SYSTECH

Systech: Combating Supply Chain Threats with Digital Brand Protection

In this issue

Gartner

Welcome

Eroding Profits and Damaged Brands – Supply Chain Threats from Counterfeiting and Diversion

There are numerous challenges that threaten the 21st century supply chain, however, two of the largest threats are counterfeited and diverted goods. $1.7 trillion is lost annually to product counterfeiting and diversion, and companies are spending over $150B annually to combat this with additive product packaging technologies – including holograms, special seals, taggants and electronic additives.

Ironically, counterfeiters are benefiting from the same things that are driving legitimate business – improvements in technology. Printing technology itself enables counterfeiters to create almost exact replicas of original product labeling and packaging. Between the threat of counterfeit goods and rampant diversion, brands are being put to the test to develop strategies to keep customers safe, protect company revenue and ensure brand loyalty.

Change Everything without Changing Anything

What if we could use existing packaging and labels to create a strong brand protection solution that helps fight counterfeiting, enables diversion detection, and could easily leverage Blockchain?

Solutions like Systech's patented e-Fingerprint® technology do exactly that. It easily integrates with existing manufacturing lines and analyzes each product's barcode at production speed, deriving a unique e-Fingerprint identifier. Now, each of those millions of "identical" UPC coded items have a unique ID able to provide genuine product authentication and diverted product identification. This unique e-Fingerprint can now be the trusted connection between the physical world and the digital world of Blockchain.

Systech is revolutionizing brand protection and we understand that you can't fight today's supply chain threats with yesterday's technology. This newsletter from Gartner highlights several thought leadership pieces from Systech and a recent Gartner research paper on combating threats to the supply chain. We hope these assets aide you in your quest to protect your brand and combat modern supply chain threats.

Research From Gartner

Combat Digital Security Threats to the Supply Chain

Refreshed: **4 February 2019,**
Published 6 October 2017 - ID G00337152

Foundational: **This research is reviewed periodically for accuracy.**

The information security threats to the modern supply chain, across data and IT infrastructure, product, and operations components are real, complex and growing. Supply chain leaders can use this research to develop a plan of attack to address this multifront battle.

Key Challenges

- A traditional focus on just the data and IT infrastructure security of the supply chain (SC) misses a crucial element, product security, which needs to be factored in for a holistic view.
- The difficulties posed by the battle for digital security require governance and collaboration between the supply chain and IT functions.
- Product security is quickly emerging as a critical area to support given the proliferation of smart products with embedded code and sensors, as well as the high-profile nature of recent product hacks. Supply chain groups must take the lead on product security in order to enable the IT team to provide solutions that fit the supply chain systems, processes and governance.

- Protecting the information security of the supply chain includes a focus on data and IT infrastructure, product and operations. It can seem difficult for companies to understand where to start, what they should be paying attention to now, and where they need to focus in the future

Recommendations

Supply chain leaders responsible for digital innovation:

- Focus on an integrated digital security approach to the supply chain, which looks holistically across IT and data, product, and operations-related technology.

- Ensure proper IT and SC risk governance and collaboration are in place to assess and identify vulnerable areas, and also to stay abreast of the latest threats and the success rates of mitigation techniques.

- Collaborate closely with IT, R&D, engineering, product management and marketing, and other groups – focusing on supply chain's role in the new product introduction (NPI)/new product development (NPD) process and sourcing – to address product security.

- Determine what capabilities you should already have in place, what you should be working on now, and what you need to be working on in the future to remain diligent about the digital security threat.

Introduction

Companies of all shapes and sizes, across different industries and geographic regions, are marching inexorably toward becoming digital businesses. This progress, of course, carries so many benefits – efficiencies in productivity, cost savings, better customer experience and connections, and competitive advantages.

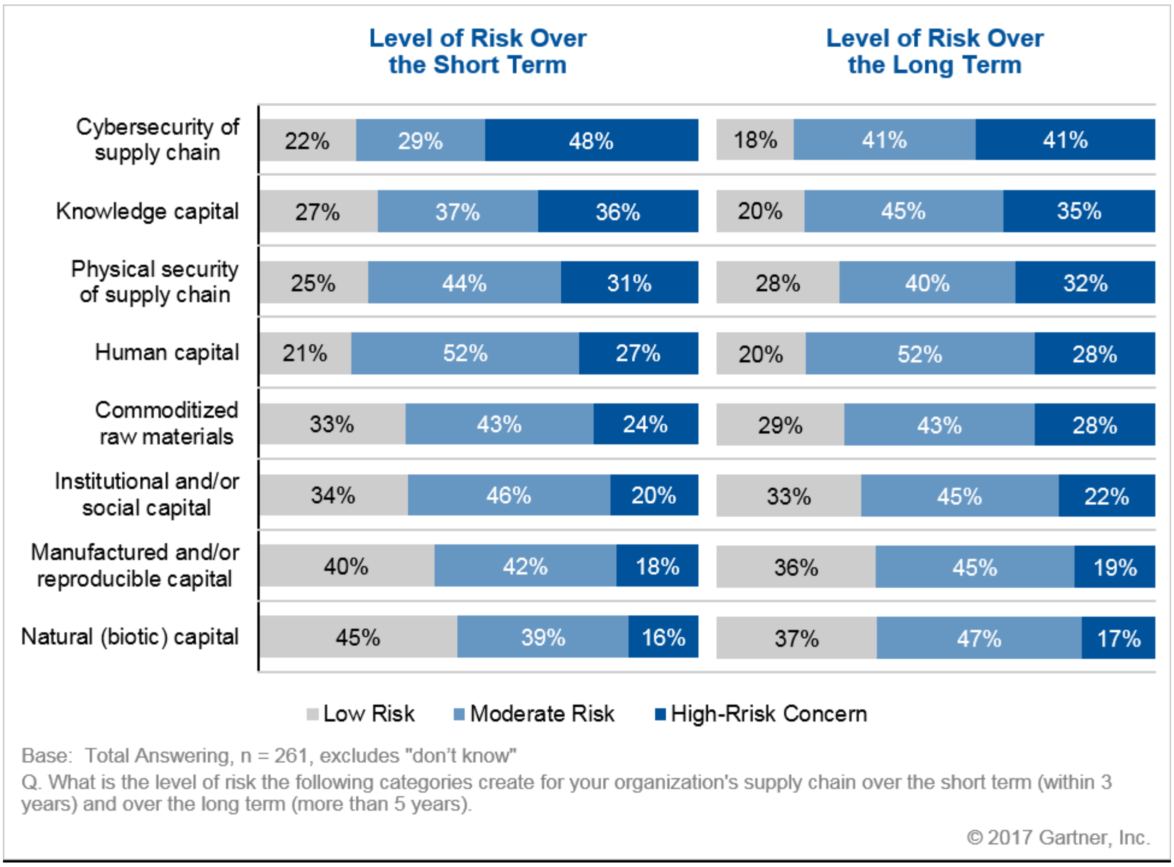
A digital business optimizes revenue, growth and efficiency by exploiting digital technology across sales and marketing channels, manufacturing, supply chain, products and services.

