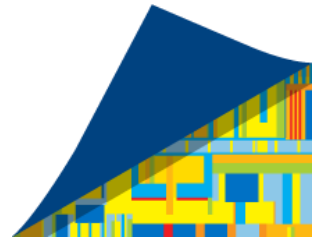
The Data Exchange Layer (DXL)

The Fabric of Security Connected

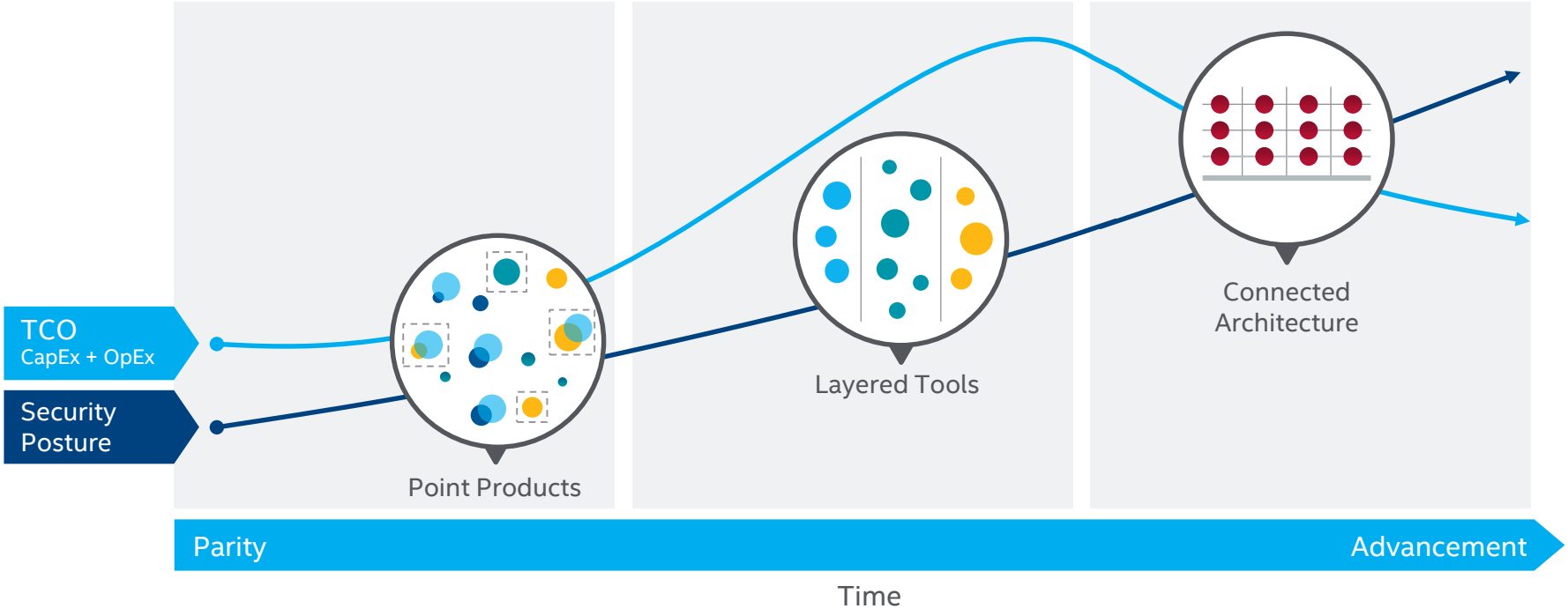
Steve Orrin

Chief Technologist, Intel Federal



Evolution of Security Product Offerings

Delivering Operationally-Effective Security



Intel Security's Data Exchange Layer

Standardize integration and communication to break down operational silos

Disjointed API-Based Integrations

Result

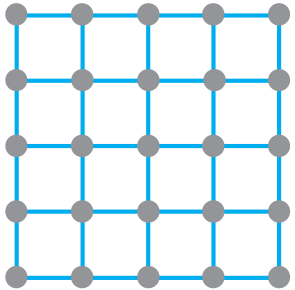
Slow, heavy, and burdensome

Complex and expensive to maintain

Limited vendor participation

Fragmented visibility

Collaborative Fabric-Based Ecosystem (DXL)



Result

Fast, lightweight, and streamlined

Simplified and reduced TCO

Open vendor participation

Simplicity- one time integration

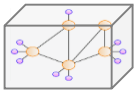
What is the Data Exchange Layer (DXL)?

