

Introduction

The world continues to change at a rapid pace, and like most organisations, the UK public sector is reacting to these changes. The threat of global terrorism, increased citizen expectations with regard to service delivery and the massive increase in cyber crime are all causing the government to adapt and rethink how they deal with what could be perceived as a dichotomy of requirements. There is no doubt that the transformation of government services represents a great opportunity to improve citizen satisfaction and enable growth in the UK. However the stakes are high, both materially and politically should mistakes be made.

Extreme Networks is ready to partner with the UK public sector to provide our industry leading solutions for what is the heart of many organisations—the IT and communications infrastructure. Extreme Networks has focussed efforts to develop best of breed solutions in the market—solutions that enable the high levels of insight and control over the most valuable asset for effective service delivery, your converged infrastructure.

The Changing Face of UK Public Sector

There are many drivers for change within the UK public sector. These include:

- Requirements for departments to share information with each other both centrally and out to the regions.
 - This is driven by the necessity to share information to improve the efficiency of service delivery and to protect the welfare of the most vulnerable members of society as highlighted by the Laming⁵ and Bichard⁶ reports as recent examples.
 - Government has enabled several services and framework contracts that encourage the sharing of secure information via a defined service. These include Government Secure Intranet¹⁰ (GSI), Government Connect¹¹ (Local Government Secure Community), the IMPACT^{8,6} programme and Police National Network⁹ (PNN). These services, security frameworks and contracts can form the basis for the sharing of services and applications between all aspects of public sector in the UK.
- Requirements for government to obtain value for money by the reduction of assets, sharing of common services and cost reductions.
 - This was highlighted by the recent Gershon² and Lyons^{3,4} reports and has been used to set targets against which government departments are measured annually. Key enablers include the reduction in physical assets such as offices and buildings, and the effective use of solutions that encourage virtualisation of resources such as location independent working and mobility.

- Citizen's expectations with regards to the quality and availability of services are being driven by the Private Sector.
 - Government must catch up and transform the way that services are delivered to provide equality of service provision and ensure that government is perceived as value for money. This includes the sharing of information across departments, a range of service delivery choices and rationalisation of government processes. The need for transformational government and a suggested delivery plan is highlighted in the recent Sir David Varney reports¹ sponsored by the Cabinet Office and will be reflected in the Comprehensive Spending Review in 2007 and beyond.
- New technology enables the introduction of new, innovative services across the Public Sector including central government, local government, health, education etc.
 - The use of the Internet, mobility solutions and intelligent, content-aware networks will drive the identification and delivery of new, high value services.
- Security is high on everyone's agenda, and none more so than within government.
 - Government has a responsibility to protect the identity, welfare, rights and assets of individuals while at the same time allowing this information to be used in a constructive way for improved national security and improved service delivery.
 - Government is becoming more and more constitutionally liable for security, the protection of the UK as a whole, and the protection of individuals.

The Role of Infrastructure, Why does it Matter?

All of the drivers above place requirements at the heart of the service delivery mechanism, the IT and communications infrastructure. The infrastructure forms a key part of any organisation's business activity and can make the difference between a set of lack lustre services with low user confidence to a platform that enables the creation of service excellence and innovation. A highly effective service delivery platform will enable an organisation to drive forward and pioneer the use of high value IT and communication services that will have a transformational effect on performance, costs and user perception of services.

Key requirements for such a transformational Infrastructure include:

Availability—Services must be highly available 24 hours a day, seven days a week during normal conditions, under duress and during security attacks. Network maintenance, activities and security must have minimal impact on the availability of the network and must be delivered in a cost optimised way. It should be possible for an organisation to tailor the availability where and when it is needed.

Scalability—The infrastructure must provide value for money in the support of today's requirements while presenting a clear upgrade path for increases in capacity and features. Forklift upgrades of infrastructure are very rarely a viable option and so the network must provide enhanced flexibility and scalability to enable an organisation to quickly react to changing user demands and the introduction of new technology.

Security—Security is of vital importance and cannot be stressed enough. The infrastructure must protect the information that it carries from theft and deception. It must also be aware of security threats in its own right and of attempts to attack the infrastructure for malicious effect. The network must detect and react to threats as they happen (Day-Zero attack mitigation) to preserve the security of information, the security of the users and the integrity and availability of the solution. Security is not an option today; it must be built in from the start as an integral and pervasive part of the infrastructure. Within public sector, the governance of security is mandated by organisations such as CESG, NISCC and the Pan Government Accrider. Government created solutions that encourage the secure sharing of information such as Government Secure Intranet¹⁰ (GSI), Government Connect¹¹ and Police National Network⁹ (PNN) carry strict security accreditation guidelines that are enforceable via compliance with a Code of Connection. Infrastructure security is a key part of compliance with these Codes of Connection.

