WHITEPAPER

A Complete Approach To Security

How To Achieve Agile Security Operations

THREATWATCH

- Cyber threats cost the UK economy £27 billion a year
- 200,000 new threats are identified every day
- 58% of businesses believe they face “substantial or critical” cybersecurity risks
- 66% of breaches take months or even years to be discovered, up from 56% in 2012

The security landscape is changing. How are you adapting?

Most reports on information security begin with setting the scene for the accelerating threat landscape. It's an alarming picture of overwhelming adversaries firmly in control. We know that when it comes to cyber threats, it's no longer a question of if your organisation will be targeted, but when. Two thirds of businesses report the frequency of attacks has increased by 5% or more in the last 12 months, while 58% of CFOs believe they now face substantial or critical cyber security risks.

There isn't a security professional in the country who isn't aware of the ever-increasing threat and attack vectors. Spend on security technologies has grown to £22billion in 2012, more than double that of 2006 at £9billion. And yet, despite the millions and millions of additional security devices that will have been deployed in this time, the number of reported security breaches continues to rise. The big challenge for security today is how to maintain business availability in the face of rising threats, and when the traditional approach of layering on security technologies is no longer effective.

Businesses are changing how they consume IT

Inside the organisation too, change is happening fast. 50% of employees use a personally owned device to access the organisation's business critical applications. The desire for business agility to adapt to market conditions and enable competitiveness is transforming how IT is both delivered and consumed by users. Employees need universal access to data and they expect mobility, remote access and cloud-based applications in order to do their jobs. This, and the coming panacea of connected devices, people and processes, means IT leaders have no option but to embrace the explosion in devices and connectivity complexity.

All of this demands a sea-change for security. IT leaders must enable their customers to use the Internet, cloud computing and business applications to their full potential in a secure way. Clearly, securing each and every device is impractical and the old approach to security no longer applies when corporate assets are distributed in private homes, in the cloud, in data centres and company buildings.

We know security is changing.
It's time for a different approach.

Introducing complete security strategy

Why you need a complete approach

43% of organisations agree that information risk is making our businesses less agile (Economist Intelligence Unit, 2013).

In security, we know there is no such thing as 100% protection - we live in a world of compromises. No security team has access to unlimited budget and we don't want to spend money on taking care of every threat. We have to make intelligent investment decisions on what we choose to protect and what risks we choose to manage. We have to decide what the right compromises are for the business.

It means we must understand and accept some risk. Aiming for no risk is redundant. We have to work within the parameters of both known risk and vulnerabilities, and unknown risks. We don't know what might be coming at us, but we do know it's a question of 'when' and not 'if'

The old school 'swiss cheese' approach of layering on enough technology to cover the maximum number of holes is no longer suited to business needs. Security technology is still absolutely critical and the innovations in next generation devices are essential to maintaining protection, but by adding every new 'mousetrap' to catch every new threat, we just shift the IT challenge from hardware and onto management and human expertise. And this creates another issue for security. Do you have the expertise and resources to maintain burgeoning security systems? Security talent is at a premium, but the need for expert interpretation in threat management can't be ignored.

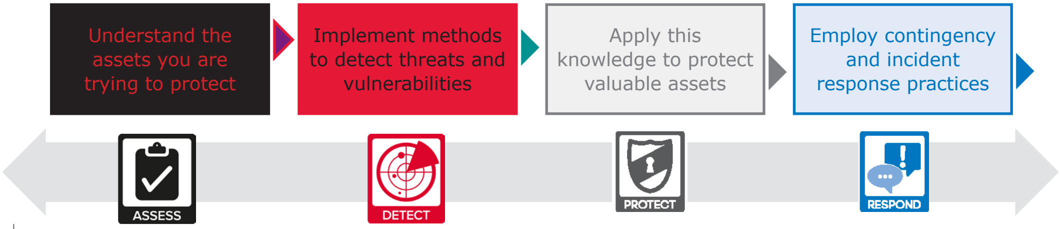
What's required? Four pillars for enabling end-to-end security agility

96% of businesses already feel that their existing IT security functions do not meet their needs (EY 16th Annual GLobal Information Security Survey). But businesses can adapt their security posture and get risk under control by taking a complete approach to security. By focusing on people, platform and process in addition to protection, organisations can create agile, responsive information security.