Driving efficiency through enhanced communication

Real-Time Messaging

Data Exchange Layer Fabric: Real-time messaging infrastructure for security products built on message queue telemetry transport (MQTT).

Standardized Content



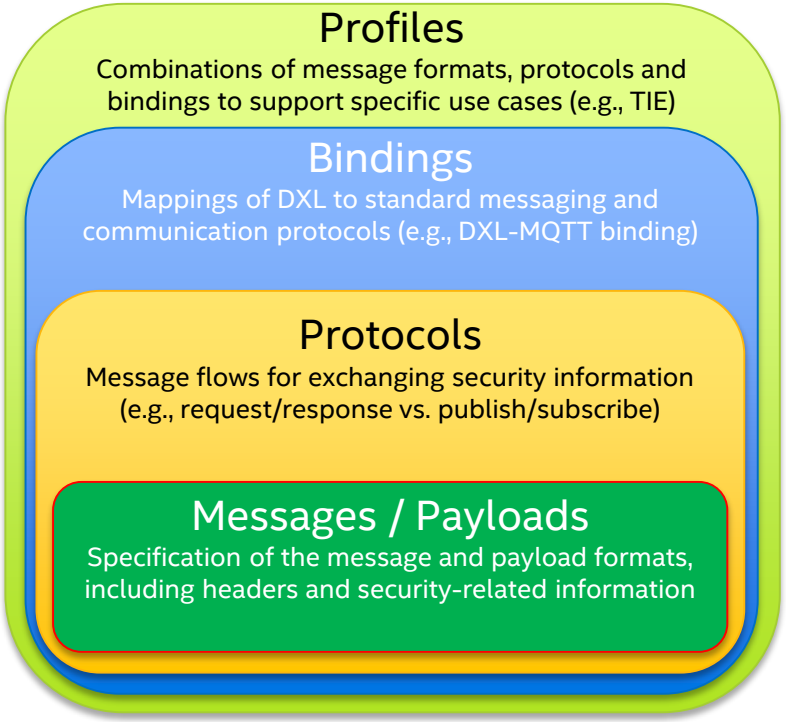
Common Information Model (CIM): Provides enterprise security state and context. Includes information about devices, users, location, reputation, and more.

Adaptive Workflows

DXL Clients: Security products use the Data Exchange Layer to publish or consume information.

