ZTEdge™
By Ericom Software

# To Secure the Public Sector from Cyberattacks, in Zero We Trust

# Contents

# Introduction

Government agencies at the national, state and local levels are being cyberattacked at levels never before seen. The number of attacks almost doubled from the second half of 2021 to the same period in 2022, with 56 known attacks in the 3rd quarter alone – and most likely, many more unknown.

The public sector accounted for almost 20% of all reported attacks in 2021 – 50% more than financial institutions and second only to the industrial sector.

## Countries Which Experienced Public Sector Attacks, 2022

| | | | | |
|---|---|---|---|---|
| 01 ALBANIA | 02 ARGENTINA | 03 AUSTRALIA | 03 AUSTRIA | 01 BAHRAIN |
| 01 CHINA | 02 COLOMBIA | 01 COSTA RICA | 01 CUBA | 04 CZECHIA |
| 24 GERMANY | 02 GREENLAND | 03 INDIA | 01 IRAN | 03 ISRAEL |
| 01 MAURITIUS | 05 MEXICO | 01 MONTENEGRO | 01 MOROCCO | 01 MOZAMBIQUE |
| 11 RUSSIA | 09 SPAIN | 02 SWEDEN | 05 SWITZERLAND | 01 TURKEY |
| 08 BELGIUM | 09 BRAZIL | 01 BULGARIA | 12 CANADA | 02 CHILE |
| 03 DENMARK | 01 ECUADOR | 04 ESTONIA | 01 FINLAND | 34 FRANCE |
| 23 ITALY | 01 JAPAN | 01 LATVIA | 02 MALAYSIA | 01 MALI |
| 03 NETHERLANDS | 01 NEW ZEALAND | 01 PHILIPPINES | 01 POLAND | 06 PORTUGAL |
| 03 UK | 07 UKRAINE | 74 USA | | |

In almost three-fourths of ransomware attacks on state and local governments, threat actors succeeded in encrypting data, resulting in disruption to the many essential services that governments provide. Beyond being inconvenienced (and possibly endangered) by the inability to obtain basic services, costs of restoring and rebuilding IT systems and recovering data must be covered by public funds. Over 20% of public sector organizations attacked reported recovery times of over one month.

# Who Attacks Government Agencies, and Why?

## The Rise of Nation-State Attacks

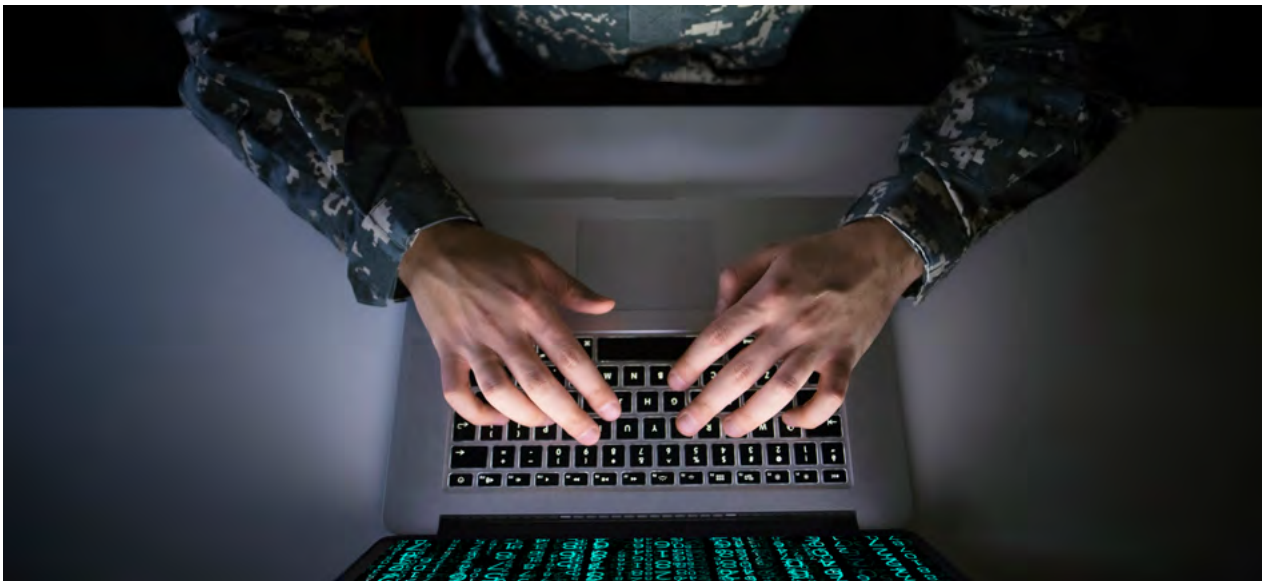
Historically, state-sponsored cyberattacks – the type that dominate Netflix thrillers – have constituted a relatively small proportion of the incidents with which public sector organizations contend. That has changed dramatically as nation-state actors have grown increasingly aggressive, especially since the outbreak of the Russia-Ukraine war, which Microsoft termed a “full-scale hybrid conflict."