Multimedia and Convergence—The days of separate networks for each type of information (voice, video and data) are over. Today's solutions must provide an integrated approach to service delivery while respecting the differing requirements that each traffic flow and application may require. The infrastructure must provide converged support for different traffic types while preserving the required network characteristics for each. These characteristics must be preserved under high load, duress and even during an attack.

The convergence of voice, video and data onto one infrastructure solution presents a great opportunity to public sector if this can be achieved while retaining parity of service of a separate network approach. Some identified advantages are: reduction in cost, flexibility in operation, delivery of converged applications, virtualisation of resources and improved business continuity.

Open Standards—It is neither wise nor technically and commercially viable to establish an effective total infrastructure from a single source. Vendor choice and the use of open standards will allow each organisation to design and implement the optimum infrastructure for their requirements without that choice being dictated by the use of proprietary standards. This allows the organisation to build a solution using components from best of breed suppliers and to tailor the solution as they require both technically and from a cost perspective.

Mobility—Public sector organisations must provide choice to both their own users and the citizens they serve on how access to services is provided. Expectations are set by the private sector for a range of options including desktop, Internet, wireless and mobile devices. There is significant value to the public sector for a mirroring of these choices for government services. This not only provides choice to the user but allows the department to enable cost savings through the reduction of fixed assets.

The use of solutions that support mobility can have other benefits such as reduced cost of staff moves and changes, improved business continuity support and virtualisation of resources.

Security Accreditation—Government organisations such as CESG and NISCC set strict guidelines regarding the security classification of data and the protective measures that must be put in place to protect that information. They have an overall responsibility to ensure the National Security of the UK from an IT/communications perspective, to monitor changes in technology and threats and recommend suitable countermeasures. This results in guidelines, codes of connection and a need for regular auditing of security. The supporting infrastructure must demonstrate sufficient security robustness to allow the department to achieve accreditation and compliance against these defined standards.

Environmental—With a growing focus on environmental considerations and a need for all organisations to more carefully consider the environmental impact they make there is an obvious role that IT and communications can play. This includes the use of technologies such as broadband, voice/data convergence and video conferencing to develop a flexible workforce with a reduced need to travel to and from a central place of work.

The environment impact of the IT infrastructure itself is also to be considered, for example the heat and power requirements of the infrastructure and how this can be optimised.

Public sector organisations are encouraged to put in place wide ranging environmental impact policies and there is a growing set of central government targets that are to be met.

Extreme Networks—What Difference Can we Make?

Extreme Networks has become the best of breed supplier for infrastructure solutions by focussing on what we do best and delivering excellence in our chosen field of intelligent, converged infrastructure. Our absolute focus on innovation and our core strengths has enabled us to be recognised worldwide as a leader in our field.

Factors which we believe are essential to deliver a class leading infrastructure solution in this space are:

Focus on Excellence—By focussing on becoming the best vendor for intelligent, converged infrastructure, Extreme Networks has developed and marketed innovative, cost effective and industry leading solutions. We have avoided the trap of diversification, which can result in a confused position within the market, proprietary standards and vendor lock in to a solution that is not best of breed in any area. Our approach and excellence is supported by many industry awards and many glowing customer references.

Ultra High Availability—The ability of the infrastructure to offer outstanding levels of availability is essential in today's reliance on IT systems that form the heart of many private and public sector organisations. Key features such as built in five 9's availability, EAPS , CLEAR-Flow and ExtremeXOS™, our modular switch operating system (all described below) contribute to ensure that the network manager can have absolute confidence in the availability of the infrastructure during normal conditions, failures, maintenance, duress and when under attack.

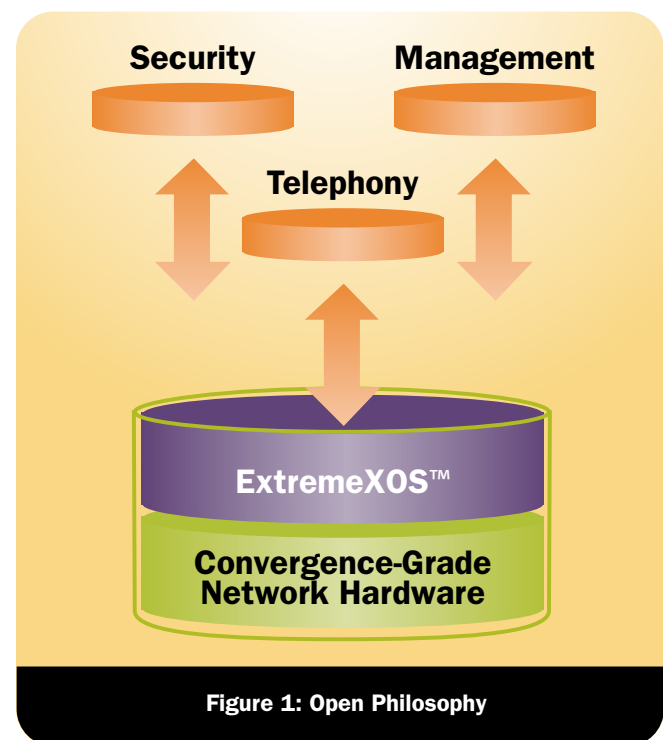
Predictable Performance—Many vendors offer near wire-speed performance, but while this is important, the full benefits of this can only be realised if that performance is available on a predictable basis even when the network is under duress. This may include during high load/duress, during a security attack, or when all features of the switch are enabled. Extreme Networks offers wire-speed switching performance which allows the network manager to offer clear SLAs to the user community with confidence that the infrastructure will manage and protect that performance.

