Case Study

Public Sector
Embracing Digital Transformation

Six Pillars of Security

Cyber attacks are on the rise. Steve Orrin, CTO at Intel Federal, outlines the attack vectors, six pillars of cybersecurity, and how Intel can help.

Summary

With cyber-attacks on the rise in all industries, security is more important than ever. In this episode, Darren Pulsipher, Chief Solution Architect, and Steve Orrin, Federal CTO at Intel Federal, outline the attack vectors, the six pillars of cybersecurity, and how Intel can help. The level of complexity organizations must deal with to secure their data, systems, and applications has never been more difficult.

Podcast: SoundCloud Channel

Video Link: Youtube Channel

Intel and the Cybersecurity Pillars

With cyber-attacks on the rise in all industries, security is more important than ever. In this episode, Darren and Steve Orrin, Federal CTO at Intel, outline the attack vectors, the six pillars of cybersecurity, and how Intel can help.

Steve has seen security evolve in the 25 years he's worked in the field, both as a science and as an art. At the same time, the level of complexity organizations must deal with to secure their data, systems, and applications has never been more difficult.

Large Scale Breaches and Cyber Attacks Continue

Large scale data breaches and deep intrusions are happening up and down the stack in everything from social media platforms to financial services to health care. No type of data is exempt from being targeted with increasingly sophisticated techniques.

What is driving these hacks? One answer is that today, a wide scale or deep attack requires fewer resources and less financial investment. The scope and scale of what a hacker can do with a small investment has given adversaries an edge in a complex system.

Three Forces Impacting Enterprise and Mission Security

Another answer to what is driving the attacks is that data is a valuable asset: the new oil. Data is vulnerable as the expansion of the attack surface continues to grow.

There are more integration points, products, vendor operating systems, and devices that are involved in managing, consuming, and transporting the data. The data is further away from the control of the enterprise. Sometimes we're not even sure where our data exists. For example, perhaps you've shared your data with another organization and they shared the analytics that were performed on the data. That metadata often turns into data residue. Your data is flowing through multiple systems, consumable by an attacker after the fact.

The security industry itself is composed of thousands of security vendors and products that solve a particular piece of the puzzle, so there's only so much a CIO can do with a limited budget, and only so much they can handle given the complexity. We have to think holistically about how we can secure our data, not just how to secure one transit between point A and point B. Data is compromised at the weakest link, so we have to look at the whole chain.

The third force impacting enterprises is the locations of the attacks. They include attacks up and down the full stack of hardware, firmware, bios, software, services and applications. With the increase in the sophistication of the attacks we are seeing attacks at multiple layers at asynchronously and independently.

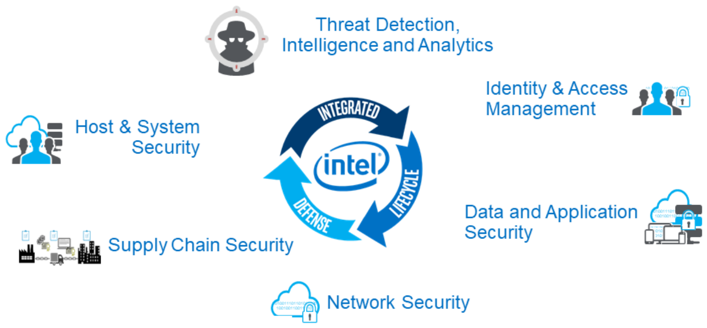
The Attack Vectors

Hackers are not just attacking the hardware or a piece of software, but through multiple vectors: people, process, and technology.

Traditionally, implementing security controls has involved proper training of people and using the right processes and technologies, but in light of recent attacks, we need to remember that the process itself is vulnerable. For example, we need to move to automated patching to reduce the window of exposure from when a vulnerability is discovered to when a patch is released and deployed by an organization. Traditionally, we've lived with the risk that attackers may have months to exploit the vulnerability.

There are other process attacks that we are just now sealing, whether it is in the build process or software development lifecycle. Integrating security early in the development lifecycle is the most important aspect to securing an application. That means developers, QA, and designers all must be involved in the security process. Part of the challenge is the siloed nature of each part of the process, where vulnerabilities can creep in the seams and transitions.

Six Pillars of Cyber-security



Threat Detection, Intelligence and Analytics
Identity & Access Management
Host & System Security
INTEGRATED
intel
LIFECYCLE
DEFENSE
Data and Application Security
Supply Chain Security
Network Security

Supply Chain Security

Supply chain security has been at the forefront only for the past few years. An organization needs to be able to trust the servers, components, and software. A good supply chain with transparency is important in order to validate that everything is coming from legitimate sources. There has been a focus, particularly in government, about the hardware supply chain, but we can't forget the software supply chain. The software supply chain is a bit more difficult than hardware since there is often a lack of visibility because products can be cobbled together from open source tools, other people's products, etc. In a recent attack, the software supply chain was the problem, and this is just the tip of the iceberg.