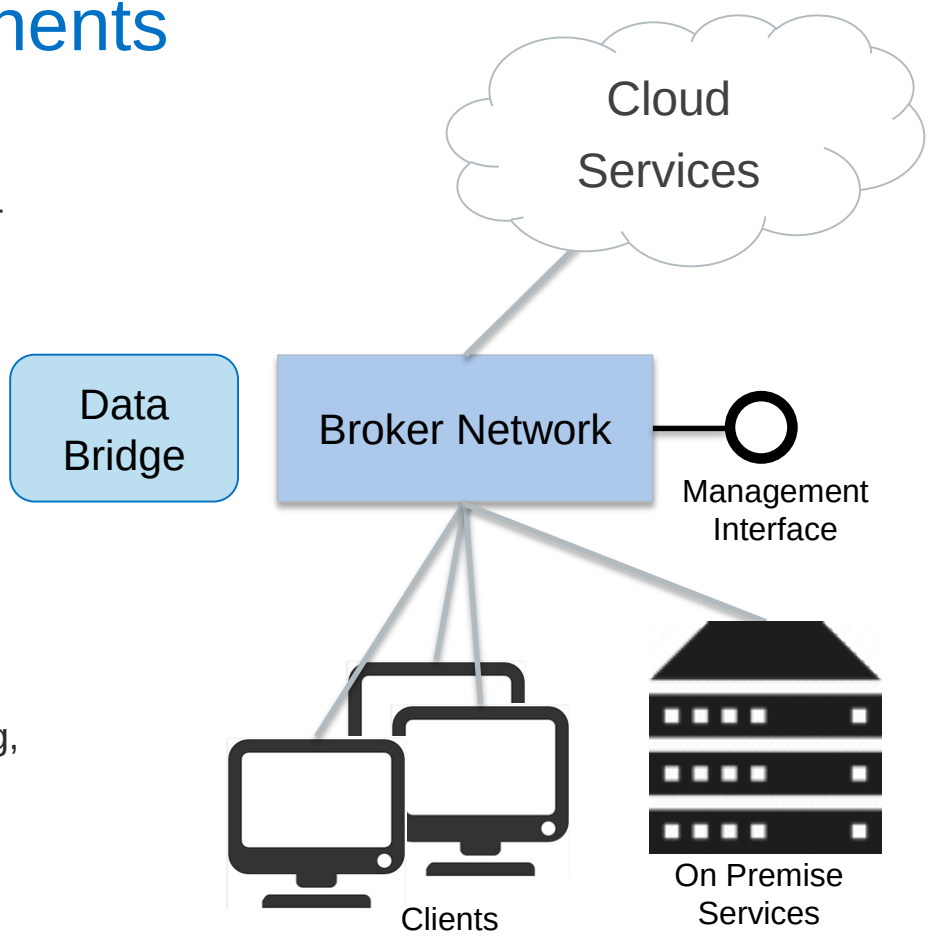
DXL Specification Design

The DXL specification is structured in different layers, similarly to the SAML specification, which are composed in order to tackle specific use cases:



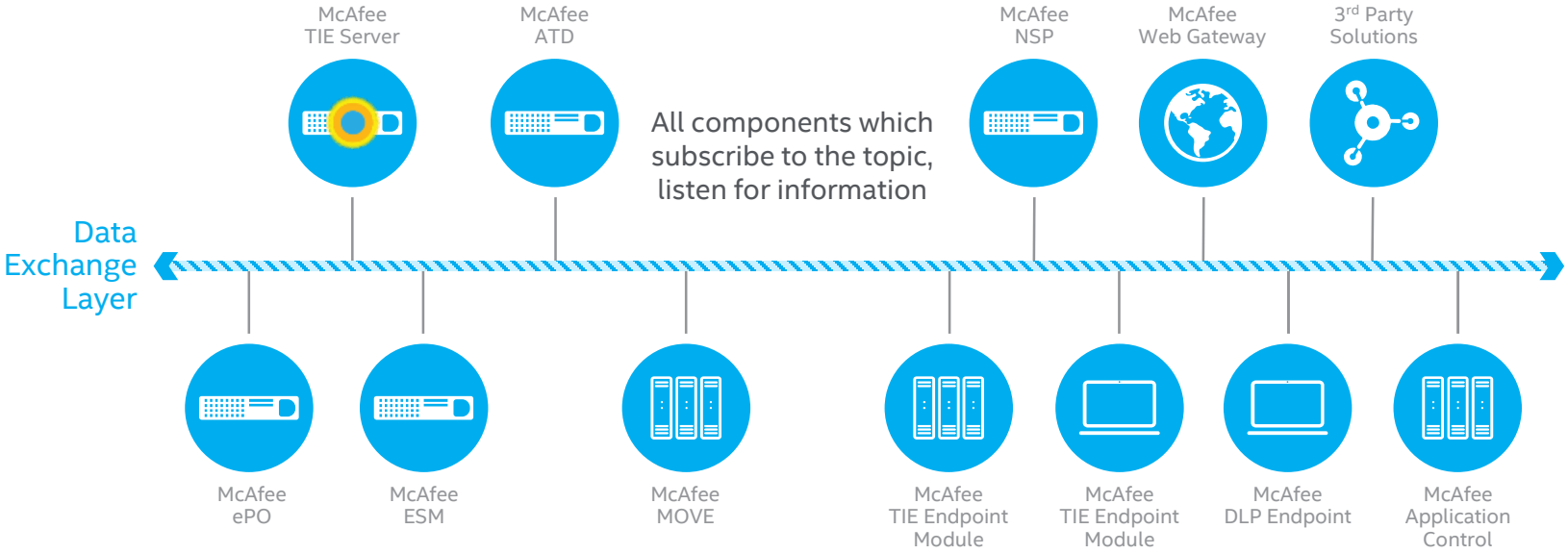
DXL Architecture Components

- Broker Network
  - Routes messages to appropriate receiver
- Clients
  - Provide access to DXL fabric
- Services
  - RESTful-like services available on DXL fabric
- Management Interfaces
  - Provides broker, client and service management.
- Data Bridge
  - Provides connection to related systems, such as TAXII servers, stream processing, and storage.



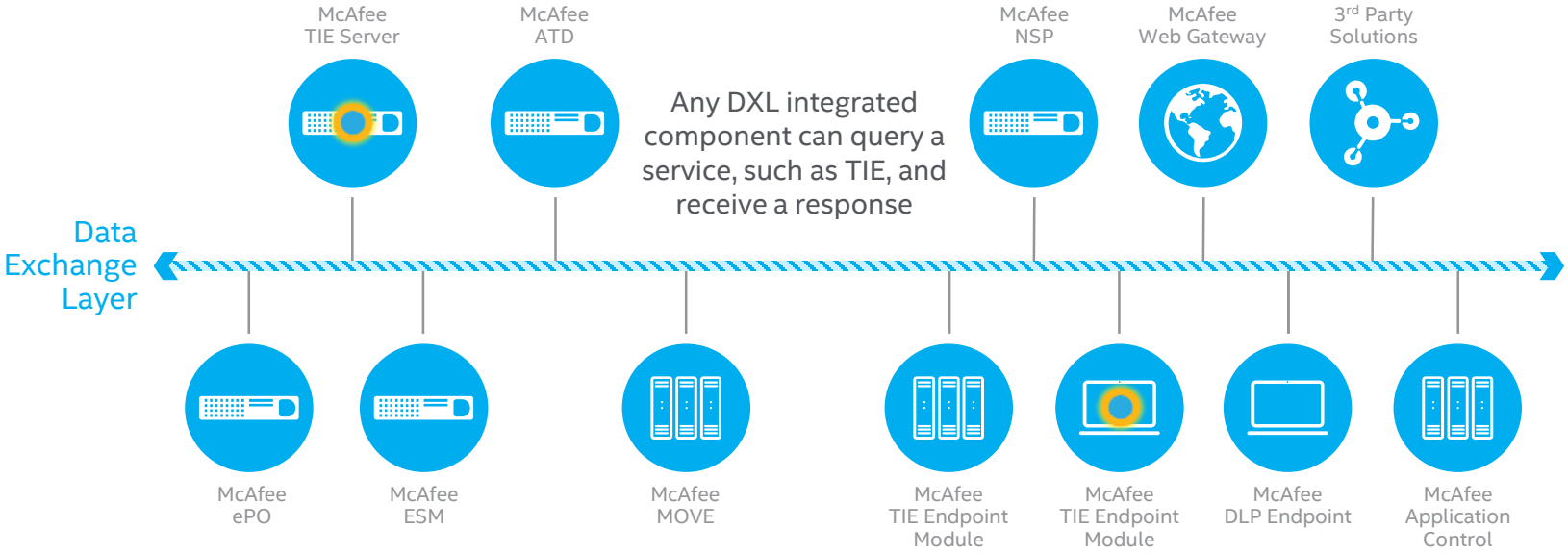
Intel Security Data Exchange Layer (DXL) in action…

