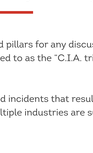
Building Your Organization's Trusted Supply Chain

Starts from the Silicon Up

Why Security in the Supply Chain Matters

In Aberdeen's study of 288 Chief Supply Chain Officers, **the business impact of security-related issues affecting the supply chain** ranked behind only that of the global pandemic, product recalls, and reduction in customer demand. Over the previous 12 months:

82% indicated that security-related issues had caused **operational disruptions**



72% said that security-related issues had resulted in **loss of revenue**

In the modern, digitally-enabled supply chain, your organization's decision-makers need to consider not only the traditional IT security capabilities needed for its trusted users – but also the capabilities necessary to ensure the security and integrity of trusted processes, software, and platforms (hardware / OS / systems). **Today, building your organization's trusted supply chain starts from the silicon up.**

Security in the Supply Chain Part 1: What Could Possibly Go Wrong?

For organizations of any size, the time-honored pillars for any discussion of security in the digitally-enabled supply chain are referred to as the "C.I.A. triad," shorthand for *confidentiality*, *integrity*, and *availability*.

Some high-profile examples of security-related incidents that resulted in significant operational disruptions to supply chains in multiple industries are summarized in the following table:

	Example	Attacker Actions	Business Impact
Trusted Users	Target (2013)	User credentials stolen from a vendor	40M payment cards, 70M customer records compromised
	Home Depot (2014)	User credentials stolen from a vendor; malware installed on Point of Sale terminals	50M payment cards compromised
Trusted Processes	SolarWinds (2020)	Malicious code injected into a commercial remote infrastructure monitoring and management solution	Up to 19K customers at risk of unauthorized access
	Accellion (2020)	Multiple zero-day vulnerabilities exploited in a commercial file-sharing application	Private data exposed for hundreds of customers and millions of individual users
	Kaseya (2021)	Vulnerability exploited in a commercial remote infrastructure monitoring and management solution	> 70 managed service providers and up to 1,500 of their subscribers at risk of ransomware attacks
Trusted Software	Apache Struts (2017)	Unpatched vulnerabilities exploited in open source web application software	Personal financial data at Equifax compromised for 143M people
	Apache Log4j (2021)	Vulnerability in an open source logging utility allows attackers to install malware, take control, or steal data	Countless applications deployed by untold thousands of organizations at risk

Confidentiality refers to systems, applications, and data being accessible only to authorized users or systems.

Integrity refers to systems, applications, and data being unaltered, except for intentional changes by authorized users or systems.

Availability refers to systems, applications, and data being accessible when needed to authorized users or systems.

Security in the Supply Chain Part 2: How Your Servers Can Become the Foundation for Trust

Aberdeen's study of 304 organizations with respect to IT modernization initiatives found that **3 out of 5 (60%) plan to refresh their servers within the next 2 years;** the typical server refresh cycle is about 4 years.

Managing security-related risks was the second-biggest driver for current investments in modernizing IT infrastructure, second only to remaining competitive.

Your organization's next server refresh creates the perfect opportunity to plan for the security and integrity at the very foundation of your trusted supply chain.

Are your servers protected from unauthorized changes during bootup, updates, and execution?

Until recently, there was little mainstream attention given to safeguarding the integrity of servers during bootup, updates, and execution. This changed dramatically starting in 2018, with the disclosure of high-profile attacks on platform vulnerabilities – such as *Meltdown* and *Spectre* – that can exist "below the operating system."

Meltdown and Spectre (2018): Virtually every computer chip deployed over the previous 20 years was found to have vulnerabilities that could expose personal data or passwords from kernel-memory locations, with high likelihood of a successful exploit.

Today, leading solution providers are designing advanced security capabilities into their platforms from the silicon up, to reduce the likelihood of integrity-related compromises throughout their natural lifecycle – for example, to:

Protect the integrity of servers at multiple levels, including BIOS, firmware, credentials and encryption keys, and physical hardware

Detect unapproved changes and malicious cyber attacks

Recover BIOS, firmware, and OS to a known good state, when needed

Securely re-purpose or retire servers, by permanently erasing data and resetting security attributes

Are your servers protected from unauthorized changes from the time they are manufactured, to the time they become an integral part of your organization's supply chain infrastructure?

In 2019, the perceived risk of espionage and potential sabotage to communications, critical infrastructure, and the digital economy led several governments to ban the use of certain telecommunications hardware from non-domestic sources (e.g., 5G networking equipment from Huawei Technologies in China).

Today, leading solution providers are also offering specialized services that ensure the domestic sourcing, manufacturing, and provenance of industry-standard servers – built by vetted employees, in highly secure domestic facilities – that include the advanced security capabilities noted above.

How HPE Trusted Supply Chain and the HPE Server Security Optimization Service Can Help Your Organization Build on a Solid Foundation of Trust

To learn more about how your organization can build a trusted supply chain from the silicon up, visit

www.hpe.com/security/compute ▸

ABERDEEN STRATEGY & RESEARCH — ILLUMINATE. INSPIRE. ENACT.

Hewlett Packard Enterprise