Speedcast Cybersecurity



Seamless, end-to-end protection



Cyber attacks happen across all sectors and industries every day, with hackers exploiting open wireless networks and taking advantage of relaxed security postures. According to the latest security industry reports, the average damages from a ransomware data breach are estimated at \$3.9 million and rising.

Speedcast's dynamic cybersecurity solutions help prevent and address threats seamlessly. Leveraging best-of-breed components and real-time threat intelligence, our scalable and adaptable services meet the challenges of an ever-changing threat landscape and diverse budgets in a simple and consistent way.

- **Next Generation Firewall:** Enable, distribute, manage and enforce security policies and profiles globally and locally.
- Endpoint Protections: Secure your PCs and IoT devices against known threats by global signatures, and unknown threats by behavioural monitoring, across simple and complex networks.
- Posture Assessment: Detailed review of security architecture design, implementation and operation, including network devices, servers, desktops, web applications, and related IT infrastructure.
- VPN and Secure Remote Access Service (RAS): Securely communicate between computers or mobile devices and corporate networks from off-site, with RAS enabling administrators to securely connect via the Internet.

DEFEND AGAINST CONSTANTLY EVOLVING CYBER ATTACKS WITH SPEEDCAST'S ADAPTABLE CYBERSECURITY SOLUTIONS.

Contact a Speedcast Sales Representative or email info@speedcast.com for more information.

- Centralized Firewall Management and Reporting: Aggregate logs from all managed firewalls and enable reporting of application use, user activity, and traffic patterns across the network from a central location.
- Web and Application Filtering and Administration: Centrally manage and restrict access to various aspects of the web or applications.

© 2021 Speedcast. All rights reserved. Provision of services is conditioned on execution of a service agreement. Specifications are subject to change; other terms and conditions may apply. Trademarks and trade names are the property of their respective companies. 03/2021

Endpoint Protection

Secure Your Network and Devices from a Central Location



Proactive monitoring, threat mitigation
and auto-response

Centralized near-real-time reporting



Provides 24/7 proactive monitoring services and mitigation support



Designed for high latency, low bandwidth networks

15 building blocks for advanced endpoint security

Anti-virus and antispyware Eliminates viruses, rootkits, worms and spyware	Low system demands Conserves battery life and does not require hardware upgrades	Optional cloud- powered scanning For better detection and faster scanning	Virtualization support Stores metadata within the virtual environment	Host-based intrusion prevention system Defines rules for sys- tem registry, processes, applications and files
Exploit blocker looks for suspicious activities of typical and unknown exploits	Advanced memory scanner Monitors the behavior of malicious processes	Client anti-spam Filters out spam and scans all incoming emails for malware	Web control Limits website access by category	Anti-phishing Protects from attempts by fake websites to acquire sensitive infor- mation
Two-way firewall Prevents unauthorized access to company network	Network attack protection Improves the detec- tion of exploits for known vulnerabilities at network level	Botnet protection Protects against infiltration by botnet malware	Device control Blocks unauthorized devices from system	Threat detection and response Leverages network control and visibility of UTM to provide additional endpoint protection

Comprehensive reports and self-service portal for network and security engineers to review, assess and implement changes that will further enhance and improve network security.



Security Reports

- Firewall events
- Virus events
- Software installed
- Number of nodes

meetamp User	Action			Comment	
020-09-21 19.54: L. Eecher	2 out of date statuses were acknowledged			Master has been contacted with instructions to resolve the outdated alert.	
020-09-08 20:25: L. Eecher	2 out of date statuses were acknowledged			Master has been contacted with instructions to resolve the outdated aints.	
20 08-24 19:50: L. Eechor	1 out of date statuses were acknowledged			IT-Department has been contacted with instructions to	
220-05-29 20.49: L. Eecher					
220-06-24 18:25: CR Ched	IMO 2021: Risk A Every installed/husled no	Assessment de can have their risk assessment	lilled in via the S	if Service Portal.	
	Hostname	Designation	Importance	Importance Motivation	Actions on breakdown
	018_EWAIL	Main Communication Client	PC critical	need to run all times!! / Main Communication PC /	repair / replacement
	018_OFFICE	Master Office Client PC	high	Ships documentation / Vessel Soft / GLSM / SM3	repair / replacement
	018_MASTER_C	Master Cabine Client PC	medium	ni .	repair / replacement
	018_NAVIGATION	Nevigation Client PC	high	ADP/wNP software installed (master pc client) / SMS soft / GLSM Soft / Navigation documentation	repair / replacement
	018_ENGINE	Engine office Clien PC	high	GLSM Soft / Engine Soft / Engine documentation /	repaintoplacement
	018_DECK1	Deck office Client PC	high	Deck PC / Cargo documentation / Cargo Soft	repair / replacement
	018_SERVER	Server Clien PC	oritical	Server PC / Lan communication with all other PC's on board / GLSM Server / All time need be in working condition	repair / replacement
	018_CHARTTABLE	Chart table Clien PC	high	/ SM3 soft / GLSM Soft / Navigation documentation	repair / replacement
	FELICITY-PC	Stability PC client	high	Loading Soft for Stability	repair / replacement
	xchange	Server of Provider of comm	nic critical	Need by all time in good working condition	repair / replacement
	018_LOADING	Loadin Clien PC	nigh	Loading, cargo documentation	repair / replacement
	WIFI	WIFI Flouter	medium	In	repair / replacement
issel: Undisclosed Vesse					

Self-service Portal

Threats found

•

.

- Actions taken
 - Audit Trail