Publish/Subscribe Model



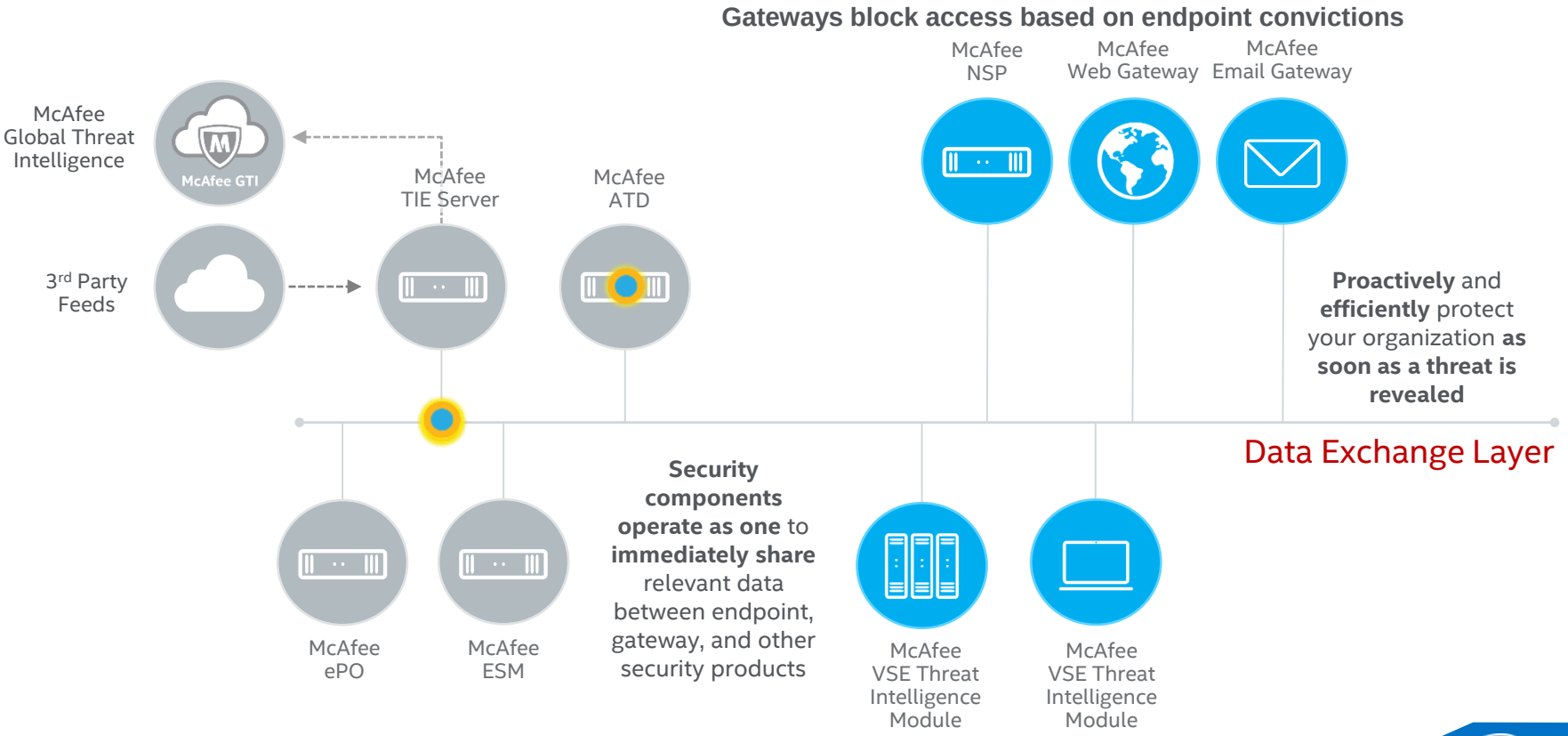
Intel Security Data Exchange Layer (DXL)

