



КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

Интеграция решений кибербезопасности в единое целое



Puzzle Systems



Директор компании Puzzle Systems

Баязитов Альберт

Кибербезопасность

вчера

сегодня

завтра

Интеграция решений кибербезопасности в единое целое



Кибербезопасность В цифрах

Worldwide Security Spending by Segment, 2017-2019 (Millions of U.S. Dollars)

| Market Segment | 2017 | 2018 | 2019 |
|-------------------------------------|----------------|----------------|----------------|
| Application Security | 2,434 | 2,742 | 3,003 |
| Cloud Security | 185 | 304 | 459 |
| Data Security | 2,563 | 3,063 | 3,524 |
| Identity Access Management | 8,823 | 9,768 | 10,578 |
| Infrastructure Protection | 12,583 | 14,106 | 15,337 |
| Integrated Risk Management | 3,949 | 4,347 | 4,712 |
| Network Security Equipment | 10,911 | 12,427 | 13,321 |
| Other Information Security Software | 1,832 | 2,079 | 2,285 |
| Security Services | 52,315 | 58,920 | 64,237 |
| Consumer Security Software | 5,948 | 6,395 | 6,661 |
| Total | 101,544 | 114,152 | 124,116 |

Source: Gartner (August 2018)

Worldwide Security Spending by Segment, 2019-2020 (Millions of U.S. Dollars)

| Market | 2019 | 2020 | Growth (%) |
|-------------------------------------|----------------|----------------|------------|
| Application Security | 3,095 | 3,287 | 6.2 |
| Cloud Security | 439 | 585 | 33.3 |
| Data Security | 2,662 | 2,852 | 7.2 |
| Identity Access Management | 9,837 | 10,409 | 5.8 |
| Infrastructure Protection | 16,520 | 17,483 | 5.8 |
| Integrated Risk Management | 4,555 | 4,731 | 3.8 |
| Network Security Equipment | 13,387 | 11,694 | -12.6 |
| Other Information Security Software | 2,206 | 2,273 | 3.1 |
| Security Services | 61,979 | 64,270 | 3.7 |
| Consumer Security Software | 6,254 | 6,235 | -0.3 |
| Total | 120,934 | 123,818 | 2.4 |

Кибербезопасность вчера

Ты помнишь,
как все начиналось...

ОТДЕЛ ИБ



- Firewall/Proxy-server
- Antivirus
- Device Control
- Data Loss Prevention
- Security information and event management

Кибербезопасность сейчас

ОТДЕЛ ИБ



- Next Generation Firewall/CASB
- Network Access Control/Zero Trust Access
- Cloud Security
- Privileged Access Management
- 2 Factor authentication
- Identity Management
- Security information and event management
- Risk Management
- Vulnerability Management
- Web Application Firewall
- DevSecOps
- Incident Detection and Response
- User Behavior Analytics
- Deception Grid
- Antivirus/EDR/XDR
- IoT security
- Users Awareness Program

Network & Infrastructure Security

Advanced Threat Protection
 Barracuda, Check Point, Cisco, CorSa, FireEye, Fortinet, Huawei, Hysolate, JopSecurity, Juniper, Lastline, McAfee, Mimecast, Opswat, Reversing Labs, Symantec, WatchGuard, Votiro.

NAC
 Armit, Aruba, Cisco, Fortinet, GenieSys, Parosoft, Pernox, Trustwave.

SDN
 BlackBridge, Cyma, Cyberta, Cysdera, Fortinet, Skyport, Tempred, Versa, Vider, Zentara, Zscaler.

DDoS Protection
 Akamai, Check Point, Fortinet, Imperva, Neustar, Oracle, Secure61, StackPath, Stormshield.

DNS Security
 Bluecat, Cisco, EfficientIP, Infoblox, Neustar, Secure61, Webroot.

Network Firewall
 Algosec, Cisco, Check Point, Endian, Fortinet, Hysolate, Huawei, OPAG, Palo Alto, SonicWall, Sophos, Stormshield, WatchGuard.

Deception
 Acalvio, Attivo, CyberTrap, Cymmetria, Guardian, Smokescreen, TrapX.

Web Security

ICS + OT
 Apero, Bayshore, Belden, CyberX, Cybersec, Endian, Indegy, Nozomi, RAS, PFP, Radint, Rhebo, Sentryo.