This predicable performance is also be available across multiple data types that the infrastructure must support and provides specific characteristics for each e.g. voice, video, data and delay/latency sensitive data. By utilising multiple Quality of Service (QoS) queues within each device and multiple VLANs, solutions from Extreme Networks offer optimum solutions for a multiservice and multimedia environment.

Open Standards—For many network equipment providers, an open network is simply a standards compliant network. At Extreme Networks, we go beyond standards by

providing the industry's first open interfaces that can offer core network functionality as services to third-party solutions. This helps ensure that our solutions will inter-work with other vendor solutions quickly and easily and in many cases provide a better overall solution than when sourced from a single vendor.

We are able to introduce new features and utility device integration as required to strengthen our proposition. An example of this is the use of standard API/XML interfaces to enable close interworking with appliances for the control of services such as VoIP and enhanced security solutions (see Figure 1).



We continue to develop new industry partnerships to help ensure our customers can enjoy more choices and higher performance now and in the future without the lock in and restriction of choice that is associated with the use of proprietary standards.

ExtremeXOS—The Industry's First Modular Operating System

In 2003 Extreme Networks was the first switch vendor to introduce a modular Operating System (OS) for intelligent Infrastructure solutions. Today, ExtremeXOS is the class leading OS from Extreme Networks, which is used across our range of products. With modularity designed in from the start, individual processes within ExtremeXOS can be upgraded, restarted, reset and such without a need to bring down or reboot the switch (see Figure 2).

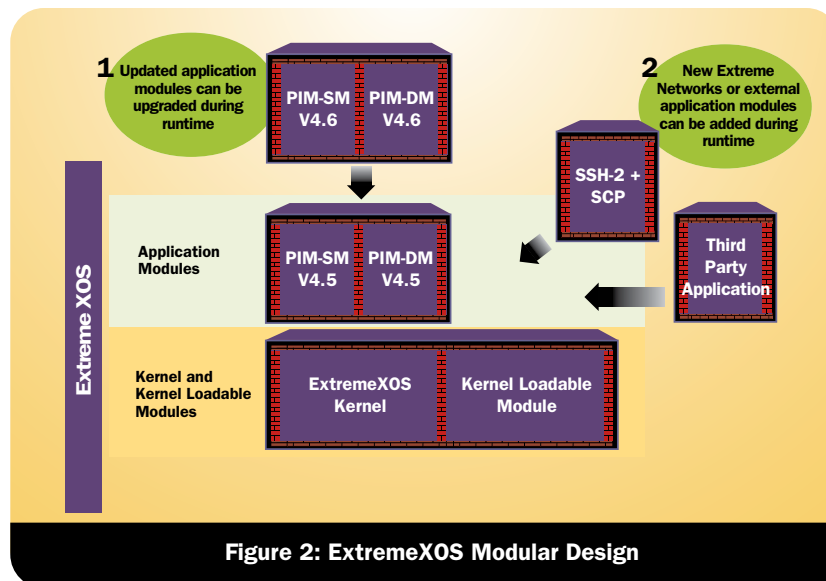


Figure 2: ExtremeXOS Modular Design

Other vendor solutions which rely on a monolithic OS require any upgrade or software issue (e.g. a security vulnerability) be resolved using a full OS restart. This results in downtime for the device and a reduction in the availability that can be offered from the infrastructure. These downtimes must be carefully planned by the network manager to ensure minimum effect on the users of the system. This has a major overhead associated with it in terms of resources needed to plan and execute any required restart.

With Extreme Networks, any issues concerning the OS can be managed in a much less invasive way giving the network manager flexibility in planning, the ability to react quicker to issues and less resource requirements to plan and implement.

Vulnerabilities are identified infrequently for Extreme Networks products and when they are, the modular ExtremeXOS solution allows corrective action to be deployed quickly and effectively.

