Securing Web Use for Police and First Responder Forces

Today, police and other first responders depend on public web data and applications as well as on dedicated private law enforcement networks. Yet the web is the primary delivery channel for cyberattacks that can compromise sensitive department information, disrupt essential operations and investigations, erode public trust, and cost millions in tax-payer funds for remediation and lost work.

In the station, on patrol or deployed in command vehicles, police face the same web-based risks as all organizations: Risk of downloading malware when browsing a site, clicking on a malicious link in a phishing email, or exposing credentials by "logging in" on a spoofed site. Investigators and detectives face greater threats when researching crime on the dark web or websites frequented by criminals.

The risk increases significantly when first responder devices are removed from the station or modem-equipped mobile unit, where standard cybersecurity protections are built into organization networks, and connected via home networks or insecure public Wi-Fi. And that risk is compounded if the devices are used to visit risky sites.

ericom security
by cradlepoint

- Air-gapped protection from web-delivered threats
- Role-based internet filtering
- Protects against phishing, even when users click
- Applies CDR to prevent attacks via weaponized downloaded files
- Cloud-based solution prevents cyberattacks, wherever users are working
- Protects force applications and data from breach and data loss
- Transparent to users

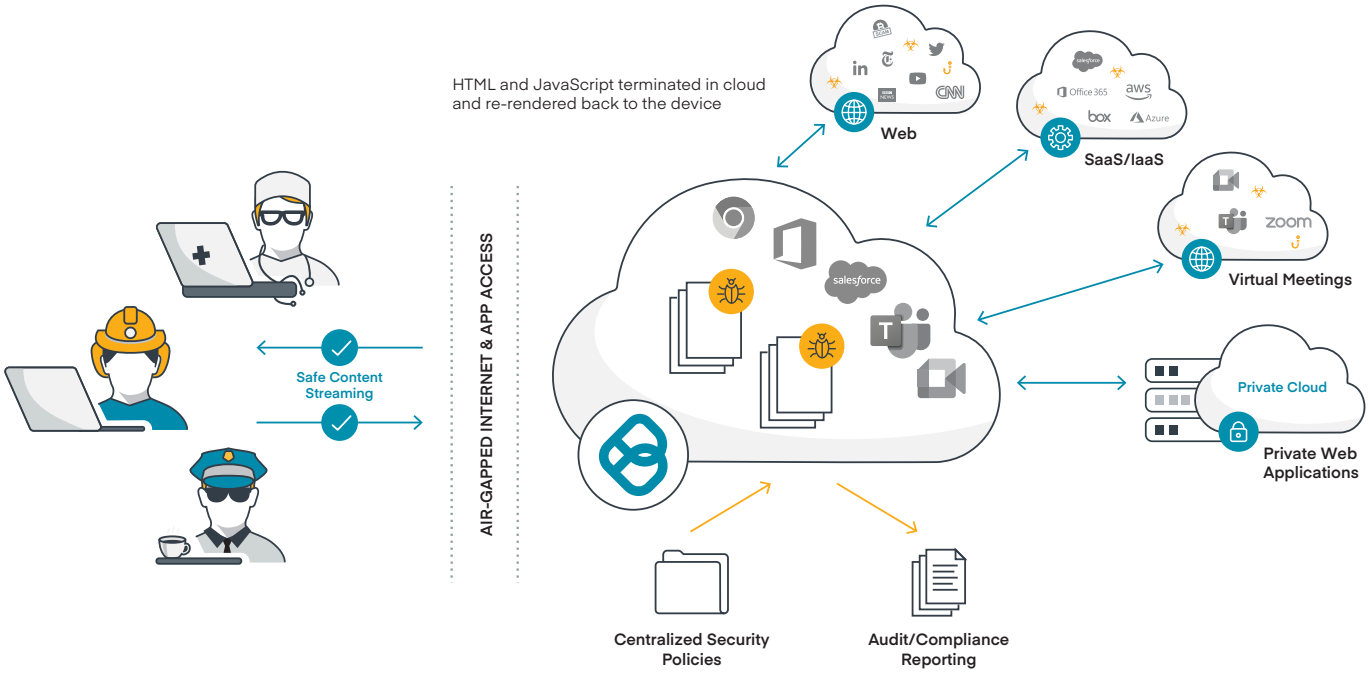
Ericom Web Isolation: Air-Gapped Zero Trust Secure Web Access

Ericom Web Isolation secures access to all websites and applications, including virtual meetings, encrypted instant messaging sites and more. Since no web content can be verified as safe, Ericom provides Zero Trust access by airgapping active web content away from the user device. By applying robust Remote Browser Isolation (RBI) technology, Ericom de-risks web interactions from any location, on any browser.