In addition to attacks on governments spurred by hot global conflicts, states like Iran and North Korea are increasingly leveraging attacks as part of low-level conflicts and to keep an eye on neighboring states. Destructive attacks are generally deployed as adjuncts to military action. In conflicts that are on a low simmer, they are used for pinpoint tactical operations or more often, intelligence gathering.

While only 12% of nation-state attacks are directly on government operations, intelligence-gathering operations also target governments indirectly via “softer” entities like think tanks, NGOs, intergovernmental organizations, universities and government officials. The bulk of nation-state attacks are aimed at enterprises and cyber defense assets, especially software companies and IT service providers, since exploiting their supply chains provides access to large numbers of government and government-adjacent client systems.

In response to this increase in nation-state cyber activity, countries worldwide have been building up SecOps capabilities to defend their app surfaces from enemies (and sometimes friends) who may be probing for ways to deliver cyberattacks or gather intelligence.

Only 12% of nation-state attacks are directly on government operations. But intelligence-gathering operations also target them via NGOs, think tanks, universities and government officials.

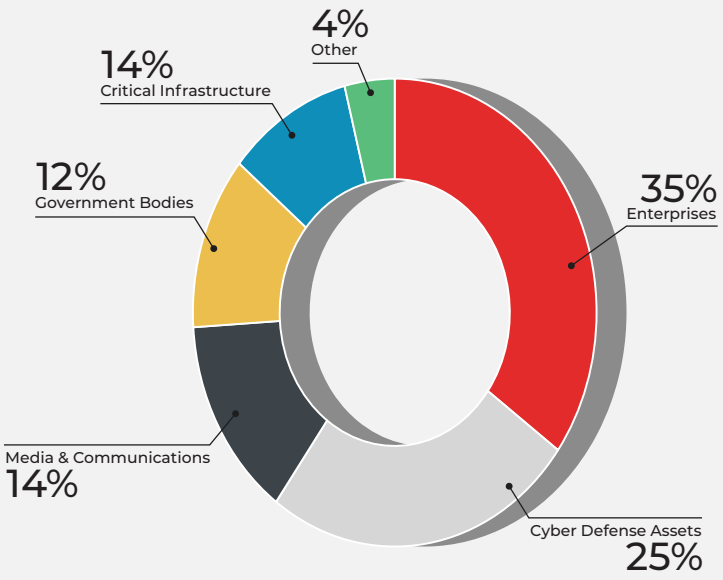


## Common Targets of National-State Attacks

Reserchers took a look at national-state attacks and determined who APTs were going after the most.

### Targets of National-State Cyberattacks

Source: Dr. Mike McGuire and HP, National States, Cyberconflict and the Web of Profit





It's important to note that foreign influence campaigns – a type of cyber threat that has grown exponentially in recent years – can have devastating impact on governments throughout the world, at all levels, to the point of undermining the institutions of government and seriously destabilizing regimes. However, because the weapon used in these campaigns is misinformation rather than malware or exploits, and they are conducted through the information ecosystem and not IT systems, they are beyond the scope of this paper.

## Criminals Target Government Agencies, Too

Despite the noteworthy increase in nation-state attacks, the cyberattacks that plague government organizations are most often the same kind of garden-variety ransomware, DDoS and zero-day attacks that plague organizations across all industries. Whether they are executed by individuals or cybercrime groups, these attacks wreak significant havoc on government agencies at local, municipal, state and federal levels throughout the world, as well as on courts, police departments, school districts, social services, and myriad other essential government services.