Network Analysis
 Awake, CCGS, Cloudtrac, Cori, Darktrace, Fideli, Ironnet, Lumify, Hacktrac, Summit, Sec8, Utima.

Endpoint Security

Endpoint Prevention
 AhnLab, Avast, Avecto, Avira, Barkly, Carbon Black, Check Point, Comodo, Cybereason, Cyland, DeepInstinct, Endgame, Engage, Ericom, Eset, F-Secure, Fortinet, Hysolate, Intego, Ivanti, Kaspersky, McAfee, Menlo, Microsoft, Morphisec, Opswat, Panda, Symantec, Sentinel, Sophos, Spicognition, Stormshield, Symantec, Tehtis, Trend, VMware, Webroot, Ziften.

Detection & Response
 BlueHeron, Carbon Black, Cynet, Dtex, Fideli, FireEye, Forcepoint, Nextthink, Promisec, Sophos, Symantec, Ziften.

Application Security

WAF & Application Security
 Acunetix, AIO, Akamai, Alertlogic, ASDAN, Barracuda, Citrix, Cloudflare, Contrast, CyclickLabs, Ergon, Fortinet, Imperva, Qualys, Radware, Rapid7, Reblaze, Riverbed, Sucuri, Trend Micro, Screen, StackPath, Templarbit, Threatstack, Trustwave, Vicarius, Walkarm, Waratek.

Application Security Testing
 Acunetix, Bugcrowd, Bugfinders, Ca, Chocomark, Erpscan, Fasoo, Hackerone, IBM, Microfocus, N-stalker, Parasoft, Portswigger, Qualys, Rapid7, RogueWave, SiteLock, Snyk, Sonarsource, Synack, Synopsys, Tenable, Trustwave, WhiteHat Security, WhiteNoise.

MSSP

Traditional MSSP
 Atat, Bar Systems, BT, CenturyLink, CSC, IBM, MigPath, Optiv, Securosis, SoluStream, Symantec, Trustwave, Verizon.

Advanced MSS & MDR
 Axiomatic, Core Security, Fortinet, GenieSys, IBM, JopSecurity, Juniper, Lastline, McAfee, Mimecast, Opswat, Reversing Labs, Symantec, WatchGuard, Votiro.

Encryption
 Axiomatic, Core Security, Fortinet, GenieSys, IBM, JopSecurity, Juniper, Lastline, McAfee, Mimecast, Opswat, Reversing Labs, Symantec, WatchGuard, Votiro.

Risk & Compliance

Risk Assessment & Visibility
 Boalbitx, Day Dynamics, Cavirin, Coastion, Cyberark, CyberGate, CISA, Cyberint, Cybage, Delve, Egress, Fierium, GreenSec, Kenna, Preshenah, OPAG, Outpost24, Panaseer, Prevalent, Redseal, Reskreen, RiskSense, Skybox, Tenable, UpGuard, Venafi, Zeguro.

Security Ratings
 Bitsight, Corax, FICO, Guidewise, Panorays, SecurityScorecard.

Pen Testing & Breach Simulation
 Cobalt, Cobus, Sift, Cyberrint, Conslate, GreenSec, Madsec, Mopac, Poyvis, Picus, Rapid7, Safebreach, Sygnia, Verodin.

CRC
 Algosec, Securosis, Lockpatho, MetricStream, Netwrix, Resolver, RSA, Rsam, Tuft.

Security Awareness & Training
 Barracuda, CyberVista, KnowBe4, PhishLabs, Proofpoint, SANS.

Security

AVIRA, DEVU, FORTINET, logentrics, MICRO FOCUS, solarwinds.



Identity & Access Management

Authentication
 AccessData, Auth0, Averaon, BehavSec, Biocatch, CA, CallSign, Centrif, Core Security, Exostar, Google, Impriata, Intrinsic ID, Iovation, Nok Nok Labs, OnDrop, Okta, SamsPass, SafePass, SecureKey, SecurePush, ShoCard, Silverfort, Tascent, ThreatMetrix, TruSona, UNBOUND, UNIKEN, V-KEY, VIRIOL, WHEEL.

IDaaS
 Centrif, IBM, IdanUS, Microsoft, Okta, Onelogin, Oracle, RSA, Thales, Welcome.