But this progress comes with risk, and as one of the operational areas integral to the digital business, supply chain is at the forefront of managing the risks inherent in becoming a digital business. And one of the largest risks right now, both perceived and real, is the security risk to the supply chain's "information" components. These components include a mix of data and IT infrastructure, product, and operational elements. Some people refer to this as "cybersecurity". A new view that adequately defines and captures the true risk for the supply chain is required. Whatever we call it – the risk is real and growing. As Figure 1 demonstrates, when we asked heads of SC about their greatest concerns over both the short term and the long term, cybersecurity comes to the top.

Further, the evidence shows there is a direct connection between the move to digital business and the spread of the "cyberworry." In Gartner's recent research on digital business and the impacts to the supply chain, we asked SC leaders what the greatest challenges placed by digital business were to them. The results are loud and clear:

- **Internal Digital IT Security:** Security of internet-connected facilities and assets was the No. 1 challenge; 5.3 mean on a scale 1 to 7, with 50% saying it was the biggest challenge.

Figure 1. Supply Chain Risk Levels, Short Term and Long Term



Base: Total Answering, n = 261, excludes "don't know"
Q. What is the level of risk the following categories create for your organization's supply chain over the short term (within 3 years) and over the long term (more than 5 years).

© 2017 Gartner, Inc.

Source: Gartner (October 2017)

- **External Digital IT Security:** Security of digital products was the No. 2 challenge; 5.3 mean on a scale 1 to 7, with 49% saying it was the biggest challenge.

This “internal/external” delineation, albeit a simplification, becomes crucial in demonstrating the way forward for SC, and indeed the many partners that SC collaborates with such as customers, suppliers and distribution partners, to name a few. Add to that the fact that several companies have supplier portals where technologies are integrated, and it creates even more complexity. The complex and highly fragmented topic of SC information security risk can and should looked at via digital security approach – thinking holistically about data and IT, product, and operations – which leads to considerable insight on the answers we are seeking.

The stakes are high.

A digitally vulnerable supply chain can lead to disruption of the actual operation of the supply chain, with the associated rise in costs and reduction of service levels that can devastate a company’s financial results.

It can also lead to significant damage to brand and reputation, product safety and integrity issues, privacy violations, trade and compliance implications, loss or theft of intellectual property, and substantial fines and fees.

Analysis

Focus on an Integrated Digital Security Approach to IT and Data, Product, and Operations-Related Technology

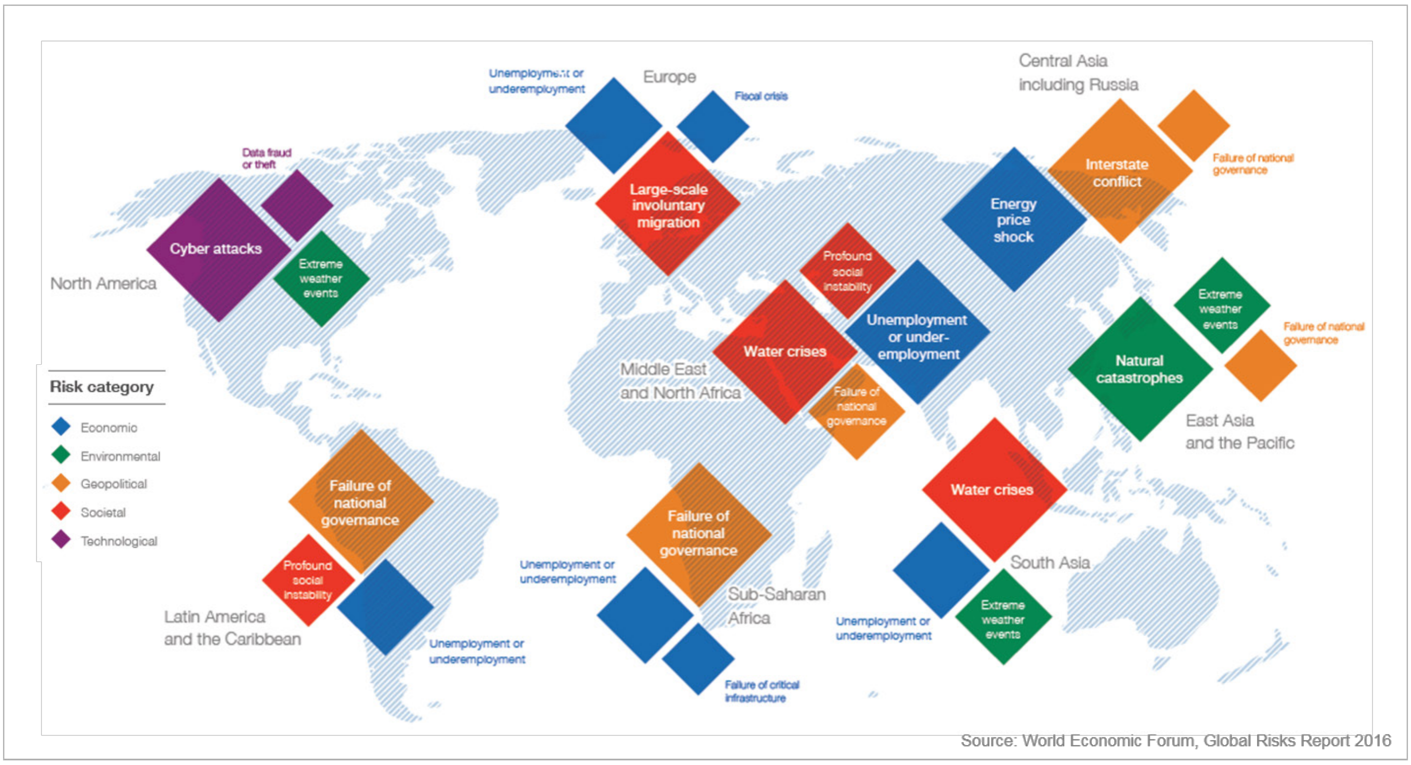
The Growing Nature of the Threats

Cybersecurity should be viewed within context of risk management (see Figure 2) before the security of the supply chain can be addressed.

This image from the World Economic Forum's 2016 Global Risks Report illustrates the many risks, and, over time, supply chains have become very good at dealing with many of these risks, such as extreme weather, natural disasters and energy price shocks. The risk of cyberattack and of data theft is most pronounced in North America.

It is important to note that this is 2016 data. The various ransomware attacks of 2017 proved how quickly some of these threats can spread, and it will be interesting to watch future iterations of this WEF analysis to see just how quickly, and where else, the cyberthreat takes top billing.

