CLOUD SECURITY MESH ARCHITECTURE – A NEW KID IN TOWN

ABBAS KUDRATI
APAC CHIEF CYBERSECURITY ADVISOR
@askudrati
https://aka.ms/abbas

AUSTRALIAN CYBER CONFERENCE 2022

About me

- **Cybersecurity practitioner and CISO with 25 years of experience in Information / Cybersecurity.**
- **Part time Cybersecurity Professor with Deakin and LaTrobe University in Melbourne, Australia.**
- **Expertise in Zero Trust, Cybersecurity Strategy, Security Operations, Risk, Compliance, Cloud Security and Architecture.**

My Publications

Get it on Amazon
Or send me a request for a free copy

Order on Amazon

Releasing soon by Dec 2022

Releasing soon by March 2023

Managing complexity

Complexity is the enemy of intelligent security

$1.37M

On average that an organization spends annually in time wasted responding to erroneous malware alerts

"The Cost of Insecure Endpoints" Ponemon Institute© Research Report, June 2017

1.87M

Global cybersecurity workforce shortage by 2022

Global Information Security Workforce Study 2017

70 **Security products** from **35** **Security vendors**

Is the average for companies with over 1,000 employees

Nick McQuire, VP Enterprise Research CCS Insight.

CYBER SCAPE 2021

Network & Infrastructure Security

Advanced Threat Protection
Barracuda, BlueHexagon, Blue Vector, Broadcom, Check Point, Cisco, Corsa, FireEye, Fortinet, Huawei, Hysolate, Joe Security, Juniper, Lastline, McAfee, Mimecast, OPSWAT, Paloalto, RESEC, Sasa Software, SonicWall, Sophos, Vectra, Voriro, WatchGuard

ICS + OT
Aperio, Bayshore, Belden, Cisco, CS, Cimpence, Cyberx, Dragos, Endian, Forescout, Halo Digital, Nextnine, Nozomi Networks, Owl, PFP, Radiflow, Rhebo, SCADAfence, Tenable, Verve

NAC
Aruba, Bivonet, Cisco, Axonius, Extreme, Forescout, Fortinet, Genians, Portnox, Pulse Secure, Trustwave

SDN
Cisco, Cyberx, Cyberia, Tempered, Transient, Versa, Zentera, Zero, Zscaler

DDoS Protection
Akamai, Check Point, Cisco, F5, Fortinet, Imperva, Neustar, Nexusguard, Nsfocus, Oracle, Secure64

DNS Security
Bluecat, Cisco, Cyber, efficient IP, Infoblox, Neustar, Secure64, Threat Stop

Network Firewall
algosec, Cato, Check Point, Cisco, Clavister, endian, Forcepoint, Fortinet, Huawei, Paloalto, Sophos, tufin

Network Analysis & Forensics
Awake, Bricata, CGS, Cisco, Cloudshark, Core, Corelight, Darktrace, Extrahop, Fidelis, Gigamon, Netscout, Secdo, SS8, Utimaco, Vectra, Verint

SASE
Cato, Check Point, Forcepoint, Fortinet, Iboss, netskope, Paloalto, Perimeter 81, Versa, Zscaler

Deception
Acalvio, Attivo, Cloudstar, Cyber Trap, Fidelis, Illusive, Morphisec, Trapx

Web Security
Akamai, Aurionpro, Authentic8, Barracuda, Broadcom, Capy, Cequence, Check Point, Cisco, Contentkeeper, Cyren, Defiant, Digicert, Ericom, F5, Forcepoint, Fortinet, Goscure, Iboss, Imperva, McAfee, Menlo Security, Micro Focus, Nanogo, Perimeter81, Proofpoint, Randed, Reblaze, Rellecliz, SH=PE, Shiel Square, Smoothwall, Sophos, Source, Trend Micro, Trustwave, Unbotify, Whitecope, Zscaler

Endpoint Security

Endpoint Prevention
AhnLab, Avast, Avira, Beyondtrust, Blackberry, Broadcom, Check Point, Comodo, Cyberark, Deepinstinct, Elastic, Ericom, ESET, F-Secure, Fortinet, Hysolate, Intego, Ivanti, Kaspersky, McAfee, Microsoft, Morphisec, Paloalto, Panda, Sentinel One, OPSWAT, Sophos, Sparkcognition, Tehtris, Trend Micro, Vmware, Webroot, Zlo