The motive for these types of attacks is financial gain from ransoms, sale of valuable records stolen in the course of a breach, or to gain access to trusted government domains that can be leveraged to distribute malicious content. In numerous cases worldwide, these attacks have brought critical services such as transfer payment distribution, registration of births and deaths, education and healthcare, issuing of passports and much more, to a screeching halt.

> *"Before the invasion of Ukraine, governments thought that data needed to stay inside a country in order to be secure. After the invasion, migrating data to the cloud and moving outside territorial borders is now a part of resiliency training and good governance."*
>
> **Cristin Flynn Goodwin**
> Associate General Counsel, Customer Security and Trust, Microsoft in "Microsoft Digital Defense Report 2022"

ZTEdge™
By Ericom Software

# How Public Sector Attacks Happen

Research has shown that three initial compromise vectors – exploits of public-facing apps, compromised accounts, and phishing -- together account for 86% of recent cyberattacks. While these vectors have long been dominant, the proportions shifted dramatically in 2021. Reports show that the percentage of cyberattacks originating with a public-facing app being exploited jumped from 37% in 2019 to almost 54% a mere two years later.

Let's take a look at each of the three major compromise vectors and their role in attacks on public sector organizations.

## Exploits of Public-Facing Applications

The apps that government agencies have rolled out in recent years streamline service provision, relieve citizens of the need for in-person visits or long waits on hold, and reduce costs. However, they also substantially increase the attack surface of government systems.

Cybercriminals are opportunistic, seeking out the attack paths that offer the best chance of success with the least effort. The large-scale transition to full and hybrid cloud computing has created attractive new attack surfaces in the form of misconfigurations and vulnerabilities associated with continuously deployed apps that often integrate open-source code. By 2021, exploiting public-facing applications was how threat actors initially gained access in almost 54% of cyberattacks.

Patching and updating, of course, are the most effective ways to prevent known vulnerabilities of open-source code and widely used software from being exploited. In fact, a recent study of organizations which suffered ransomware attacks found that 68% lacked an effective vulnerability and patch management process. VPNs, which are still used by many organizations and often unpatched despite well-documented vulnerabilities, are an easy target for threat actors.

But patching is not always enough, even if done well. Once unpatched vulnerabilities become public, cybercriminals scramble to exploit them while the exploiting is good. Patching promptly across all installations can be complex, which is why over 40% of exploits typically occur after a patch has been issued. The shortage of cybersecurity staff that is partially responsible for slow patching is particularly acute for state and local governments.

Cybercriminals are opportunistic, seeking attack paths that offer the best chance of success with the least effort. In cloud computing, app misconfigurations and vulnerabilities create attractive new attack surfaces.

Unpatched vulnerabilities in widely used solutions get most of the headlines, but they actually represent only the tip of the vulnerability iceberg.

In cases where multiple patches come available at once or patches must be applied for multiple instances, patching teams must carefully prioritize which to address first, weighing the likely risk to their particular installations against general severity rankings. Regardless of how well decision algorithms are applied, any patching delays entail risk.

In an unfortunate recent example of a nation-state attack that was enabled by an unpatched vulnerability, an Iranian state-sponsored threat group exploited a SysAid Server instance that was not secured against the Log4Shell flaw. They were able to gain access and attack Israeli public sector organizations, months after the patch had been issued. Once in, they established persistence and moved laterally within the targeted organization's network.

Unpatched vulnerabilities in widely used solutions get most of the headlines, but they actually represent only the tip of the vulnerability iceberg. An estimated 85% of vulnerabilities are due to misconfigurations, and still more result from unsecured APIs, coding bugs and other issues that inevitably creep in during development and/or during the multiple microservice deployments that are pushed through every day. Many of these vulnerabilities are visible to any hacker who chooses to probe an app surface to seek a way to get in. So regardless of how diligently an agency's security team patches known exploits, most apps offer a virtually unlimited menu of vulnerabilities to exploit.

