BUILDING YOUR CYBER SECURITY STRATEGY IN INDUSTRY 4.0

WatchGuard®

TABLE OF CONTENTS

In the booming age of Industry 4.0 (the fourth and current industrial revolution), manufacturers are replacing legacy shop-floor equipment with "smart" ways and means – enabling safer, more efficient factories with greater Overall Equipment Effectiveness (OEE.) Enterprising new Industrial Internet of Things (IIoT) technologies like construction robotics and smart assembly lines are at once enabling manufacturers to remain competitive while placing them squarely in the hacker's crosshairs, with attack vectors just as vulnerable as those seen by popular targets like retail.

The challenge is worldwide – but in the UK nearly half of the manufacturers have experienced a cyber attack.[2] In the United States, one widely felt attack occurred when malware hobbled the production platforms for several major newspapers across the country.[3] Another incident in Germany found a hacker infiltrating a steel mill by way of phishing email. In this instance, the attacker was able to access the plant's network, causing multiple components to fail and lose control, ultimately causing permanent damage to the plant's smelter.[4]

IN FACT

The manufacturing sector is now one of the most hacked industries, second only to healthcare.[1]

As cyber threats continue to plague manufacturers regardless of size or location, businesses are now forced to evaluate potential consequences that follow the implementation of new technologies, and the precedence for investing in security.

FIRST (1784)
Mechanical production, railroads and steam power

SECOND (1870)
Mass production, electrical power and the advent of the assembly line

THIRD (1969)
Automated production, electronics and computers

FOURTH (now)
Artificial intelligence, big data, robotics and more to come

IIoT is the dynamic new hire on many factory floors that is quickly proving to be an asset, brandishing a resume that holds "Quality Assurance" and "Improved Efficiency" among many other attractive skills. With IIoT, technologies like inventory monitoring, connected robotics, and asset location involve sensors attached to a physical device. The sensors collect data to drive artificial intelligence and predictive analytics, changing the way products are made and delivered and doing it with increased OEE, better safety for their human operators, and significant cost savings. In fact, by 2020 the number of connected things is expected to reach 50 billion, returning an anticipated $19 trillion in cost-savings and profits.[5]

For all its benefits however, a closer look reveals that IIoT shares the same pitfalls that have plagued the Internet of Things for so long; products packaged with bombastic innovation and – in very fine print – a cyber security footnote ("Security Sold Separately"). These devices are typically produced and purchased on the basis of cost – rather than cyber security – offering compelling new vectors of attack for cyber criminals.
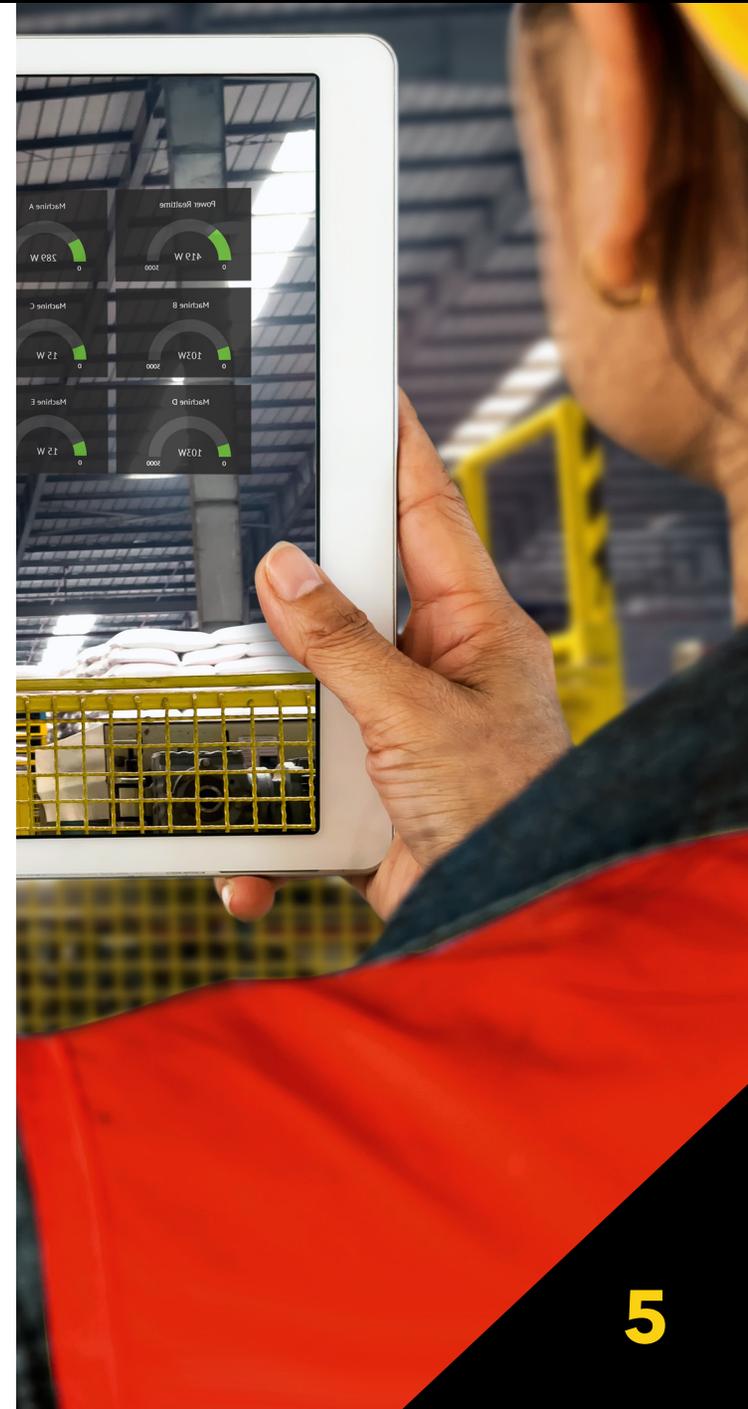
IIoT: DANGEROUS OPERATING CONDITIONS?