1:1 Query/Response Model

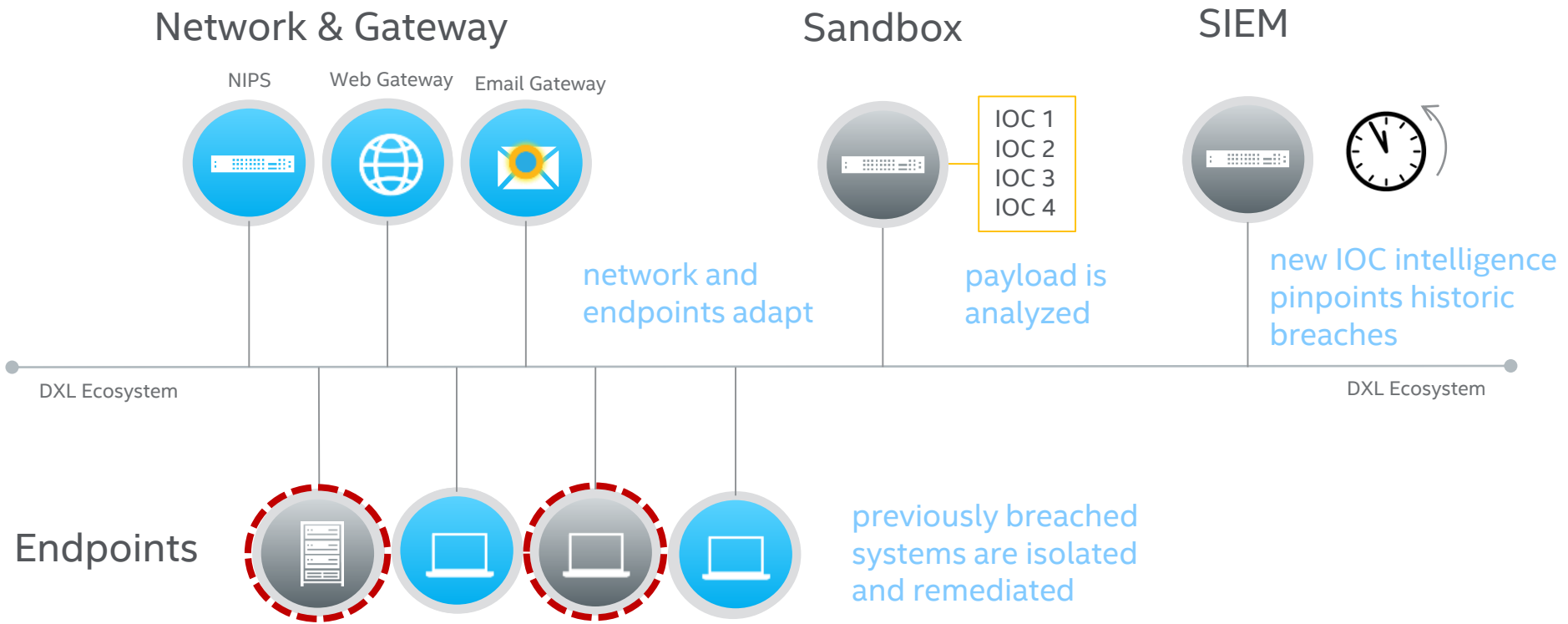


Intel Security Threat Intelligence Exchange (TIE)

