AGENDA

1. Industry Trivia

2. Today's Landscape

3. Your Opportunity

4. Customer Journey

5. Tomorrow – Where We're Going!

MATT COOK

Chief Revenue Officer (CRM)

Matt comes to Armor from Commvault, a cloud backup and recovery technology company, where he served as Senior Director for the Americas VAR, Alliances, and OEM teams. He later took over as Vice President of the company's Service Provider and Geo sales segments. Matt comes to us with a wide breadth of experience leading and growing partner programs at Commvault, Forsythe and Cisco. While at Cisco, Matt spent 7 years leading a team of direct and indirect team members supporting some of the company's largest partners in the U.S. He also successfully spearheaded the creation of Cisco's Global Virtual Distribution Model and co-led the company's global collaborative initiative known as the Global Partner Network (GPN). In this role he served as chief architect, defining and guiding Cisco's strategy for global go-to-market through channels.
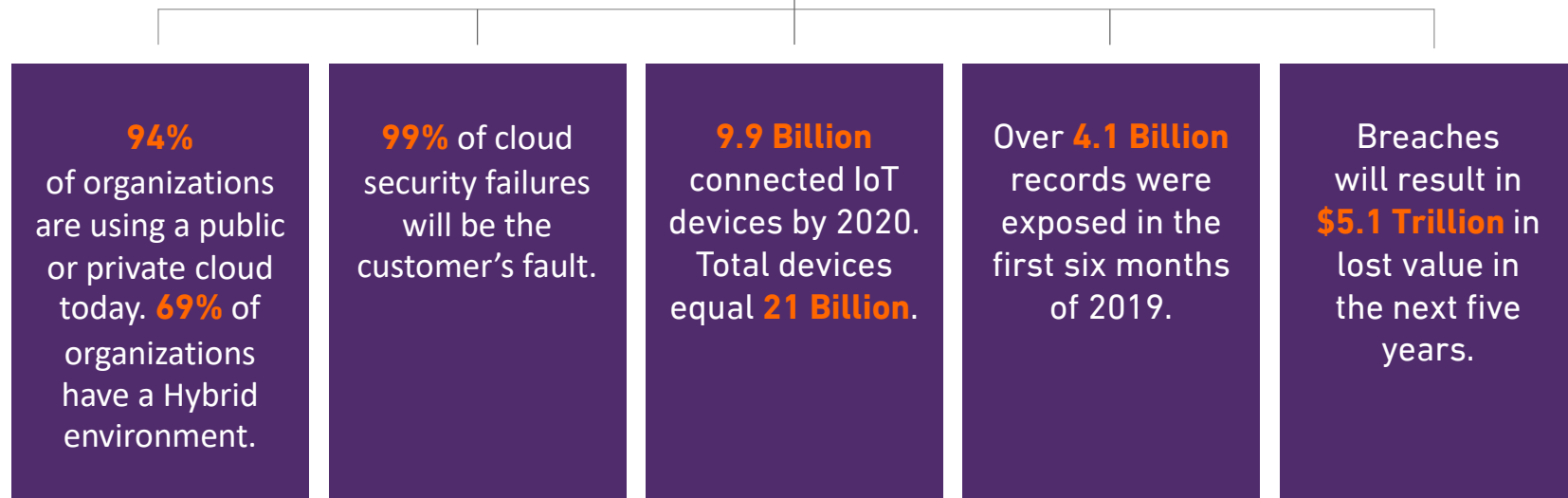
Contact me at:
matt.cook@armor.com

INDUSTRY TRIVIA

THE NEED FOR SECURITY CONTINUES TO INCREASE

94% of organizations are using a public or private cloud today. **69%** of organizations have a Hybrid environment.

99% of cloud security failures will be the customer's fault.

9.9 Billion connected IoT devices by 2020. Total devices equal **21 Billion**.

Over **4.1 Billion** records were exposed in the first six months of 2019.

Breaches will result in **$5.1 Trillion** in lost value in the next five years.