Solutions

Cloud-Managed Secure Wi-Fi

WatchGuard Cloud-managed access points have built-in Wireless Intrusion Prevention System (WIPS), extending and enhancing our security to your facilities' wireless IoT devices. Leveraging patented Marker Packet technology, WatchGuard provides the most reliable WIPS in the industry, and with the lowest rate of false positives. Better yet? The AP327X is IP67 rated so that it can withstand even the most extreme environments – rain, snow, dust, you name it.

IIoT Segmentation

Partitioning your network into segments (IIoT, Guest Wi-Fi, Corporate, etc.) helps to isolate IIoT devices from mainstream equipment, and in doing so limits the disruptive spread of an attack, should one occur. Network segmentation can easily be accomplished with a UTM firewall like WatchGuard's Firebox T35-R. A high-performance, ruggedized security appliance for protecting networks in harsh environments, the T35-R is able to withstand dust, moisture, and extreme temperatures.

"We wanted to implement something that would not only protect our business from threats, but would also instill confidence to those within our supply chain.

"Our WatchGuard appliances don't require much upkeep or maintenance – they've worked effectively since they were installed, and that's what we need for the business."

-John Bogle, IT Manager, Sunray Engineering

Shadow IT
is the use of hardware or software within a business – without the acknowledgement of the IT department – and can be as seemingly innocuous as sharing files with a colleague through a personal file-hosting account instead of the company-approved platform. In these instances, it's often an employee's personal familiarity with an unapproved solution that leads them to use it, or perhaps it allows them to work faster and produce better results.

Shadow IT is a growing concern for many manufacturers, as operations team purchase and utilize connected equipment without the knowledge of a central IT department, leading to network strain and the risk of cyber attacks. IT teams are unable to verify the security of software or appliances they don't know exist within their network, nor are they able to manage them effectively and run any necessary updates and patches.