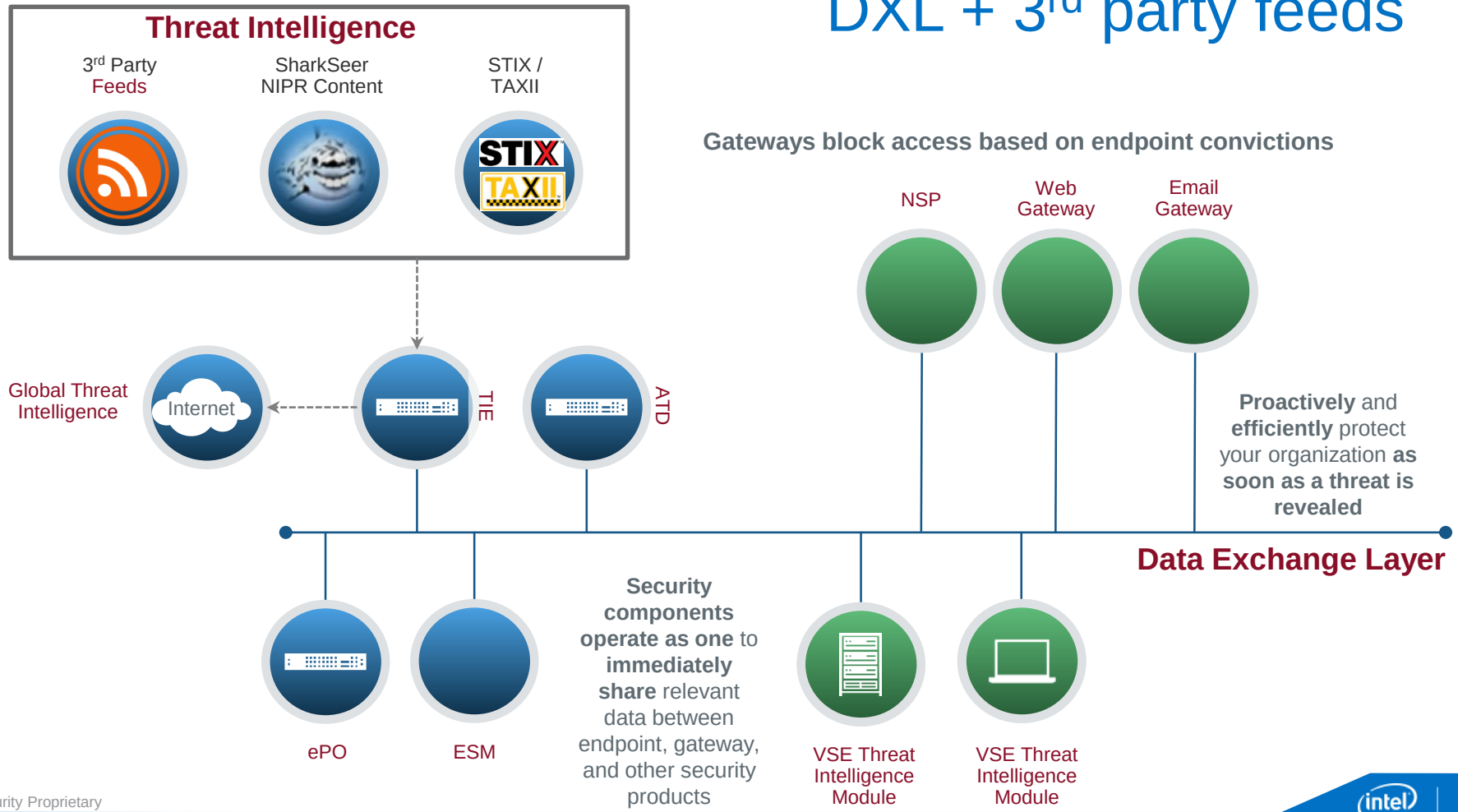
Real time protection across the enterprise



Adaptive Threat Prevention and Detection



DXL + 3rd party feeds




intel
Security

Notices

Intel and the Intel logo are trademarks or registered trademarks of

Intel Corporation or its subsidiaries in the United States and other countries.

***Other names and brands may be claimed as the property of others.**

**** Performance tests and ratings are measured using specific computer systems and/or components and reflect the approximate performance of Intel products as measured by those tests. Any difference in system hardware or software design or configuration may affect actual performance. All dates and product descriptions provided are subject to change without notice. This slide may contain certain forward-looking statements that are subject to known and unknown risks and uncertainties that could cause actual results to differ materially from those expressed or implied by such statements**

*****The threats and attack examples provided in this presentation are intended as examples only. They are not functional and cannot be used to create security attacks. They are not be replicated and/or modified for use in any illegal or malicious activity.**

******Any software source code reprinted in this document is furnished under a software license and may only be used or copied in accordance with the terms of that license.**