Common Code

All Extreme Networks software within the OS has been developed from a common code tree, allowing upgrades and enhancements to be developed quickly and propagated across our solutions. This common code has the added benefit of creating a standard user interface for our solutions such that the user experience is identical across our product range. This results in less training required initially and less additional training is required as new features are added or the network is expanded during its lifetime.

Ethernet Automatic Protection Switching (EAPS)

A failure of a network route or a network component that causes a loss or degradation to the user services is a highly visible event that may undermine user confidence in the service and may in some cases be costly in terms of efficiency loss, highly mission-critical or even life threatening. While most

solutions in the market have the ability to re-route around a problem, Extreme Networks developed Ethernet Automatic Protection Switching (EAPS). This unique solution provides a re-route around a failure in less than 50ms and has now been defined as an international standard (RFC 3619). EAPS greatly reduces the propagation of delay and latency within the network solution during a failure condition. This means that:

- Voice calls can continue uninterrupted
- Video sessions can continue uninterrupted. Video and video conferencing are being used more and more within the public sector as part of effective business processes within a strategy to reduce the environmental impact of an organisation and for critical use within the judicial process. Therefore, the video solution has a mandate to provide a service that gives parity with face-to-face meetings in terms of effectiveness and usability. If this cannot be achieved then the solutions will quickly fall into disuse and the benefits of video will not be realised. The users will not use a solution that is not highly available and does not provide a high quality experience.
- Data applications can recover quickly and should not suffer any degradation in service.
- Applications that are highly sensitive to delay and latency such as thin clients (e.g. Citrix) will suffer little to no degradation. This is a significant benefit to public sector with the increased prevalence of thin client based solutions and indeed the recent recommendations from the CIO council that thin client architectures are the preferred strategy for application support⁷. The effects of a thin client session interruption can mean for example, the loss of data when filling in an online form, loss of data when editing a document or composing an email, termination of an interactive session with another user(s). It is in this area where a network failure can have a considerable impact on the user experience, perception of the service delivery infrastructure and efficiency.

The Extreme Networks EAPS solution provides protection for the network and helps ensure availability and service consistency for the most demanding applications. This allows organisations and departments to deploy delay/latency sensitive applications with absolute confidence that the network will help protect those applications from failure.

CLEAR-Flow

It remains a challenge to understand exactly how any network is behaving and to tune the network to better serve the needs of the organization. Adaptive management techniques in the networking space are starting to emerge, making possible the rapid recognition of changing network behavior, and automatically constructing and applying changes to the network configuration to ensure maximum application performance

while at the same time hardening the network against the outbreak of viruses and other threats. For these solutions to be feasible there is a pressing need for improved visibility into network behavior and for proactive identification of network anomalies.

To this end, Extreme Networks has introduced CLEAR-Flow providing Insight and Control over the network. CLEAR-Flow, which stands for Continuous Learning Examination Action and Reporting of Flows, makes it possible to track and measure specific application flows on the network, and to proactively identify anomalies in user, host, and application behavior. CLEAR-Flow provides a level of security and reliability (see Figure 3) previously unavailable for large networks.

