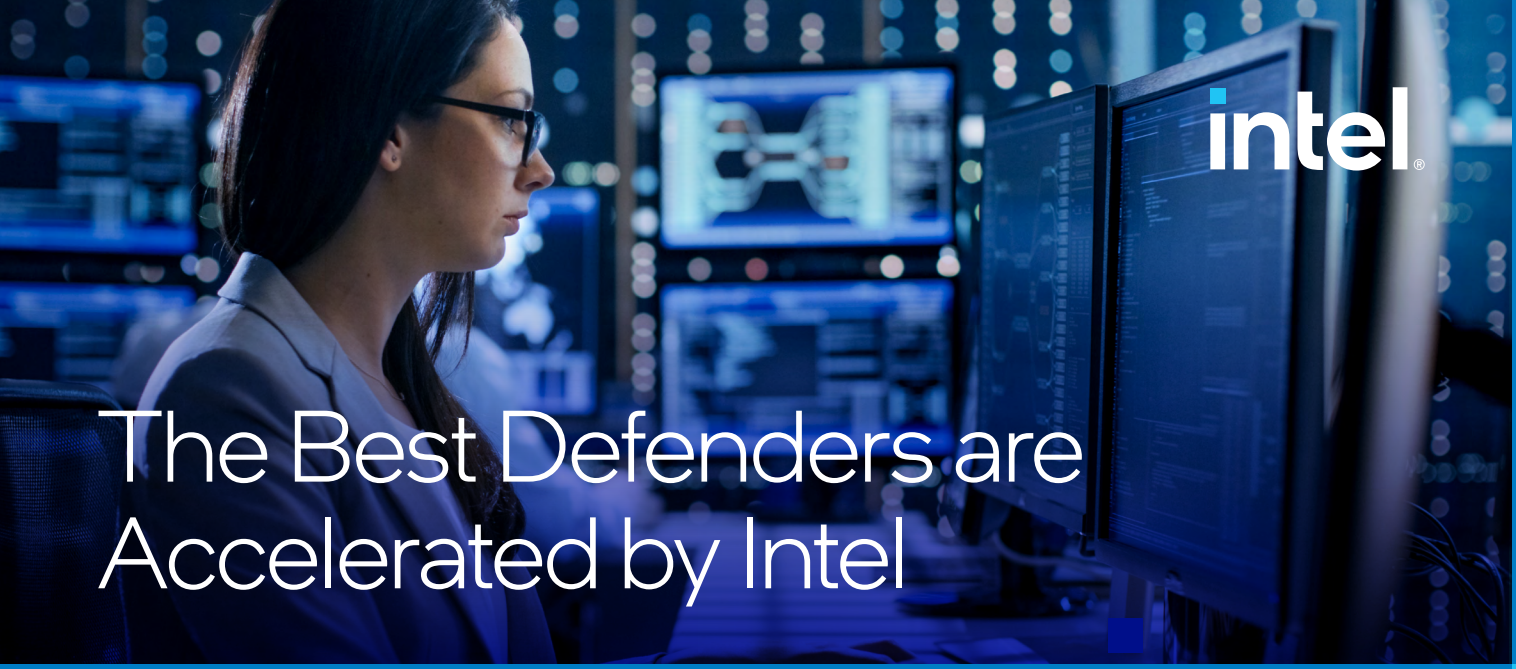


The Best Defenders are Accelerated by Intel

A formula for addressing emerging security risks

Today's technologies have created transformative benefits for society, such as the convenience, efficiencies and insights gained through cloud computing, AI and machine learning (ML). Yet they've also generated a massive amount of new security risks, with multiple points of entry for threat actors. These risks apply to nearly every organization, and they aren't going away. In fact, an estimated 93% of networks are vulnerable to cyberattacks, and by 2031, new ransomware attacks are expected to happen every two seconds.

While traditional software-based approaches to cybersecurity once provided adequate protection for organizations, today's threat landscape demands a different approach. Security must start with the silicon—the essential building block to create hardware with an innovative mix of purpose-driven architecture to accelerate software's capabilities while hardening defenses down the compute stack. Products must also be designed and rigorously tested to withstand evolving security threats and meet increasingly stringent government regulations. These products can then become foundational technology for security solutions co-engineered with trusted partners who belong to a robust ecosystem. And Intel can bring all this together, helping organizations to meet ever-changing security risks.