Legal Disclaimers

- INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.
  A "Mission Critical Application" is any application in which failure of the Intel Product could result, directly or indirectly, in personal injury or death. SHOULD YOU PURCHASE OR USE INTEL'S PRODUCTS FOR ANY SUCH MISSION CRITICAL APPLICATION, YOU SHALL INDEMNIFY AND HOLD INTEL AND ITS SUBSIDIARIES, SUBCONTRACTORS AND AFFILIATES, AND THE DIRECTORS, OFFICERS, AND EMPLOYEES OF EACH, HARMLESS AGAINST ALL CLAIMS COSTS, DAMAGES, AND EXPENSES AND REASONABLE ATTORNEYS' FEES ARISING OUT OF, DIRECTLY OR INDIRECTLY, ANY CLAIM OF PRODUCT LIABILITY, PERSONAL INJURY, OR DEATH ARISING IN ANY WAY OUT OF SUCH MISSION CRITICAL APPLICATION, WHETHER OR NOT INTEL OR ITS SUBCONTRACTOR WAS NEGLIGENT IN THE DESIGN, MANUFACTURE, OR WARNING OF THE INTEL PRODUCT OR ANY OF ITS PARTS.
- Intel may make changes to specifications and product descriptions at any time, without notice. Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined". Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them. The information here is subject to change without notice. Do not finalize a design with this information.
- The products described in this document may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.
- Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order.
- Copies of documents which have an order number and are referenced in this document, or other Intel literature, may be obtained by calling 1-800-548-4725, or go to: http://www.intel.com/design/literature.htm
- Intel processor numbers are not a measure of performance. Processor numbers differentiate features within each processor family, not across different processor families: Go to: Learn About Intel® Processor Numbers http://www.intel.com/products/processor_number
- Some results have been estimated based on internal Intel analysis and are provided for informational purposes only. Any difference in system hardware or software design or configuration may affect actual performance.
- Software and workloads used in performance tests may have been optimized for performance only on Intel microprocessors. Performance tests, such as SYSmark and MobileMark, are measured using specific computer systems, components, software, operations and functions. Any change to any of those factors may cause the results to vary. You should consult other information and performance tests to assist you in fully evaluating your contemplated purchases, including the performance of that product when combined with other products.
- Intel does not control or audit the design or implementation of third party benchmarks or Web sites referenced in this document. Intel encourages all of its customers to visit the referenced Web sites or others where similar performance benchmarks are reported and confirm whether the referenced benchmarks are accurate and reflect performance of systems available for purchase.
- Relative performance is calculated by assigning a baseline value of 1.0 to one benchmark result, and then dividing the actual benchmark result for the baseline platform into each of the specific benchmark results of each of the other platforms, and assigning them a relative performance number that correlates with the performance improvements reported.
- SPEC, SPECint, SPECfp, SPECrate, SPECpower, SPECjbb, SPECompG, SPEC MPI, and SPECjEnterprise* are trademarks of the Standard Performance Evaluation Corporation. See http://www.spec.org for more information.
- TPC Benchmark, TPC-C, TPC-H, and TPC-E are trademarks of the Transaction Processing Council. See http://www.tpc.org for more information.
- Intel® Advanced Vector Extensions (Intel® AVX)* are designed to achieve higher throughput to certain integer and floating point operations. Due to varying processor power characteristics, utilizing AVX instructions may cause a) some parts to operate at less than the rated frequency and b) some parts with Intel® Turbo Boost Technology 2.0 to not achieve any or maximum turbo frequencies. Performance varies depending on hardware, software, and system configuration and you should consult your system manufacturer for more information.
- No computer system can provide absolute security. Requires an enabled Intel® processor, enabled chipset, firmware and/or software optimized to use the technologies. Consult your system manufacturer and/or software vendor for more information

*Intel® Advanced Vector Extensions refers to Intel® AVX, Intel® AVX2 or Intel® AVX-512. For more information on Intel® Turbo Boost Technology 2.0, visit http://www.intel.com/go/turbo