Figure 2. Global Risks


Europe
Unemployment or underemployment
Fiscal crisis
Large-scale involuntary migration
Central Asia including Russia
Interstate conflict
Failure of national governance
Energy price shock
Data fraud or theft
Cyber attacks
Extreme weather events
North America
Profound social instability
Unemployment or under-employment
Water crises
Failure of national governance
Middle East and North Africa
Extreme weather events
Failure of national governance
Natural catastrophes
East Asia and the Pacific
Risk category
Economic
Environmental
Geopolitical
Societal
Technological
Failure of national governance
Profound social instability
Latin America and the Caribbean
Unemployment or underemployment
Failure of national governance
Unemployment or underemployment
Sub-Saharan Africa
Failure of critical infrastructure
Water crises
South Asia
Unemployment or underemployment
Extreme weather events

Source: World Economic Forum, Global Risks Report 2016

Source: World Economic Forum

One of the major challenges with information risk is the incredible variety of the type of attacks and threats. The European Union Agency for Network and Information Security (ENISA) has done some great work in trying to delineate these threats, and it has created a very instructive "mind map" of the approaches of the culprits. Figure 3 shows a high-level summary of these threats – however, for each of these high-level threats, there are levels and sublevels of detail below.

For supply chain in particular, awareness has increased dramatically over the course of the past year due in part to the highly publicized attention these threats have gotten. For example:

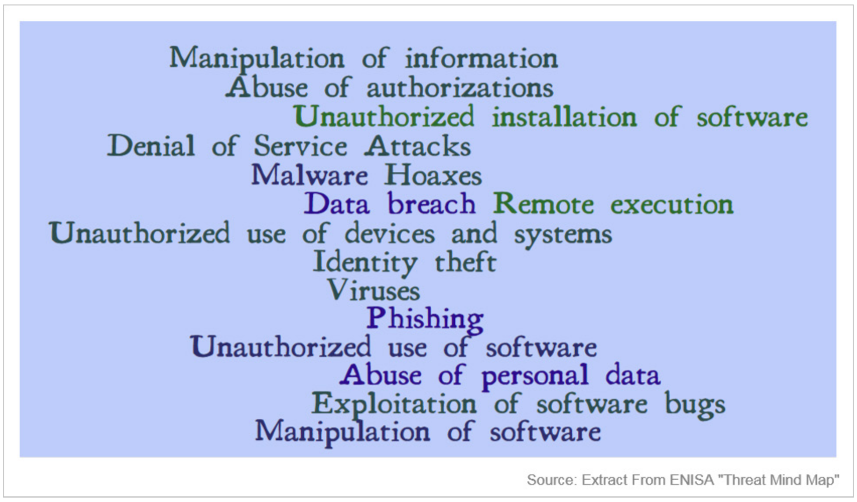
- Some of the earliest reported breaches were on the infrastructure side, where several retailers including TJX Companies, Target and Home Depot reported the theft of customer data through their information infrastructure; in these cases, point of sale (POS) systems and Wi-Fi networks. These breaches continue however, with a high profile data breach more recently at Kmart.
- Last October's denial-of-service attack on the DNS host on the East Coast of the U.S. was traced back to compromised Internet of Things (IoT) devices, including cameras, and it demonstrated clearly how products could be hacked.
- The ransomware (a type of malware) attacks of 2017 shut down actual supply chain operations:
    - "Petya" wreaked havoc for A.P. Moller-Maersk, a Danish transport and logistics company with branches worldwide.
    - "WannaCry" impacted Honda in June 2017 when it was forced to shut down production at one of its Japanese manufacturing facilities.

Complexity of the Response Tools to Address Many of These Threats

With so many threats, there are of course many potential tools and solutions to understand and deploy. The data in Figure 4 was presented at Gartner's Security and Risk Management Summit 2017. This graphic maps out the interest in specific security tools on one axis, versus the level of investment on the other. Tools that manage cloud security, data loss prevention (DLP), mobile security, data access governance (DAG), vulnerability management, incident response, threat intelligence, application security, network security and endpoint security demonstrated high levels of end-user interest and planned investment in the survey results.

These tools are typically within the domain of the IT department. Yet, it is important for supply chain to partner with corporate IT to understand which of these tools are being leveraged across the company and how they can be applied to the supply chain

Figure 3. Summary of Threats

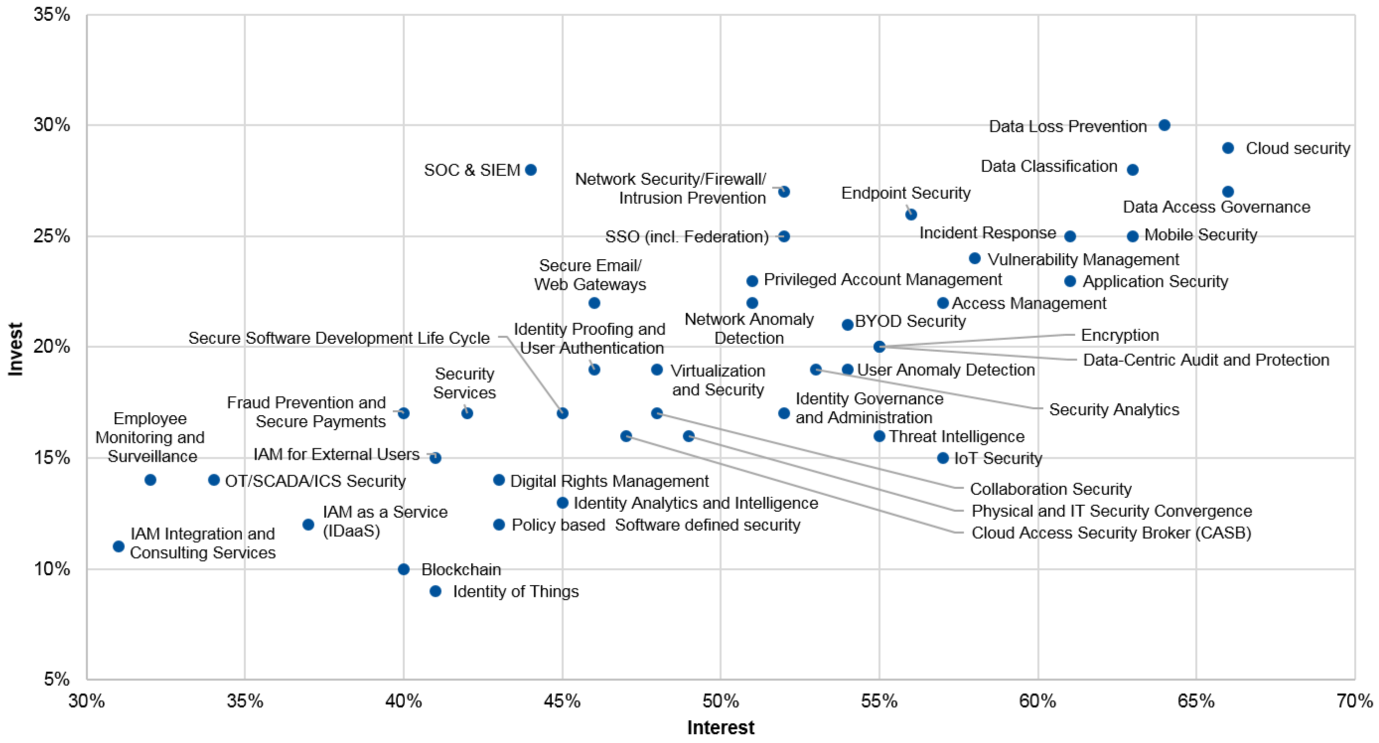


Manipulation of information
Abuse of authorizations
Unauthorized installation of software
Denial of Service Attacks
Malware Hoaxes
Data breach Remote execution
Unauthorized use of devices and systems
Identity theft
Viruses
Phishing
Unauthorized use of software
Abuse of personal data
Exploitation of software bugs
Manipulation of software

Source: Extract From ENISA "Threat Mind Map"

Source: Adapted from ENISA

Figure 4. Level of Investment and Interest in Security Tools



© 2017 Gartner, Inc.