Endpoint Detection & Response
Belden, Binary Defense, Bitdefender, Blackberry, Broadcom, Cisco, Comodo, Cybonet, Cynet, Dtex, Elastic, Fenrir, Fidelis, Fireeye, Forcepoint, Fortinet, Goscure, Huntress, Kaspersky, Nightwatch, Nexthink, Paloalto, Panda, Promsec, RSA, Secpod, Sentinel One, Sophos, Tanium, Tehtris, Vmware, Webroot, Ziften

Application Security

WAF & Application Security
Aiu, Akamai, Arxan, Barracuda, Cequence, Citrix, Cloudflare, Contrast, Ergon, F5, Fortinet, Imperva, Netsparker, Netspi, Onapsis, Oracle, Paloalto, Penta Security, Portshift, Protego, Qualys, Radware, Rapid7, Reblaze, Riverbed, Safe-t, Sec Works, SH=PE, Signal Sciences, Sqreen, Stackpath, Sucuri, Templarbit, Threatx, Trend Micro, Trustwave, Veracode, Wallarm, Waratek

Application Security Testing
Acunetix, Beyond, Bugcrowd, Checkmarx, Cigniti, Cryptsoft, Erpscan, Fasoo, Hackerone, IBM, Kryptowire, Micro Focus, N-Stalker, Nowsecure, Onapsis, Parasoft, Perforce, Portswigger, Qualys, Rapid7, Security Compass, Sitelock, Sonarsource, Synack, Synopsys, Tenable, Trustwave, Veracode, Whitehat, White Source

MSSP

Traditional MSSP
Accenture, AT&T, Atos, Secureworks, BT, Cordant, Dell, Deloitte, Fujitsu, Forsite, IBM, Mcafee, NTT, Optiv, Rapid7, Secureworks, Trustwave, Verizon, Wipro

Advanced MSS & MDR
Arctic Wolf, Alert Logic, Cipher, Cisco, Cloudstar, Cyber Hoot, Deepwatch, Eset, Fortinet, Fujitsu, Kivu, Mcafee, Nttcs, Optiv, Pantaxis, Proofpoint, Rapid7, Redseal, Secureworks, Sentinel One, Sophos, Trustwave, Unisys, Verizon, Wipro

Data Security

Encryption
Anjuna, Baffle, Bitlocker, Cipherloq, Cipherwise, Cipher Cloud, Cloudlock, Cloudsec, Crypsis, Cryptsoft, Cyphertrust, Cyphertec, Dell, Dfinity, Dome9, Envil, Fortanix, Fortinet, Hyperfish, Hyperproof, Hyperscience, Ionic, Jumio, Kryptowire, Lockbit, Mcafee, Microsoft, Nitrokey, Nuance, Nuvoloso, Proofpoint, Protegrity, Pulsecure, Qualys, Quantum Xchange, Quantum Xcelerator, Quantum Xcelerator, Sophos, Symantec, Thales, Thycotic, Vectra, Vera, Wickr, Wire, Wisekey

DLP
Broadcom, Checkpoint, Code42, Cososo, Dasera, Fidelis, Forcepoint, Gtb Technologies, Mcafee, Searchinform, Somansa, Zecurion

Data Privacy
Actifile, Bigid, Cavewall, Did, Enterprise Ground Labs, Ground Labs, Hyperproof, Hyperscience, Netapp, Nuix, One Trust, Privitar, Secupi, Simeio, Symitar, Titus, Vera, Wirewheel, Trustarc, Trust-hub

Data Centric Security
Code42, Cryptsoft, Dtex, Datiphy, Druva, Egress, Enterprise Ground Labs, Ionic, Microsoft, Opentext, Proofpoint, Reglore, Sensitive Data, Sonrai, Vera

Mobile Security
Appdome, Better, Blackberry, Bluecedar, Cellrox, Check Point, Communitake, Cyberbodapt, Deepinstinct, Emune, Fyde, Inpedio, Kaspersky, Kryptowire, Lockout, Mobileiron, Nortonlifelock, Nowsecure, Pradeo, Psafe, Saltdna, Silent Circle, Soti, Telesign, Ateskalabs, Tigerconnect, Trustlook, Vaulto, Vmware, Wandera, Wickr, Zimperium

Risk & Compliance

Risk Assessment & Visibility
Balbix, Cavirin, Cidalfire, Coalition, Cyberseer, Cybersaint, Cyber Sec, Delve, Cyglass, Infosec, Kenna, Kocaler, Mnemosec, Nopsec, Outpost24, Prevalent, Redseal, Riskrecon, Riskwatch, Tenable, Upguard, Venafi, Vendrider, Zeguro, Zerofox

Risk Quantification
Arcoda, Bitsight, Corax, Fico, Goldenwire, Kenna, Prevalent, Risk Lens, Safe Breach, Tenable

