



INSIGHTS | SOLUTIONS BRIEF

WEI Cybersecurity Solutions

While many of today's cybersecurity services are primarily focused on perimeter security, there is a growing need for advanced solutions powered by artificial intelligence (AI), machine learning (ML), and automation. As threat actors launch more sophisticated and aggressive campaigns, the security tools that enterprises rely on must evolve. Resources for a proactive cyber approach and the ability to measure ROI from these modern solutions have never been more prevalent. WEI's security team is ready to identify, assess, and develop a holistic solution that reduces MTTD and MTTR, adds value to your organization's cloud practice, and minimizes overall risk.

To protect a complex IT environment and the business it serves, security leaders must know what they are protecting. Our team can help you start your journey, whether it is from scratch or building upon your existing infrastructure.

Security At A Glance



Modern Security Operations Center

Protect your organization with a modern SOC that will greatly improve your ability to detect, respond, and prevent advanced threats and threat actors. Ensure you have an advanced SOC solution that has the ability to scale at anytime, to effectively detect and respond to cyber events that can cripple an organization. Whether your security team is building their SOC, needing a lift with their existing SOC, or looking to implement a next-generation SOC – they can rely on WEI to deliver a solution that drastically improves MTTD and MTTR. A cloud-delivered integrated SOC platform featuring automation, artificial intelligence (AI), and machine learning (ML) are elements that can help ensure your SOC gives your security analysts the solutions they need.

- SIEM
- SOAR
- Endpoint Security
- Threat Detection & Response
- Incident Response
- Security Analytics
- SOCaaS
- Threat Hunting
- Threat Intelligence
- UEBA



For over 30 years, WEI has developed, implemented, and monitored custom-tailored IT solutions across all areas, including cybersecurity. Our deep technical bench stands ready to deploy the most complex solutions to simplify your IT needs.

Cloud Security

As more workloads migrate to the cloud, organizations are selecting the cloud platform that best fits each project. This multi-cloud proliferation has expanded the attack surface of most organizations as many security leaders are managing a hybrid cloud or multi-hybrid cloud environment. Wherever you are in the cloud journey, our experts will craft a custom-tailored security solution that focuses on the present while keeping the future at top of mind. With a thorough cloud security assessment, our team will identify all areas of the cloud -- even the hidden ones -- to enable full visibility for improved detection and response.

- CASB
- CIEM
- Cloud Compliance
- Cloud Security Assessment
- CNAPP
- CSPM
- CWPP
- SAST
- SSE

Network Security

Effective network security reduces exposure to risks that disrupt business operations. Otherwise, these risks can result in costly losses to an organization. When your network is disrupted, so is business operations.

Our experts design a multilayer defense with in-depth strategies defining the boundaries of your various network segments according to function, risk, and role. Policy-driven gateway segments filter traffic between those network segments, ensuring that authorized workloads flow freely to their prescribed destinations while containing malicious code to limit exposure to critical infrastructure. Our team integrates automation and intelligence tools that proactively detect, alert, and remediate threats.

- NGFW
 - Application Control
 - User-based Policies
- SASE
 - ZTNA
 - Cloud Secure Web Gateway
 - Next-gen CASB
 - Branch & SD-WAN
- 5G Security
- Access Control
- Advanced Network Threat Protection
- Behavioral Analytics
- Data Center Security
- Data Loss Prevention
- Internet Security
- Intrusion Prevention
- IoT Security
- Malware Analysis/Sandboxing
- Next-Gen CASB
- Network Segmentation
- Secure DNS Traffic
- Wireless Security
- Workload Security

Email Security

**Powered by Mimecast*

As a vital part to our professional operations, email also exists as common penetration point for threat actors. With one click, the most experienced of employees can unknowingly download infected files while falling victim to a clever phishing scam. Similar to locks on your enterprise's front door, AI-powered email security detection is a required piece to any established cybersecurity practice. Gaining real-time insight into your organization's email attack surface enables security teams to better understand current risks and respond and remediate to threats faster – no matter how large or complex the email environment is.

- Brand Protection
- Cloud App Security Broker
- DMARC, SPF, DKIM Analysis
- Email Fraud Defense
- Insider Risk Protection
- Security Awareness Training
- Targeted Attack Protection
- Threat Response Auto Pull
- URL Filtering
- Web Security

Identity & Access Management

A centralized IAM strategy effectively addresses authentication concerns in the new norm of work from anywhere, siloed hybrid environments, and fragmented user experiences. Ultimately, WEI's IAM solutions can enable your organization's hosted applications to be made available to employees from anywhere, reduce IT workload, and simplify licensing with no hidden costs. Whether it is for in the cloud or on-prem, our forward-thinking approach enhances network access control and identity management, all of which work toward the establishment of zero-trust network access. All information is aggregated for consumption by your firewalls to enforce granular secure policies based on user identify. Authentication methods our solution supports includes SAML, Oauth, RADIUS, LDAP, TACACS and MFA.

- Digital Access Management
- Digital Identity Management
- Identity-as-a-Service
- Identity Governance & Admin
- Network & User Identity Authentication
- OTP Software Token
- Public Key Infrastructure
- Privileged Access Management
- SSO, Adaptive, Passwordless, & MFA
- Token Cloud Management
- User Rights & Access Reviews
- ZTNA

Vulnerability, Asset & Attack Surface Management

Vulnerability Management

Continuous and often automated, a robust vulnerability management process will identify, assess, and address any security weakness within an organization's computer systems, networks, and applications. WEI's helps enable security teams to remain a step ahead of threat actors as our proven practice is designed to remediate such threats before exploitation occurs.

Asset Management

You cannot protect what you don't know is there, which makes it critical to identify each of your organization's cyber-enabled technologies. After your assets have been identified, our team can assist in ongoing monitoring as additions, subtractions, and changes to your technology are inevitable.

Attack Surface Management

IT security leaders have their hands full manually tracking assets between multi, private, and public clouds, inheriting assets via mergers and acquisitions, and access from supply chain partners and remote workers. Our team is ready to step in to assist with discovery, mapping, context, and prioritization, and remediation.

Talk to WEI Today

The solutions that comprise WEI's cybersecurity practice are tailored to effectively reduce detection and response time for your enterprise. In an era where threat actors are deploying the most advanced cyber threats ever seen, our team stands ready to make this complex practice simple for your team to monitor and remediate. For questions about WEI's cybersecurity solutions, please contact our team.