SOC = security operations center; SIEM = security information and event management; SCADA = supervisory control and data acquisition; ICS = industrial control system; SSO = single sign-on; BYOD = bring your own device.

Source: Gartner (October 2017)

operations-related technology, like IoT capabilities, operational technology and physical technology. It is also important to understand what infrastructures are connected via supplier portals to ensure there is a plan for preventing impact on your own data from suppliers who are attacked.

The resulting environment is fragmented and complex, with myriad threats, many tools and an incredibly robust risk profile. End to end across the entire SC, it includes the partners upstream and downstream such as suppliers, contract manufacturers, service providers and distributors; the processes that build and deliver the products; and the information and operational technology that is used to manage the modern supply chain.

Digital Security – A New Way of Looking at the Problem

The term cybersecurity no longer captures the extent of current threat environment, particularly in relation to the supply chain. Thus, Gartner's supply chain research organization is transitioning to the term "digital security".

The term "digital" more adequately represents the idea of the physical worlds and the virtual worlds coming together to form new business models. And when we think about security for the supply chain, we need to be thinking again about a blurring of the lines between the physical (products, manufacturing and logistics assets, etc.) and the virtual (the data, algorithms and applications that are used).

When we look at all of the potential activity (see Figure 5), it essentially boils down to protecting three categories of supply chain information components: data and IT infrastructure, product, and operations components.

Data and IT refers to IT in the traditional sense: the data, applications, servers, networks and even end-user devices that we use in our supply chain operations. Customer data, supplier data, bills of materials (BOMs), transportation management systems (TMSs), planning systems, and so on.

In regard to the product category, many more of our products are “smart” – containing embedded code, logic bearing components, etc. This is business as usual in high tech, consumer electronics and industrial manufacturing; but, increasingly we are seeing this trend in medical devices, healthcare products, and even some sectors of consumer products (like the smart toothbrush that gives you real-time analytics on your brushing activity).

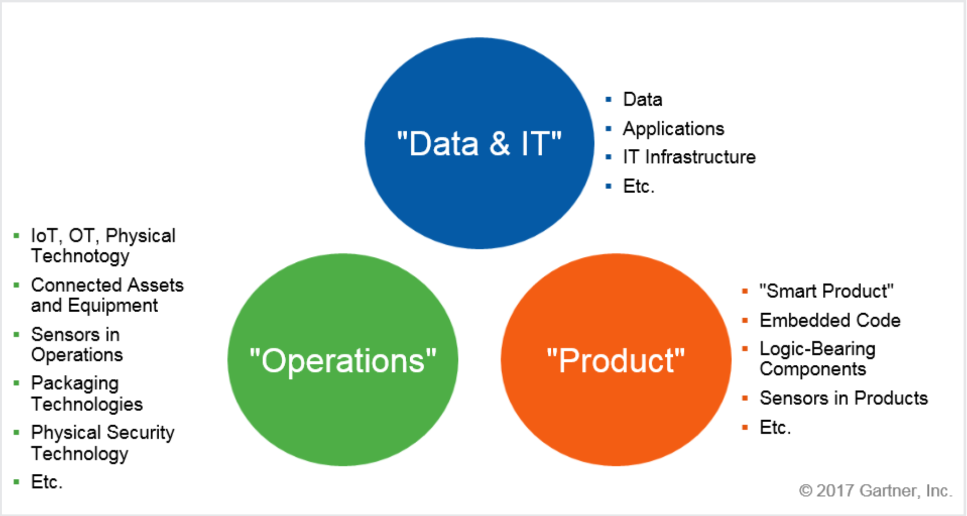
The last category is technology for operations – or as one interviewee called it, “the connected stuff” – IoT, OT and physical technology. For supply chain, IoT includes the connected assets, machines and equipment we use, especially in manufacturing and logistics, and increasingly in demand sensing. It is helpful to think of OT as the hardware and software that monitors and controls how physical devices perform, and physical technology as things like networked locks, and also the smart labels and packaging that enables product integrity and condition monitoring.

All of these components are susceptible to security breaches, so the question becomes how we secure them. First, we must understand the current challenges.

Recommendations:

- Transcend traditional definitions of IT security, and recognize that when it comes to the supply chain, digital security includes both the physical – products, manufacturing and logistics assets, etc. – and the virtual – the data, algorithms, and applications that are used
- Use the digital security for supply chain framework, illustrated in Figure 5, internally to cut through the complexity and fragmentation, and as a guide for the many types of information categories that need to have protection in place.
- Share the framework with your partners such as

Figure 5. Digital Security for the Supply Chain Includes Three Categories of Information Components



Source: Gartner (October 2017)

such as suppliers, contract manufacturers, service providers and distributors to give all parties a common vocabulary and playbook that will, in turn, help advance the cause of digital security protection across your greater supply network.

Address the Major Digital Security Challenges

Digital security challenges encompass governance, talent, pace of threat expansion, time constraints and change management.

Pre-eminent Challenge: Governance

The first challenge uncovered when addressing digital security for the supply chain is governance. In many companies, a cross-section of teams look after product security – SC, R&D, engineering and product management. Therefore, companies need to have good coordination to ensure that proper security is in place for the company's products.

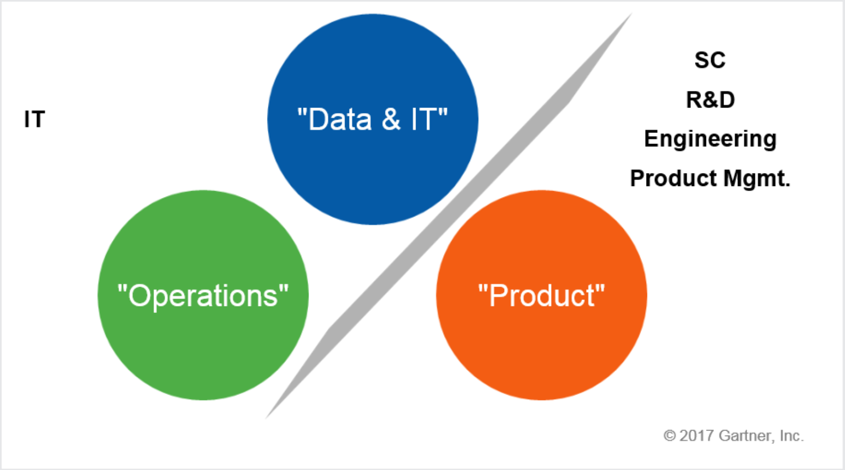
As Figure 6 demonstrates, in many cases, the IT group is responsible for the security of both IT and operations, but not the product. In some companies, there are separate groups for OT/IoT/physical technology security; but for now we will assume it is all in the hands of the IT department. So there needs to be good coordination between IT and supply chain. This coordination begins with asking:

- What are the threats to the supply chain?
- What are the most critical areas of the supply chain to secure?
- What tools are being leveraged in some areas in the organization that can possibly be leveraged for the Supply Chain?

