Extreme™
Customer-Driven Networking

Solution Brief

Extreme Manufacturing Solutions

Transforming the Factory Floor

Introduction

Manufacturers today are confronted by three related challenges: expanding their business in a highly competitive global marketplace, adapting production resources to fast-changing customer requirements, and reducing operating costs through increased efficiency, automation, and transparency.

Concurrent with these business challenges are technological issues impacting nearly every stage of the manufacturing process, from the exponential growth of data-driven sensors and mobile devices in plant operations, to the convergence of traditionally separate Operations and IT systems, to increasingly stringent compliance requirements for data security, intellectual property, and asset tracking.

Despite these imperatives, 54% of U.S. manufacturers say they lack a unified view of what's happening on the plant floor (Aberdeen Group). Largely as a result of legacy control systems that are more expensive to maintain and operate with each passing quarter, IDC notes that manufacturers are increasingly investing in "standardizing production processes across their network of factories to create better visibility, coordination, and orchestration."

Critical Technology Issues for Factory Floor Transformation

Legacy Networks Compromise Business Perforance

An IndustryWeek study found that manufacturers average 3.6 application downtime incidents in a year, with each incident costing anywhere from $10,764 to $32,500, depending on the size of the company. CA Technologies reported that the average manufacturing revenue loss due to general IT downtime is $196,000 per company each year. In addition to continuity challenges, these legacy factory networks also create security vulnerabilities, with proprietary hardware and software incorporating minimal consideration of extended connectivity and security features in their original designs. According to McAfee, "Industrial networks top the list of systems most vulnerable to cyber-security issues," and as embedded sensors and mobile applications are increasingly integrated with these systems, they provide an easy target for gaining access to manufacturing operations, plant assets, and business applications.

Technology Migrations Impede Execution

Factory floor managers migrating these legacy networks from proprietary hardware-driven architectures to standards-based designs are challenged to manage these transitions without either disrupting production or sacrificing agility to support dynamic customer needs. Incremental deployments of standards-based technologies, from high speed wireless architectures that enable real-time mobileaccess to production designs and speed remote management and maintenance, to centralized wired and wireless management applications that leverage policies to support production flows, can help streamline these factory floor transitions and provide new capabilities to support emerging applications like mobility, cloud, and virtualization across both plant and factory operations.

Security Systems Inadequate Against Emerging Threats

With a focus on streamlining the entire production chain, manufacturers are increasingly federating their operations systems with suppliers, partners, and vendors to increase transparency and provide real-time and historical views into factory workflows and assets. While this introduces new efficiencies through increased automation and expanded information sharing, these extended ecosystems also create security vulnerabilities that if breached can result in compromised customer data and intellectual property, and potentially severe impacts to business continuity.

Traditional appliance-based security approaches focused on features such as content filtering and anti-virus are inadequate for protecting the network against multiple threats, especially those that may originate from inside the network. Manufacturers increasingly require both granular and broad-based approaches to ensuring data security and effectively detecting, preventing, and mitigate evolving security threats to intellectual capital, customer information, production, and assets, from outside and within their extended production networks.

Required Capabilities	Recommended Solution	How We Do It Better
Stabilization of existing wired and wireless infrastructure	• Extreme Switching	Single pane of glass management system provides centralized visibility and end-to-end granular control of the unified network
Pervasive Wi-Fi connectivity and bandwidth for clinician workflow and communications	• Extreme Wireless • Extreme Switching • Extreme Routing	Hybrid deployment architectures (bridged at AP or controller), single sign-on to simplify management. Application and device based policy controls. Embedded flow-based ASIC flow sensor technology per port, 3M flows/s collection capability
Automation of device onboarding with audit controls	• ExtremeControl • Extreme Surge	Automated, secure, and fast provisioning and control of devices on the wired/wireless network
Critical device and agentless application	• Extreme Analytics	Agentless performance and security monitoring of device communications
Staff supporting and consulting to provide best in breed IT service delivery	• Professional Services	Extreme services including onsite customer consulting, design, and implementation services as well as comprehensive training curriculum
Determining unknown security risks and meeting government compliance standards	• Extreme Management Center • Information Governance Engine	Automatically assesses network configuration compliance with HIPAA, PCI, and GDPR. Eliminates manually validating the compliance of network device configurations across your network
Simplified and agile network infrastructure	• Fabric Connect	Leveraging simplicity to create agility, this empowers rapid and seamless service delivery
24/7 Operational Support	• Maintenance	Support Center (GTAC) provides technical support 24 hours day, 365 days a year

Extreme™
Customer-Driven Networking

http://www.extremenetworks.com/contact / Phone +1-408-579-2800