Pen Testing & Breach Simulation
Attackiq, Cobalt, Cyberbit, Cyberwatch, Cyberx, Cyfirma, Cymulate, Deepfix, Fireeye, Knowsecurity, Mandiant, Picus, Rapid7, Safebreach, Ute, Xm Cyber

GRC
algosec, Archerx, Galvanize, Lockpath, Metricstream, Network, Onspring, Resolver, RSA, Sai Global, Trustmap, tufin

Security Awareness & Training
Barracuda, Cisco, Cybrary, Cyberguide, Hoxhunt, Security Mentor, Cyberlab, Knowbe4, Proofpoint, Sans

Momentum Cyber

Security Operations & Incident Response

SIEM
AT&T Cybersecurity, Blackstratus, bmc, Cyclant, Devo, Dnif, exabeam, Fortinet, HanSight, Huntsman, IBM, Logentries, Logpoint, Logrhythm, logz.io, McAfee, Micro Focus, Netsurion, Eventtracker, Palantir, Rapid7, RSA, Sawmill, Securonix, solarwinds, splunk, sumo logic, TIBCO, Trustwave

Security Incident Response
Arctos networks, atarlabs, ayehu, Cyberfortune, Cyber Triage, D3 Security, Darklight, Demisto, DFLabs, Encode, Fireeye, IBM, Kivu, McAfee, Microsoft, Netskope, paloalto, Query.ai, Radar Cyber Security, Rapid7, Raytheon, Sec, servicenow, Simplify, splunk, Swimlane, Threatconnect, Verint, witfoo

Security Analytics
Awake, Broadcom, Cyxtraft, Darktrace, Dtex, Empow, exabeam, Fluency, Fortinet, HanSight, haystax, Imvision Technologies, IronNet, Logrhythm, Micro Focus, observe it, paloalto, Patternex, Reservoir Labs, Vidium, RSA, Sec, Securonix, sumo logic, Teramind, Thetaray, Vectra, Veriato, vmware

Threat Intelligence
4iq, Anomali, Blueliv, Bluevoyant, Centripetal, Cisco, Cyberint, Digital Shadows, Domaintools, Eclectiq, Forsight Security, Flashpoint, Group-ib, HanSight, Intel471, Intsights, Kela, LexisNexis, Lookingglass, Malware Patrol, Nucleon, Recorded Future, Reversinglabs, Riskbased Security, Riskio, Sixgill, Skurio, Spycloud, Threatconnect, Threatquotient, Threatstop, Trustar, Webroot

IoT

IoT Devices
Armis, Bastille, Blackberry, Centri, Cyber, Mdx, Cylus, Dellfer, Forescout, Kaiji, Levl, Mocana, Ordr, Nexus, Nscure, Rubicon, Sensus, Tenable, Tenable, Tenable

Automotive
Blackberry, Blue, C2a, Cellmental, Cymotive, Enigmatos, Foretellix, Guardknox, Harman, Karamba Security, Ng, Otonomo, Saferide, Trillium, Upstream

Connected Home
Bitdefender, Cujoai, F-Secure, Fortress, Nortonlifelock, Rubica, Sam

Messaging Security
Agari, Area 1, Bae Systems, Barracuda, Blackberry, Cisco, Clearswift, Cybonet, Cyren, Fireeye, Forcepoint, Fortinet, Goscure, Greathorn, Inky, Knowsecure, Mailguard, Mcafee, Micro Focus, Microsoft, Mimecast, Nortonlifelock, Phishlabs, Proofpoint, Sasa Software, Sonicwall, Sophos, Trend Micro, Trustwave, Vade Secure, Valimail, Voriro, Webroot, Wickr, Zerospam, Zix

Digital Risk Management
Acid, Cyber Intelligence, Digital Shadows, Digital Ocean, Dnstwister, Nanogo, Phishlabs, Rellecliz, Risk IO, Safeguard Cyber, Zerofox

Security Consulting & Services
Accenture, Adaptive, Align, Aon, Bdo, Bsi, Bt, Cdalfire, Cerbo, Cisco, Deloitte, Dhs Group, Ey, Fireeye, Gahtech, Gray Castle, Hcl, Ibm, Ioactive, Kivu, Kpmg, Leidos, Lifeq, Mindpoint, Nccgroup, Nec, Nsigo, Ntt, Optiv, Pwc, Revealrisk, Security Compass, Setaccess, Sygnia, Wipro

Blockchain
Anchain, Blockarmour, Chainalysis, Edge, Guardtime, Idee, Interstellar, Nuid, Remme, Validnetwork, Xage, Zamna