Ericom Web Isolation effectively isolates first responder devices from the internet and protects sensitive department data through three key measures:

1. **Web browsing sessions are executed in isolated cloud-based containers** to airgap user devices from the internet and protect networks from malware, ransomware and even zero-day exploits. Only safe rendering data reaches responder devices, where they interact with it seamlessly, on their regular browsers.
2. **Granular policy controls prevent data loss and exposure** by restricting functions such as uploads, downloads, clipboard interactions, printing, copy/pasting and more, based on user identity and type of website. Data loss prevention (DLP) prevents exfiltration of PII and other sensitive data. Unknown websites may be opened as read-only to prevent credential theft.
3. **File sanitization (CDR) scrubs web downloads** and email attachments to remove threats embedded in documents and files.

Web filtering enables detectives and investigators to securely access high-risk sites like gambling, gaming, pornography and Dark Web sites for investigations while blocking access for users who do not need to access these sites for their work. DNS filtering ensures that private data is protected from exposure.



Ericom Web Application Isolation: Protect Apps from Breach

Ericom Web Application Isolation (WAI) protects private applications and public-facing web applications while enabling legitimate interactions. It cloaks apps from malware attacks and probes to prevent hackers from discovering misconfigurations, unpatched services or other vulnerabilities to exploit. As a clientless solution, it secures private applications and SaaS and web apps from unmanaged device risk, so users can securely gain access from any device.

First responder organizations need cyber defenses that can protect sensitive data and prevent breaches and ransomware attacks, even if a user clicks on a phishing link, opens a malicious site, or downloads a weaponized file.

How Do Attacks Happen?

Three initial compromise vectors – exploits of public-facing apps, compromised accounts, and phishing -- together account for 86% of recent cyberattacks. Common to all of these vectors is, of course, the central role of the web.

Exploits of public-facing applications

The surfaces of public-facing websites and online portals for reporting incidents or requesting assistance can be probed by cybercriminals seeking vulnerabilities to exploit to breach systems or infect them with malware -- or both.

Compromised accounts

Credentials may be stolen when a user logs in using unsecured public wifi, be purchased on the Dark Web following a breach, or be revealed by the user in a phishing attack.

Phishing

Individuals like first responders, who operate in high-stress, fast-paced environments, may be particularly vulnerable to pressure to respond quickly to seemingly important appeals. And once they click on a malicious link, malware that penetrates the user device can rapidly move throughout organization systems.

Malicious websites

Malware on malicious or infected websites may infect user devices via drive-by downloads, infected links, content or attachments, or diversion of user credentials.

Why Are First Responder Forces Attacked?

Police and other first-responders are attacked for many of the same reasons as other organizations, along with a few that make them particularly attractive to threat actors.

Financial: First responder systems contain a wealth of private data about citizens, businesses and employees. This data is highly valuable as bait for ransom demands, when sold, or when used in subsequent cyberattacks.

Political: Law enforcement agencies may be targeted for political and ideological reasons, or by hacktivists seeking to embarrass police departments or access confidential information about controversial incidents.

Criminal: Criminals may seek to disrupt first responder operations to destroy evidence, disrupt investigations, intimidate officers, or otherwise interfere with police work.

The Bottom Line

Ericom Security Solutions protect the first responder organizations that protect and serve the public. They protect sensitive data from exposure, prevent malware from reaching systems even when users click on bad links, and safeguard organizations and their public-facing applications from web-originated cyberattacks. The solutions are cost-effective, easy to integrate with existing infrastructure and simple to use.

Discover how Ericom Web Isolation can empower your organization to secure data and networks from phishing and web-delivered threats without over-blocking the internet access users need.

Contact us today for a personalized demonstration or to learn more about our scalable cloud-delivered service at ericom.com/contact-us.