How prevalent is this cyber security threat today? A recent survey found that **businesses have between 17 to 20 TIMES more Cloud applications running than the IT department estimated.** [6]
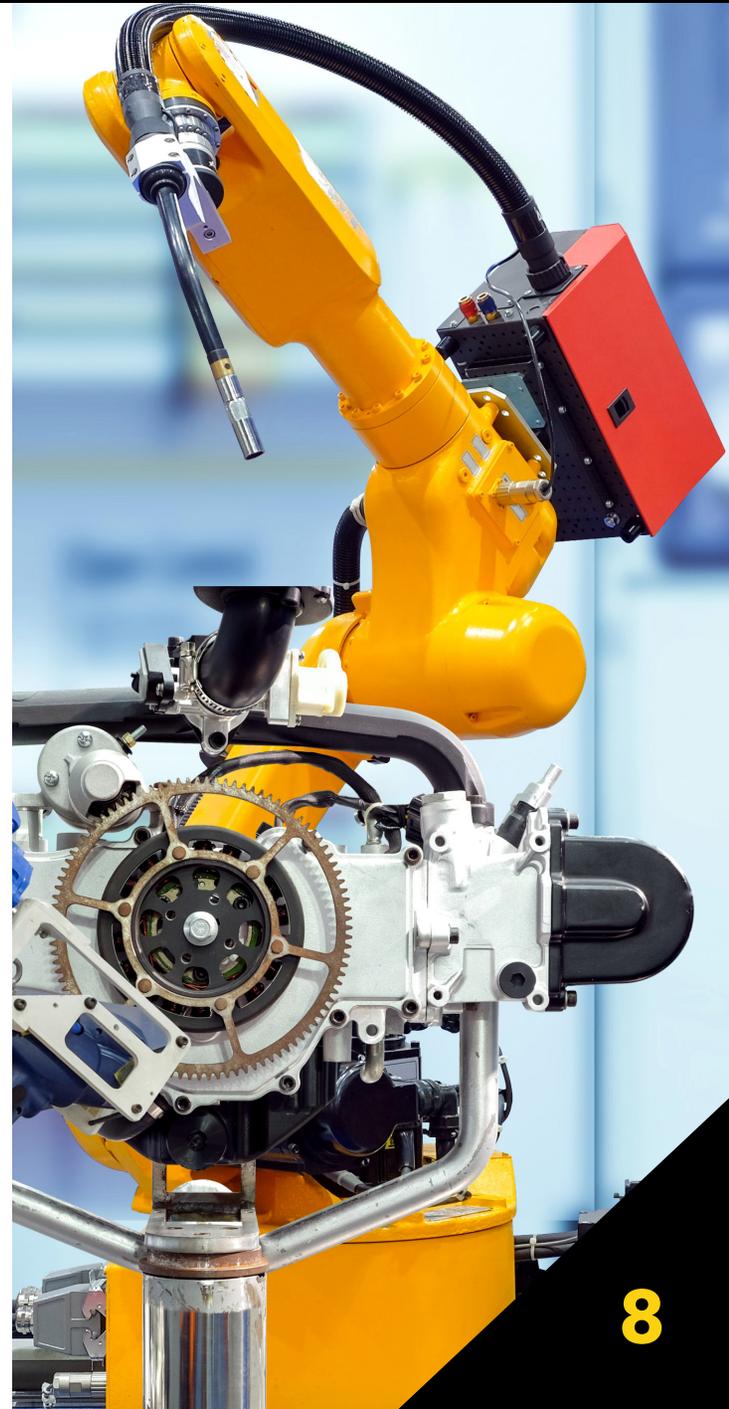
Solutions

Unauthorized Device Visibility

You cannot secure a network that you do not understand. WatchGuard's Network Discovery service allows IT staff to map out the network behind their firewall with all known devices using data from a nmap scan, DHCP fingerprinting, HTTP header information, or the WatchGuard FireClient app. Assets in the network are identified by icons and represented with the below information, allowing new or unfamiliar devices to immediately stand out when they appear without this data, and enabling IT to take corrective action.

- Host Name
- IP Address
- MAC Address
- Type of device – iOS, Android, MAC, Windows, etc.
- Open ports – and protocols that may be running