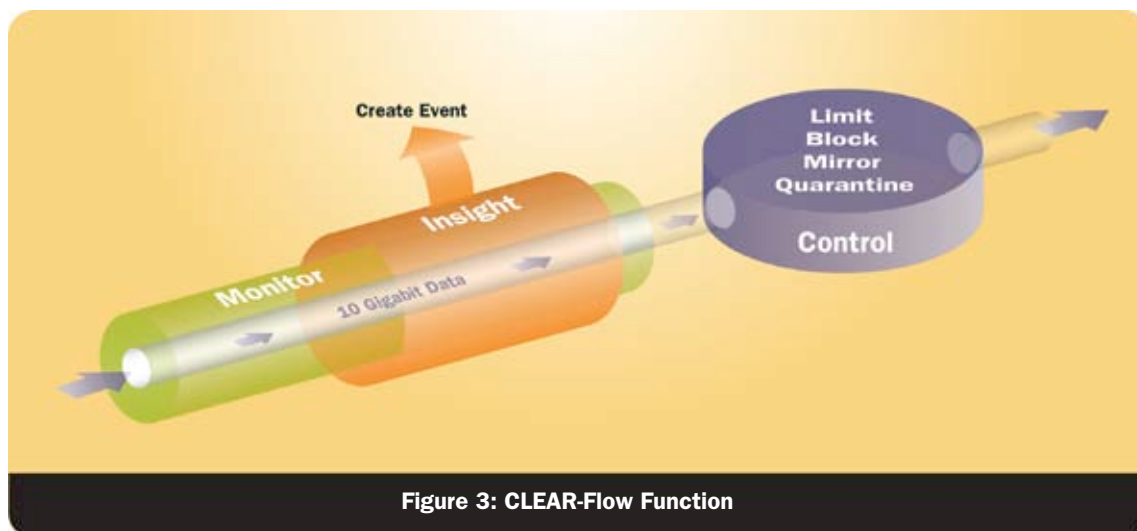


Figure 3: CLEAR-Flow Function

CLEAR-Flow is able to autonomously react to conditions that it detects within the data plane of the infrastructure using pre defined guidelines set by the network manager. These reactions can range from rate limiting on a port, mirroring of the port to denial of service on a particular port. The conditions and reactions are configured simply using four available methods.

1. Via the Extreme Networks Universal Port Manager (UPM). This is a graphical tool that enables the simple creation and management of rules that govern the management of identified network events.
2. Using pre defined rule sets defined by Extreme Networks for common network conditions.
3. Via the CLI-based user interface.
4. Engagement with Extreme Networks Professional Service who can assist with the analysis, definition and implementation of a set of rules tailored to your organisation.

Pervasive and Total Security

Security has become a top three networking concern. While the security and network vendors have responded well with hardware and software solutions, Extreme Networks has recognized that the network interior continues to be vulnerable to attack and abuse.

External threats such as hackers and internet carried viruses can be mitigated by the use of firewalls. However, the growing prevalence of mobile network devices such as laptop PCs, PDAs, Wireless LAN and USB sticks mean that security threats such as viruses, worms, and trojans can enter the interior of the network from an infected device and begin rapid propagation. Systems exist and are widely deployed that allow these threats to be partially mitigated. However many of these solutions make use of inline security appliances such as internal firewalls, and Intrusion Detection Systems (IDS) that are deployed throughout the network estate. This can result in solutions that are difficult to administer with in-line resources that can have a negative effect on performance and availability. Plus, these appliances can only work where they exist and can only work with the traffic that actually traverses them, so it is highly likely that overlay solutions such as this result in networks with security gaps that can be exploited by malicious users and/or hackers.

Extreme Networks offer an alternative and complementary approach to these existing solutions by implementing security at the heart of the network, i.e. within the data plane. This results in a pervasive security solution that offers minimal effect on throughput and availability, and a solution that exists at all points within the network infrastructure. The unique modular OS from Extreme Networks, ExtremeXOS, in association with CLEAR-Flow offer deep packet inspection at

wire-speed. This is used to detect potential security issues and autonomously react at a network level.

Additional security can be added by the deployment of Sentriant™, a virtual security appliance. Sentriant reacts with ExtremeXOS and CLEAR-Flow to provide more in depth analysis of potential security issues and uses this analysis to instruct the network on the appropriate mitigating actions (see Figure 4).