Security begins with Intel

Intel is uniquely positioned to lead the technology industry in a security evolution due to our vast product portfolio and end-to-end ownership in product development. We believe that system trust is rooted in security—if hardware isn't secure, then a system cannot be secure. That's why our goal is to build the most secure hardware on the planet enabled by software—and we've made unparalleled investments in people, processes, and products to meet this goal.

We've also established four pillars that guide our commitment to security.

- **Integrity and trustworthiness**
  This includes establishing a verifiable foundation of trust in a system
- **Any data, anywhere**
  We focus on workload protection with an emphasis on securing data, as it is used in new and novel ways
- **Disruption-free security**
  This guides us to address and resolve any usability impediments to security
- **Solutions**
  Our "security your way" approach is centered around innovation and flexibility to empower choice for customers and developers

These pillars, our Security-First Pledge, and our security assurance programs, which center around researching vulnerabilities to strengthen our products (even after they're in the market), continue to guide us as we deliver industry-leading security solutions. Yet all our efforts would be incomplete without our current ecosystem partners, who integrate our products into solutions that address critical security issues, as well as the future ecosystems we're investing in to solve tomorrow's challenges.

Securing the best partners for your solutions

In fact, Intel's vision is to empower our ecosystem partners to build cutting edge security technologies on our platforms, so they can meet customers' unique security needs. We also look for ways to help promote our partners, which can open up new opportunities and abilities to develop customized, innovative solutions for customers. This guide represents one way we can do that—by helping you connect with the right ecosystem partners to solve your security challenges and defend your business.

Our cybersecurity ecosystem partners

The following partners deliver security solutions featuring Intel technologies to protect your business from today's evolving challenges. Note that some of these partner synopses feature the designator *Accelerated by Intel.* The Accelerated by Intel program is an Intel brand endorsement that identifies solution providers who have optimized their offerings with Intel® technologies. Partners are empowered to deliver solutions with faster time-to-business value and can offer enhanced user experiences.

Anjuna

www.anjuna.io

Anjuna Seaglass™ is the first Universal Confidential Computing Platform, designed to run any application in any major cloud with complete data security and privacy. Anjuna partners with Intel to virtualize confidential computing-capable CPUs and provide seamless remote attestation capabilities. By doing so, Anjuna Seaglass isolates your workloads in a protected environment that intrinsically secures your data in every state—in use, in transit, and at rest—and allows you to control application-level trust policies, ensuring that only trusted code can access sensitive data.

Industries: financial services, government, SAAS, blockchain

Additional information: Anjuna Seaglass Datasheet ▪ Anjuna / Intel Confidential Computing 101 ▪ HashiCorp Vault on Intel SGX ▪ Confidential Computing for AI ▪ 77:1 Advantage Against MITRE MATRIX ▪ An Ecosystem Solution for Confidential Computing

Crowdstrike

www.crowdstrike.com

CrowdStrike, a global cybersecurity leader, and Intel have pioneered a strategic collaboration for AI and hardware-assisted security. Their partnership drives ecosystem unification to improve security across the computing stack edge-to-cloud to give customers heightened security necessary to defend against the modern threat landscape. CrowdStrike Falcon® Insight XDR delivered on the Intel® vPro® platform brings a defense-in-depth security foundation across the hardware, firmware and software stack, optimized to uncover fileless attacks and advanced persistent threats (APTs).

Additional information: CrowdStrike and Intel Corporation: Addressing the Threat Landscape Today, Tomorrow and Beyond ▪ Help Shrink the Attack Surface of Endpoints with Hardware-assisted Protection ▪ Hardware Enhanced Exploit Detection (HEED) ▪ Accelerated Memory Scanning (AMS)

Endpoint protection

Adopting endpoint security practices can safeguard endpoints—meaning any device that receives a signal, such as laptops, tablets, smartphones and Internet of Things (IoT) devices—from unauthorized access and digital threats that can compromise data and performance. Any comprehensive endpoint security strategy will include hardware-enabled protections and remote management tools to help protect endpoints that connect to the corporate network. Intel offers the enterprise endpoint security leadership to deliver this strategy. Our expertise is backed by unmatched surface area coverage, which comes from protecting 1+ billion computing endpoints[1], and more than two decades of focused experience.

Our partners leverage these strengths when they build solutions featuring our Intel® vPro platforms. The security features built into these platforms help customers to significantly lower their risks of major PC-related security events; securely manage devices inside and outside the firewall, over the cloud and enable cyberattack recovery; and reduce downtime or workflow disruptions. We can further help partners develop solutions to protect against endpoint cyberattacks with Intel® Threat Detection Technology (Intel® TDT), which augments traditional, software-based security solutions, with hardware telemetry and accelerated memory scanning.