9
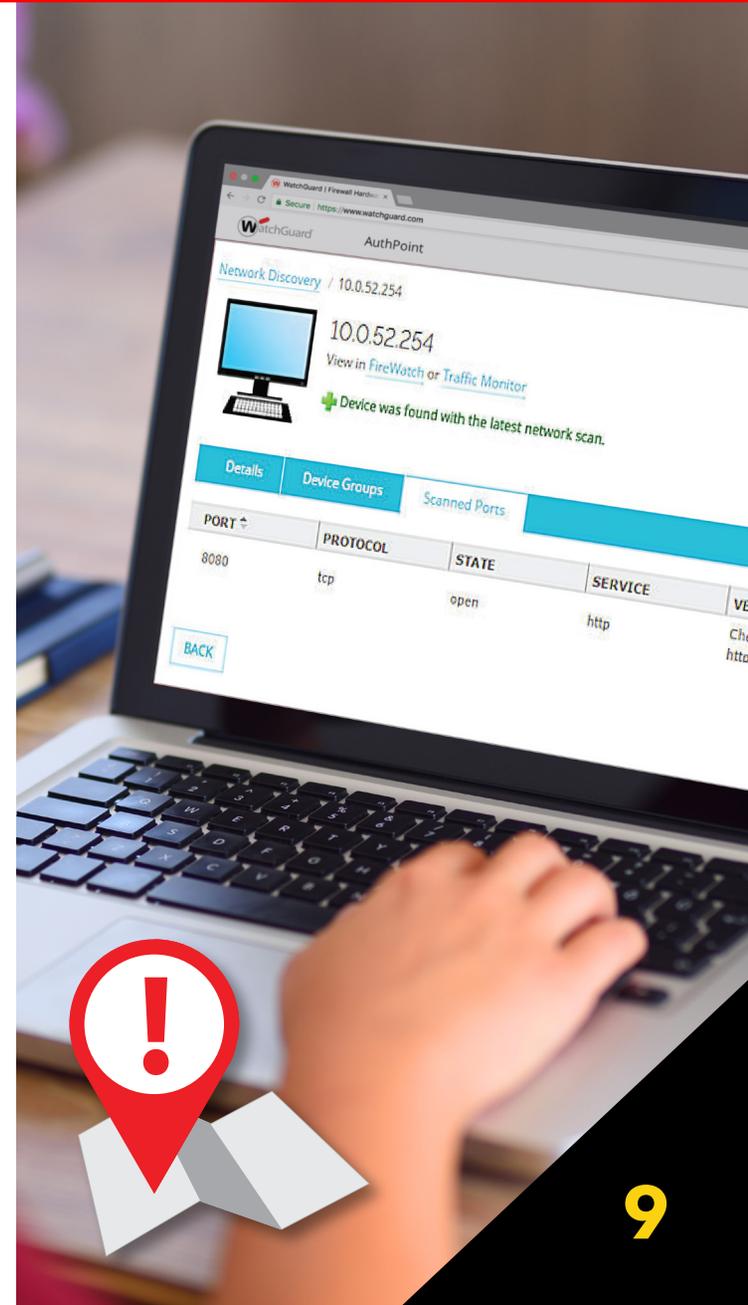
The theft of IP (intellectual property) has been a long-standing menace within the manufacturing sector, and unfortunately shows no signs of losing steam – **a staggering 47% of breaches that take place within a manufacturing business involve the theft of IP.**[7] This data robbery could include anything from product proposals to proprietary