SOLUTION BRIEF

Keep Cities Running By Making Them Cyber Secure

Introduction

Citizens depend on their city governments for a variety of city services – from paying bills and traffic tickets to accessing public records. As more of these services are happening online, city governments need to guarantee that the treasure trove of PII and banking information they're collecting, accessing and storing is secure. Governments also need to make sure that their services stay online to ensure that their cities don't come to a halt, leading to lost revenue.

What are some of the top challenges facing these organizations?

Modernizing Legacy Technology

With limited budgets and resources, city governments can struggle with the need to keep things moving with the desire to update legacy technologies to be more secure. As more citizen services become available online, that choice could be the difference between a normal day at the office and a major security breach. It's important that the organizations that manage these services have the latest technology in place to protect their citizens.

How Can eMazzanti and WatchGuard Help

eMazzanti Technologies understands that city governments have limited resources and budgets. That's why we package and license our products to be cost effective and easy to deploy. WatchGuard Total Security Suite includes all our network security services plus our reporting and Cloud-management platform through one license and one appliance. Leveraging Cloud-managed solutions can help keep infrastructure and overhead costs down, saving you time and money.

Furthermore, WatchGuard's multi-factor authentication (MFA) solution, AuthPoint, is deployed and managed through our WatchGuard Cloud platform and leverages a free mobile app – requiring no infrastructure costs and no hardware costs. Quickly and easily deploy MFA to protect user credentials for employees wherever they are.

SOLUTION BRIEF

Making Sure Emergency Services & Dispatching Organizations Can Answer the Call

Introduction

Citizens depend on their city governments to provide necessary emergency services like paramedics, fire fighters and more. All of these departments are notified where to go and why through their local dispatching department. These organizations face a variety of threats, and we've seen the impact of how breaches can affect them. In 2018, Baltimore, MD, experienced a breach that damaged their computer-assisted dispatching systems for over 17 hours, forcing dispatchers to handle calls manually and causing extensive delays in response time. How can these departments that depend on technology stay secure from attacks?

Internet for Personal Use

Overall, fire departments have seemingly limited attack vectors when it comes to cyber threats. However, one of the most important things that these stations need to provide (that also creates the greatest security risk) is reliable Internet access for station and personal devices. But just because your Wi-Fi connection is fast, that doesn't mean it's secure.

Your Wi-Fi could be your biggest security gap. Hackers prefer to go after the weak link in the security chain and it doesn't take much to hack into the Wi-Fi network using easily accessible tools and a plethora of online how-to videos. Even the most rookie hacker can intercept traffic flowing over Wi-Fi and steal valuable data from your smartphone, tablet, smartwatch, or laptop. Make sure that the wireless solutions you deploy are protected from the six known wireless threat categories.

How Can eMazzanti and WatchGuard Help

WatchGuard offers the only truly secure wireless platform in the industry. As a WatchGuard Platinum partner, we offer their patented wireless intrusion preventions (WIPS) technology. It is the only Miercom-verified platform that can secure wireless access points from the six known wireless threat categories. Best of all, WatchGuard access points are the only solution on the market that can be used to secure other brands of access points – meaning no need to rip and replace your existing deployment to gain the additional security benefits of WatchGuard WIPS.

Security Education

Many cyber attacks against city governments, including dispatchers and other first responders, target users through phishing emails and other ransomware attacks. Yes, there are technologies that can help protect against the effects of these attacks, but the best thing IT managers can do is educate and train their employees on how to avoid them. No wonder 38% of location governments believe that greater awareness is needed to ensure the highest level of cybersecurity. [1]

How Can eMazzanti and WatchGuard Help

Educating your workforce is one of the most important ways to protect your department from an attack or security breach. eMazzanti and WatchGuard have partnerships with industry-leading security education platforms and would be happy to connect you with a few of our favorites.

WatchGuard DNSWatch, included in Total Security Suite, is a Cloud-based service adding DNS-level filtering to detect and block potentially dangerous connections and protect networks and employees from damaging attacks. WatchGuard analysts triage any critical alerts, following up with an easy-to-understand accounting that includes detailed insights about the potential infection. However, when the attack uses phishing and an employee clicks the link, DNSWatch not only blocks the attack, but automatically redirects them away from the malicious site and offers resources that reinforce phishing education. This service is also available for users on the go with a DNSWatchGO or Passport license.

Working with eMazzanti Technologies and Watchguard

For those city governments looking to install and manage Watchguard products so that the municipality is safe and secure. Watchguard and its Platinum Partner, eMazzanti Technologies can help. eMazzanti Technologies is headquartered in the New York Metro Area and has extensive experience in cybersecurity assessments, planning and implementation. For over 20 years the firm has worked with many of the tri-state local governments, public services, and mission critical entities to ensure their protection and safety.