1 Security Begins with Intel at RSA Conference 2023

Beekeeper AI

www.beekeeperai.com

BeeKeeperAI's flagship product EscrowAI™ provides a push-button, privacy-enhancing, secure collaborative computing platform leveraging Trusted Execution Environments (TEEs) that utilize the robust confidential computing capabilities of Intel® Xeon® Scalable processors with Intel® Software Guard Extensions (Intel® SGX), and soon those with Intel® Trust Domain Extensions (Intel® TDX). EscrowAI automates the collaboration within the TEE and enables end-to-end encryption that protects personally identifiable information, protected health information, or any private data, as well as an algorithm's intellectual property (IP). Due to its zero trust security protections, EscrowAI accelerates the approvals and contracting process enabling model developers and data stewards to initiate their projects quickly— reducing the development time from years to months.

Industries: healthcare, financial services, stewardship

Additional information: Accelerating Development of Clinical AI Algorithms ▪ Beekeeper AI Secures AI Algorithms

A story of partnership

A global biopharma was challenged with accessing sufficient data to validate its algorithm, which was developed to identify patients with a rare disease. Using EscrowAI, the company trained and tested its model on datasets containing very sensitive and legally protected data, which led them to develop a powerful patient identification model. This model helped them more quickly diagnose patients while always keeping the patient data and the model IP protected.

Specifically, EscrowAI enabled the company to submit an encrypted machine-learning classification model to the platform where it was containerized and prepared for use within the TEE. The data steward curated and encrypted the real-world dataset and made it available within their HIPAA-compliant Azure environment. For computation, EscrowAI initiated a confidential Intel SGX application enclave within the data steward's compliant tenant. Once the trusted computing base was proven through attestation, the dataset was brought into the enclave and the model computation was initiated. Data sovereignty was maintained throughout the process because the TEE operated within the data steward's secure environment. EscrowAI ensured that identifiable, sensitive data remained encrypted at rest, in transit, and during computation within the secure enclave. Upon completion of the run, the algorithm's output was checked by EscrowAI to ensure it matched a pre-agreed form and did not contain protected data. A summary performance report was sent to the algorithm developer's project space within EscrowAI that provided statistics on the algorithm's performance without exposing any identifiable, sensitive data.

Zero trust

In this approach to security, enterprise resources can be securely accessed regardless of location, network, or technology using real-time context and rule-based authorization. In fact, Zero Trust takes nothing for granted, but instead operates on the assumption that cyberattacks can happen at any time—and that every interaction must begin in an untrusted state. This enables continuous defense against intrusions and malicious code, offering protection for an organization's hardware, software, data, and users. Intel is working with industry leaders and partners across market segments to accelerate Zero Trust benefits, which include supporting the transformation to cloud-centric networking and enabling security and networking-as-a-service through secure access service edge (SASE). Intel provides our partners with the foundational expertise and the most comprehensive range of security technologies to power their Zero Trust solutions. These offerings include our leadership in crypto and packet acceleration and networking AI/ML, SASE reference architectures, and of course, the broadest silicon footprint from client to networking to cloud.

Fortanix

www.fortanix.com

Fortanix has a data-centric approach to cybersecurity that can help minimize data breaches and accelerate regulatory compliance. Their flagship product, Data Security Manager (DSM), helps security, data, risk management and DevOps teams collaborate. It also simplifies cryptographic operations to secure sensitive data. And the Fortanix Enclave Development Platform (EDP) protects applications at runtime; provides a preferred method for writing Intel SGX enclaves from scratch; and allows developers to use Rust, which (in combination with Intel SGX) makes applications secure from vulnerabilities and outsider attacks.

Industries: healthcare, financial services, federal, manufacturing

Additional information: Solutions with Intel SGX ▪ Intel Security Solution for Fortanix Confidential AI ▪ Intel and Fortanix solution brief ▪ Rust enclave development (GitHub)

Fortinet

www.fortinet.com

The range of solutions Fortinet provides deliver benefits like proactive threat detection, the ability to identify malware and hacker attacks, and virtual traffic monitoring and enforcing. The solutions include security processors, security fabric and FortiOS, which ties all security fabrics and network components together. Additionally, their Fortinet Fabric-Ready Partner Program empowers an open ecosystem to focus on developing innovative solutions related to infrastructure automation, cloud security, secure networking, 5G and telco, OT/IoT security, Zero Trust security, and network and security operations.