Fraud & Transaction Security
Bincatch, Block Fraud, Brighterion, Cardinal, Datavisor, Early Warning, Emalage, Ethoca, Evercompliant, Feedzai, Fico, Fiserv, Forter, Group-ib, Guardian Analytics, Identitymind, Identrust, Kount, Lexisnexis, Magicube, Mastercard, Netguardians, Nice, Nicetech, Nsfocus, Nudata Security, Oneera, Riskified, Sift, Signifyd, Simility, Secure, Talon, Transunion, Uniken, Technology, Whitecope

Identity & Access Management

Authentication
Acceptto, Authd, Averon, Behaviosec, Bioconfidence, Blackberry, Callsign, Centrify, Core, Duo, Exostar, Forgerock, Fudo, Google, Idee, Imprivata, Intrinsic ID, Jumio, Lexisnexis, Nok nok, Pindrop, Ping, Plainid, Saaspass, Safepass, Secure Auth, Secure Key, Secure Push, Silverfort, Tascent, Transmit, Transunion, Trusona, Unbound ID, Unifyid, Uniken, V-key, Veridium

IDaaS
Avatier, Centrify, IBM, Identiva, Bantus, Welcome, Microsoft, Okta, Onelogin, Oracle, Ping, RSA, Thales

Privileged Management
Beyondtrust, Centrify, Cyberark, Fudo, Hitachi, IBM, Manageengine, Micro Focus, One Identity, Remediant, Secure Link, Thycotic, Xton

Identity Governance
Axiomatics, Deep Identity, Helpsystems, Sailpoint, Saviynt, Simeio

Consumer Identity
Akamai, Authd, Forgerock, Id Experts, Id.me, Jumio, Loginradius, Microsoft, Ping, Pureid, Saphire, Sap, Secure Key, Trulioo, Verato, Veriff, Zamna

Cloud Security

Infrastructure
Container: Anchore, Capsule8, Deepfence, Neuvector, Polyverse, Portshift, Qualys, Sysdig, Twistlock
Bettercloud, Bridgecrew, Cavirin, Check Point, Dome9, Cloudway, Cloudpassage, Guardicore, Hytrust, Iboss, Illumio, Lacework, Paloalto, Portshift, Shiftleft, Sonrai, Stackit, Tenable, Vmware, Zscaler

CASB
Avanan, Bitglass, Broadcom, Cipher Cloud, Cisco, Coronet, Managed Methods, McAfee, Microsoft, Netskope, Oracle, Proofpoint, Securiqo, Skyformation, Symantec

"In design principles, means that software / architecture / infrastructure is designed from the foundation to be secure"

Built-in Security

Built into platform design

Security management and operation simplified

No add-on resources

Bolt-on Security

Not integrated

Complex

Operational burden

Limited Utilization

Vendor Contract Lock in

Summary: Top Security and Risk Trends

The Top Security & Risk Management Trends for 2021 (Gartner Webinar)

1. Remote Work Is the New Normal
2. The "Cybersecurity Mesh" Architecture
3. Security Product Consolidation
4. Identity First Security
5. Machine Identity Management
6. Breach and Attack Simulation Tools
7. Privacy Enhancing Computation
8. Boards Are Adding Cybersecurity

Gartner

Best of Breed — Pros and Cons

Pros	Cons
• No vendor lock-in • Components can be best in class • No CISO has been fired by best-of-breed purchases • Vendors focus on their area of expertise	• No centralized policy management • No centralized threat database • Slower incident response • Multiple vendors for support and licensing • No centralized playbooks and automation • Integrations are spotty or nonexistent • Different vendors have different types of management, usage and scripting

How to Build a Cybersecurity Mesh Architecture

Security Analytics and Intelligence Layer

Identity Layer

Policy and Posture Management Layer

Dashboard Layers

Cybersecurity Mesh Architecture Complete

CSMA — Pros and Cons

Pros	Cons
• Faster incident response • Centralized policy management • Centralized threat database • ML/AI helps with threat hunting • Centralized playbooks and automation • Staff is better aligned with tools from single vendor (smaller learning curve) • Third-party integrations into threat DB • Single vendor for support and licensing	• Perceived vendor lock-in if you go single vendor CSMA • Components may not be best in class • No vendor has all the building blocks

Recommendations

- Build supportive layers for a long-term CSMA strategy — security analytics, identity fabric, policy management, dashboards.
- Evaluate security controls with interoperability in mind: inversion of control APIs, standards support, extensible analytics.
- Familiarize yourself with current and emerging standards, and open-source code projects as a potential alternative to supplement vendor interoperability gaps.

Cybersecurity Mesh Architecture (CSMA)

© 2021 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates.