## Compromised Accounts

Compromised accounts offer threat actors numerous opportunities for both financial gain and malicious action. For instance, the rich data about citizens and businesses in agency files and apps is worth a great deal on the open market. In addition, phishing and other social engineering attacks originating from trusted government identities have high rates of success. And compromised accounts enable nation-state actors to penetrate systems, move laterally within applications, and establish persistence for espionage or destructive attacks.

MFA is widely cited as a primary protection against account compromise via stolen credentials. While it is a valuable safeguard, the rapid spread of session-stealing cookie and SIM-jacking techniques is undermining its strength and increasing the need for new authentication techniques. A number of new passwordless authentication technologies like FIDO, WebAuthn and CTAP are being discussed and implemented in some solutions but none has yet reached critical mass.

Many government networks and apps are used by myriad employees, contractors, supply chain partners and often, the public at large. With social engineering rampant and new ways to bypass MFA increasingly available, account compromise is likely to remain a frequent initial attack vector – and a quick way to exfiltrate data and cause general havoc.

> Social engineering attacks originating from trusted government identities have high rates of success.

> The percentage of attacks that used compromised accounts more than doubled in 2020 due to the pandemic-spurred increase in VPN use.

### Remote Access to Private Apps

VPNs represent a common way for organizations to provide remote user access to desktops and private apps – as well as a common way that accounts are successfully compromised. The percentage of attacks in which access was gained through compromised accounts more than doubled in 2020 versus previous levels, due to the pandemic-spurred increase in remote work via vulnerable VPNs. VPNs broaden the attack surface by exposing open ports. Once a user connects to the network, they often have access to all within the perimeter, which often translates to overly privileged access across apps and resources. VPNs also often lack strong authorization controls that can protect against brute-force attacks and credential stuffing.

Major zero-day vulnerabilities in leading VPNs have been exposed over recent years, including a flaw in the FortiOS SSLVPN found in late 2022. The flaw was widely exploited to deploy trojanized versions of its IPS engine on government networks in what were likely nation-state attacks. This, despite the fact that customers were privately notified to patch their VPNs well before the vulnerability was publicly announced.

## Unmanaged Device Access

Today, many government employees and 3rd party contractors are still working remotely at least part of the time and often on their own unmanaged BYOD devices. But even post-pandemic, only 20% of government workers are able to securely access systems, data and apps from their personal devices and 40% of employees find government security policies to be overly restrictive.

Taking matters into their own hands, many users make liberal use of shadow IT such as Dropbox and Gmail, increasing the risk of breaches and data exposure should their credentials be stolen. The U.S. Cybersecurity & Infrastructure Security Agency (CISA) has warned organizations about the expanded attack surface represented by web browsers on endpoint devices, particularly for users who connect via personal devices.

In a Deloitte survey covering 3rd party risk management, 71% of respondents named digital risk as their top priority. Due to their access to government data and applications, contractors are attractive targets for criminals seeking channels into government systems and information. Use of personal BYOD and unmanaged devices by 3rd party contractors vastly increases the likelihood of accounts being compromised. Since unmanaged devices generally lack enterprise-grade security controls, they may be infected with keyloggers, session-stealing malware or other spyware that enables threat actors to steal user credentials for corporate apps, including basic enterprise apps like Windows365, Microsoft Teams, Salesforce, Zoom and countless others.

The 2021 US Executive Order on Improving the Nation's Cybersecurity requires agencies to improve detection of vulnerabilities on Federal Government networks, starting with endpoints. Agencies that depend on 3rd party contractors will need to find efficient techniques for securing user access without the labor and expense of managing endpoints.

Agencies that depend on 3rd party contractors must find efficient techniques for securing their digital access without the labor and expense required to manage BYOD and external devices.

ZTEdge™
By Ericom Software

Almost all defense-related agencies and many government organizations prohibit use of virtual meeting apps, yet when it comes to getting work done, many users bypass restrictions in favor of the convenience and productivity virtual meetings provide.

## Virtual Meeting Apps Present Unique Risks

Beyond the significant risks associated with most web apps, including attacks on app surfaces and risk from unmanaged devices, virtual meetings like Zoom, Microsoft Teams and similar solutions present particular risk. Exposure of IP addresses, exfiltration of data or PII via screenshares, chat and even video (that whiteboard behind someone's chair!) along with potential attendance of uninvited – and unwanted – attendees are just some of the concerns about using virtual meetings.