In many companies, there is also an information security group, and that group may or may not roll up into the actual IT group. For the purposes of this analysis, we will include the information security group as part of the IT organization.

This is a perfect example of IT and SC needing to work closely together – we see this time and again as we look across many of the initiatives that are underway in companies across the globe. Even the risk to supply chain of having the corporate internet knocked out is growing by the day, as more and more core applications move to the cloud. The immediate action item to prevent this is ultimately in the hands of corporate IT, but supply chain groups need to be aware of this risk and have proper disaster recovery plans in place, if they get taken offline for hours, a day, a week or longer.

Figure 6. Security Responsibilities Delineated



Source: Gartner (October 2017)

There is evidence that we are making progress. At some companies, especially in the high-tech industry, this governance is actually in place already. Supply chain has historically proven adept at governance issues, and we are seeing this play out in digital security. Companies are telling us that this topic is getting board-level visibility, so the companies who are further along in this effort have built cross-functional security SWAT teams – including not only IT and SC and R&D/engineering, but also legal, compliance, marketing, PR, sales and HR – reporting back to the board on a regular basis.

For these teams, governance can include digital risk assessments and oversight of work to mitigate identified risks. This is the strategic/proactive role; and then there is also a tactical response oversight role. The same cross-functional management body can be used to the review and guidance forum for emergency risk management teams when breaches occur and need real-time attention.

In fact, Gartner has seen evidence that companies are starting to address the digital security threat, in part, due to this focus on governance. In our 2015 Digital Business study there was a 17% gap between the importance of mitigating cyber risk and the respondents' readiness or ability to mitigate it. In our recent 2017 study, respondents have narrowed that gap to 12%.

Additional Challenges

There is still a gap between importance and readiness, because there are both people challenges and technical constraints once we get past the governance hurdles. To hear some of the interviewees describe it:

The challenges break down as follows:

- **Lack of technical talent:** Much has been written about supply chain's overall need for talent acquisition and development, and the need is even more pronounced in this critical area.
- **Pace of threat expansion:** As demonstrated by ransomware attacks in this past year alone, the number of threats and the ability of these attacks to spread quickly is proving difficult to keep up with.
- **Time constraints:** The typical supply chain organization is perpetually challenged with trying to balance a portfolio of improvement and/or innovation initiatives.
- **Change management:** Supply chain must understand that security is not someone else's problem, that only a collaborative effort between IT and SC can properly address the problem. Companies told us that the change management issue was an even bigger problem with their suppliers, as they find those suppliers lagging in the proper know-how to combat this threat. There is also a lack of importance given to product security in the design phase, and change management will be required there as well.

Recommendations:

- Establish robust governance mechanics and collaboration capabilities between IT and supply chain.

- Consider a corporatewide governing body that goes beyond SC and IT and offers board-level accounting on digital security threats across the business. Leading companies that we spoke to are having these meetings now, and are including public relations, legal, compliance, finance, HR, product, sales and marketing, in addition to operations and IT. This team should be charged with digital risk assessments and oversight of work to mitigate identified risks, as well as for tactical response oversight.

- Be creative in sourcing the talent you will need to fight this battle. In some of the companies we spoke to, there were former military information security associates who had been brought into the SC organization specifically to help the company address these issues.

- Be vigilant in monitoring threats. By tightly aligning with IT, SC can help understand, anticipate and protect against the latest threats – both proactively and reactively. Reporting should go back to the risk committee.

- Evaluate the threat to digital security within your overall umbrella of supply chain risk management from a time and resource management perspective, and prioritize accordingly. Some companies we interviewed have now placed digital security at a higher level of urgency than their disaster contingency planning.

- Drive change management by starting with a stakeholder analysis, determining who must change and what must change. Companies are discovering that they should start with their Tier-1 suppliers and get those suppliers to understand the magnitude of the digital security threat. Also, concentrate on the change management required to get product security built into in the design phase.

Take the Lead on Product Security

A digital security view places a spotlight on the end goal of our supply chains – the product. Too often, with the focus on traditional information security and the emerging work around IoT and OT, the product itself gets lost. For aerospace and defense, high tech and industrial manufacturing, security has already been an area of focus. But now, with smart products proliferating across all industries, products of all shapes and sizes now include embedded code and logic-bearing components, which are all susceptible to malfeasance.

In 2016, Gartner issued a prediction:

By 2019, 65% of smart products will be proven "hackable," compelling chief supply chain officers (CSCOs) to collaborate more closely with CIOs, CTOs and CISOs, as well as all engineering functions, on digital security.

Additionally in the Gartner 2015 Digital Business survey, More than 70% of survey participants expect that supply chain challenges to realize digital products with embedded software will be moderately or extremely difficult to overcome. In our discussion with IT security leaders, it is clear that product security is not something they hold as a priority; instead, it falls on the supply chain and other teams (R&D, product management and marketing, for example) to put this in place. And throughout our interviews, it was clear that supply chain leaders are in fact focused on the security of their products, given how high the stakes are in brand, product safety, product quality and compliance.

One toy manufacturer has already seen the damage that can be done. Just prior to the 2015 holiday shopping season, a toy manufacturer discovered that a new interactive doll was vulnerable to hacking through Wi-Fi connections to the internet. Consequently, Fortune Magazine ranked the toy at the top of its annual Worst Toys of the Year list.[1]

Organizations see value in addressing this at both the source and NPD/NPI functional areas, and this is their priority right now. In our discussions with supply chain organizations, leaders from both these functional areas are stepping forward to take the lead in ensuring product security.

Recommendations:

- Address the product security threat in the NDP/NPI process. Think holistically about the product as something that can be hacked. Go beyond thinking about just cost, quality and availability.

- Ensure the extended supply chain is capable of meeting the efficiency, cost, service, quality and security requirements necessary to support the new product launch as well as postlaunch product life cycle management activities associated with developing and selling digital products.

- Invest in supplier risk assessment, SC compliance and process design as top priorities to deliver successful digital products and combat the digital security threat. Segment your suppliers and assess your vulnerability to risk based on the extent of logic-bearing componentry in the bill of materials.

Protect Supply Chain Digital Security With a Superset of Approaches

A Shortlist of Tools

With limited time and resources, it is important to cut through the complexity of all the tools and techniques that are available to wage the digital security battle.

In discussions with supply chain leaders in the security space, we learned that there are a variety of tools being deployed to mitigate risks across the three information components we have been discussing. These tools are not listed in any particular order, and are presented in Table 1.

The list ranges from some very established capabilities on the IT side to some newer approaches such as end-to-end SC visibility.

