FOR IMMEDIATE RELEASE
March 26, 2020

Contact: Elise Silagy
Marketing Coordinator
Elise.silagy@virtualarmour.com

VirtualArmour Service Offering - Response to COVID-19 Business Continuity

Denver, CO, March 2020: COVID-19 pandemic has forced a rapid shift in business to a remote workforce, something most companies were not prepared to do. With employees working from home for the first-time many IT departments are overwhelmed regarding their cybersecurity and the expansion of their Remote Access VPNs. While having employees work from home reduces the risk of spreading and contracting the virus, this also puts business data at risk to malicious security threats. An unprotected remote workforce increases a company's chance of security threats and can lead to detrimental consequences for a business – some even being forced into bankruptcy. In order to protect the remote workforce and prevent data loss, businesses will need to keep a close eye on security or hire an outside Managed Security Services Provider (MSSP) to ensure their information is secure. VirtualArmour has expertise in supporting a work from home capability for our current customers and with the business shift, have experienced a major uptick in inbound requests to provide this capability.

Over the next several weeks, many businesses will be evaluating the steps they need to take to protect their business from security threats. VirtualArmour CEO, Russ Armbrust commented on the current economic situation, "We are seeing a huge shift in the business environment, I believe this is not only a short-term impact but the shift will become a long-term solution for a way to conduct business. I believe we will start to see many companies embrace the work from home lifestyle for their employees to boost profitability and save on cost in the near future." As for steps that can be taken in the immediate future, VirtualArmour suggests:

Implement Virtual Private Networks (VPN): *VPNs allow employees to access the resources they need securely. VPNs are a useful security tool for remote workers because it provides access to company resources by way of a private network. This protects companies by encrypting web traffic from hackers looking to access private information. An additional layer of protection that works side by side with VPN, is firewall protection.*
Remote Access VPN Service: Secure your remote workforce and empower always/anywhere productivity. We design, deploy, & monitor VPN connections for businesses and institutions of all sizes.

Device Protection: *Devices outside the office are more vulnerable to attacks. Advise staff about the risk of having their devices outside the office and how to reduce the loss of their devices.*
SIEM Health Check Service: SIEM Health Check will evaluate and review an existing SIEM deployment against industry best practices. VirtualArmour will review overall SIEM environment for correct software levels, EPS licenses, and reporting.

Reporting on Security Issues: *Put in place a system where employees can report any security issues they might encounter while working remotely. There will be an increase in the number of email scams regarding the Coronavirus. Advise employees about email scams and how to identify if the email is authentic or not.*
Vulnerability Scanning Service: VirtualArmour has a team of engineers that can monitor and find potential security threats 24/7. Once a threat is detected, an engineer will take action within minutes to remove the threat. Our engineers will alert you to the incident, file a report, and record it in our client portal.

About VirtualArmour
VirtualArmour is a global Managed Security Services Provider (MSSP) that delivers custom security services tailored to meet the needs of our clients. VirtualArmour manages the entire security lifecycle, from initial alerting, to the investigation phase to resolution. Visit us at www.virtualarmour.com