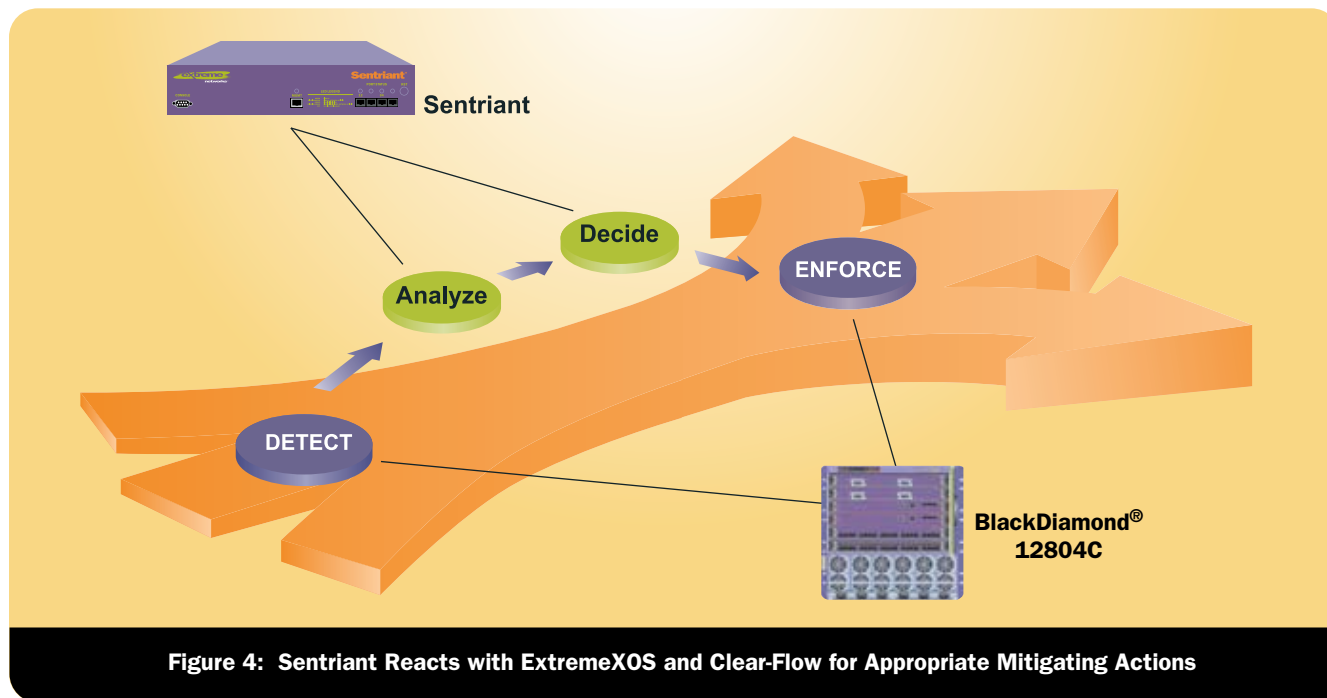


Figure 4: Sentriant Reacts with ExtremeXOS and Clear-Flow for Appropriate Mitigating Actions

Sentriant AG is the next generation in endpoint security software for verifying that endpoint devices meet security policy requirements and do not introduce worms, trojans or

spyware into an organization's network. Sentriant AG tests each endpoint and verifies the endpoint device meets the organization's security requirements before allowing access to the network (see Figures 5 and 6).

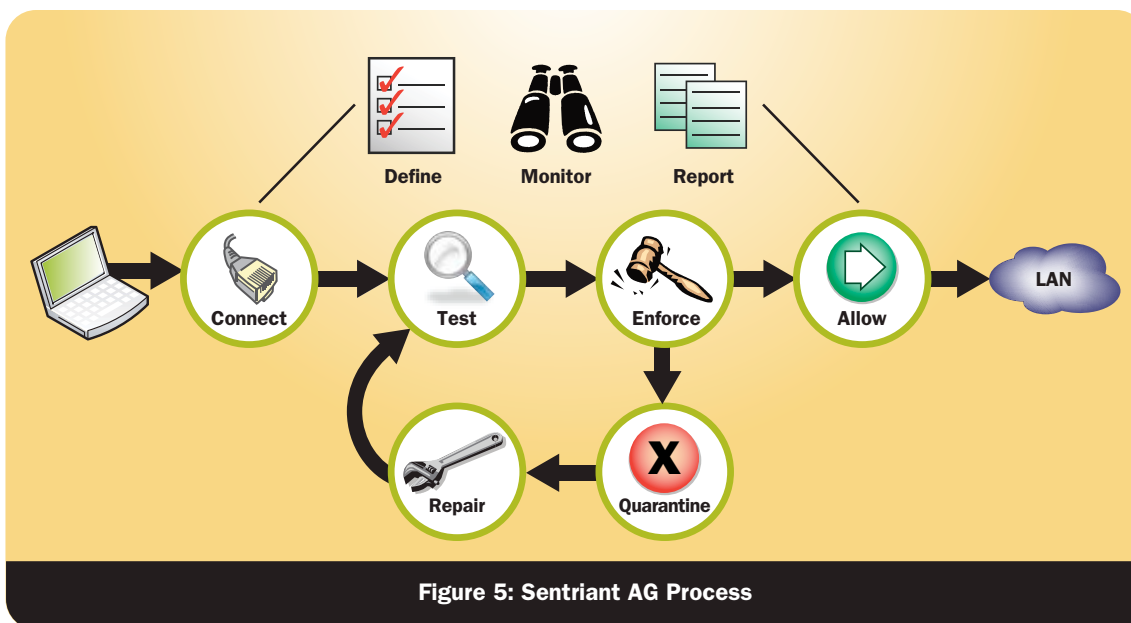
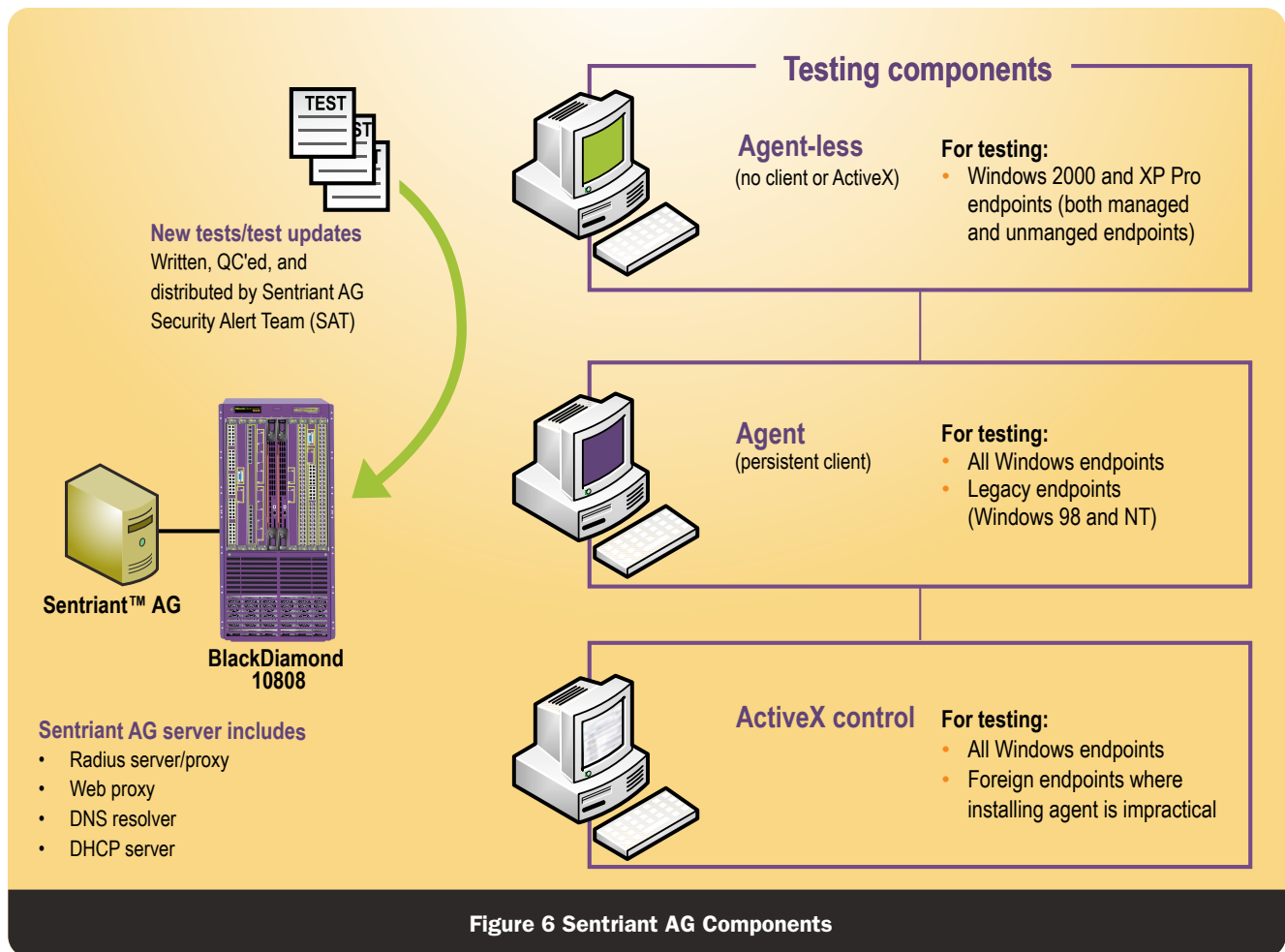