Table 1. Tools Being Deployed for Supply Chain Digital Security

Digital Security Component	Tools
Data and IT	■ Cloud Security ■ Apps and Data Security ■ Endpoint and Mobile Security ■ Network and Gateway Security ■ Security Monitoring and Operations ■ Threat and Vulnerability Management
Product	■ Configure and Test/Code, Verification ■ Vendor Risk Management ■ Asset and Inventory Management ■ Risk Management and Business Continuity ■ Product Life Cycle Management (PLM) and Product Portfolio Management (PPM) ■ Working With Standards Bodies
Operations	■ Dedicated Track and Trace ■ End-to-End SC Visibility ■ Asset and Inventory Management ■ Mobile Connectivity ■ Risk Management and Business Continuity ■ Working With Standards Bodies

Source: Gartner (October 2017)

Several companies discussed an interest in using blockchain approaches to address both product and operations security. None of the companies had actually deployed anything, but all had an awareness of the distributed flow of information and decentralize transactions that blockchain can create, and its potential application in securing product and operations.

Note again how important it is for SC and IT to collaborate, since some of the approaches that are being used on the operations side are also being looked at on the product side. This way, supply chain can understand what approaches are working best, and what to deploy on the product side.

Recommendations:

- Familiarize yourself with the tools and techniques IT is using to safeguard the data, apps and information infrastructure that makes up your supply chain.

- Investigate, collectively with IT, and put in place the tools that reflect your risk profile and tolerance at the product and operations layers.

- Use the list in Table 1 as a starting point for the tools and techniques you can use to safeguard the digital security of your supply chain.

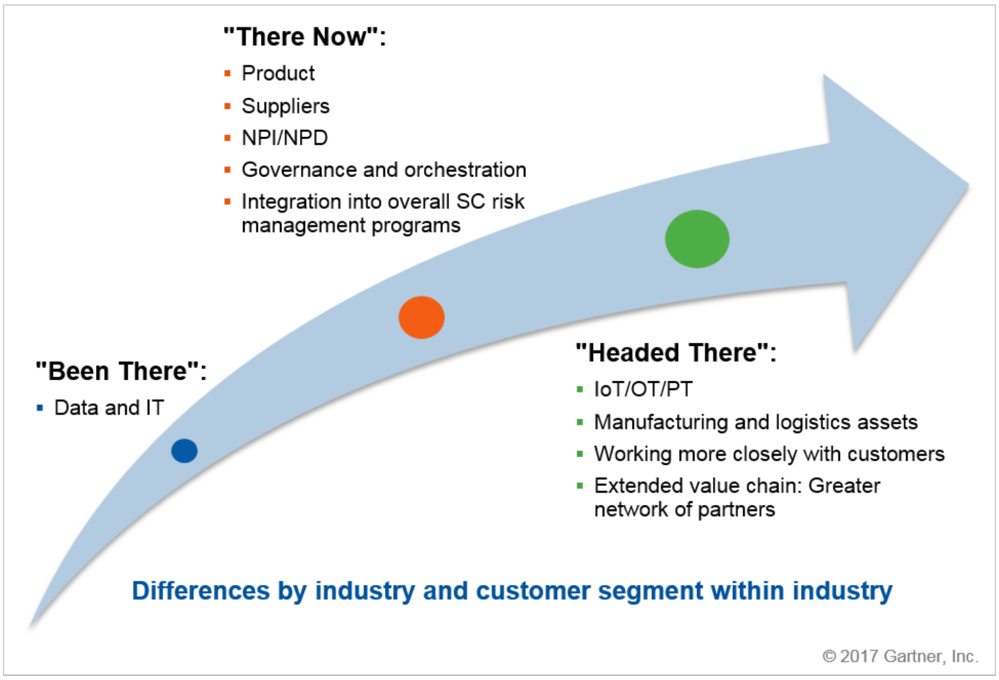
Develop a Timeline for Supply Chain Digital Security

We have shown that the digital security approach – thinking holistically about data and IT, product, and operations – provides a common model for better governance and collaboration between IT and supply chain and their business partners. We have also shown how it can help narrow the list of tools that companies can use in their efforts to protect the information integrity of the supply chain.

The third major benefit of looking at supply chain security through a digital security lens is that it helps provide companies with a sense of timing. When we spoke with organizations about this topic, it was clear that their focus is now beyond only IT. Many organizations feel as if they already have data, IT infrastructure and application security in place – whether it relates to HR systems, finance systems, or marketing and sales. Supply chain is considered part of the overall corporate information portfolio that IT security needs to protect; and that protection is, and has been, happening already. This does not detract from its importance in any way, it is simply where IT security teams have been focused in their quest to protect all the information assets of the company, supply chain included.

Clearly, if an organization does not already have IT security in place to protect the data and IT infrastructure and applications for the supply chain, this needs to be addressed first and foremost. The question then becomes, “What should companies be doing once the IT security is in place?” Figure 7 shows one possible path. Note, this path is

Figure 7. Timeline for Digital Security for the Supply Chain


"There Now":
Product
Suppliers
NPI/NPD
Governance and orchestration
Integration into overall SC risk management programs
"Been There":
Data and IT
"Headed There":
IoT/OT/PT
Manufacturing and logistics assets
Working more closely with customers
Extended value chain: Greater network of partners
Differences by industry and customer segment within industry
© 2017 Gartner, Inc.

Source: Gartner (October 2017)

not exact, and it is not universal. And there are differences in where organizations are on this path, based on the industry or even the customer segment they are looking at. This path takes the same three components from Figure 5 and arranges them in a timeline of sorts – securing IT first, then product next, and finally the IoT/OT/physical technology components of the supply chain as a "future state."

There are definitely certain supply chain digital security components that companies are working on right now. These efforts include much of what we have discussed in this research:

- Organizations now are showing a focus on their product security, and enabling this through the source and NPI/NPD functions.

- Companies are also now thinking about the governance and collaboration between SC and IT, engineering, R&D, and product management, and how that impacts their product security efforts.

- Companies are currently evaluating how digital security risks fit into their overall supply chain risk management portfolio.

After these capabilities are in place, companies can advance in their efforts. Security professionals in the supply chain who are most advanced along this path talk consistently about what efforts are on the horizon. Most organizations are not at this stage yet, and some will get there more quickly than others.

But in the future, companies will need to be thinking about all the connections in their supply chain, and planning for security for the IoT/OT/physical technology that their supply chain(s) rely on. They will need to protect the connected assets in their supply chain, particularly their manufacturing and logistics assets. There have already been examples of manufacturing and logistics capabilities hacked, and companies are starting to pay attention. There will be greater focus on the physical technology that ensures product integrity such as serialization and track and trace. We are seeing these capabilities in sectors such as pharmaceuticals and food and beverage, but they will become more widespread across all industries.

As companies advance along this timeline, they will need to focus intently on their customers. Organizations will need to go beyond concerns about protecting customer data, which of course is vitally important, to understand all of their customers' digital security requirements and how they can work closely with their customers to ensure their smart product arrives unhacked and remains unhackable over the course of its life cycle. So in this timeline we are seeing companies focus upstream first, then downstream.