Privileged Management
 Bomgar, ManageEngine, One Identity, Remediant, Hitachi, Thycotic, IBM, Wheel.

Identity Governance
 Axiomatic, Core Security, Destiny, Opentext, SailPoint, Saviynt, Simeio.

Consumer Identity
 Auth0, Pirean, IDExperts, ID.me, Jovrain, Logiradius, Microsoft, Pirean, SecureID, Trulioo, Vchain, Verato.

IoT

Blueliv, Centriq, HainTools, Group1, Intights, Recorded Future, Sixgill, RealMetrix, CyberArk.

IoT Devices

Automotive
 BlackBerry, Bluebird, Camos, Gattasol, Cycura, Cymotive, Group1, Harlan, Inng, Otonamo, Prilium, Upstream.

Connected Home
 CUJO, F-Secure, SAM, Symantec, Rubica.

Messaging Security

AGARI, Axiomatic, Area 1, AstralID, Bar Systems, Barracuda, Cisco, Clearswift, Cybnet, Cybereason, EdgeWave, FireEye, Forcepoint, Fortinet, GreatHorn, Gwava, Inky, IronScales, Mailguard, McAfee, Microsoft, Mimecast, PhishLabs, Proofpoint, Safe Software, SonicWall, Sophos, Spamina, Symantec, Trend Micro, Trustwave, VadeSecure, VailMail, Votiro, Webroot, Wickr.

Security Consulting

Accenture, Appsec, Booz | Allen | Hamilton, BT, Corvid, Deloitte, DEAR GROUP, EY, FireEye, IBM, Leidos, NCCGROUP, NEC, NISOS, Optiv, PwC, SRI, STROBE, FRIEDBERG, SYGNIA, WATKINS.

Blockchain

BlockArmour, Chain, Craxel, Edge, Guardtime, IDEE, Manifold, NuID, Remme, ShoCard, Vchain, Xage.

Fraud & Transaction Security

Autotix, Biocatch, Block Fraud, Brighterion, Caesars, DataVisor, EBay, Emailage, Ethoca, EverCompass, FICO, Feedzai, FirstData, Forter, Group1, Guardian Analytics, IdenTrust, Iovation, Kount, MagicCube, NetGuardians, NSI, Pondera, Riskified, Sift Science, Signifyd, Simility, SoSecure, TokenID, ThreatMetrix, Uniken, Technology.

