GOVERNMENT SOLUTION BRIEF

Internet of Things Smart – Government Solution

The Internet of Things (IoT) is ushering in an era of smart cities and smart government. The benefits of smart government include reduced operating costs, increased responsiveness, improved sustainability, higher efficiency, constantly-available process data, and greater citizen satisfaction. In the consumer world, people have become familiar with smart consumer devices that enable interaction with the smart home via mobile phone. As this moves into government and commercial realms, significant new considerations must be managed. Along with flexibility, access to rich data, and entirely-new applications and configurations, come elevated concerns about security, safety, privacy, reliability, and manageability.

One important aspect of smart government is the use of IoT to efficiently control resources used for lighting, heating, and cooling. Smart buildings optimize energy usage via hundreds of IoT sensors and controls. All of these devices must be easily on-boarded to the network and protected against unauthorized usage. Smart buildings often house sensitive research gear, medical devices, and thousands of analytical instruments that require strictly-controlled and monitored network access.

With the advent of thousands of IoT network devices, government networks have become more complex, posing a growing challenge for the IT staff supporting them. Network managers are reassessing their approach to smart device support and how to best apply business intelligence to the network. IoT devices can range from smart LED street lights and parking meters, to complex analytical devices. In the government medical research field, devices joining the Internet of Things include Wi-Fi enabled IV pumps, blood gas analyzers, telemetry systems, mobile x-ray machines, ultrasound units, hemodialysis devices and glucose meters. These all require the highest reliability and bandwidth, as well as security to control and analytics to monitor all network activity.

Smart cities are on the rise due to the proliferation of low cost Internet-connected devices that make it easy to monitor and control municipal functions like parking, traffic, lighting, security, and environmental control. Video can be readily captured across the city. Insightful and actionable data on the workings of government are available in real time, delivered via smart phone. Smart cities are able to reduce expenses by optimizing energy consumption. Sensors for parking, traffic, lighting, environmental control, potholes, and transportation make possible new services involving infrastructure, buildings, and public transportation.

ELEMENTS OF SMART GOVERNMENT

The Internet of Things and the proliferation of smart phone users are two of the driving forces behind smart government. Industrialized wireless motion and flow sensors, small durable video cameras, air and water quality monitors, temperature and noise monitors, and Wi-Fi based instrumentation are all readily available to provide inputs for the smart city. On the control side, digitally-controlled LED lighting, water flow control, remotely-controlled traffic lights, heating and cooling, pedestrian displays, and power distribution are all important for implementing smart government. Highly-reliable network infrastructure is what enables all of the smart government technologies to work together flawlessly.

IoT sensors are capable of continually generating big data to better understand how a building or city functions. The resource flows are available to optimize efficiency and minimize costs. Storing and analyzing the data requires local or cloud-based database systems and computer analysis engines. Depending on whether the data is intended for public or private consumption, the results may be shared with authorized individuals via smart phone apps, presented to pedestrians via outdoor digital displays or viewed by government analysts on their computer displays.

Critical Technology Issues for IoT and Government

INSUFFICIENT CONNECTIVITY AND BANDWIDTH FOR INTERNET OF THINGS DEVICES AND CONTROLLERS

Internet of Things sensors, devices, and controllers require continuous connections to the network. Sensors may be located in difficult to reach compartments and in portable equipment and often tend to be mobile. One of the major IoT benefits is that these devices and sensors provide an enormous amount of data that can be analyzed and turned into actionable information. The types of IoT data include video, audio, location tracking, temperature, pressure, motion, and status. This presents the challenge of providing adequate wireless and wired bandwidth to handle the streams of data and to rapidly respond as necessary. To operate smoothly, there can be no bottlenecks from the Wi-Fi access points, back through the wired switches, and all the way to the broadband Internet connection and the data center. These connections must be highly available or fault tolerant to insure uninterrupted service.

RISK TO SECURITY AND PRIVACY

In the midst of the diversity of devices on the network, data security and privacy must be fully maintained. While the network must be capable of connecting all devices, it must also be very selective in doing so. Authorized devices should be expeditiously and effortlessly on boarded, while unauthorized devices must be prevented from gaining access to the network. The best way to implement this is with a defined policy as to which devices, users, and apps can access the network resources from defined locations at specified times of day. This policy needs to be implemented consistently across the network. Firewalls prevent access from outside sources and web filters prevent visits to malicious sites that can damage the network. The smooth implementation of network policy across all resources requires integration with firewalls and web filters. The network must be capable of both controlling and monitoring all devices and network activity. Unapproved applications and rogue devices pose a constant risk to the network. If a rogue device were to appear on the network, it could either enable unauthorized access or interfere with other devices. A means to monitor all devices and applications that operate across the network is vital.

With new devices coming and going on the network, it can be a challenge to provide easy onboarding of both government-owned and guest devices, and to authorize them to access appropriate resources. Some devices should be restricted to network access only from designated locations, while it is important for other devices to maintain network access from all locations across the network.