There are four key requirements security professionals need, in order to enable end-to-end security:

- Assessing risk and adapting strategy
  - Understand the risk to the business
  - Decide what risks we can accept and what we can't
- Real-time and proactive threat detection
  - Manage known risks by detecting threats in real-time
  - Mitigate unknown threats through proactive detection and feed this back into your protection
- Protecting valuable assets
  - Ensure you have the right technologies to protect what's valuable
  - And don't spend money on things you don't need
- Respond to incidents and breaches
  - Expect to be compromised and have an incident response plan

Complete security framework



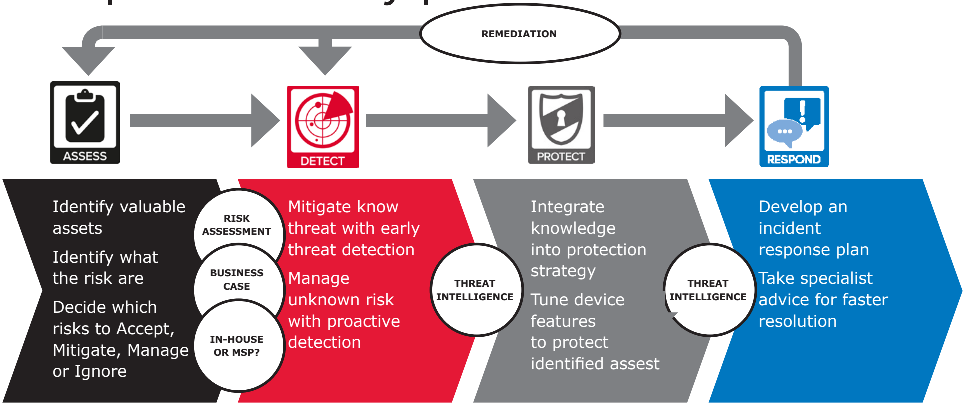
Understand the assets you are trying to protect

Implement methods to detect threats and vulnerabilities

Apply this knowledge to protect valuable assets

Employ contingency and incident response practices

Complete security process



Identify valuable assets

Identify what the risk are

Decide which risks to Accept, Mitigate, Manage or Ignore

Mitigate know threat with early threat detection

Manage unknown risk with proactive detection

Integrate knowledge into protection strategy

Tune device features to protect identified assest

Develop an incident response plan

Take specialist advice for faster resolution

ASSESS

- **Risk assessments**
- **Penetration testing**
- **GRC solutions**
- **SDLC assessment**
- **Application assessments**
- **Offensive solutions**

Assess

The first port of call for many security strategies is penetration testing to expose vulnerabilities. While this reveals security weaknesses, it doesn't expose the priority of security gaps, or the intelligence to improve underlying business processes.

Often, assessments are undertaken once a year or so, using different suppliers to get this year's flavour of the risk. It means organisations are working on out of date risk information 364 days of the year, and at the mercy of partisan suppliers with a solution agenda.

Instead, look at implementing an established security framework where you have compliance needs, or for businesses outside of regulated industries, begin with a framework such as ISO 27001 and develop your own assessment parameters according to your critical business functions.

Assess the unique vulnerabilities of your business to identify the greatest risks and enable decision-making on implementing appropriate preventative protection.
Get independent advice in assessing your perimeter to identify additional weaknesses. If you don't operate security monitoring or have a SIEM solution in place, look for external expertise to extend your security capabilities.

Risk Assessments	Security Assessments	Security as a service	Threat Analysis
What are the acceptable risks and what are the crucial areas to protect?	Network Applications Employee training and education	Push monotiring data and analytics to the cloud and consume as an expert service	Assess on demand and model the potential problem

DETECT

- **24x7 real-time threat monitoring**
- **Real-time cybersecurity intelligence**
- **Proactive threat detection**
- **Advanced correlation**
- **Fraud detection**
- **Application abuse**
- **Confidentiality breaches**
- **Integrity breaches**
- **Availability breaches**

Detect

The key to agility is security intelligence. Collating and correlating data from inside and outside of the organisation enables visibility across the whole of the the IT infrastructure.

With a combination of known and unknown risk to mitigate and manage, as well as security devices to maintain, visibility across the whole of your infrastructure is essential for enabling security intelligence and staying in control of risk.

Early threat detection is only possible with real-time monitoring and correlation of data from across the organisation. It relies on understanding the IT estate and having a platform that collects and correlates data from multiple sources.

But data is not the same thing as intelligence. And security intelligence can't be bought off the shelf – it's unique to the individual business and works through a symbiotic relationship of security managed by expert people.

A security monitoring or SIEM solution enables contextual monitoring for security threats 24 hours a day. Security specialists are essential to this process and expert interpretation of security events is needed to spot patterns and identify links in disparate types of data.
A combination of people and process are the components for managing known risks and assimilating intelligence.

Taking an end-to-end approach to security shifts security operations from reactive to proactive. By accepting risk, it's necessary to get on the front foot and proactively detect threats to the organisation. With the right information, businesses don't have to wait for threats, they can use analytics to actively disrupt, deny and deceive adversaries.

PROTECT

- **Managed security services**
- **Authentication**
- **Content Security**
- **Firewalls**
- **Intrusion Detection and Prevention**
- **Load Balancing**
- **Remote Access**
- **Switching & Routing**
- **Wireless Security**
- **Security as a Service**

Protect

Armed with the knowledge of which assets we cannot risk, applying the right level of protection through security technologies can be focused on what it required without spending budget on what might be required.