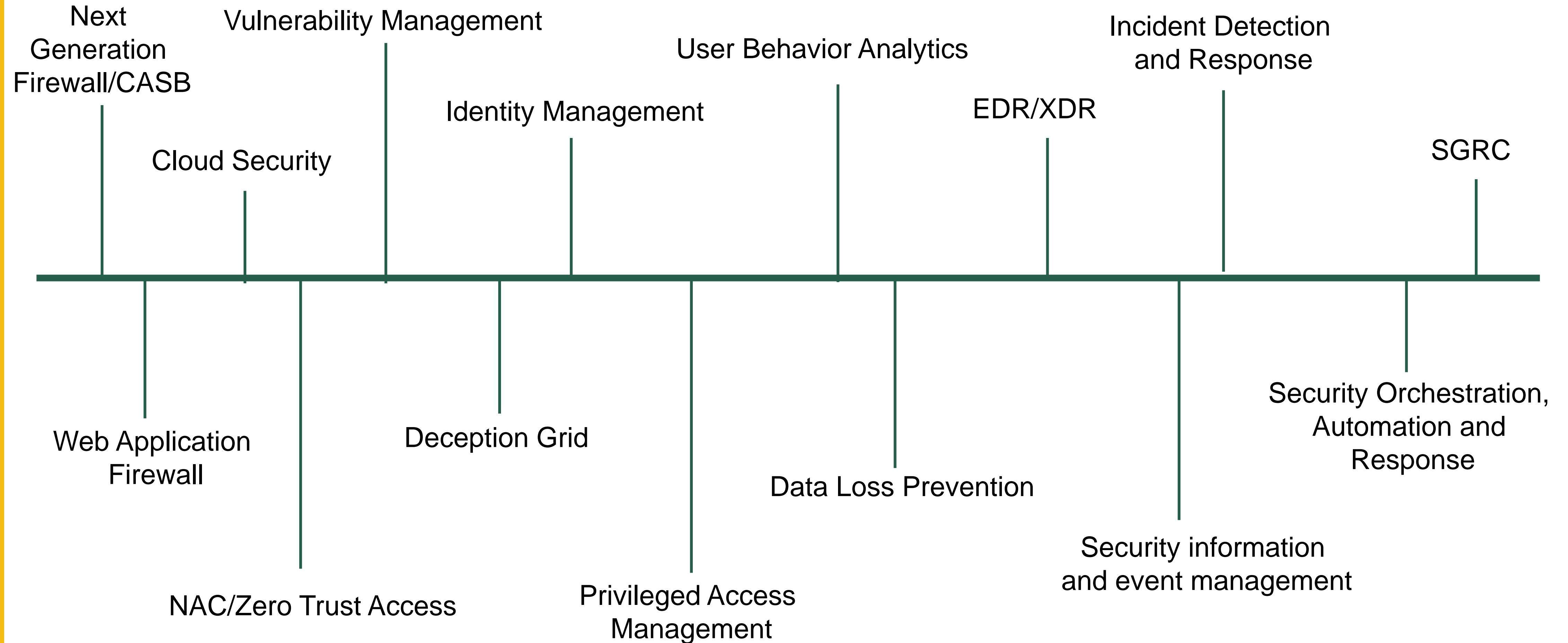
Cloud Security

Container
 Anchore, Aqua, Clair, Deeprepe, Layer8, NewVector, Polyverse, Sysdig, Twistlock.

Infrastructure
 BetterCloud, Praxinet, Cavirin, Check Point, Elastic, CloudPassage, Cybereason, Ezeuwal, Trust, Lacework, Paloalto, IBM, CloudStack, IBM, VMware.

CASB
 Avanan, Bitglass, CyberCloud, Cisco, CrowdStrike, McAfee, Microsoft, Netskope, Oracle, Proofpoint, Securosis, SkyInformation, SretnoKey, Symantec.

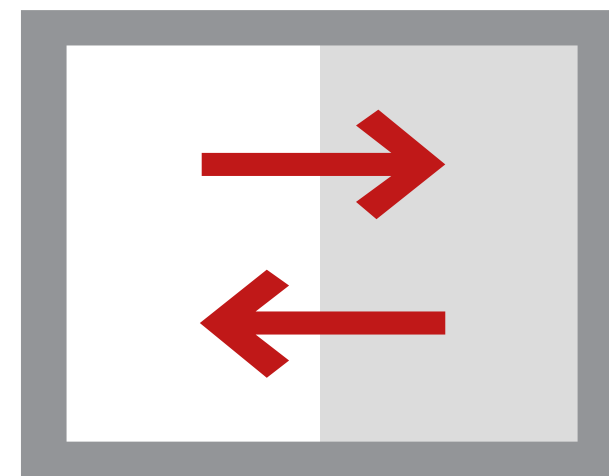
Кибербезопасность Завтра. Как управлять



Кибербезопасность

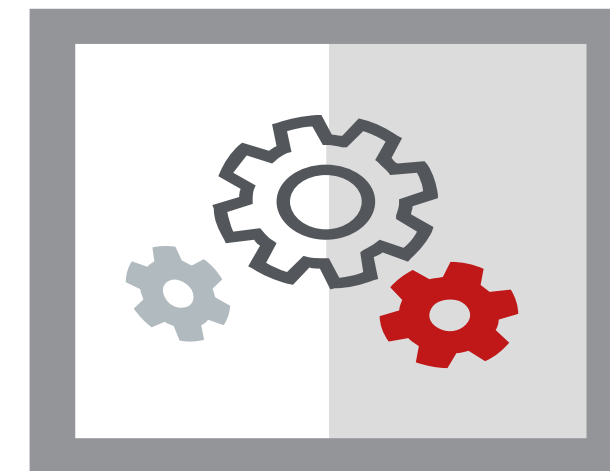
Как управлять? Интегрировать!