LACK OF IOT DEVICE CONTROLS — VISIBILITY INTO NETWORK DATA AND IOT DEVICES

Smart device adoption really means the growth of Machine-to-Machine (M2M) and Machine-to-People (M2P) automations. With this workflow evolution, IT must proactively monitor and manage systems that include sensors, assets, analytical and medical instruments, smart devices, and telemetry systems that can require constant communication with core applications.

Visibility into communications, locations, performance, and patterns of activity of all network-based IoT devices, including medical and lab instrumentation, is important for insuring the security and safety of the government functions. This is also vital for optimizing the infrastructure and for both short- and long-term planning for device automation and support. Network analytics equip IT to better understand how well new systems and devices are being adopted. The analytics bring big data to help understand the health and usage of the smart government infrastructure.

UNKNOWN SECURITY RISKS

A constant risk to the network, and ultimately the government agency, are unauthorized users, unapproved applications, and rogue devices that may operate on the network and either permit unauthorized access or interfere with other devices. Monitoring all users, applications, and devices that operate across the network is vital. Insight is needed to prevent security breaches and hacks that could compromise government systems, citizen and employee data, infrastructure technology, and nationwide sensors. ExtremeControl automates onboarding of devices and applies rule-based policies across the agency's entire wired and wireless infrastructure.

Without proper precautions, one instrument or device could be incorrectly configured for DHCP services which can disable an entire device VLAN. A means to monitor all devices and applications that operate across the network is vital. ExtremeControl automates onboarding of devices and applies rule-based policies across the agency's entire wired and wireless infrastructure.

Extreme Solutions

Extreme's network policy-based management framework has been proven to reduce IT manpower requirements by up to 90% for device-heavy networks, compared with the industry average. Extreme Networks delivers an industry-unique solution that does not require the explicit use of VLANs and associated architectures. For non-Extreme-based infrastructure, the implementation and enforcement of capabilities like of QoS and 802.1q are reliant upon the layer 2 infrastructure and its underlying architecture (often VLANs, subnets, and ACLs). Extreme provides a set of software tools and operating systems to control policy from a single node to every device enterprise-wide. An analytics platform correlates usage with network performance and the intelligent control plane adapts in real-time. Extreme has extended control beyond the physical network to your cloud infrastructure, optimizing your network and applications regardless of where they reside.

The solution described below provides government departments and agencies with the network infrastructure necessary to insure reliable implementation of the Internet of Things and smart government capabilities across the network. This includes efficient onboarding and management of both government-owned and personal devices on the network, as well as adequate data bandwidth to accommodate the data streams involved. The entire network can be managed from a single window. That window can set policy for all devices to determine which resources each device can access across the network. The policy is based on a range of parameters that determine access rights based on user, device type, location, time of day, and 40 more attributes. Our open, standards-based, and comprehensive SDN enables simple integration with third party technology such as web filters and firewalls. Extreme Networks' software-driven networking solutions give every user a better experience, every community a better connection, and every IT organization a better partner.

AROUND-THE-CLOCK SUPPORT

The government never closes and neither does Extreme Networks' 100% in-sourced Global Technical Access Center (GTAC). Our 24/7 support ensures that all questions are answered promptly to keep the network functioning at all times. We are proud that our support team achieves 98% first call resolution. Extreme Networks is the only company in the industry that takes an architectural approach to bringing products to market from R&D to product release. As a result, all of our network products from wireless to wired are managed by a single ExtremeControl console for easy administration by resource-constrained IT teams.

To learn more, visit our solutions web pages — Public Sector, Higher Education, K-12 and Primary/Secondary, and Healthcare.

Public Sector Solution Guides

Internet of Things Network Campus Solution
IoT and Medical Device Safety for Healthcare
BYOD Campus Solution

REQUIRED CAPABILITIES	RECOMMENDED SOLUTION	HOW WE DO IT BETTER
Pervasive Wi-Fi Connectivity and Bandwidth	• ExtremeWireless™ Access Points and Controllers • AP Licenses, Radar Licenses • 2x V2110 Virtualized Controller for High-Availability (for up to 1050 APs)	• Highly-scalable • Highly-available • Seamless and secure • Easily-managed Wi-Fi connectivity
Wired Edge and Backhaul	• ExtremeSwitching™	• High-performance wired backhaul, cross-platform stacking, embedded application controls. PoE+
Device Onboarding and Network Access Control, Monitoring of Network and All Devices, Secure Guest Access	• Extreme Management Center • Extreme Access Control	• Consistent device policy based on over 40 attributes centrally implemented, enforced end-to-end • Simple device onboarding, 100% fidelity of all IP assets • Internet filter and firewall integration, MDM integration
Device and Application Usage Visibility and Insight	• ExtremeAnalytics™	• Visibility into applications and websites being accessed with user experience measurements from every part of the network
24/7 Operational Support	• Maintainance • Training • Professional Services	• Support Center (GTAC) provides technical support 24 hours day, 365 days a year • Extreme Networks SupportNet offerings let you choose the exact level of service ideal for your organization

Extreme®
Connect Beyond the Network

ValuTrack
TECHNOLOGY SOLUTIONS

https://valutrack.com/contact/ / Phone: 866-825-8382