ARMOR OUTCOMES AT A GLANCE

PAIN POINTS	TRADITIONAL APPROACH	ARMOR'S APPROACH
Procuring, Installing, and Monitoring All Necessary Cybersecurity Solutions Needed to Respond to Threats (Such as FIM, IDS, Vulnerability Scanning, Malware Protection, etc.)	▪ Multiple cybersecurity tools are needed to secure a customer's environment. ▪ SIEM, SOAR, and security expertise are required to manage, interpret, and action/remediate the output of the tools. ▪ Customers need to provide integration and management, monitoring, and administration. Customers need to create, manage, and tune rule-sets. ▪ Customers also need to deal with the impact of potentially long dwell times and significant false positive rates.	▪ Rather than having separate contracts for each service or solution, Armor offers a single contract for your security and compliance needs. ▪ Armor Anywhere will reduce your business risk and increase your resource efficiency by delivering industry-leading dwell time and false positive rates. ▪ Armor's security operations center (SOC) provides 24/7/365 support, which includes guided remediation. ▪ Armor consolidates best-in-class cybersecurity tools, including malware protection, file integrity monitoring, intrusion detection, intrusion prevention, vulnerability scanning, and recommendation scans. ▪ These tools are integrated with SIEM and SOAR capabilities to deliver a turnkey solution tuned and configured to identify threats.
Increase of Threats and Breaches	▪ Customers need to have their own threat intelligence team or procure and integrate third-party feeds. ▪ Cybersecurity experts are needed to identify and understand the different threats in an environment.	▪ Armor Anywhere includes threat intelligence and threat research from Armor's Threat Resistance Unit. It also includes community insights from Armor's 1,500 customers, as well as subscribed threat feeds.

PAIN POINTS	TRADITIONAL APPROACH	ARMOR'S APPROACH
Native Cloud Connections	▪ Customers need to import event logs and collate rule-sets for interpretation for each environment within each of the log sources. ▪ A cybersecurity engineer and analysts are needed to understand the logs and alerts being flagged. ▪ Subscriptions to log storage are needed to comply with some compliance mandates and for forensics and research.	▪ Native log sources are available for ingestion, normalization, and correlation. ▪ Log storage is included for the agent security capabilities. ▪ Long-term log storage is available with Armor Anywhere.
Cybersecurity Resources and 24/7/365 Environment Monitoring	▪ Full-time equivalent (FTE) resources are needed to support the organization's environment during the business work day/week. To ensure that 24/7/365 coverage is available, organizations will need to hire additional resources.	▪ 24/7/365 Security Operations Center (SOC) monitoring and support is included with Armor Anywhere. Armor's SOC is manned by cybersecurity experts with extensive years of experience.
Incident Management	▪ A resource is required to remediate the incident, stop the breach, and perform root cause forensic analysis to prevent it from recurring.	▪ Detailed incident tickets and guided remediation are included with Armor Anywhere. ▪ Armor's SOC is available to help guide customers with remediation.
Transferring Cybersecurity Solutions from One System to Another	▪ Services need to be reinstalled and reconfigured when a service is moved.	▪ Armor Anywhere moves with the instance and operates as "security as code."
Cybersecurity Solution Not Scalable to Meet Business Needs	▪ When new instances are deployed, manual intervention could be required and additional licenses would need to be procured.	▪ Armor Anywhere is a scalable solution that is easy to install, with a single line of code. Armor Anywhere has a bursting option and customers pay based on utilization for this feature.
Cybersecurity Tool Maintenance and Life Cycle Management	▪ All of the individual point tools, as well as any SIEM or SOAR platforms, will need to be managed, maintained, patched, and configured. Upgrades are also needed over time. ▪ New technology adoption means a "forklift upgrade" and revalidating integration and rule changes.	▪ Armor maintains, monitors, and upgrades the cybersecurity tools as part of the Armor Anywhere offer.

ARMOR

PAIN POINTS	TRADITIONAL APPROACH	ARMOR'S APPROACH
Deployment Time	▪ It takes days, weeks, or even months to deploy and configure certain cybersecurity solutions.	▪ Armor Anywhere deploys and protects in minutes.
Managing Datacenters	▪ Most solutions require infrastructure deployment. This requires planning, heating, cooling, and datacenter costs. Whether physical or virtual, these require ongoing patch management and integration.	▪ Armor provides a secure hosting solution that requires no infrastructure planning on the customer's part. Armor handles the infrastructure and provides a turnkey solution.
Security Health	▪ Customers monitor the continuous availability of the security tools and then diagnose and fix any issues.	▪ Armor constantly monitors the health of the infrastructure and informs on current status. Armor provides guidance to remediation and restore service. Support is also available as part of the service.
Log Storage	▪ Customers need to provision, manage, retain, and secure log data for compliance and analysis purposes. ▪ An expert resource is also needed for data storage management.	▪ Extended log storage is available with Armor Anywhere for up to 13 months. ▪ Logs are available for search and analysis purposes.
Log Search and Visualization	▪ Customers procure and maintain tools to run analytics and visualize their data.	▪ This feature is included with Armor Anywhere.
Compliance	▪ Compliance is burdensome for customers. Compliance audits take both time and resources to meet.	▪ Armor Anywhere is an audit-ready compliance solution. It addresses certain compliance controls within frameworks, such as HIPAA, PIC DSS, and SOC 2. Through its technology stack, Armor Anywhere saves time and money while simplifying and reducing the burden of meeting compliance standards.
Visibility	▪ Customers typically manage multiple dashboards depending on the number of vendors they deploy. Customers might also attempt to integrate these tools into one dashboard which will require significant resources, time, and expertise.	▪ Armor delivers unified visibility across public, private, or hybrid environments on a single pane of glass via the Armor Management Portal.

ARMOR