MARKET OPPORTUNITY WITH ARMOR

Spend for public cloud services will reach **$331 Billion** in 2022

~ $13B Cloud Security Market

CSPM MARKET 2024: 80% reduced cloud-related security incidents

CROSS-SELL, UP-SELL & SELL-THROUGH existing Armor portfolio & ancillary services
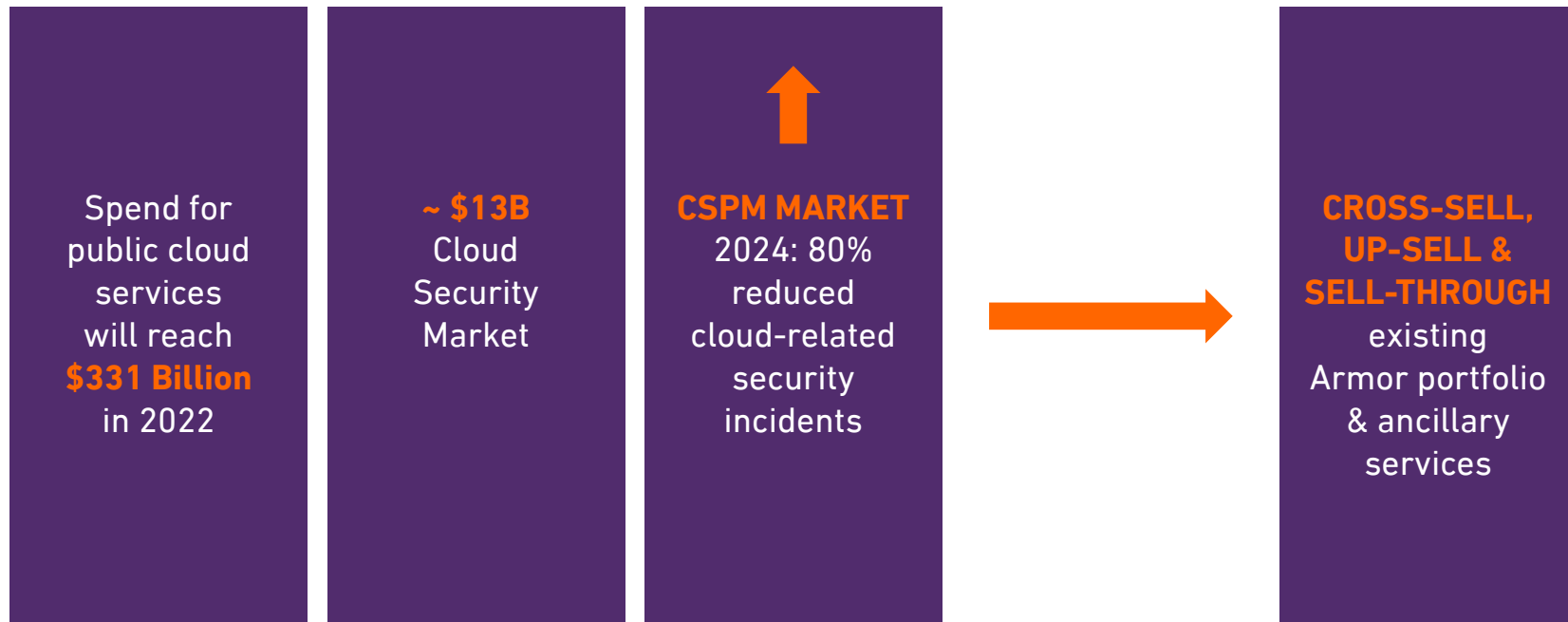
TODAY'S LANDSCAPE

THE ARMOR PLATFORM DELIVERS

INDUSTRY-LEADING THREAT DETECTION AND RESPONSE

CONTINUOUS COMPLIANCE

24/7/365 SOC EXPERTISE

ONE PLATFORM FOR EXECUTIVES, DEVELOPERS, AND SECURITY PROFESSIONALS

SAME DAY TURN-UP—PROTECT IMMEDIATELY
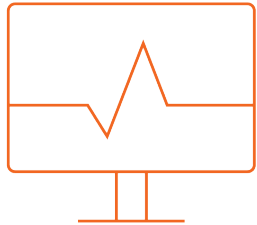
ARMOR—SECURITY ACROSS ALL ENVIRONMENTS

SECURITY AT EVERY LAYER

- Armor Anywhere
  - IDS
  - Malware Protection
  - FIM
  - Vulnerability Scanning
  - Patch Monitoring
  - Threat Hunting
  - Response
- Armor Dynamic Threat Blocking
- Armor Log and Data Management
- Armor Automated Security and Compliance – Prisma Public Cloud

MULTICLOUD

aws

Azure

Google Cloud

ARMOR

On - Prem

MULTIPLATFORM

- Containers
- Container OS

docker

kubernetes

- Host OS
- PaaS

Unified Visibility and Control

INDUSTRIES

WE DO BEST IN INDUSTRIES THAT HAVE A CLEAR COMPLIANCE OVERLAY

HEALTHCARE   **FINANCIAL**   **RETAIL**   **TECHNOLOGY**

We do best in industries that have a clear compliance overlay and application and data sensitivity.