Host & System Security

Once we have a trusted supply chain, the next step is in hosting system security. The foundation is secure boot technologies and crypto capabilities to lock down and secure physical devices and systems where the applications work and data will run. This system supports the higher-level stack security features in the hardware.

Data and Application Security

Above the host and system security is where you build your application workload security. Data must be protected throughout its lifecycle, at rest, in use, and in transit. We've been doing security for data at rest and in transit for a long time using transport encryption, TLS, and IP sec, and other encryption capabilities, and then full disk and file encryption. The missing link has been data "in-use" encrypted memory with hardware isolation. In the last few years, technologies and solution stacks are enabling that last mile of exposure around data protection.

Network Security

In parallel with this stack of supply chain hosts and data security, we need network security. Integrity and availability of networks is important to withstand denial of service attacks. The data needs to get to where it needs to go securely. We also must monitor and protect networks from external intrusions, whether that network is enterprise or a distributed network throughout the cloud and the edge. Security here is not about simple firewalling; it's about active production.

Identity & Access Management

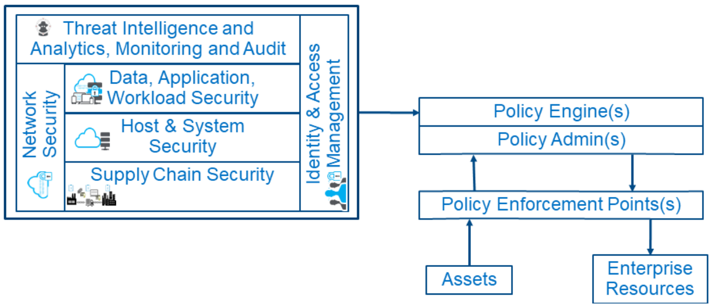
Identity and access management is a foundational capability. We not only need to know who is logging in, but who is logging in to what device. The human is actually a small piece of the puzzle. We need to have identity for all the things, processes, and services that are accessing and managing the data. A person might do their job with just a few keystrokes, but there may be 20 different devices and 100 services and processes that act on the data. We need to have policies and authorization for all of those entities. And as we move more into autonomous processes, there are fewer humans involved, so it becomes even more important to have a strong identity for those processes without a human in the loop.

Threat detection, Intelligence, and Analytics

This last pillar is a combination of many things including threat intelligence, analytics, monitoring, and auditing. It's the overarching visibility into making sure everything is running the way it's supposed to run, and if something is wrong, the ability to quickly understand where it's coming from and why. This is the umbrella that drives data security and everything must feed up and feed down. There is a shift from working in a siloed environment, say a vendor who is only concerned with network security, to working across the system as a whole. Successful companies have diverse teams with people from different domains to meet complex security needs.

Cyber Security Domains: Achieving Zero Trust with Intel Technologies

Intel provides foundational capabilities in each of the six pillars, whether it's our compute life cycle assurance initiative to help get the broader OEMs and component providers collaborating on a trusted supply chain, to providing the foundational building blocks of system security, to secure boot starts with the hardware. We have execution technology and boot guard technology with crypto acceleration built in so users can turn it on for data at rest, data in use, and data in transit protection without performance impact.



Threat Intelligence and Analytics, Monitoring and Audit
Network Security
Data, Application, Workload Security
Host & System Security
Supply Chain Security
Identity & Access Management
Policy Engine(s)
Policy Admin(s)
Policy Enforcement Points(s)
Assets
Enterprise Resources

In the case of threat detection intelligence, Intel provides primitives such as TPD where an upper-level stack solution can provide visibility and threat detection where we've never had it before.

Intel is a technology provider, but we also work in the space of people and process. A good example is the supply chain. We've built a process with the ecosystem to enable an enterprise to be able to validate the components and credentials for a given platform and its components. Similarly, there are processes involved with data and use protection through capabilities in the hardware such as SGX being able to encrypt the memory and isolate the data and code for a given application.

Intel is enabling secure processes for leveraging the technologies at scale. Another key part around process is fitting into an organization’s overall risk framework. Intel gives you the evidence and attribution you need within our technologies to map that into your existing risk framework.

The last piece is people. Dealing with random human behavior is sometimes the hardest part of security, whether it’s phishing scams or engineered attacks on weak passwords. Training is crucial, but it often isn’t enough. Processes and technologies can help augment training by, for example, making passwords stronger or eliminating phishing if a user’s credential can’t be compromised. At the end of the day, however, continuous training and education will always be critical along with mitigating technologies.

Security is difficult, but there are lights at the end of the tunnel with all the innovations in the ecosystem and with organizations open to doing things differently. We need to keep our eye on two things: the adoption of risk frameworks, and zero trust. Tying these two worlds together, the cyber security domain to policy engines and enforcement can provide a comprehensive approach to security. There is a lot of activity here, and a lot of work still to be done.