Almost all defense-related agencies and many government organizations as well prohibit use of these apps, yet when it comes to getting work done, users tend to bypass restrictions in favor of the convenience and the productivity benefits virtual meeting solutions offer. For instance, during the Covid pandemic, many British government organizations – including the Cabinet – continued meeting online despite Ministry of Defense warnings and discovery of zero-day bugs that allowed hackers to spy on users via their webcams.

ZTEdge™
By Ericom Software

## Malicious Emails

In over 14% of cyberattacks, malicious emails serve as the initial attack vector. Phishing is simply a numbers game: Send enough messages or malicious attachments to enough users and sooner or later, someone will bite. Agencies with large numbers of users or which receive huge volumes of emails, chats and SMSes, and especially those that require attached forms or scans, are at particular risk. Inevitably, some user will click through to an expertly spoofed site and provide their credentials to "sign in" or click on a malicious attachment or link.

As is standard practice in many industries, government employees are often required to participate in periodic anti-phishing training sessions. In assessments of training success, government workers ranked impressively well in terms of phishing vulnerability. In agencies of almost all sizes, they scored under the average "Phish-prone™ Percentage across all industries (in parentheses below.)

| | 1-249 employees | 20-999 employees | 1000+ employees |
|---|---|---|---|
| **Government – pre-training** | 28% (28.8%) | 26.4% (30.2%) | 24.8% (35.2%) |
| **Gov't – within 90 days of training** | 16% (17.5%) | 15.5% (17.9%) | 15.2% (17.4%) |
| **Gov't – after 1 year of ongoing training** | 3.9% (3.8%) | 3.9% (5%) | 7.1% (5.8%) |

Source: KnowB4 2022 Phishing by Industry Benchmarking Report

Rather than depending on employees to be a human firewall that protects your agency, your agency should be protecting users – and citizens – against phishing attacks.

But here's the catch: Given the vast number of emails received by government employees every day, even a 3.9% open rate – the lowest rate on the chart above, and one meant by a training vendor to prove their success -- represents thousands of opportunities for credential theft and malware and ransomware delivery every month in even small agencies, and many millions in larger ones.

What phishing training vendors refer to as the "human layer" of cybersecurity is, in fact, not a protective layer at all: It is a sieve. Rather than depending on employees to protect your government agency, your agency should be protecting users – and citizens – against phishing attacks.

# How Can the Government Sector Prevent Attacks?

The sheer abundance of malware and the rapidity with which new malware and zero days are created and morphed makes reliable detection an unreachable goal. The most widely deployed security tools rely on insufficient detection techniques. And when detection fails, your agency is not protected.

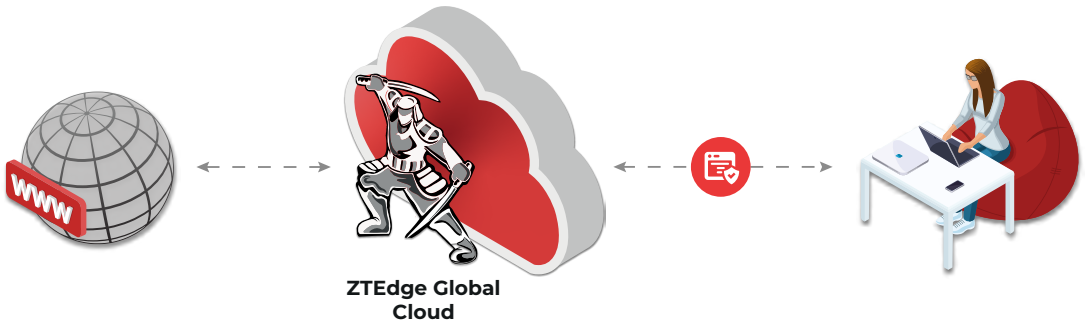
Fortunately, today Zero Trust isolation-based technologies provide effective ways to safeguard your endpoints, apps and resources.

> Today Zero Trust isolation-based technologies provide effective ways to safeguard your endpoints, apps and resources.

## Adopt a Zero Trust Preventative Stance

The internet provides the essential connectivity between users, data and on-premises, web/SaaS and cloud-native apps, enabling virtually all interactions in today's digital economy, as well as cyberattacks.