Governments select, implement and manage their security solutions.

For more information contact info@emazzanti.net or reach us at 844-360-4400.

1 IBM report

SOLUTION BRIEF

Protect, Serve and Cyber Security

Introduction

Law enforcement agencies are a particularly attractive target for hackers due to the vast amount of sensitive and confidential data they collect and store. This data must be accessible in and outside the confines of a police station for use by officers and detectives in the field, which can create a huge attack vector for hackers and an even bigger security risk for IT managers. For law enforcement organizations, protecting this information is not just an IT issue, but a matter of public safety.

Collection and Access to Evidence

Police and Sheriff departments across the US are increasingly collecting various types of digital evidence including reports, pictures, videos and other electronic records. But the IT managers at these organizations have to find the balance between securing digital evidence while still making it securely accessible to officers in the field through mobile data terminals (MDTs) in their vehicles or other devices in and outside the station. Leveraging security tools like multi-factor authentication (MFA) and secure VPN are great ways to ensure that sensitive data is only accessed by those with the credentials.

How Can eMazzanti and WatchGuard Help

WatchGuard AuthPoint provides easy-to-use, flexible MFA solutions to protect users wherever they go. By leveraging our mobile app, officers and staff can easily verify their identity through a push notification, QR code scan or one-time password. This ensures that people accessing data are who they say they are and keeps hackers at bay even if they gain access to user credentials.

WatchGuard offers robust VPN capabilities that are easy to set up and manage, while ensuring the security of your traffic as it leaves and enters your network.

CJIS Compliance

All of these agencies need to ensure their compliance with CJIS regulations to guarantee their access to this powerful criminal justice information resource. CJIS has 13 main policy areas whose standards these departments must meet, including incident response, security awareness training, identification and authentication, mobile device security and more. Additionally, CJIS regulations mandate that any traffic be encrypted by FIPS 140-2 certified appliances. It's important for city governments to find vendors that know how they cover this regulation and how their solutions can keep them secure.

How Can eMazzanti and WatchGuard Help

All WatchGuard firewall appliances are FIPS 140-2 certified or pending certification, which ensures secure, encrypted network traffic. Furthermore, the WatchGuard Cloud network management platform provides essential management logging capabilities that assist with CJIS auditing and accountability requirements. WatchGuard also offers multi-factor authentication and secure Wi-Fi solutions to assist with the CJIS requirements for identification and authentication and mobile devices. Last but not least, WatchGuard offers robust and flexible VPN capabilities, as well as our Total Security Suite license to ensure systems and communications protection and integrity.

Cybersecurity					
Guidelines	Recommendation	WatchGuard Solution			
		Fireboxes & Off-Network	AuthPoint	Secure Wi-Fi	Management
Security Awareness Training	Security Education and Training	√			
Auditing & Accountability	Management and Logging Tools				√
Access Control	Remote Access, VPN, Secure Wi-Fi	√		√	
Configuration Management	Access Management				
Identification & Authentication	Multi-factor Authentication		√		
Media Protection	Secure Data at Rest and in Motion				
System & Communications Protection and Information Integrity	Encryption, Antivirus/spam, Firewalls/ UTMs and VPNs	√			
Mobile Devices	Wi-Fi Management & Security				√

Planning Processes & On-site Security	
Guidelines	Recommendation
Formal Audits	Triennial Audits
Incident Response	Planned Detection, Analysis, Containment, Recover and Reporting of an Incident
Personnel Security	Security Screenings for Personnel, Vendors and Contractors
Physical Protection	Secure Physical Locations
Information Exchange and User Agreements	Store & Verify Written Agreements

Critical Breach Response

IT teams at these critical departments must consider a different approach to breach response. While most IT pros would recommend reimaging a machine that's been hacked or compromised, law enforcement agencies must balance preserving evidence with the need to restore access to devices. For law enforcement agencies, the best thing they can do is try to prevent attacks by educating officers and staff on cybersecurity awareness while also deploying security solutions that keep users safe.

How Can eMazzanti and WatchGuard Help

WatchGuard Total Security Suite offers layered security to protect your officers and staff from known, unknown and evasive threats. Best of all, your Total Security Suite license includes access to WatchGuard Cloud, our reporting and management platform, with no additional charge.

WatchGuard DNSWatch, included with Total Security Suite, creates an additional layer of security providing DNS-level protection and content filtering that keeps your business safe from phishing, ransomware, and other attacks. This security service also provides refresher education, reminding users how to spot these types of attacks and stay safe in the future.