DXL - Data Exchange Layer



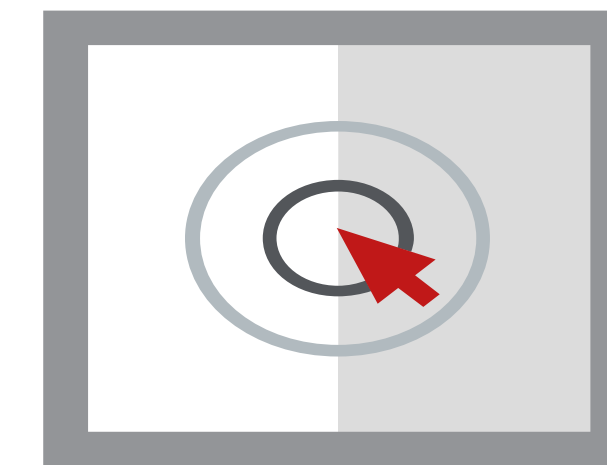
Открытый

DXL полнодуплексная коммуникационная платформа объединяющая решения ИБ в единую экосистему.



Абстрактный

DXL стандартизованный коммуникационный уровень абстракции для любых приложений вне зависимости от их собственной архитектуры



Простой

DXL предельно упрощает интеграционные сценарии, являясь при этом открытой платформой для включения новых приложений.



Быстрый

Благодаря высокой производительности, гибкости и масштабируемости укрепляется основа для обнаружения и реагирования на инциденты ИБ.

Security Information Application Framework

Кибербезопасность Интегрировать!

DXL – открытая платформа

The Data Exchange Layer (DXL) framework был создан что бы быть открытым

SDK позволяет совершать простые “1:many” интеграции для передачи данных и вызовов