Industries: healthcare

Additional information: Innovating with Visionary Security Technologies and Solutions ▪ Fortinet and Intel Secure Device Onboard Security Solutions

A story of partnership

While Internet of Things (IoT) devices can deliver great efficiencies, insight, and control, they can also create plenty of security issues. Security teams are often forced to make assumptions about devices and the network access they should receive. To empower these teams with greater insights, Intel and Fortinet co-engineered a solution featuring an automated onboarding service with network access control capabilities to dynamically configure edge security policies for IoT devices. Specifically, this solution includes the Intel® Secure Device Onboard (Intel® SDO) service and the Fortinet FortiNAC SDO.

Together, these technologies create a zero-touch onboarding experience with automated security. The solution quickly validates a device's identity and determines the level of network trust it should receive. The overall result is a more secure deployment of IoT devices that can scale using automated processes—without high costs. To learn more, read Fortinet's solution brief.

Noname Security

www.nonamesecurity.com

The Noname API Security Platform secures APIs both in development and in production, allowing organizations to deliver secure apps and APIs faster while protecting them from attacks. Noname's solution addresses each of the four pillars of API security: API discovery to inventory environments; posture management to uncover misconfigurations or vulnerabilities; runtime protection to stop attacks in real time, and API security testing, which helps developers uncover API-specific vulnerabilities. This full-lifecycle approach provides the industry's greatest flexibility and breadth and depth of coverage.

Additional information: API security for Intel ▪ Intel and Noname Security video ▪ Noname Security builds scalable and cost effective API security solution ▪ Noname API Security and Intel Trust Authority ▪ Noname Security and Intel solution brief ▪ API Security for Cyber Protection (insight.tech)

Pure Storage

www.purestorage.com

Pure Storage helps organizations embrace the future of the cloud and data flexibility with a true as-a-service model. All products within the Pure Storage portfolio run on Intel. By leveraging Intel technologies, their solutions can offer modern analytics on cloud native architecture with fast S3 storage; significantly reduce costs for SAP HANA environments; architect a secure, highly available Kubernetes Data Services platform for RedHat OpenShift; provide expertise on migrating to OpenShift 4 at scale; and deliver disaster-proof containerized apps.

Additional information: Power Genomic Solutions with a Modern Data Experience

Confidential computing

With more data in the cloud and at the edge than ever before, keeping it secure has become increasingly difficult. Businesses may assume they already have solutions to meet this challenge, because they have technologies in place to protect their data in transit or at rest. Yet Intel and our partners are able to provide something more: solutions that are designed to help keep data secure at every stage of its journey—in transit, at rest, and in use. We do this with confidential computing, which is designed to secure data in use by isolating it in a hardware-based enclave. Confidential computing solutions, featuring Intel technologies like Intel SGX and Intel TDX, provide organizations with multiple security benefits. They include the ability to collaborate with multiple parties while maintaining privacy and promoting compliance; the flexibility to set trust boundaries appropriate to workloads; and enhanced protection from advanced attacks, tampering and theft.

VMWare

www.vmware.com

Since the inception of virtualization technology, VMWare has collaborated with Intel to deliver innovative solutions. Today, we offer solutions with both our VMware Cloud Foundation and Intel technologies, including Intel® Optane™ DC Persistent Memory, Virtual Intel® Software Guard Extensions (vSGX) and Intel vPro. With these solutions, enterprise customers can extend available resources and easily distribute workloads between on-premises, public cloud, and the edge. They also allow for confidential computing, modern chip-to-cloud PC management, and modernized data centers that enable IT transformation.

Additional information: VMWare and Intel Virtualization Solutions

A story of partnership

Today's businesses are generating an increasing amount of data, which has led to a significant customer pain point: how to quickly analyze this vast amount of data. Doing so requires large capacity memory within the server, as well as persistent, secure storage. VMware and Intel are meeting this challenge with technologies that also provide IT organizations with a clear path to digital transformation.

These technologies include VMware vSAN 8 with Express Storage Architecture (ESA), which allows data to be processed and stored with improved efficiency, scalability, and performance. And when combined with 4th Generation Intel® Xeon® Scalable processors and VMware vSphere, vSAN 8 software can power the most demanding workloads. Our solutions also feature Intel® Optane™ DC persistent memory, which offers the latency of memory with the persistence of storage.

These technologies represent just a few ways VMware and Intel are supporting IT organizations. They rely on our solutions to deliver consistent infrastructure and operations across data centers and public clouds to accelerate application speed and agility for business innovation and growth. To learn more, visit VMware's solutions page.