Microsoft Cybersecurity Reference Architecture

Security modernization with Zero Trust Principles

May 2021 – https://aka.ms/MCRA

Security Operations / SOC

Threat Experts | Detection and Response Team (DART) | MSSP/MDR

Azure Sentinel – Cloud Native SIEM, SOAR, and UEBA for IT, OT, and IoT

- Azure – *& 3rd party clouds*
- Endpoint – *& Server/VM*
- Office 365 – *Email and Apps*
- Identity – *Cloud & On-Premises*
- SaaS – *Microsoft Cloud App Security*
- *Other Tools, Logs, and Data Sources*

Extended Detection and Response (XDR)

Azure Defender — **Microsoft 365 Defender**

Advanced Detection & Remediation | Automated Investigation & Remediation | Advanced Threat Hunting

This is interactive!

1. Present Slide
2. Hover for Description
3. Click for more information

Security Guidance

1. Security Documentation
2. Microsoft Best Practices
3. Azure Security Top 10 | Benchmarks | CAF | WAF

Software as a Service (SaaS)

Microsoft Cloud App Security

- *App Discovery & Risk Scoring (Shadow IT)*
- *Threat Detection & Response*
- *Policy Audit & Enforcement*
- *Session monitoring & control*
- *Information Protection & Data Loss Prevention (DLP)*

Identity & Access

Conditional Access – Zero Trust Access Control decisions based on explicit validation of user trust and endpoint integrity

Endpoints & Devices

Microsoft Endpoint Manager
Unified Endpoint Management (UEM)
Intune | Configuration Manager

Microsoft Defender for Endpoint
Unified Endpoint Security

- Endpoint Detection & Response (EDR)
- Web Content Filtering
- Threat & Vuln Management
- Endpoint Data Loss Protection (DLP)

Hybrid Infrastructure – IaaS, PaaS, On-Premises

Azure Security Center – Cross-Platform Cloud Security Posture Management (CSPM)

- Secure Score
- Compliance Dashboard

On Premises Datacenter(s) | *3rd party IaaS & PaaS* | Microsoft Azure

Extranet: NGFW, Edge DLP, IPS/IDS, Azure AD App Proxy *Beyond User VPN*

Intranet: Azure Arc, Azure Stack

Express Route, Private Link, aws, Azure Marketplace

- Azure Firewall & Firewall Manager
- Azure WAF
- DDoS Protection
- Azure Key Vault
- Azure Bastion
- Azure Lighthouse
- Azure Backup
- *Security & Other Services*

Information Protection

Classification Labels

- Azure Purview
- Microsoft Information Protection (MIP): Discover, Classify, Protect, Monitor
- File Scanner *(on-premises and cloud)*
- Data Governance
- Advanced eDiscovery

Compliance Manager

Azure Active Directory

- Passwordless & MFA: Hello for Business, Authenticator App, FIDO2 Keys
- Identity Protection: Leaked cred protection, Behavioral Analytics
- Azure AD PIM
- Identity Governance
- Azure AD B2B & B2C

Defender for Identity

Active Directory

Securing Privileged Access – Secure Accounts, Devices, Intermediaries, and interfaces to enable and protect privileged users

Privileged Access Workstations (PAWs) - Secure workstations for administrators, developers, and other sensitive users

Microsoft Secure Score – Measure your security posture, and plan/prioritize rapid improvement with included guidance

Microsoft Compliance Score – Prioritize, measure, and plan improvement actions against controls

Windows 10 Security

- *Network protection*
- *Credential protection*
- *Full Disk Encryption*
- *Attack surface reduction*
- *App control*
- *Exploit protection*
- *Behavior monitoring*
- *Next-generation protection*

IoT and Operational Technology (OT)

Azure Sphere

Azure Defender for IoT

- *ICS, SCADA, OT*
- *Internet of Things (IoT)*
- *Industrial IoT (IIoT)*
- *Asset & Vulnerability management*
- *Threat Detection & Response*

Azure Defender – Cross-Platform, Cross-Cloud XDR

Multi-asset detection and response for infrastructure and platform as a service (IaaS & PaaS), Proactive Threat defenses

People Security

- Attack Simulator
- Insider Risk Management
- Communication Compliance

GitHub Advanced Security – Secure development and software supply chain

Threat Intelligence – 8+ Trillion signals per day of security context

Service Trust Portal – How Microsoft secures cloud services

Security Development Lifecycle (SDL)

Thank You !

Abbas Kudrati
APAC Chief Cybersecurity Advisor
Abbas.Kudrati@Microsoft.com
@askudrati
https://aka.ms/abbas