Доступ к данным в режиме реального времени и обмен запросами на обслуживание



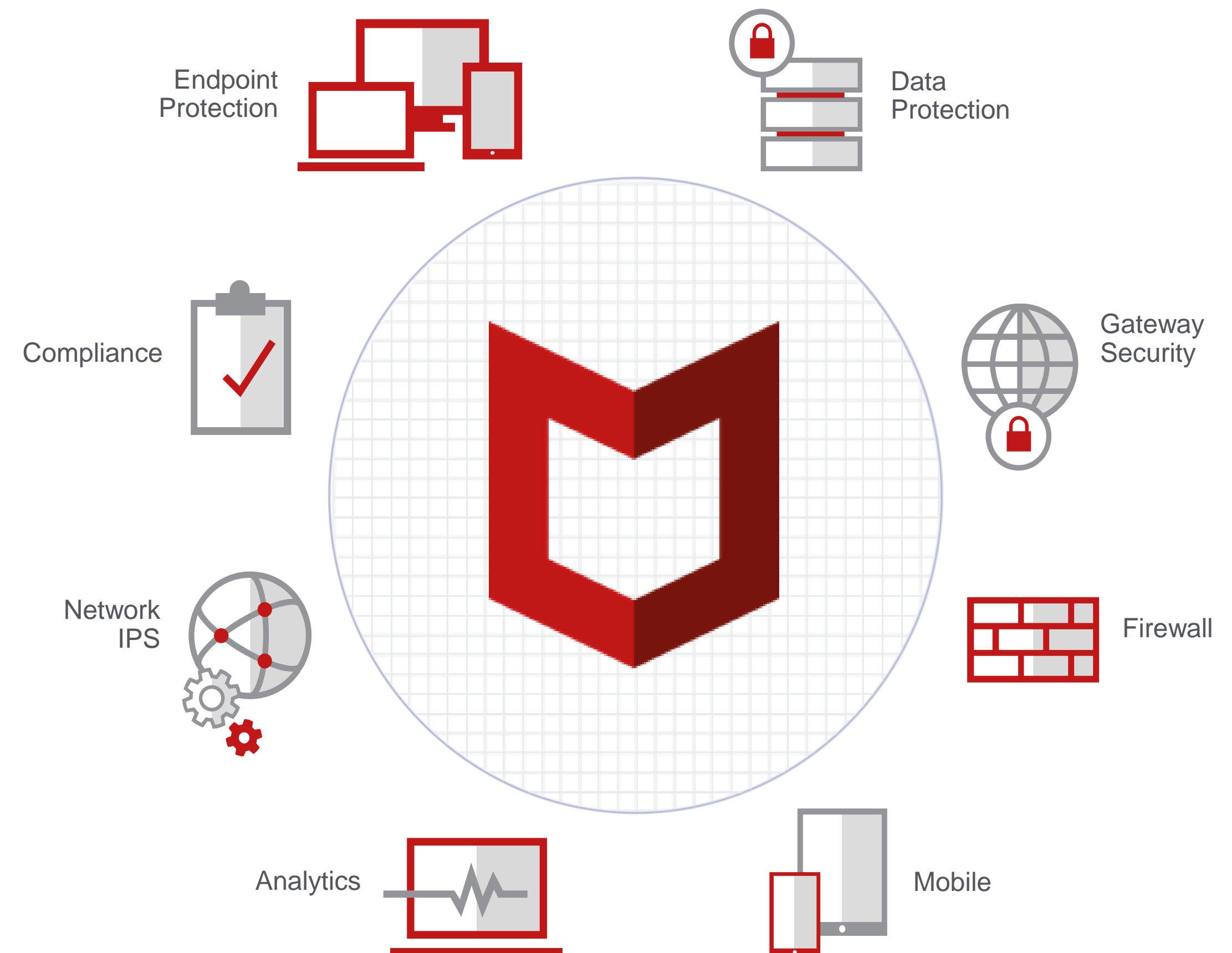
Кибербезопасность

Интегрировать - Эволюция DXL

Наш опыт - McAfee

Первоначально DXL использовался исключительно для решений McAfee (“Security Connected”).

- McAfee Endpoint Security (ENS)
- MVISION ePO
- MVISION EndPoint
- McAfee ePolicy Orchestrator (ePO)
- McAfee Threat Intelligence Exchange (TIE)
- McAfee Active Response (MAR)
- McAfee Investigator (MI)
- McAfee Enterprise Security Manager (ESM)
- McAfee Advanced Threat Defense (ATD)
- McAfee Web Gateway (MWG)
- McAfee Application Control (MAC)
- McAfee Network Security Platform (NSP)
- McAfee SiteAdvisor (SAE)
- McAfee Data Loss Prevention (DLP)
- Intel Internet of Things (IoT)