manufacturing processes, all of which represents tempting fodder for competitors and ransomware-armed hackers alike, potentially leading to loss revenue and customers. **One US-based company that manufactures glues and epoxies has seen its products counterfeited by way of IP theft, resulting in losses to the tune of $15 million a year.** [8]
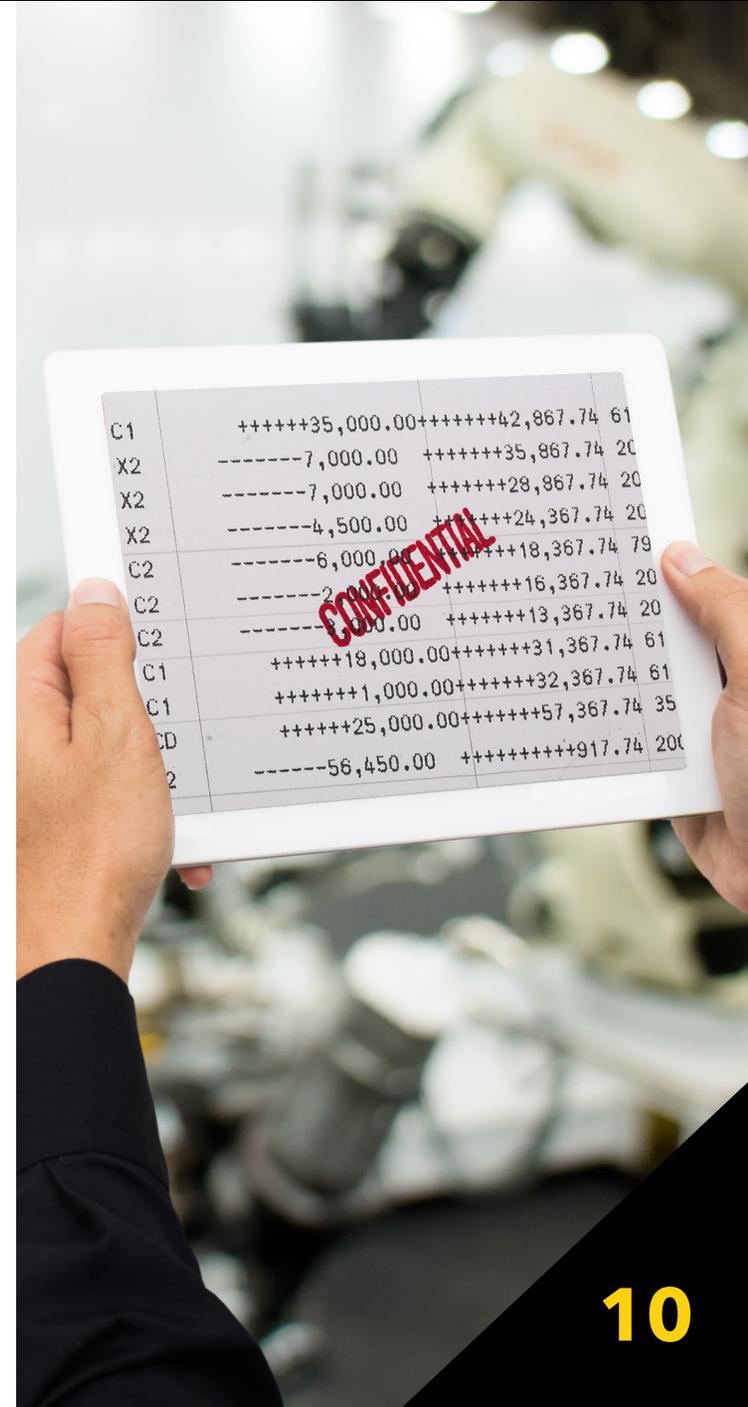
Solutions

