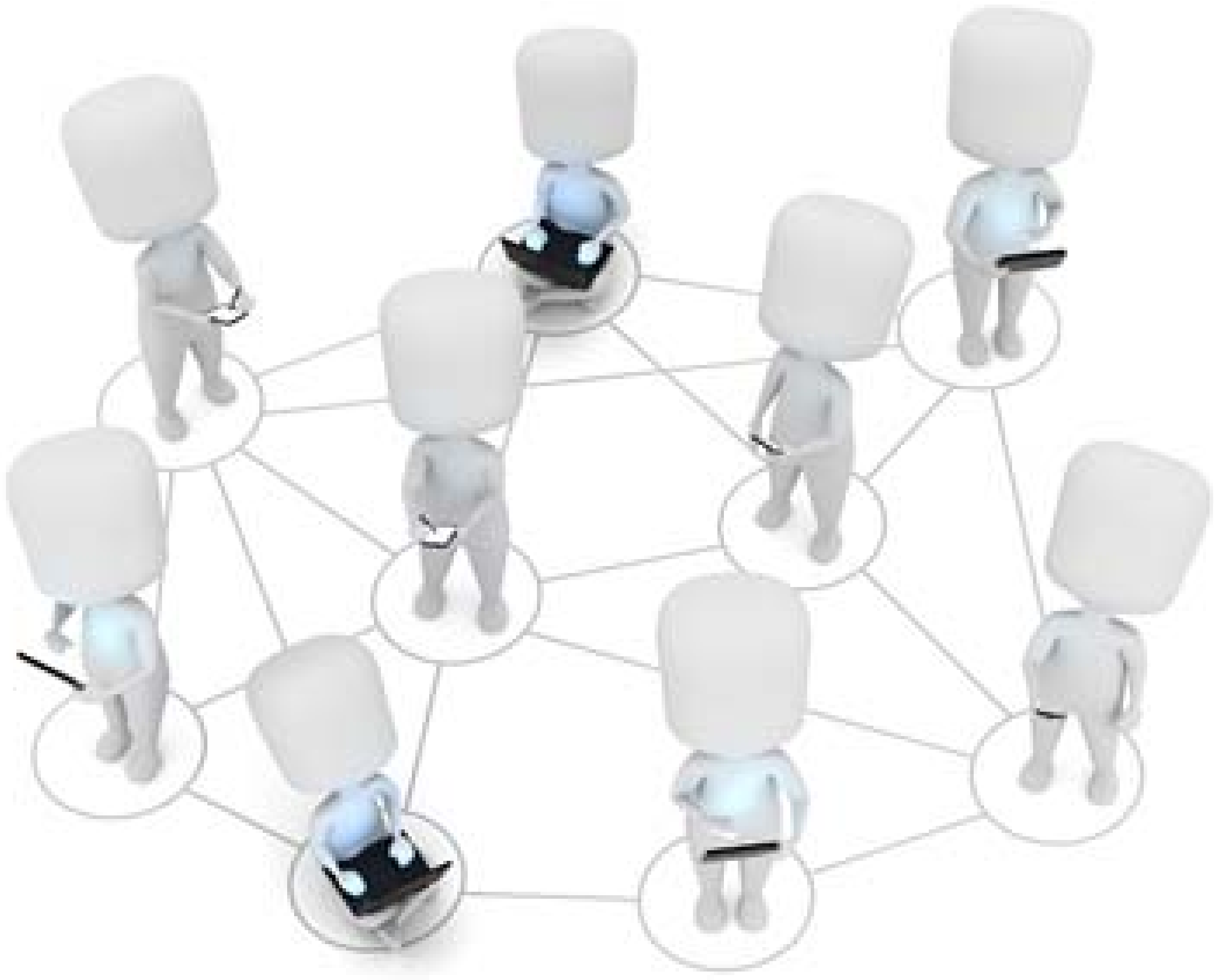
Anti-Virus Software

Anti-virus (AV) is a protective software used to prevent, detect, and remove malware (malicious software). Malware may include: viruses, Trojans, worms, key loggers, hijackers, dialers, and other codes that vandalise or steal your computer contents.

The internet, email, memory sticks, remote users' laptops, CDs, all play a part in increasing exposure to such attacks. Anti-virus software is the back bone of your protection; it examines what is being introduced and checks it against a database of known malware that is continually being updated. If a match is found, the malware is blocked.

AV can be installed on endpoint devices, servers, email gateways, firewalls, etc.

AVIRA CLEAR SWIFT F-Secure KASPERSKY lab McAfee SOPHOS Symantec TREND MICRO



Device Control Software

Many of the devices today, e.g. mobile phones, iPods, iPads, enable data to be transferred more easily from your computers.

Device control enables you to specify what devices can be connected to your network/ computers and what can be downloaded to them. You are in control of the transfer of data.

Application Control Software

Application control software allows you to control/block the installation and running of applications/software. For e.g. you may wish to prevent the use of iTunes, Bit torrents, games and other anti-productivity software or stop illegal pirate software from being installed. Some application control software can stop macros and malware from running.

Check Point SOFTWARE TECHNOLOGIES LTD.   Lumension IT Secured. Success Optimized.   SOPHOS   Symantec.