YOUR MARGIN OPPORTUNITY
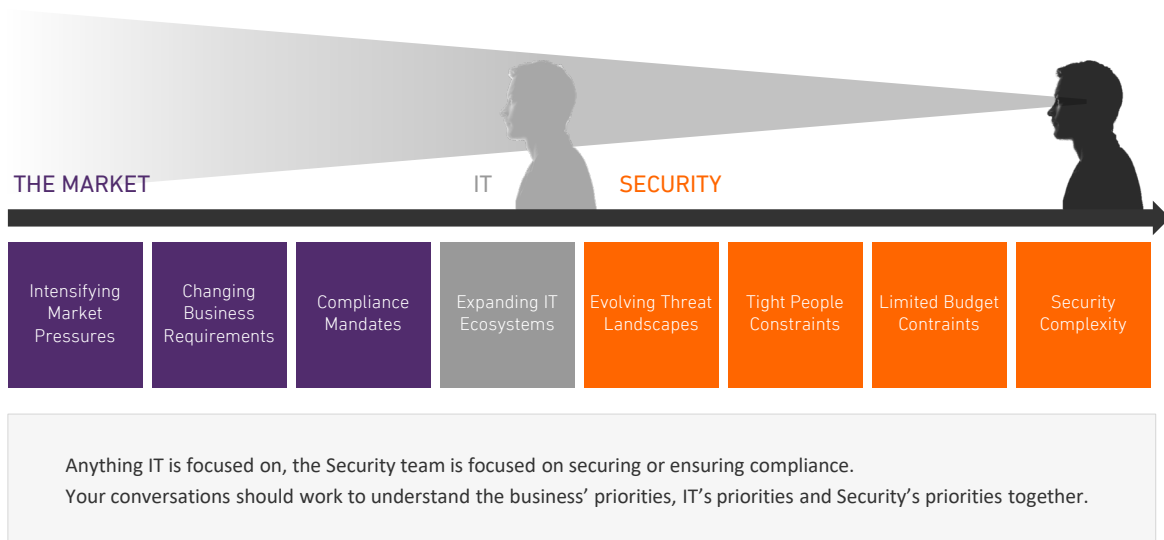
MARGIN WITH ARMOR 40%.

CUSTOMER JOURNEY

THE ULTIMATE IMPERATIVE: PROTECT THE FUTURE OF THE BUSINESS

This means:

- Securing new business models and strategic initiatives the company is undertaking

- Enabling company growth without commensurate growth in risk

- Helping the business comply with applicable mandates easily and for the least amount of cost and impact

- Enabling operational enhancements and improvements without concerns for risk

If IT has the business' back. It's Security that has IT's back

THE MARKET   IT   SECURITY

| Intensifying Market Pressures | Changing Business Requirements | Compliance Mandates | Expanding IT Ecosystems | Evolving Threat Landscapes | Tight People Constraints | Limited Budget Contraints | Security Complexity |

Anything IT is focused on, the Security team is focused on securing or ensuring compliance.

Your conversations should work to understand the business' priorities, IT's priorities and Security's priorities together.

SECURITY MATURITY MODEL

	Initial 1.0	Developing 2.0	Defined 3.0	Managed 4.0	Optimized 5.0
PEOPLE	Activities unstaffed or uncoordinated	Infosec leadership established, informal communications	Some roles and responsibilities established	Increased resources and awareness, clearly defined roles and responsibilities	Culture supports continuous improvement to security skills, process, technology
PROCESS	No formal security program in place	Basic governance and risk management process, policies	Organization-wide processes and policies in place but minimal verification	Formal infosec committees, verification and measurement processes	Processes more comprehensively implemented, risk-based and quantitatively understood
TECHNOLOGY	Despite security issues, no controls exist	Some controls in development with limited documentation	More controls documented and developed, but over-reliant on individual efforts	Controls monitored, measured for compliance, but uneven levels of automation	Controls more comprehensively implemented, automated and subject to continuous improvement

WHERE WE'RE GOING

Q & A

MATT COOK

Chief Revenue Office (CRM)