Multi-Factor Authentication

A critical step to securing access of valuable data within your network is the deployment of an MFA, or multi-factor authentication solution. WatchGuard's AuthPoint goes beyond traditional 2-factor uthentication (2FA) by considering innovative ways to positively identify users looking to access the network, and our large ecosystem of 3rd party integrations means that you can use MFA to not only protect access to the network, but also VPNs and Cloud applications.

Data Loss Prevention

Included with every Total Security Suite subscription, WatchGuard's DLP (Data Loss Prevention) is a comprehensive service that helps keep your confidential data private. It prevents data breaches and enforces compliance by scanning text and files to detect sensitive information attempting to exit your network. If sensitive information is identified, the connection is blocked or quarantined, and the administrator is notified.

11
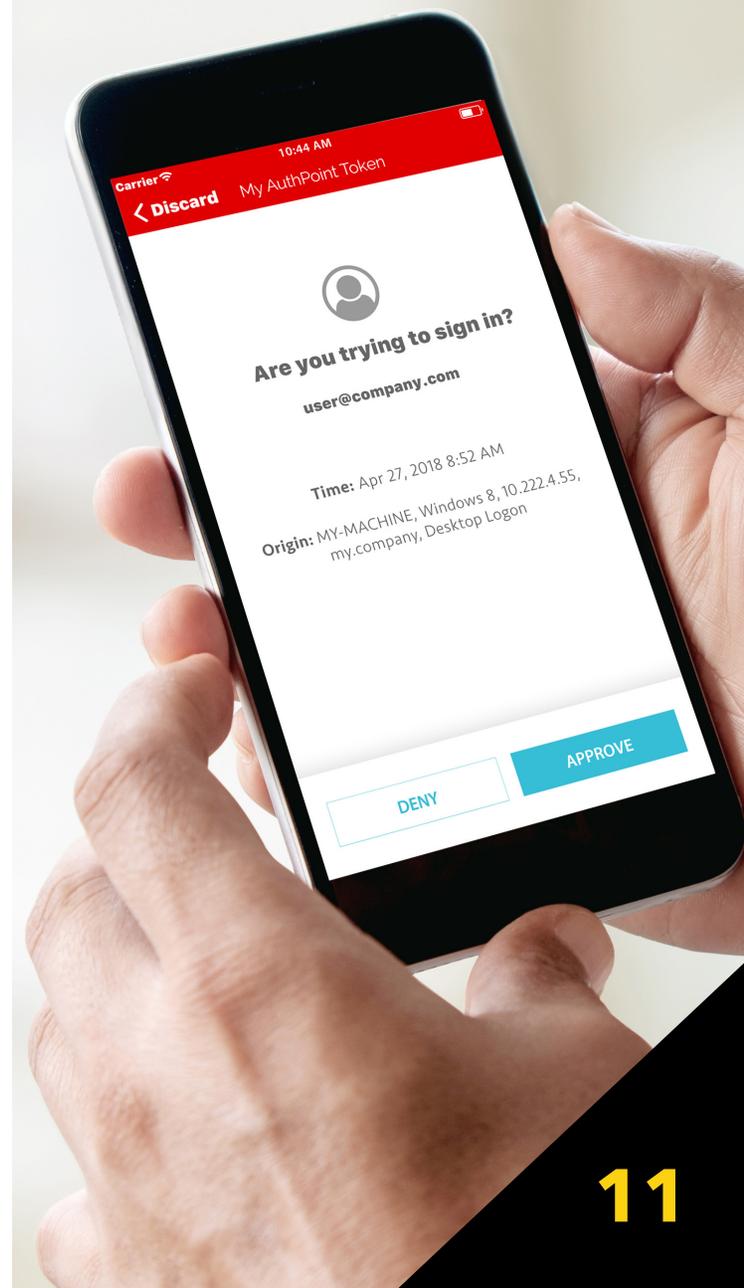
A global shortage of IT talent has left large staffing gaps across all industries, **with a projected shortage of 3.5 million cyber security professionals worldwide by 2021**.[9] This is especially worrying for the manufacturing sector due to its reliance on a different digital infrastructure than that of other industries, further limiting qualified candidates: OT (Operational Technology), the hardware and software utilized on the production floor, and ICS (Industrial Control System), the systems and instrumentation used for industrial process control. Additionally, inadequate cyber security staffing increases the risk of employees falling for targeted attacks like phishing, a growing threat typically deterred by IT department-administered education and awareness.

With manufacturing taking an average of five months to fill open positions,[10] businesses looking to maintain a strong security posture – regardless of job postings – should evaluate solutions that don't require a large or dedicated IT workforce to maintain efficacy.

Solutions

### Zero-Touch Firewall Configuration

Sending a member of your IT team to a branch office or factory for onsite configuration is probably out of the question when resources are tight, but luckily WatchGuard makes it easy to deploy security right from your office – no need to travel. RapidDeploy is a powerful, Cloud-based deployment and configuration tool that comes standard with WatchGuard Firebox appliances. All you have to do is power up the appliance and connect it to the Internet. The rest can be handled remotely from any location.
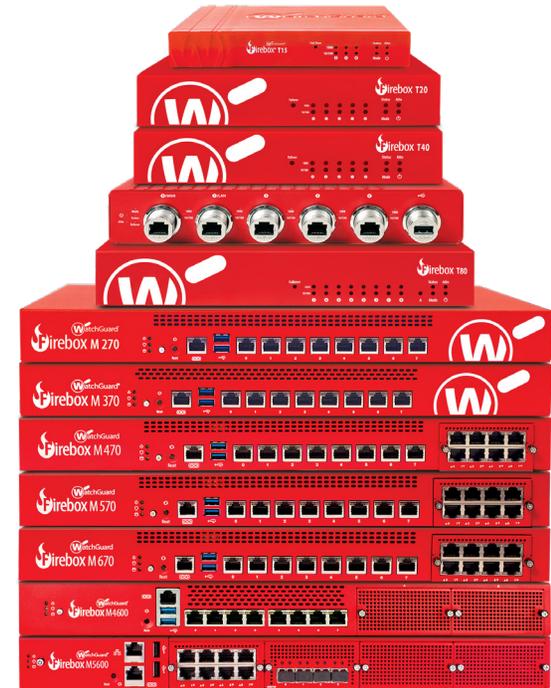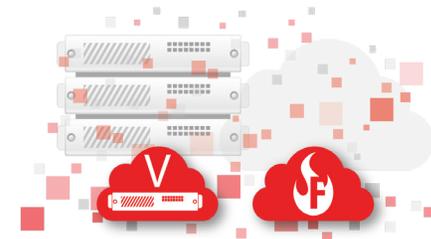
Automating Threat Prevention and Detection with AI