Кибербезопасность

Интегрировать - Эволюция DXL – Solution Partners

SIA
Partners

Connected Today



In Testing or Development Today



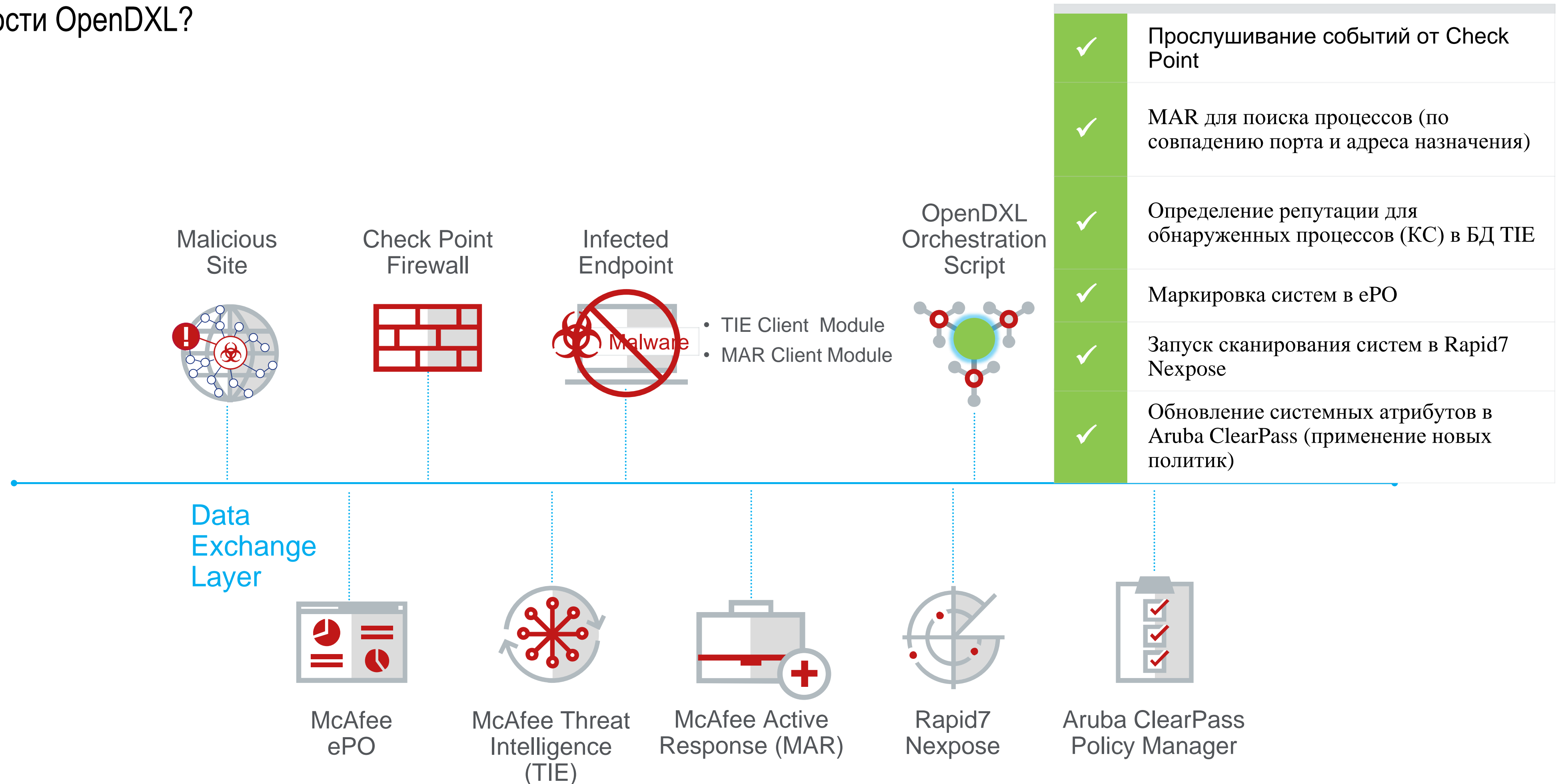
In Design



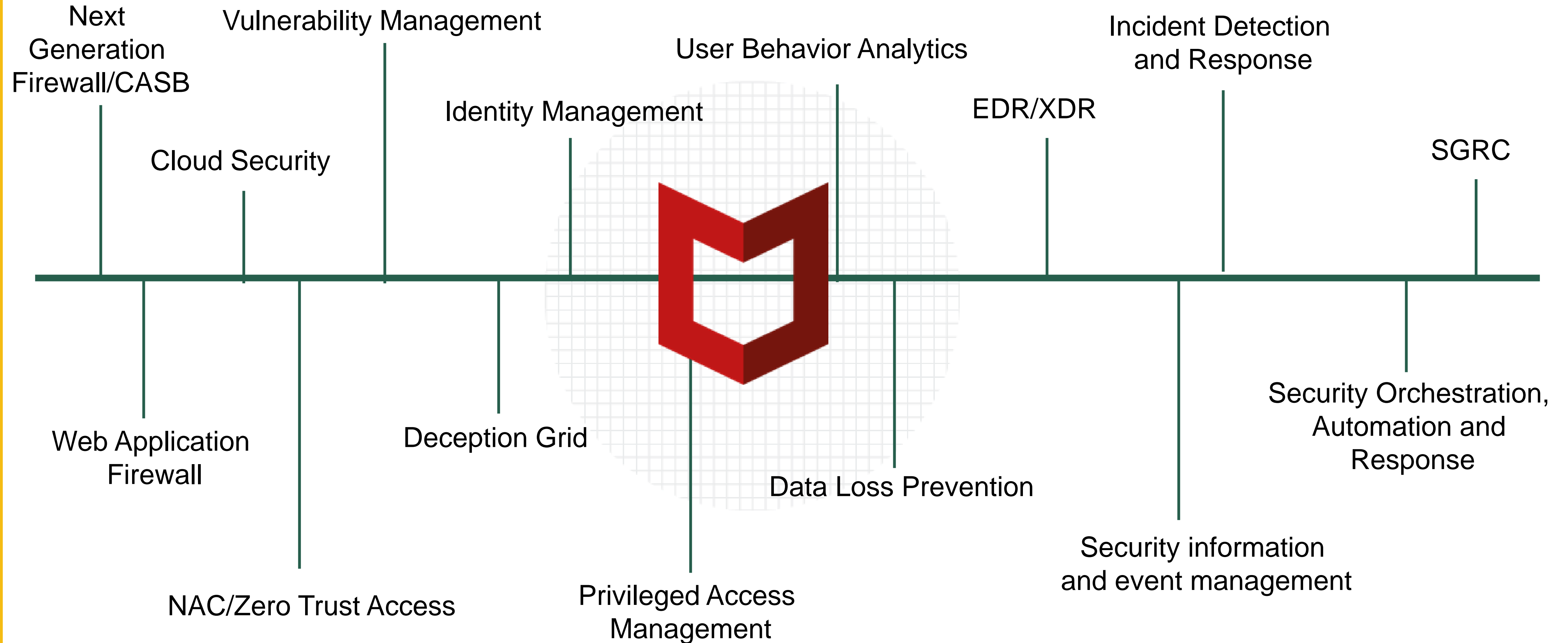