There are over 40 different types of security tools available – more than can (or need to) be deployed - to protect critical assets and plug security gaps it's essential to:

- Identify and prioritise the right tools
- Minimise system complexity
- Have a management capability in place

Agnostic advice is invaluable in designing relevant security architecture. Consider consolidating devices and functions into integrated, next generation hardware and minimise the vendor set you deploy to streamline maintenance, support and management resource requirements.

You won't have unlimited resources to ensure your devices are maintained and running the latest updates, so look for additional support and management as a service where appropriate.

RESPOND

- Forensic solutions
- Incident response
- Response toolsets
- Offensive solutions

Respond

Even by implementing a complete, best practice approach to security, organisations should still expect to be compromised.

Be ready to respond to an attack or a breach. Ensure you have an incident response plan with procedures and systems in place to quickly respond to a security breach when it happens, as well as contingency or work-arounds for critical systems and applications.

When a breach happens, time to resolution is the number one concern. The ability to identify and neutralise the threat is vastly improved by having complete visibility and access to security intelligence from across the organisation.

Deploy forensic solutions to identify the nature of the attack, its point of origin and the source. Assess the impact of the breach, recommend immediate remediation to stop or divert the attack, and implement preventative measures to ensure it won't happen again.

The business impact of security breaches can be greatly reduced by having not only a response plan, but a recovery plan to mitigate any damage. This should involve specialists across your business such as IT, HR and Legal as well as external stakeholders and suppliers.

Identifying who needs to be made aware of the breach and inform them of the required actions for containment and remediation will accelerate resolution, for instance through activating data back-ups, isolating a compromised section of the network or resetting access codes and permissions.

ARBOR NETWORKS
ARUBA networks
Blue Coat
Check Point SOFTWARE TECHNOLOGIES LTD.
CISCO
CITRIX
ExtraHop
f5
IMPERVA
JUNIPER NETWORKS
LogRhythm
riverbed
RSA The Security Division of EMC
SecurEnvoy
skybox security
SOURCEfire
websense ESSENTIAL INFORMATION PROTECTION

Extending your security capabilities

How do we solve the conundrum of more security bases to cover and less resources and budget to do it with?

Adopting a risk-based approach demands new expertise and maintaining an intelligent platform demands scale as well as continuous expert management. Security decision-makers know they can't deliver every aspect of security within their walls. They need to understand where investments in either technology or managed services are appropriate and define what to keep in-house, what to push to the cloud, and what to consume as a service.

When working with Managed Security Service providers, review SLA's, performance tracking and reporting, and assess capabilities to deliver on-site services or of-site or cloud managed services.

Managed Security Services extend organisations security capabilities by introducing deeper expertise, access to 24x7 resource and scale for gathering and analysing threat intelligence fay beyond the scope of individual organisations.

SECUREDATA managed services portfolio

- Managed Firewalls
- Managed Next Gen Firewalls
- Managed Web Content Security
- Managed Remote Access
- Managed 2 Factor Authentication
- Managed Wireless
- Managed IDS / IDP
- Managed SIEM
- Managed Load Balancing
- Managed Switches/Routers
- Cloud Internet Gateway
- Cloud SIEM
- Cloud Global Load Balancing
- Cloud Phishing as a Service

The key areas where specialist service providers can add value and range to security teams include:

- Cyber intelligence unmatched by single organisation operations
- Proactive security services, to enable clients to shore-up security defences, outpacing current threats
- On-tap expertise across security and cloud technology domains
- Provide a detailed catalogue of metrics to inform customer stakeholders
- Offer a comprehensive portfolio of propositions

Macro-level intelligence

Cyber intelligence correlated from multiple internal and external sources

Proactive security

Detect and divert threats before they happen

Elastic expertise

Push monotiring data and analytics to the cloud and consume as an expert service

Complete metrics

Regular, comprehensive security metrics and analysis

Agility

Quick strategic response to evolving threats

24x7 real-time monitoring

Continuous 24x7, expert monitoring and interpretation of security data

Summary

The security landscape is changing quickly and organisations need to adapt. A holistic, complete approach to security presents a model that controls risk, enables security and allows for sensible budget investment.

By implementing a complete security strategy, we achieve significant operational benefits:

- Early warning threat detection
- Controlled risk mitigation
- Governance and compliance
- Visibility for disaster recovery

The real advantages however are the ability to unlock new business value:

- Enable users to work how, when and where they want to. Security teams, can now say ‘yes’
- Improve system availability and reduce business downtime
- Reduce the number of incidents and disruption in future
- Improve IT and business agility
- Abstract and integrate security intelligence into big data projects

Change is disruptive, but it’s also inevitable. Embrace the new cybersecurity landscape and apply new thinking and methodologies to liberate your business, your team and your potential.