Check Point SOFTWARE TECHNOLOGIES LTD. Symantec. websense ESSENTIAL INFORMATION PROTECTION™

Data Loss Prevention (DLP)

Data loss prevention (DLP) is a set of information security tools that:

- prohibit users from sending flagged sensitive/critical information or alternatively sanction the distribution of the information once authorised
- enable you to monitor exactly what is being sent over the network.

Central policies are applied to monitor and control the data transmission. DLP products use business rules to examine file content and tag confidential and critical information. A user who accidentally or maliciously attempts to disclose confidential information that has been tagged will be denied. This may include the internal circulation of company information.

DLP seeks to overcome insider threats – data leak prevention and address legal requirements such as Data Protection laws.

DLP products generally have the following components:

Endpoint: Monitor and control activities
Network: Filter data streams
Storage: Protect data at rest

Patch Management

A patch is an additional piece of software code designed to fix problems with, or update a computer program or its supporting data. This includes fixing security vulnerabilities, flaws and other bugs, and improving usability or performance, and often enabling additional functionality.

"Over 90% of security exploits are carried out through vulnerabilities for which there are known patches."
Source: Gartner Group

Effective patch management software, coupled with a patch management policy, is key to ensuring defence of your networks.

The rise of widespread worms and malicious code targeting known vulnerabilities on unpatched systems, and the resultant downtime and expense they bring, is a key reason why organisations are focusing on patch management.

Lumension IT Secured. Success Optimized.

Microsoft

Security

Risk Management

Risk management includes penetration testing, log management and auditing.

A penetration test, occasionally pentest, is a method of evaluating the security of a computer system or network by simulating an attack from malicious outsiders (who do not have an authorised means of accessing the organisation's systems) and malicious insiders (who have some level of authorised access). The process involves an active analysis of the system for any potential vulnerabilities that could result from poor or improper system configuration, both known and unknown hardware or software flaws, or operational weaknesses in process or technical countermeasures. This analysis is carried out from the position of a potential attacker and can involve active exploitation of security vulnerabilities.

Log management involves the collation, storage, centralisation and long-term retention of all data generated by IT systems. This includes log analysis, log search and reporting.

Log management helps you to gain visibility, insight and control over your organisation’s IT data. It is driven by security, network operations (such as system or network administration) and regulatory compliance to assist with troubleshooting issues, meeting compliancy/audit requirements and as a means to investigating security threats.

Compliancy Software

Organisations today must comply with a greater number of regulations than ever before, many of which deal with information and system security. While the intent of these regulations is good, their proliferation is burdensome.

There are software solutions that now understand what individual regulations require for companies to conform. They can be used to attain predetermined levels of compliancy then assess what is required to reach higher levels of compliancy.

Software can produce reports that are acceptable to your auditors demonstrating your compliancy. This software can pay for itself by reducing regulation implementation time and audit costs.

Lumension® IT Secured. Success Optimized.™

loglogic™

Security

Creating strong, secure, hacker-proof passwords

This simple guide provides you with some quick steps to creating enhanced password security. Regardless of your current security configuration, these measures can be easily implemented to ensure that passwords are not the weakest link in your security system.

Passwords should:

- have a minimum of eight characters
- include a combination of uppercase, lowercase, numbers and punctuation
- be based on a phrase to heighten security (also more memorable)
- change – the more important the account, the more frequently the password should change.

Replacing vowels with numbers, reversing a phrase, removing vowels and replacing at the end of a sentence all contribute to a more secure password. Some computer systems allow an administrator to enforce a password policy.

Avoid:

- storing your password online/writing passwords down
- using a password twice
- logging into a secure site from an e-mail link. To avoid scam attacks, always type the URL into a browser yourself.

Conclusion

When somebody ‘knock knocks’ on your network door it’s not sufficient to know just “who’s there?” You need to know: what they want; what they’ve got in their pockets; where they want to go; and are they who they say they are.

Then when you let them enter, you need to know: where they are going and what they are doing.

Finally, when they leave, it’s important to know what they’ve taken with them and what they’ve left behind…….

Tek Response can help you know more than just “who’s there.”

Our market leading **firewalls** combined with secure **second factor authentication** ensures no one enters without authority.

The best **intrusion prevention** and **detection** solutions ensure that once they are in they only go where you want and don’t leave behind things you don’t want.

Our highly competent **web** and **email content scanning** solutions ensure only ‘nice’ things are in their pockets. Leading **application** and **device control** solutions, teamed with our **data loss protection** solutions, control what they take away with them.

Security

Enhancing our Security ‘Presence’

Tek Response enhanced its existing security capabilities in June 2009 with the acquisition of Presence Ltd. This expanding team of security specialists, married with Tek Response’s existing capabilities, provides a single point of contact for organisations’ security solutions. With accreditations to supply solutions from some of the most respected security vendors in the world, Tek Response has built on Presence’s reputation to deliver proven security solutions to a variety of vertical sectors across the UK.

Security

Talk to us about your security strategy….

- Firewalls
- Encryption
- Authentication
- Virtual Private Networks
- Intrusion Prevention and Detection
- Email Content Control
- Web Content Control
- Anti Virus Software
- Security Consultancy
- Device Control Software
- Application Control Software
- Data Loss Prevention
- Patch Management
- Risk Management
- Compliancy Software
- Security Consultancy

Additional Tek Response specialities include….

- Storage
- Software
- Networking
- Server
- Access
- Virtualisation
- Hosted and Managed
- Mobility
- Professional Services and Support

Telephone 0370 350 2552 or email info@tekresponse.co.uk