Industry Value Constellation

Intel Edge to Cloud Cybersecurity Solutions

Safeguard Your OT and IT Infrastructure from Cyberthreats

Intel is ready *right now*, with holistic cybersecurity solutions that organizations can deploy today—from endpoints, across the network, and to the cloud.

The Market Imperative

The Internet of Things (IoT) is no longer simply an emerging trend. Organizations are focused on transformational initiatives that deliver pivotal business outcomes. At the core of digital transformation is the alignment and integration of operational technology (OT) with information technology (IT) systems. But with the proliferation of IoT edge devices—one estimate predicts 29.3 billion networked devices globally by 2023[1]—unsecured endpoints are not visible to, or protected by, legacy IT security systems.

While cybersecurity may be top of mind for the CISO, many organizations are not prepared to keep up with the speed of ever-changing threats—from endpoint devices across the network to the data center. They face multiple challenges on the path to an across-the-board security practice.

What's needed is a comprehensive view of both OT and IT security risks, and a measured strategy for enterprise-wide cybersecurity. From the retail store to the factory floor, across city infrastructure to the hospital bedside, security leaders need a holistic approach to protecting themselves from cyberattacks.

Cybersecurity decision-makers are discovering why 24/7 real-time visibility into an ever-growing attack surface is essential to reducing risks. For edge devices such as lighting sensors, video cameras, and HVAC controllers; endpoint detection and response (EDR) solutions make this possible through a range of functions:

- Recording and saving endpoint behaviors
- Using data analytics to detect suspicious behaviors
- Providing contextual information
- Blocking malicious activity
- Offering remediation recommendations

It's not just about securing endpoints but also the networks they are connected to. This is where a zero-trust approach comes in, protecting networks from malicious lateral movement by securing edge-based workloads. A zero-trust framework helps build a more secure network architecture by eliminating any inherent trust of users, devices, or data—regardless of physical location or access history.

Ultimately, cybersecurity systems—from the edge to the cloud—need to be designed in at the start. They must be a foundational element across hardware and software to prevent harmful applications from breaching endpoints or taking down a network. And these systems are being deployed across organizations in almost every industry today.

Edge devices, users, data, and resources are spread across the globe. The difficulties in connecting them quickly and securely increases the risk of compromise. With more staff working from home, endpoints are often not protected with strong passwords, the latest security patches, and are simply out of reach to IT. Plus, OT devices typically do not have operating systems suitable for widely used IT security tools. Security teams need a holistic approach to safeguarding today's widely distributed data and devices.

Optimize Cybersecurity Initiatives

Cybersecurity strategies and solutions are at work today across industries and use cases addressing the unique challenges of every segment:

- Municipalities face cyber risks across essential infrastructure such as utilities, roadways, and transportation systems. End-to-end security is key to preventing service interruptions, keeping citizens safe, and meeting air and water quality regulations.
- Electricity grids are particularly vulnerable to cyberattacks. Utilities must safeguard them by modernizing substation equipment with multiple levels of protection from hardware-enabled security to cloud-based management.
- A disrupted supply chain has economic impacts, yet implementing safety measures for ports and cranes, goods in transport, and data in motion comes with tremendous challenges. From the loading dock to the end customer, cybersecurity deployments intersect across the widest range of endpoints, networks, and IT systems.
- The average hospital room can have as many as 20 connected medical devices[2], which are especially vulnerable to attack. With highly sensitive patient data and regulatory compliance requirements, healthcare organizations are implementing robust cyber-hygiene practices from the bedside to medical software systems.
- From ecommerce payments to point-of-sale software, online and physical retail systems are loaded with customer financial information and are prime targets for cybercriminals. The reputation of retailers large and small depends on rock-solid security from the edge, across the retail network infrastructure, and to the cloud.
- Building owners are interconnecting legacy systems with smart control solutions and the latest digital technologies to offer comfort, convenience, and safety to their tenants. Bringing together OT edge devices with existing systems requires protecting the building network from cyber risks on every front.
- Industrial facilities are vulnerable to attacks that break automated assembly lines, fracture process control systems, or even close plants entirely. Manufacturers need device-level endpoint protection through methods like mutual authentication.