Traditional approaches to cyber security typically rely on manual processes and preestablished policies to block attacks – a challenge if your IT team is small and already overwhelmed with alerts and false positives, leaving attacks to go unnoticed for months at a time. With a foundation of artificial intelligence – like WatchGuard's IntelligentAV, APT Blocker, and ThreatSync services – predictive protection saves time, correlates data, makes faster decisions, minimizes human error, and predicts future threat trends.
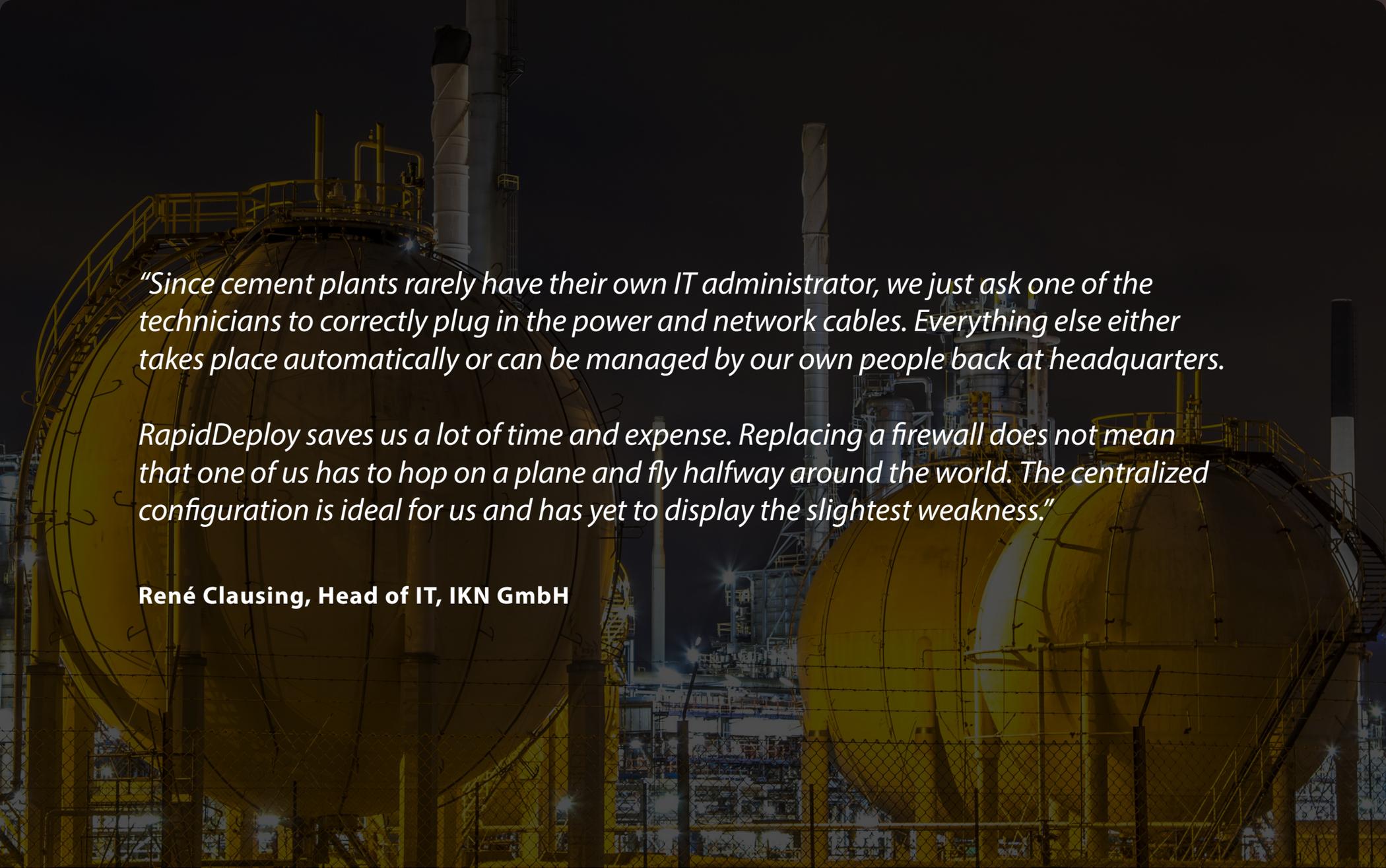
"Since cement plants rarely have their own IT administrator, we just ask one of the technicians to correctly plug in the power and network cables. Everything else either takes place automatically or can be managed by our own people back at headquarters.