Part No. WGCE67319_041720

SOLUTION BRIEF

Keeping the Lights On and the Water Running: Protecting Utilities & Water Agencies

Introduction

In 2015, the University of Cambridge and Lloyd's of London published a report that stated that an attack on the United States electrical grid could potentially leave states and **93 million people between New York City and Washington DC without power. The estimated impact on the economy could be between $243 billion and $1 trillion.** These organizations are facing an increasing amount of unwanted, potentially malicious traffic and need to find the right balance between securing our infrastructure while still granting necessary remote access.

With a large attack surface, legacy technology and limited resources, it's no wonder these organizations are a key target for hackers.

Remote Access

One of the greatest needs for utilities and water departments is to ensure that staff can reliably access wastewater treatment and utilities SCADA systems. While remote access and an Internet connection is required for these systems to operate efficiently, it creates a huge vulnerability for water and utility departments. One way to protect against this is reduce the attack surface, redirecting all remote access through a single, secure authentication service to monitor and track activity. Securing these SCADA systems behind a firewall is recommended to guard against wrongdoers gaining access to critical infrastructure.

How Can eMazzanti and WatchGuard Help

WatchGuard offers the ruggedized Firebox T35-R, which lev erages signatures to protect against known industrial control system (ICS) and SCADA threats and enable security use cases in harsh deployment environments. Furthermore, our multi-factor authentication platform, AuthPoint, helps ensure that the people accessing your systems are truly who they say they are and protects against any stolen or compromised credentials.

Cybersecurity Guidance and Tools

Waterworks and utilities departments need to worry about protecting their SCADA infrastructure at all costs. The American Water Works Association (AWWA) provides guidelines to help these organizations figure out how to protect these critical infrastructure systems and help prioritize upgrades to legacy systems.

How Can WatchGuard Help

WatchGuard solutions help you follow the AWWA guidelines to improve cybersecurity practices in a variety of ways.

Cybersecurity					
Guidelines	Recommendation	WatchGuard Solution			
		Fireboxes & Off-Network	AuthPoint	Secure Wi-Fi	Management
Governance & Risk Management	Written Cybersecurity Plan; Vulnerability Assessment; Network Assessment; Wireless & Guess Access			√	
Encryption	Wireless Encryption; VPN	√			
Operation Security	Isolate Functions including Internet Browsing, Email, etc.				
Access Control	Physical Access; Wireless & Guess Access; MFA; VPN	√	√	√	
Business Continuity & Disaster Recovery	Emergency Response Plan; Back-ups & Storage				
Server & Workstation Hardening	Whitelisting; Software Patching; Antivirus & Anti-malware	√			
Application Security	Strong Credential Policies; MFA		√		
Data Security	Meet PCI DSS & HIPAA Standards	√	√	√	
Telecommunication, Network Security & Architecture	Enterprise Switches, Routers, Firewalls, Spam Filtering, Website Blocking, IPS/IDS; Network Management; Wi-Fi	√		√	

Planning Processes & On-site Security	
Guidelines	Recommendation
Physical Security of PCS Equipment	Access Control to PCS Equipment
Service Level Agreements	Define and Manage External SLAs
Cyber Informed Engineering	Provide Cybersecurity Training and Education to all Employees and Contractors
Education	
Personnel Security	

Working with eMazzanti and Watchguard Technologies.

For those city governments looking to install and manage Watchguard products so that the municipality is safe and secure. Watchguard and its Platinum Partner, eMazzanti Technologies can help. eMazzanti Technologies is headquartered in the New York Metro Area and has extensive experience in cybersecurity assessments, planning and implementation. For over 20 years the firm has worked with many of the tri-state local governments, public services, and mission critical entities to ensure their protection and safety.

Governments select, implement and manage their security solutions.

For more information contact info@emazzanti.net or reach us at 844-360-4400.

About eMazzanti

At eMazzanti Technologies we do more than just fix things when they break. We're strategists, problem solvers, facilitators and vigilant watchkeepers. We are a team of certified IT professionals that can rapidly deliver technology solutions to help your organization grow and keep pace with your competition. Our areas of expertise range from law firms to high-end global retailers, providing advanced retail and payment technology, digital marketing services, cloud and mobile solutions, multi-site implementations, 24×7 outsourced network management, remote monitoring and support. We specialize in Cybersecurity and keeping your IT infrastructure safe from the ever increasing hacker threats.

701 Grand St, Hoboken, NJ, 07030 | T 844.360.4400 | info@emazzanti.net | www.emazzanti.net