Кибербезопасность

Интегрировать - Примеры DXL

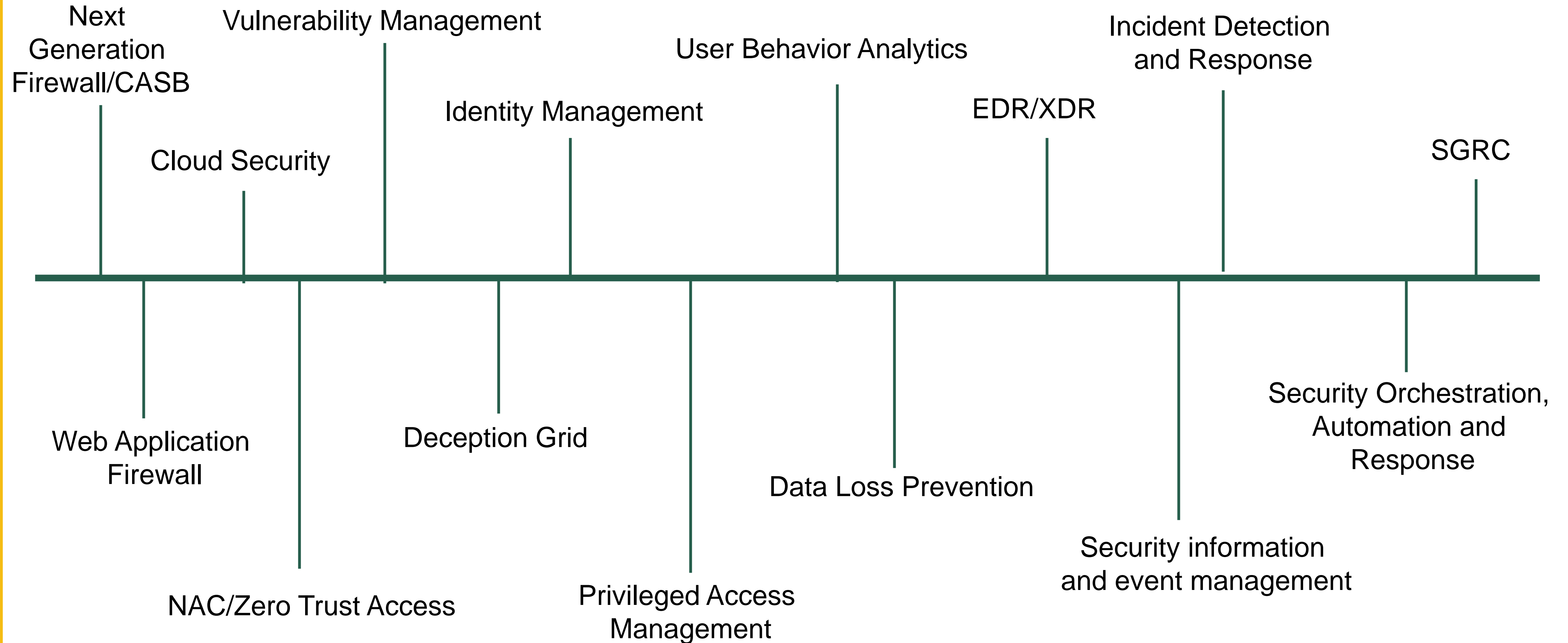
Возможности OpenDXL?



Кибербезопасность завтра



Кибербезопасность завтра





КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

Спасибо за внимание!