Figure 5: Sentriant AG Process



This results in unique solutions that offer Day-Zero and other rapid propagating threats attack mitigation that are pervasive across all points in the infrastructure. This reduces the resources, costs and threats that are associated with overlay solutions for security and allows the network manager to have absolute confidence that the infrastructure is helping protecting itself from attack using industry leading, highly intelligent security solutions.

Wireless Solutions

Today's organizations know that mobility drives productivity, cost savings, and greater customer satisfaction. Mission-critical wireless applications are being deployed in hospitals, retail environments, educational facilities, as well as in corporate conference room and offices. Wireless devices range from laptops to latency-sensitive Voice over Wireless LAN (VoWLAN) handsets. Each type of device provides installation, performance, security, and management challenges. To compound the challenge, resource-constrained IT departments do not have the luxury to hire dedicated resources for wireless support.

Extreme Networks wireless solutions offer installation and operational simplicity, highly-scalable performance, and essential wireless and wired security. These solutions are designed to remove the complexity from wireless such as Radio Frequency (RF) eccentricities, multiple domain management, QoS and security. Installation is easy and enterprise-grade reliability helps ensure that IT managers do not get wireless support calls in the middle of the night.

Extreme Networks has the advantage of being able to design, deploy, and manage an integrated wired and wireless solution—using its complete line of award winning switches with comprehensive security, QoS, and management (see Figure 7). This helps provide simplicity throughout all phases of your wireless solution lifecycle, and offers a lower total cost of ownership.