Finally, organizations will need to address the extended value chain – the network of partners that all supply chain organizations work with; first-, second- and third-tier suppliers; manufacturing partners; and distribution partners. There are similarities here with the thought process involved with Gartner's supply chain capabilities maturity models, where higher levels (Stage 4 and Stage 5) of maturity are associated with scalable, value-added orchestration across a broad spectrum of both internal and external partners. The same orchestration is needed to combat digital security threats, with the added complexity that those managing end-to-end security for the supply chain need to include the supplier risk assessment, screening, contractual coverage and compliance monitoring.

Recommendations:

- Apply this timeline as a guide for your supply chain digital security efforts.

- Work with IT to get an inventory of the systems and data and ensure that IT and data security for your supply chain systems and processes are already in place.

- Focus on product security now, through supplier management and the NPI/NPD process.
- Ensure that there is proper governance and collaboration in place now between supply chain and IT. If necessary, create a cross-organizational committee focused on security that includes SC digital security and has board-level visibility.
- Assess and understand where digital security fits into your overall SC risk management portfolio and, if needed, realign resources accordingly. With IT and product security in place, turn to the greater network your SC participates in:
    - Work closely with your customers to understand their digital security requirements and make sure you are meeting their needs.
    - Turn your attention to your greater network of upstream and downstream partners and understand and assess their own digital security efforts once first-tier suppliers and customers have been addressed.
- Map out your most critical manufacturing and logistics assets that are accessible via the IoT and work with IT and/or OT resources to ensure their security.
- Drive security for the physical technology of your SC by putting the necessary safeguards in place to protect against theft and break-in, and also have the traceability and serialization capabilities needed to ensure product integrity (separate and distinct from product security, which is about embedded code).

Evidence

This research is informed by a qualitative survey on the IT side (in 2016) and phone interviews on the supply chain side (in 2017); also via follow up discussions at events and through some inquiry. Overall, more than two dozen points of view have been captured for this research from companies in high tech, industrial manufacturing and life sciences – both pharma and med device.

Additional surveys include:

- Gartner Digital Business and the Impact on the Supply Chain (2015 and 2017)
- Gartner 2017 Security and Risk Investment Survey
- Gartner CSCO survey, 2016: A Gartner survey conducted to find out and understand the business priorities of supply chain leaders, what drives their supply chain strategies, improvement goals, effective practices, and organizational design. The research was conducted using a mixed methodology of both online and computer-assisted telephone interviewing (CATI) during November 2015 through December 2015 among 261 respondents in North America, Western Europe and Asia/Pacific. Eighty-nine percent of respondents came from organizations with $1 billion or more in annual revenue. Respondents came from the following industries: consumer packaged goods (CPG; 11%), retail (14%), chemical (8%), industrial (22%), high tech (20%), life sciences (17%) and healthcare (8%). The survey was developed collaboratively by a team of Gartner analysts who follow supply chain and was reviewed, tested and administered by Gartner's Research Data Analytics team.

[1] "This is the Worst Toy of the Year by Far." Fortune.

Source: Gartner Research, G00337152, Mark Atwood, Virginia Howard, Foundational: Refreshed 4 February 2019, Published 6 October 2017

THE CASE AGAINST HOLOGRAMS

How a once fabled technology is now widely avoided (and disparaged) as a product security solution

Introduction

Holograms were invented by Hungarian physicist Dennis Gabor in the 1940s and then refined through his further research in the following decade, an invention for which he won the Nobel Prize in Physics. Holograms remained largely confined within the scientific domain until the 1980s when a process was developed for printing them onto metallic film. This in turn led to their application as a security product, initially on banknotes and credit cards, and then on consumer products.

The early effort to use holograms as an anti-counterfeiting tool began with Johnny Walker Scotch whisky and the blockbuster drug Zantac. Within a few years, holograms would start to play an increasingly important role, not only as a distinguishing feature on a package but also for branding purposes. And with that development came the idea that holograms can help to identify genuine products from the increasingly brazen attacks by counterfeiters. The logic was simple – consumers will be reassured when seeing a hologram, which would either be missing or of poor discernible quality on fake replicas.

That argument no longer holds. The increasing trend among brand owners, and even governments, is to walk away from holograms as a security product. The largest state in India, Uttar Pradesh, dropped holograms from their excise tax stamps – a move that is now being considered by other Indian states as well [1]. Similarly, several large pharmaceutical and CPG companies have either dropped holograms from their packages or are currently preparing to migrate to other competing solutions.

So, what happened to this once celebrated technology? At one level, the answer is simple – holograms themselves became highly susceptible to counterfeiting and therefore trust in their effectiveness rapidly declined. There are, however, other causes that are more nuanced and relate to brand marketing, consumer behavior and technology trends.

This short white paper will explore the causes behind the decline in the use of, and more importantly, the perception of holograms as an effective security solution.

