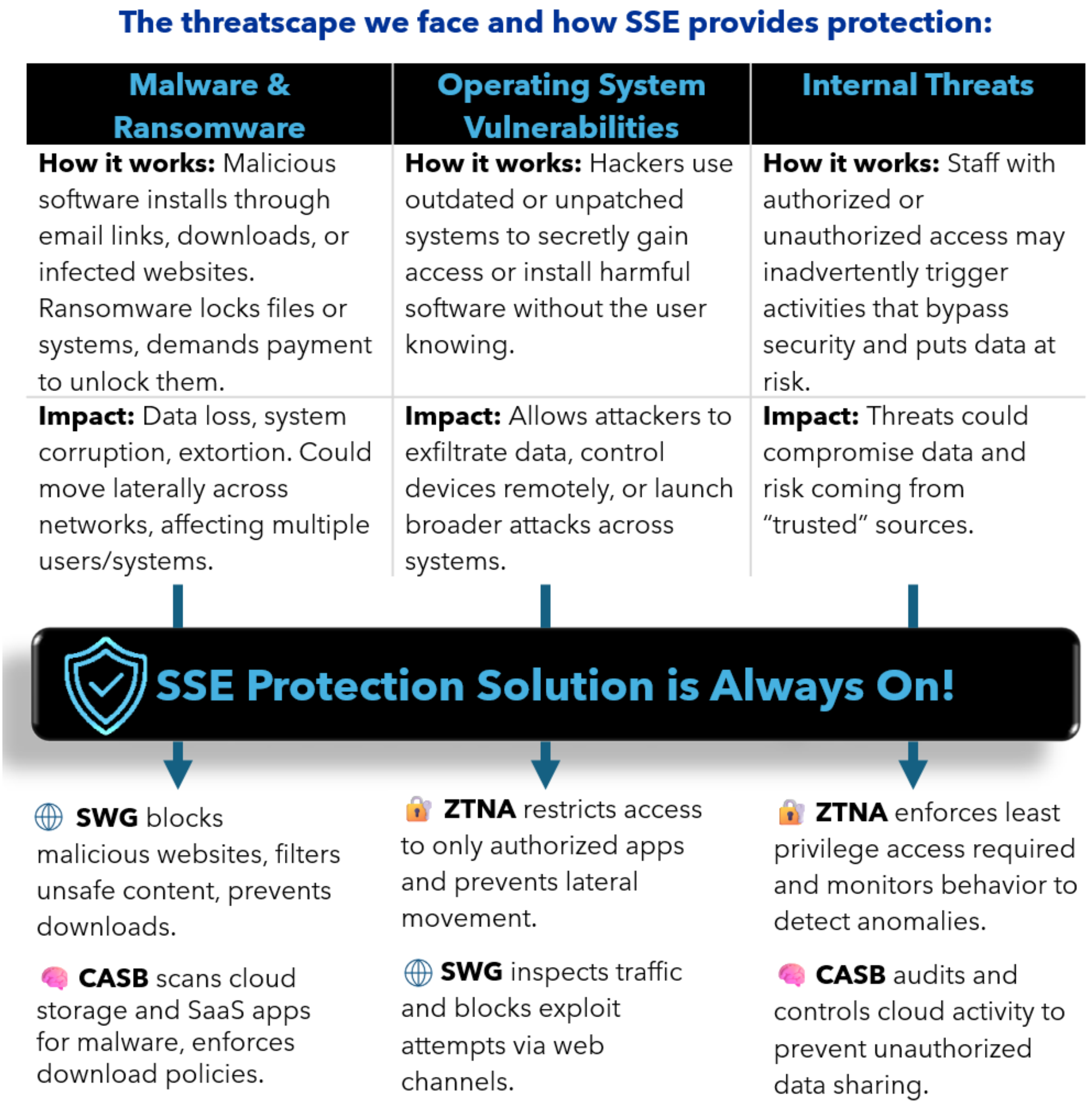
WaTech
Washington Technology Solutions

Security Services Edge (SSE) Onboarding project

Deepening our journey to Zero Trust

Following our initial awareness communication, this message offers a more comprehensive overview of how Security Service Edge (SSE) components safeguard our systems and data.

WaTech is committed to protecting our state workforce from critical threats that could result in data breaches, system disruptions and widespread network vulnerabilities. The SSE platform mitigates these risks through advanced, intelligent security controls. Below, we outline common threats and demonstrate how Secure Web Gateway (SWG), Cloud Access Security Broker (CASB) and Zero Trust Network Access (ZTNA) provide layered protection.



The threatscape we face and how SSE provides protection:

Malware & Ransomware	Operating System Vulnerabilities	Internal Threats
How it works: Malicious software installs through email links, downloads, or infected websites. Ransomware locks files or systems, demands payment to unlock them.	**How it works:** Hackers use outdated or unpatched systems to secretly gain access or install harmful software without the user knowing.	**How it works:** Staff with authorized or unauthorized access may inadvertently trigger activities that bypass security and puts data at risk.
Impact: Data loss, system corruption, extortion. Could move laterally across networks, affecting multiple users/systems.	**Impact:** Allows attackers to exfiltrate data, control devices remotely, or launch broader attacks across systems.	**Impact:** Threats could compromise data and risk coming from "trusted" sources.

SSE Protection Solution is Always On!

🌐 **SWG** blocks malicious websites, filters unsafe content, prevents downloads.

🧠 **CASB** scans cloud storage and SaaS apps for malware, enforces download policies.

🔐 **ZTNA** restricts access to only authorized apps and prevents lateral movement.

🌐 **SWG** inspects traffic and blocks exploit attempts via web channels.

🔐 **ZTNA** enforces least privilege access required and monitors behavior to detect anomalies.

🧠 **CASB** audits and controls cloud activity to prevent unauthorized data sharing.

Starting August 2025, SSE will begin rolling out in phases. Join the onboarding queue to secure your spot! Onboarding users is a gradual process, and agencies need to prepare for this transformational security service!

Who do I contact if I have questions?

- Project specific: Kelly Sanders, SSE Project Manager
- WaTech specific administration: Michelle Marquez, SSE Administrator
- Enterprise service delivery: Cesar Rivera, SSE Business Owner
- Security benefits of the SSE service: Daniel Langley, SSE Security Business Owner

For more information:
Visit our SSE Project Updates Page