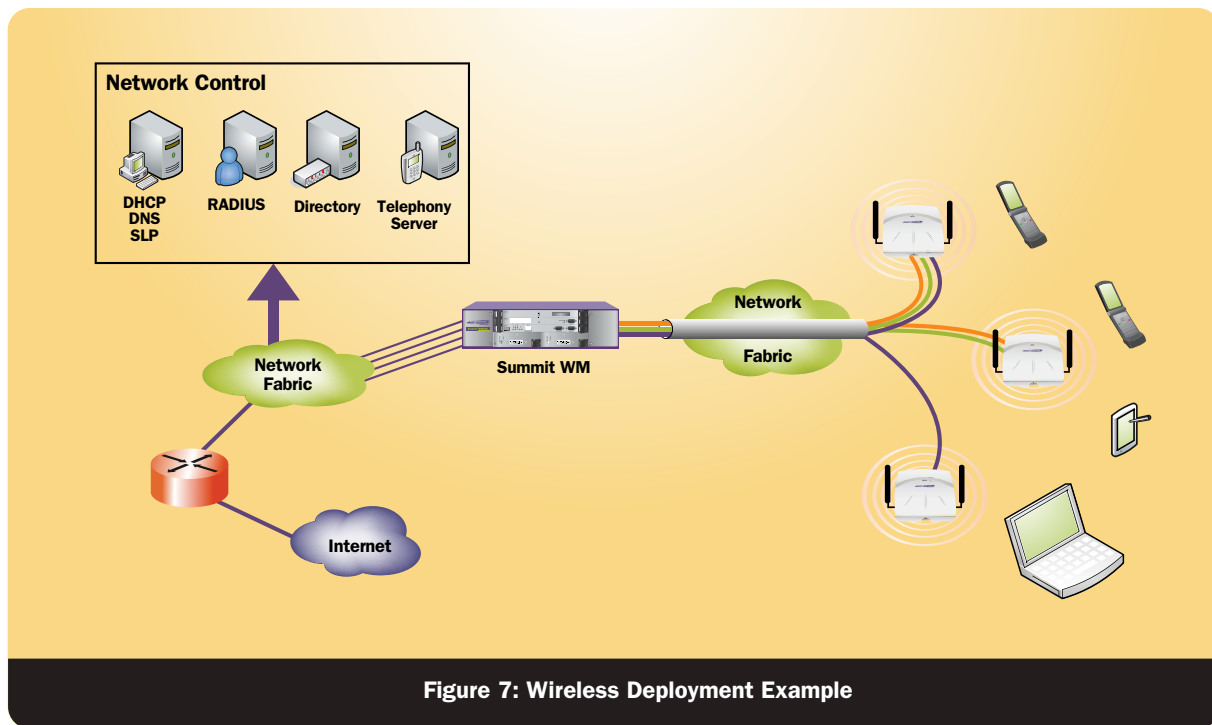


Figure 7: Wireless Deployment Example

Mobility

Extreme Networks is leading the industry in the use of solutions for mobility within an organisation. This would include for example the virtualisation of resources where access to services is independent of a user's location, the ability to quickly and securely add users to the network, and mobility as an enabler for effective business continuity solutions.

The Extreme Networks Universal Port Manager and the VoIP Handset provisioning module allow the network to automatically detect when IP phones (from multiple vendors) connect to the network and then apply a default profile to the edge port to which the phones are attached. In this way there is no need for network manager intervention at the time of entry to securely provide service to a new device when it is connected. This allows users to automatically connect to the network at any point to access their services thereby removing any dependency on user location.

Convergence

Extreme Networks recognises the inherent value of a converged network solution to the public sector where voice, video, data and other services are supported by a common underlying infrastructure (IP). This includes:

- Reduced cost of infrastructure
- Improved staff mobility
- Increase in flexible working
- Virtualisation of resources

- Introduction of new, converged applications
- Increased use of remote/home working.
- Improved business continuity.

Extreme Networks is able to offer industry-leading convergence solutions using relationship and solution integration with the leading supplier of converged solutions, Avaya®. Extreme Networks and Avaya are engaged in a strategic alliance to jointly develop and provide converged communications solutions. This alliance unifies Avaya's global market leadership in IP Telephony and related applications with Extreme Networks expertise and focus in a high-performance, secure network infrastructure.

The use of open standards and high performance, secure, available infrastructure enables a solution built using Extreme Networks to offer exceptional support to converged applications delivered by other third-party suppliers including suppliers of VoIP, IP Telephony and video-based solutions.

Security Accreditation

Extreme Networks solutions are used by many of the world's leading public sector organisations including the security services. Extreme Networks Security Professional Services are able to offer advice and assistance with compliance against specific security requirements. This includes advice and assistance with generic security considerations to specific accreditation of an Infrastructure as part of a specific project. This includes compliance with UK HM Government standards.

