

CIOReview

The Navigator for Enterprise Solutions

CYBER SECURITY SPECIAL

AUGUST 22, 2016

CIOREVIEW.COM

20 Most Promising Cyber Security Solution Providers 2016

In the light of newer and more engaging paradigms being adopted into the organizational infrastructure, such as BYOD and remote work stations, networks are increasingly becoming vulnerable to catastrophic cyber attacks, due to both premeditated and inadvertent actions.

Poised at the helm of helping security teams oust such harmful incidents from happening, experts have come with ways to identify and eliminate potential threats. Cloud-based cyber security tools that cover the end-to-end value chain of an organization to proactively monitor and thwart threats are already making their rounds, reducing cost of ownerships for stakeholders. Stringent firewalls, guided by data analytics algorithms regularly probing into suspicious and iterative patterns, keep perpetrators at

check. Also there are comprehensive endpoint security solutions that ensure appropriate authentication with which security administrators can grant and revoke role-based as well as ad-hoc access to applications, files, and network on a whole.

In an effort to help decision makers uphold the safety of their working environments, a panel of prominent CEOs, CIOs, VCs, analysts, along with the CIOReview editorial board has assessed scores of cyber security solution providers and picked out a list of prime choices.

We have considered the vendor's ability in designing and building advanced cyber security solutions that cater to the enterprise defense needs. We present to you CIOReview's 20 Most Promising Cyber Security Solution Providers 2016.



Company:
Secure Halo

Description:
A cyber security consultancy specializing in enterprise risk assessments and the protection of sensitive information

Key Person:
Sean Doherty
President & Founder

Website:
securehalo.com

Secure Halo

Holistic Approach to Enterprise Security Resiliency

In today's data-driven era, businesses are increasingly becoming susceptible to information breaches and security threats. Although enterprises invest considerably in defensive measures such as firewalls or anti-virus solutions for securing their valuable assets, they may underestimate the vulnerabilities that emanate from other access points. "Threat trends, such as the explosion of ransomware and the exploitation of supply chain weaknesses, are not static," says Sean Doherty, President, Secure Halo. "Yet, we continue to see the standard corporate response is often limited to advance malware detection programs or legacy endpoint protection without understanding actual risks and weaknesses." To defend valuable data against dynamic cyber attacks, businesses must focus on successfully identifying the areas of elevated risk across multiple enterprise domains, particularly from trusted insiders and external business dependencies.

**“
 At Secure Halo, we assess
 vulnerabilities across six major
 domains—insider threats,
 physical security, mobility, data
 security, internal and external
 business operations
 ”**

"We hear from CIOs about budgetary challenges and organizational skills constraints coupled with outsourcing risks. By framing cyber security as an enterprise risk issue and not just an IT issue, we help CIOs make the business case for proactive investments and departmental due diligence that will prevent loss of intellectual property,



Sean Doherty

damage to the brand, and possible devaluation," asserts Doherty. Businesses interested in achieving cyber resilience so they can both prevent and recover from breaches, can look to Washington, DC-area firm Secure Halo, which provides enterprise risk assessment and cyber security consulting across business and technical layers.

Using the firm's patent-pending and U.S. SAFETY Act-designated Threat Vector Manager (TVM) methodology and Enterprise Security Assessment (ESA), TSC experts analyze risk across six fundamental domains to provide an objective 360 degree view of current security posture. "By assessing insider threats, physical security, mobility, data security, internal and external business operations, TSC identifies vulnerabilities in the people, processes and technology of an enterprise," states Doherty. TVM's "Find-Fix-Protect" approach produces an industry benchmarked risk profile score and domain maturity level within the six enterprise domains. With detailed findings, customers are equipped to exceed compliance requirements, make better

informed security resource decisions, qualify for lower cyber insurance rates, and create a cross-departmental security approach for greater resiliency.

Mapped to meet the NIST Cyber Security Framework, various national and international standards, and industry-specific best practices, "TVM and the ESA can identify the most serious threat vectors to data, as well as the limitations of any existing policies and controls protecting it," comments Doherty. One Fortune 50 company used the TSC assessment methodology to identify and contain the source of international supply chain leaks and enterprise-wide vulnerabilities that had caused persistent compromises to new products prior to launch. Another company, one of the nation's largest utilities, developed its entire security plan based on what it learned in a TSC assessment. It earned kudos from its board, had an action plan to justify spending and hiring, and received a reduction on cyber insurance renewal due to its efforts.

Viewing cyber insurance as another tool in the enterprise risk mitigation toolbox, Secur Halo helped pioneer the Critical Asset Protection (CAP) facility designed to address the cyber liability exposures within the U.S utility and energy sector. TSC continues to strengthen its synergy with global underwriters by providing pre- and post-binding enterprise risk assessment to quantify risk in support of cyber insurance policies for critical infrastructure and other industries. Moving forward, "We will continue to refine our enterprise assessment and other services to provide the best value and support to our customers and help them protect their vital assets from unpredictable, modern threats," concludes Doherty. **CR**