Zscaler

www.zscaler.com

Zscaler extends Zero Trust cybersecurity across the network to users, devices, and workloads while offering value to customers at an unparalleled scale. Their solutions range from fully cloud based to Zero Trust SD-WAN for branch offices and private data centers. These solutions include products that help provide safe, fast internet and SaaS access; deliver the quickest, most secure access to private apps and services; secure connectivity between workloads spread across public clouds, data centers, and public/private edge; monitor performance to ensure optimal digital user experiences; and use AI to detect and disrupt the most sophisticated threats. Additionally, Zscaler's cybersecurity solutions are proven; they blocked 29 billion threats in 2023 alone.

Multi-industry priorities: improving cybersecurity posture without reducing headcount, end user digital experience, remote access across the enterprise, decreasing complexity

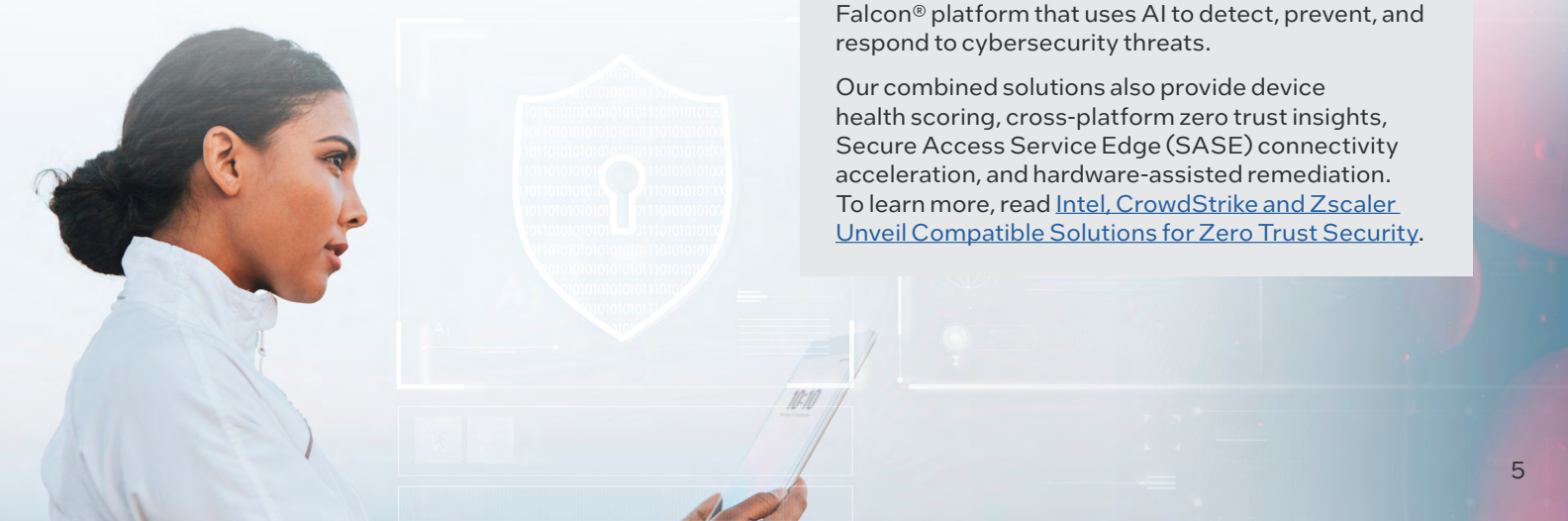
Additional information: Digital transformation success stories

A story of partnership

With a growing number of remote workers, the concept of Zero Trust has evolved to become a mainstream security best practice for minimizing uncertainty by enforcing accurate, least-privileged access to information. To deliver this conditional access from edge to cloud, Zscaler is working with Intel and CrowdStrike. In fact, we're helping IT organizations implement comprehensive Zero Trust strategies that include hardware and software security technologies.

Both Zscaler and Crowdstrike have integrated hardware security into their solutions, so customers receive hardware-assisted benefits right out of the box. Specifically, Intel® Xeon-based optimizations power Zscaler's Zero Trust Exchange, which establishes trust and enforces policies to reduce the attack surface, risk of data loss, and the complexity of perimeter-based security. And Intel vPro threat detection offers optimizations for the CrowdStrike Falcon® platform that uses AI to detect, prevent, and respond to cybersecurity threats.