To protect digital-dependent operations and infrastructure, organizations are increasingly implementing security solutions based on Zero Trust principles. Strong authentication, microsegmentation and security posture management limit access and shrink attack surfaces. The internet, however, remains impossible to verify as safe and therefore, according to Zero Trust principles, should not be trusted. Yet no business or government agency or even military branch can function without it.



ZTEdge™
By Ericom Software

In the past, productivity, efficiency and user experience were all sacrificed to ensure that systems were protected from web-borne threats. But fortunately, those days are gone.

## Isolate What You Can't Trust

Faced with this conundrum over a decade ago, the US National Nuclear Security Administration developed an innovative airgapping approach to protect its systems from web-delivered threats, using virtual machines on isolated servers. More recently, the Defense Information Systems Agency (DISA) issued an RFI for cloud-based airgapping, which they called "Browser Isolation."

While the concept was great, performance was not. As a result, until recently, organizations that require strongest safeguards from data breaches and cyberattacks, such as film and VFX studios as well as the military, continued to maintain systems that were fully separated from the public internet. Productivity, efficiency and user experience were all sacrificed to ensure that systems were protected from web-borne threats. But fortunately, those days are gone.

ZTEdge™
By Ericom Software

# Remote Browser Isolation: High Performance Protection from Internet Threats

Today's advanced cloud-native remote browser isolation solutions are finally delivering the capabilities that CISA envisioned: Military-class protection from internet-borne threats, including zero days, with performance that is transparent to users and a host of policy-driven controls. In its 2020 Capacity Enhancement Guide on Securing Web Browsers and Defending Against Malvertising for Federal Agencies CISA urged federal agencies to join the Department of Defense in adopting browser isolation. The MPA has more recently done the same, citing browser isolation in its Content Security Best Practice Guidelines.

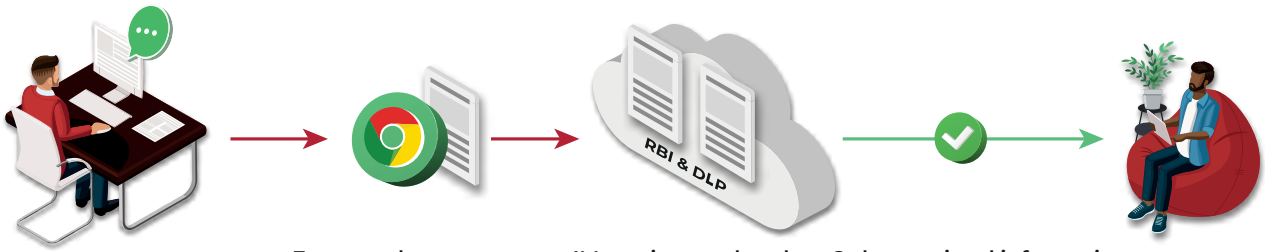
RBI prevents threats from reaching endpoints and networks and increases productivity by reducing over-general website blocklisting and allowlisting. It protects against zero-days that detection-dependent technologies miss and allows government agencies to protect users from phishing, instead of depending on users to protect them.

RBI opens websites in cloud-based containers, sending only safe rendering data to whichever standard browser the user prefers. All active content – including threats like drive-by downloads, ransomware, exploit kits and zero-day malware -- remains isolated in the cloud, safely away from the endpoint and agency networks. Links to unclassified sites are opened in read-only mode so no credentials can be entered.

In addition to the capabilities cited in the CISA Guide, strong browser isolation solutions provide granular controls to prevent exfiltration or leakage of confidential data via shadow IT or email, through policy-based browser controls that can block file uploads and downloads and control functions like cut/paste and printing. The strongest solutions enforce data loss protection (DLP) even for E2EE messaging apps, like WhatsApp.