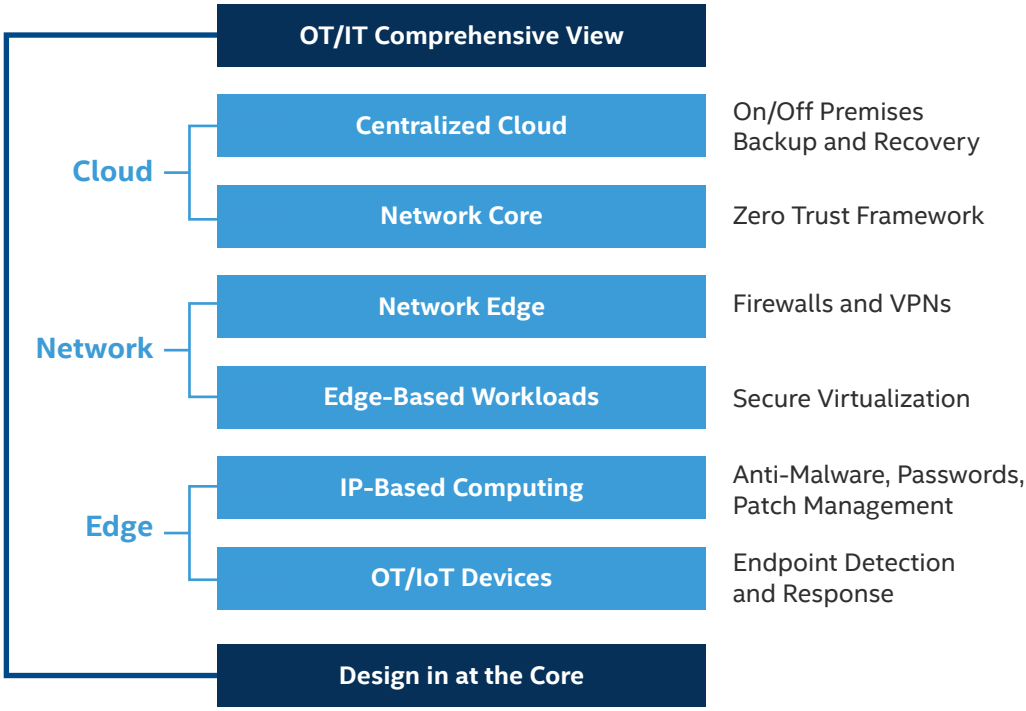
Key Technology Imperatives

With the explosion of connected devices over the past decade, organizations now see these devices as a competitive differentiator, from providing smart city services to citizens, to creating a safer working environment for employees. But the proliferation of the IoT comes with challenges. With a wider attack surface, keeping these edge devices and platforms from being compromised requires security to be a top-to-bottom design consideration when developing and deploying cybersecurity solutions.

1. **Design in at the start:** Critical OT and IT applications should have security built into the system architecture at the beginning of a project. Bolting on security as an afterthought raises costs, reduces system performance, and limits the ability of an organization to mitigate risk.
2. **Start at the core:** A hardware and software stack designed from the ground up is the basis for reliable and resilient security. For example, Intel® QuickAssist Technology (Intel® QAT) is built into 4th Gen Intel® Xeon® Scalable processors. Intel QAT accelerates cryptography and compression, can significantly boost CPU efficiency and throughput, while reducing data footprint and power utilization.
3. **Protect the network edge:** The edge is a location, not a thing. Multiple edges exist from the device, which could include cameras and digital displays to the infrastructure edge that serves as a gateway to the network.
4. **Don't sacrifice performance:** A system needs to be both secure and fast to keep up with the processing demands on devices. It's essential to consider hardware features such as secure boot, secure device onboarding, crypto acceleration, and secure virtualization.
5. **Use tools powered by AI:** Risk management and risk scoring based on AI and machine learning (ML) algorithms can help address the most critical threats in near-real time to stop attacks almost immediately.

The reality is that complex, multi-vendor solutions need to be architected in a way that is cost-effective, reliable, manageable, scalable, and, most important, secure.

Cybersecurity Edge-to-Cloud Architecture



A holistic OT/IT cybersecurity architecture is key—from the edge, across the network to the cloud.

Ready to Scale

Partners CrowdStrike, Onclave, and Veridify deliver Intel-optimized cybersecurity solutions that meet the technical thresholds and best practices that make them ready for scale.

CROWDSTRIKE

CrowdStrike

CrowdStrike has optimized its solutions for Intel® Threat Detection Technology, available on Intel® Core™ and Intel vPro® platforms. This delivers accelerated memory scanning to uncover fileless attacks that have become the number-one entry method for all attack types.

With CrowdStrike's cloud-native approach to endpoint protection, security teams can benefit from:

- Reduced overhead that increases efficacy and performance
- Greater protection through hardware-based security
- Optimized hardware-based exploit detection to uncover exploits earlier
- Detection of advanced persistent threats (APT)

ONCLAVE

Onclave

Onclave delivers security from the edge to the core with its zero-trust-based network overlay that protects networks by cryptographically securing vulnerable OT and IoT workloads. Providing each workload its own root of trust eliminates the attack surface, prevents breaches, and secures the network from malicious lateral movement.

With Onclave's trusted platform solution, security teams can benefit from:

- Verified trust at each endpoint before access is granted to any device, system, or user
- Simplified network management with a single, integrated platform
- Cryptographically secure OT/IoT workloads
- Network overlay that does not require changes to existing infrastructure

Veridify Security

Veridify

Veridify Security's DOME™ SaaS solution provides device-level cybersecurity for OT and IIoT networks, protecting edge devices that lack built-in security. More than monitoring, Veridify's DOME stops cyberattacks in real time. DOME's Sentry retrofits to existing OT devices, auto-installs in seconds, and by supporting NIST's Zero-Trust framework, provides immediate protection to secure communication, data, and commands that run building automation and industrial automation devices.

With DOME, security teams can benefit from:

- Device-level security protection, enabling firmware updates and secure supply chains
- Zero-touch onboarding that eliminates the need for cybersecurity or IT skills
- Security protection without the need for a persistent cloud connection
- Crypto-agile with legacy and quantum-resistant solutions for long lifecycle protection

Learn more about Intel's comprehensive approach to security.

intel.

[1] Cisco Annual Internet Report

[2] Business News Daily