BULLWALL FOR GOVERNMENT

Government institutions around the world are high-value targets for ransomware gangs. Between 2018 and 2023, U.S. government entities experienced cumulative downtime costs exceeding $860 million due to ransomware incidents.

A SUCCESSFUL RANSOMWARE ATTACK CAN HAVE GRAVE CONSEQUENCES THAT REACH FAR BEYOND THE FINANCIAL IMPACT.

From disrupting everyday services, such as benefit payments and access to e-government portals, to blocking emergency services and accessing vital national security systems, the need to stop ransomware attacks swiftly and decisively has never been greater.

WHY BULLWALL?

BullWall provides a specialized ransomware containment solution that protects government institutions by quickly detecting and halting ransomware attacks before attackers can encrypt or exfiltrate data.

By stopping attacks in their tracks, BullWall helps government institutions avoid data breaches that could provide bad actors with access to public health systems, public utilities, tax records and law enforcement databases, to name but a few.

69%

of state and local government organizations **reported being targeted by ransomware**

90%

of these attacks **resulted in data encryption**

The State of Ransomware in State and Local Government 2024, Sophos

> *We cannot take our eyes off the ball,* ***and BullWall Ransomware Containment has given us the additional eyes to help tackle this activity.***
>
> **IT MANAGER**
> of a Large UK Council

HOW GOVERNMENT AGENCIES & DEPARTMENTS BECOME A RANSOMWARE TARGET

PHISHING EMAILS

91%

of all cyberattacks begin with a phishing email to an unsuspecting victim. Public sector organizations experienced an astounding 360% growth in phishing attacks over a 12-month period.

UNPATCHED SOFTWARE & VULNERABILITIES

60%

of breach victims reported being compromised by known vulnerabilities. U.S. agencies CISA, NSA and FBI have stated that malicious cyber actors exploited older software vulnerabilities more often than recently disclosed ones.

COMPROMISED RDP & VPN ACCESS

90%

of ransomware incidents featured RDP abuse by threat actors, and 56% of organizations experienced cyberattacks that exploited VPN security vulnerabilities in the past year, according to recent studies.

THE IMPACT

The impact of an attack far outweighs the simple financial loss of paying the ransom. Several other factors also have long-lasting implications for the future of the affected department or agency.

LAW ENFORCEMENT & JUDICIAL SYSTEMS DATA EXPOSURE

A ransomware attack that compromises government data can violate federal and state data protection laws, such as the Federal Information Security Modernization Act (FISMA), the Privacy Act, and GDPR.

DISRUPTION OF CRITICAL PUBLIC UTILITIES

A ransomware attack on public utilities can have devastating consequences, disrupting essential services such as electricity, water supply, and waste management. By encrypting critical systems and demanding payment for restoration, attackers can incapacitate operational technology, leading to power outages, water contamination risks, and delays in emergency response services.

NATIONAL SECURITY & DEFENSE RISKS

If attackers gain access to defense networks, they could halt communications, disable surveillance systems, or even manipulate sensitive data, putting national security at risk. Such breaches can also expose vulnerabilities to adversaries, leading to espionage or cyber warfare threats.

WHAT IS RANSOMWARE RESILIENCE IN GOVERNMENT?

Ransomware resilience is the ability to prevent, contain, and respond to ransomware attacks, minimizing damage and ensuring rapid recovery of data and operations to maintain business continuity.

PREVENTION

Reduce the risk of disruptions to operations, which can be costly and damaging to productivity.

CONTAINMENT

Minimize the impact to business operations when ransomware gets through, and significantly reduce recovery efforts.

RECOVERY

Resilient organizations recover quickly to limit operational downtime and return stronger.

BE RANSOMWARE READY... WITH BULLWALL

BullWall's unique approach to ransomware provides server-based protection without an endpoint agent to secure critical IT infrastructure and maintain operational continuity across all stages of an attack—before, during, and after.

Phishing emails are cybercriminal's delivery method of choice.

BullWall is the only solution that immediately contains an active attack, regardless of the delivery method, ensuring resilience and business continuity.

Unpatched software and existing vulnerabilities within government systems provide bad actors with easy access to your network.

BullWall protects you from both known vulnerabilities and hidden threats you may not even be aware of.

Bad actors prefer to switch off preventative security solutions using compromised Remote Desktop Protocol (RDP) sessions before launching an

BullWall protects **all data and critical IT infrastructure** – the true targets of a ransomware attack.

ABOUT BULLWALL

BullWall is the pioneer in ransomware resilience, providing robust defenses against the relentless threat of ransomware.

Learn more at www.bullwall.com.

BULLWALL