**ZTEdge Web Isolation**

- Isolate risky web content away from endpoints
- Prevent advanced malware embedded in risky websites, even zero-days, from reaching networks
- Provides Zero Trust web browsing, despite the "unverifiability" of the web
- Integrated CDR examines and when needed, disarms and reconstructs documents in isolation before downloading them with desired functionality intact
- Displays sites opened via clicks on potentially suspicious URLs in "read-only" mode to prevent credential theft
- Integrates easily with existing secure web gateway (SWG)




Encrypted message with sensitive data

IM session rendered remotely; files scanned

Only permitted information shared over IM session

# Application Isolation: Secure Agency App Surfaces from Attack

In recent years, attacks on app surfaces have become a significant threat to public sector organizations. The CISA Binding Operational Directive on Vulnerability Remediation Requirements for Internet-Accessible Systems, requires government agencies to review and remediate critical known vulnerabilities within specified periods. While essential, remediation of known vulnerabilities can't secure business applications from unknown vulnerabilities, zero days, misconfigurations, over-privileged access and more. With government organizations moving to hybrid and cloud-native, protecting app surfaces is increasingly important.

Many organizations use web application firewalls (WAFs) to protect their apps from attack. But WAFs both under- and over-perform, by missing unknown threats yet blocking so many apps that admins often set them to alert-only mode.

Web application isolation (WAI) solutions apply RBI in reverse to protect the surfaces of private apps, cloud/SaaS apps, and those on the public web from malware attacks, threat actors and even zero-day exploits. This cloud-delivered technique creates an airgap between apps and threat actors – in effect, cloaking app surfaces from prying eyes and probes while enabling all functionality. With no visibility to the surface of an agency's applications, hackers cannot discover misconfigurations, unpatched services or other vulnerabilities to exploit.

**ZTEdge Web Application Isolation**

- Airgap web and cloud applications from attackers and/or potentially malicious devices
- Cloak application's web "surfaces" from probes and attacks
- Deploy stand-alone or along with a WAF to bolster security
- Leverage an existing IAM solution or utilize the identity capabilities that come standard in ZTEdge

ZTEdge™
By Ericom Software

# Virtual Meeting Apps Need Special Protection

Virtual meetings like Zoom, Microsoft Teams and similar solutions are sophisticated apps that require seamless alignment of multiple functions – video, audio, chat, screensharing and more. Most browser isolation solutions are not up to this challenging task, putting virtual meetings out of reach for security-forward government organizations and especially defense-related agencies.

ZTEdge Virtual Meeting Isolation (VMI) is the sole RBI solution that preserves an excellent virtual meeting experience while enabling granular browser controls to limit who can share video and screens, and which apps can be shared when screenshares are permitted. To protect sensitive data from being revealed inadvertently (or possibly maliciously) via chats or screenshares, it applies DLP even to end-to-end encrypted chats and blocks confidential information. And to keep unwanted participants from eavesdropping through stolen meeting links or open ports, VMI extends isolation capabilities to all participants, not just those within the organization.

**ZTEdge Virtual Meeting Isolation**

- Control sharing of screen, audio, and chat-based content at user or group level
- Supports Zoom, Microsoft Teams, Google Meet and others
- Cloud service--requires no endpoint agents
- Meetings may include both isolated and non-isolated participants
- Protects against advanced web-based malware
- Users enjoy standard virtual meeting experience in an isolated environment

ZTEdge™
By Ericom Software

# Prevent Credential Theft and Resulting Account Compromise and Data Loss

## Unmanaged Device Access

For government agencies of all sizes, integrating RBI can effectively safeguard users from some of the most widespread ways to steal credentials. First, some RBI solutions open phishing sites in read-only mode to protect users from falling prey to social engineering attacks. In addition, by airgapping user devices from websites, RBI keeps keyloggers, trojans and other spyware off endpoints, so they cannot "see" how users sign in. RBI also prevents malicious actors from stealing session cookies from user browsers and thus prevents MFA from being bypassed.

## Stop Application Compromise and Data Loss via Unmanaged Devices or Stolen Credentials

While your agency might successfully prevent theft of your users' credentials as they work, billions of credentials from millions of breaches are available for purchase from hackers. And more likely than not, some might be used to access your agency's accounts. By transforming the browser into a crucial control point, WAI allows government agencies to control access to sensitive data and corporate applications from potentially compromised unmanaged devices used by contractors and BYODs as well as from stolen credentials. To ensure that protections are in place, government organizations should seek a clientless solution that IT manages in the cloud, without depending on users.