RapidDeploy saves us a lot of time and expense. Replacing a firewall does not mean that one of us has to hop on a plane and fly halfway around the world. The centralized configuration is ideal for us and has yet to display the slightest weakness."

René Clausing, Head of IT, IKN GmbH

Industry 4.0 is transforming manufacturing facilities and increasing productivity, staff safety, and cost-savings, while also inviting new security challenges. Those who look to protect the equipment – and people – occupying their shop floors by way of enterprise-grade, easy-to-deploy solutions will find them with WatchGuard.

THE WATCHGUARD SECURITY PORTFOLIO

Network Security

In addition to delivering enterprise-grade security, our platform is designed from the ground up to focus on ease of deployment, use, and ongoing managing, making WatchGuard the ideal solution for SMB, midsize, and distributed enterprise organizations worldwide.

Secure Wi-Fi

WatchGuard's Secure Wi-Fi Solution, a true game-changer in today's market, is engineered to provide a safe, protected airspace for Wi-Fi environments, while eliminating administrative headaches and greatly reducing costs. With expansive engagement tools and visibility into business analytics, it delivers the competitive advantage businesses need to succeed.

Multi-Factor Authentication

WatchGuard AuthPoint® is the right solution to close the password-driven security gap that leaves companies vulnerable to a breach. It provides multi-factor authentication on an easy-to-use Cloud platform. Our unique approach adds "mobile phone DNA" as an identifying factor to ensure that only the correct individual is granted access to sensitive networks and Cloud applications.

[1] Precision Manufacturing, "Manufacturing Sector – Now One of the Most Frequently Hacked Industries", November 2016
[2] The Telegraph, "Half of UK manufacturers fall victim to cyber attacks", April 2018
[3] Los Angeles Times, "Malware attack disrupts delivery of L.A. Times and Tribune papers across the U.S."
[4] Sentryo, "Cyberattack on a German steel-mill", May 2016
[5] Newgen Apps, "13 IoT Statistics Defining the Future of Internet of Things", January 2018
[6] Quick Base, "5 Shadow IT Statistics to Make You Reconsider Your Life", January 2018
[7] Attila, "Protecting the Manufacturing Sector from Cybercrime", November 2018
[8] VOA News, "Fighting Chinese Counterfeiters", October 2009
[9] Forbes, "The CyberSecurity Talent Gap is an Industry Crisis", August 2018
[10] SDC Executive, "Small Manufacturers Prone to Cybersecurity Attacks", January 2019

About WatchGuard

WatchGuard® Technologies, Inc. is a global leader in network security, secure Wi-Fi, multi-factor authentication, and network intelligence. The company's award-winning products and services are trusted around the world by nearly 10,000 security resellers and service providers to protect more than 80,000 customers. WatchGuard's mission is to make enterprise-grade security accessible to companies of all types and sizes through simplicity, making WatchGuard an ideal solution for midmarket businesses and distributed enterprises. WatchGuard is headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America. To learn more, visit WatchGuard.com.

North America Sales: 1.800.734.9905   •   **International Sales:** 1.206.613.0895   •   **Web:** www.watchguard.com/wifi