Our combined solutions also provide device health scoring, cross-platform zero trust insights, Secure Access Service Edge (SASE) connectivity acceleration, and hardware-assisted remediation. To learn more, read Intel, CrowdStrike and Zscaler Unveil Compatible Solutions for Zero Trust Security.



Intel® Ignite is a global early-stage startups acceleration program and cybersecurity

Explore Intel's unwavering dedication to cybersecurity, reaching beyond conventional boundaries to anticipate the future challenges in the field with Intel Ignite, our startup accelerator designed for early-stage, deep tech startups. The primary objective of Intel Ignite is to engage with future leaders in disruption. Through expediting the growth of these companies, we empower them to unlock innovation and construct the secure computing landscape of tomorrow. During the last four years, Intel Ignite has assessed over 400 security companies and selected 20 to participate in the program. Discover some of the remarkable cybersecurity ventures that have graduated from the Intel Ignite program below.

Apheris
www.apheris.com

Make sensitive data available for machine learning (ML) without sharing . Ensure compliance. Commercialize data across boundaries. Enable federated learning. Apheris provides governed, private, and secure computational access to data for ML and analytics. Enabling federated learning and data collaborations across boundaries.

Crypto Quantique
www.cryptoquantique.com

Crypto Quantique provides secure root of trust and remote device provisioning, as well as management solutions for Internet of Things (IOT) at scale.

LayerX
layerxsecurity.com

LayerX Enterprise Browser Extension turns any browser into the most protected and manageable workspace, while maintaining a top-notch user experience.

Mine
www.mineos.ai

MineOS is an end-to-end data privacy and governance solution, helping enterprises to map their data and drastically simplify data privacy operations.

Ox Security
ox.security

OX integrates security seamlessly into the software development lifecycle. By consolidating fragmented tools, OX's Active ASPM platform enables automated remediation based on prioritization from active context.This empowers DevSecOps and AppSec teams to release products swiftly without compromising security.

Oligo Security
oligo.security

Oligo provides effective application security by using runtime context to identify which vulnerabilities are actually exploitable while adding real-time protection against exploits and malicious use.

Roseman Labs
rosemanlabs.com

Our data collaboration platform enables companies to use each other's data without exposing the underlying source data by computing on decentralized, encrypted data.

Subsalt
getsubsalt.com

Subsalt creates synthetic data that satisfies the anonymized and de-identified data exemptions in major data privacy laws. This allows valuable data to be shared with internal teams, vendors, and partners without risk of non-compliance, user consent issues, or data breaches.

Intel Capital and Cybersecurity

Intel's commitment to cybersecurity extends beyond today's ecosystem. In fact, we have our venture capital organization to invest in the cybersecurity ecosystems of tomorrow. Intel Capital's goal is to identify companies that are not only solving significant and emerging challenges for Chief Information Security Officers (CISOs), but also show the potential for exponential growth. By investing in these companies, we help them fulfill their promise and enable innovation. Below are the companies that are currently part of Intel Capital's cybersecurity portfolio.

Application security

- Moderne: automated code remediation
- Oxeye: cloud-native application security testing
- Zenity: security for low-code/no-code development

Data security

- Duality: secure data collaboration product
- Fortanix: data encryption security platform
- Immuta: data access controls security platform
- Opaque: secure collaborative data analysis

Identity and access management

- Grip: SaaS security control plane and access management

Infrastructure security

- Eclypsium: Zero Trust supply chain risk management
- JupiterOne: cyber asset attack surface management

Network security

- Augtera Networks: network AI for NetOps
- Tetrate: end-to-end application networking security and WAF
- Trinity Cyber: advanced network threat prevention

Security operations

- Intezer: autonomous security operations

Vulnerability and risk

- Censys: industry-leading cloud and Internet asset discovery solutions
- Synack: continuous pen testing and breach simulation
- SecurityScorecard: security ratings and cybersecurity risk management

Additional Resources

To learn more about Intel's commitment to security, as well as our programs and benefits for cybersecurity partners, please visit the following resources:

- Security Begins with Intel
- Intel's Security-First Pledge
- Intel Confidential Computing
- Intel Endpoint Security
- Intel Zero Trust Cloud Framework
- What is SASE?
- Intel® Security Engines
- Intel vPro Platform
- Intel Threat Detection Technology (Intel TDT)
- Intel Software Guard Extensions (Intel SGX)
- Intel Trust Domain Extensions (Intel TDX)
- Intel Partner Alliance
- Accelerated by Intel One-pager
- Accelerated by Intel Quick Reference Guide