Controls on web/cloud app access include blocking uploads and downloads, disabling or limiting copy, paste and printing, and restricting or blocking data input. WAI can also scan uploads with DLP to prevent data loss. To prevent threat actors from compromising authorized user accounts via stolen credentials, WAI enables remote users using unmanaged devices to log into agency accounts solely via the WAI cloud platform. Attempted logins from other devices or directly from the authenticated user's device – even with legitimate credentials and session cookies – will fail if it is not done via the WAI cloud.

**ZTEdge ZTNA**

- Clientless secure access for unmanaged and managed devices
- Enable IP-based access control to prevent remote app account access via stolen credentials
- Enforce user, group, location and/or device-based policies for SaaS/web app access
- Restrict data capture functionality like clipboarding, printing, downloading, etc.
- Enforce DLP policies to the individual user and PII field levels to protect sensitive data
- Examine and, if needed, disarm and reconstruct documents in isolation before uploading or downloading them
- Provides visibility into which users are accessing SaaS apps from where and when

ZTEdge™
By Ericom Software

## Replace or Strengthen Vulnerable VPNs with Zero Trust Network Access (ZTNA)

Combining ZTNA with WAI – a type of clientless ZTNA - provides strongest protection against the dangers of credential theft, account compromise and data loss for all users, accessing government systems from any device, including unmanaged devices and BYOD.

ZTNA is a smarter, more secure remote solution for accessing private apps and user desktops that replaces vulnerable VPNs. Based on Zero Trust principles instead of outdated perimeter controls, it uses Identity and Access Management (IAM) to apply granular software-defined per-user policy-based controls that enforce least privilege access.

With these protections, in conjunction with micro-segmentation, ZTNA minimizes the potential damage resulting from data breaches via brute force attacks or log-in via the billions of stolen credentials that are available on the web. It also protects against "malicious insiders," who have legitimate network access, but who may be interested in either stealing data or harming systems.


Combining ZTNA with WAI – a type of clientless ZTNA - provides strongest protection against the dangers of credential theft, account compromise and data loss for all users, accessing government systems from any device, including unmanaged devices and BYOD.

# Conclusion

Shutting down cyberattacks by blocking major threat entry vectors goes a long way to choking off the spate of successful attacks on government agencies and departments. Protecting vulnerable endpoints, data and apps from attack can prevent state, local and municipal governments, agencies and departments ranging from defense, infrastructure, budget and health and human services from security and regulatory risk, reputational damage. And it can protect governments and the citizens it served from being burdened by costs, inconvenience and embarrassment of data loss and exposure and recovery.

**Sources:**
1. Cyber Incident Overview
2. The Nature of Cyber Incidents, Kaspersky
3. The State of Ransomware in State and Local Government 2022
4 Microsoft Digital Defense Report 2022
5. Iranian Hackers Exploiting Unpatched Log4j Bugs to Target Israeli Organizations
6. The Endpoint Ecosystem 2022 National Study
7. Capacity Enhancement Guide for Securing Web Browsers
8. Emerging Stronger, Deloitte
9. Executive Order on Improving the Nation's Cybersecurity
10. UK Government Uses Zoom Despite MoD Security Concerns
11. State, Local Govts' Cybersecurity Staffing Challenges Raise Risks
12. Konbriefing
13. KnowB4 2022 Phishing by Industry Benchmarking Report
14. CISA Binding Operational Directive on Vulnerability Remediation Requirements for Internet-Accessible Systems

ERICOM

Ericom Software is a leading provider of cloud-delivered, Zero Trust cybersecurity solutions that protect today's digitally distributed organizations from advanced security threats. The company's ZTEdge™ platform is the industry's most comprehensive and cost-effective Security Service Edge (SSE) solution. Ericom solutions leverage innovative remote browser isolation, application isolation, micro-segmentation, and virtualization technologies, and are delivered on the Ericom Global Cloud, a distributed high-availability elastic cloud platform powered by more than 50 distributed POPs globally

Learn more about our solutions at www.ericom.com or contact us to learn how we can help protect your organizations from cyberattacks.

## Discover how ZTEdge Isolation-based solutions can protect your agency or organization from cyberattacks.

**Request a demo**


www.ericom.com

info@ericom.com

US: (201) 767-2210

Europe: +44 (0) 1905 777970

ROW: +972-2-591-1700