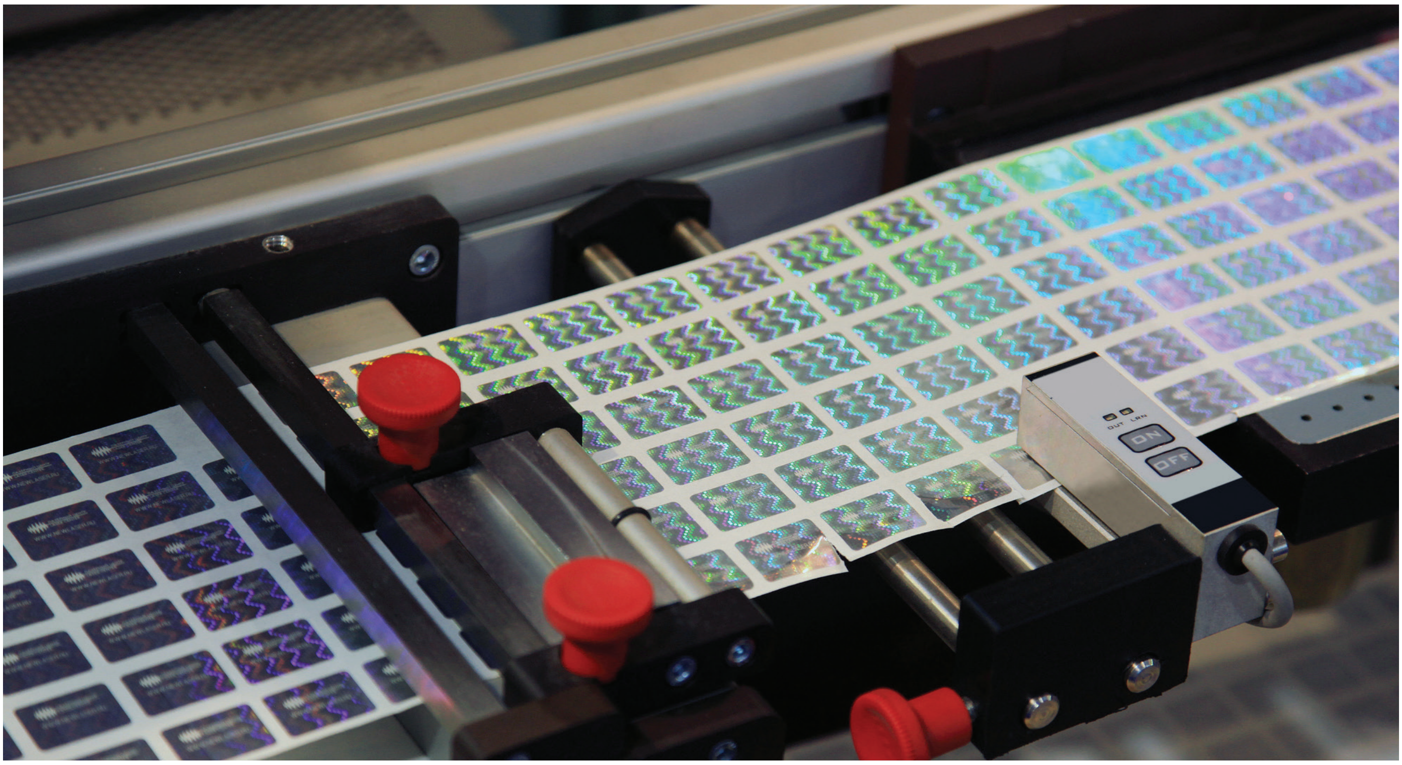
A technology in decline

Holograms are barely considered to be a security feature anymore and many brand owners have opted to retain their use largely for brand imagery or to provide sparkle upon a package. This section will outline five key reasons that have led to this decline and which bode negatively for the future application of this technology as a product security solution.

1 The ease of duplication

About a decade back, whispers began emerging in the brand protection community that holograms and holographic seals aren't truly as immune to copying as was claimed by their suppliers [2]. To tamp down such concerns, the hologram industry – led by their international trade body – unleashed a campaign to claim that such talk was nonsense and that holograms really were the best thing out there to arrest the growing menace of counterfeiting across all product segments [3,4].

Fast-forward to the current environment where we find that the rapid pace of technology development over the intervening ten years has transformed holographic production from what was once the province of sophisticated manufacturing into a commonplace and almost routine industry. That is not to say that the making of holograms is straightforward by any means, only that the cost



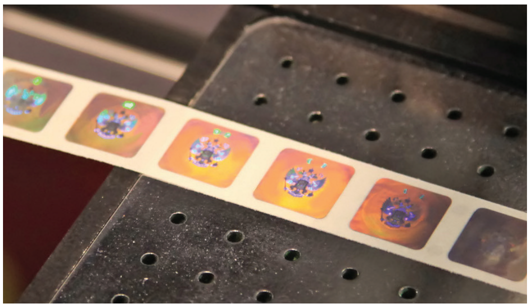
and craft behind the art is now unexceptional. While several large and distinguished suppliers remain, a veritable cottage industry has also arisen as a result, particularly in China and India, which caters to the now widespread global supply of low-cost holographic seals and foils [5].

The emergence of a large and eager supplier base has transformed holograms from a niche to a commodity product and created the conditions for widespread copying of genuine security holograms. Any original hologram can now be easily replicated at high volumes. As a result, many brand owners who have spent substantially to create packages with an embedded security hologram have seen their efforts and investments squandered once a counterfeit variant appears in the marketplace.

To put it simply, there is now widespread belief among brand owners and security specialists that holograms no longer offer the protective benefits that were once hailed to be so supreme.

2 The cost of education

The hologram industry has become defensive of late and continues to push the claim that a well-designed hologram integrated into a product or its package is difficult to exactly replicate [6]. There is no question that this claim is accurate, and in fact replicated holograms are generally of poorer quality – though there are a few curious cases where the fake one can be of better quality than the original. And the even odder situation where fake versions have a hologram, but the genuine products do not [7].



One fact is clear, however. Even if the duplicate hologram may not be anywhere near the quality of an original, it is usually sufficient to fool an ordinary consumer who is unable to notice the difference. To make proper use of the hologram investment, the brand owner must therefore devote significant marketing effort to educate the consumer base. While there are some notable examples of this effort through online education [8,9], it is also unquestionably true that product managers loathe to publicly expose their counterfeiting problem and take the even greater step of alerting consumers on how to differentiate their products from counterfeits.

The cost of education, therefore, does not only relate to the monetary aspect of the marketing investment but also the cost associated with dilution of their brand equity from such public exposure.

3 The problem of psychology

Consider the following conundrum. A banknote is bustling with security features and yet consumers pay no attention to them. In fact, the collection of passive security features – watermark, optically variable ink, hologram, etc. – is largely a wasted effort in terms of consumer engagement to identify counterfeits. The reason according to neuroscientists is simple ... human attention is fleeting. We just can’t be bothered to take the time to scrutinize something as commonplace, yet important as, the banknotes in our wallets [10]. What then would drive us to do the same for the many products we purchase and use daily?

This significant obstacle represents the greatest challenge that brand owners must face when considering use of holograms and other passive technologies such as security seals. To properly verify a product, the human consumer must actively interrogate the package, which most are reluctant to do. And even if that behavior can be instilled, it is

immensely complicated by the two forgoing issues described above: counterfeit holograms can be very similar to genuine ones and there is a marketing lethargy to educate people to distinguish between them.

It is a staple of behavioral science that conscious engagement with a product serves as the most effective means to direct the attentional spotlight, an act that is not inspired by a passive hologram.

4 The changing times

The security hologram industry is immersed in a tidal wave against their business interests due to the simple fact that the current trend is toward active authentication. Like specialty inks and micro-printing, holograms are a passive technology that require mere visual inspection and a qualitative decision on authenticity. This is not fundamentally an authentication process but rather a best guess that the product is original. Furthermore, the passive technologies do not permit any type of consumer engagement, something that is of increasing importance to marketing heads who demand value additions from their investment.

Brand owners are therefore increasingly turning to technologies that provide an actual binary result – yes or no in terms of authenticity – and turning away from the qualitative and nebulous offerings in the passive category. This trend started with mass serialization where a unique number is inserted into a QR code and placed on a package, and which can in turn be verified by a smartphone app. While this solution prevailed for a few years, the security and other concerns with this technology led to the emergence of an entirely new approach to authentication that has been classified as the third-generation (3G) solution set [11].

Holograms are static, non-interactive products that have limited utility in a 21st century digital world where brand owners covet the value-added benefits that come from engagement.

5 An invitation to counterfeit

The application of holograms as a security feature has become a high-risk investment for the various reasons discussed above. In the absence of any other technology layer, the hologram is among the most ineffective security solutions currently available. In fact, a hologram can even serve as an invitation to counterfeit because of an interesting dilemma. And to make matters worse, the hologram is not immune to this problem even if it is layered with another technology such as a serialized QR code.

Whereas consumer apathy makes it difficult to direct the attention needed to scrutinize a hologram, a false sense of security paradoxically emerges due to the branding familiarity we associate upon seeing them. Security specialists worry that even the mere presence of a hologram can produce false reassurance as a result. And given the general inability of consumers to properly identify an original hologram, counterfeiters can take advantage of that weakness in conjunction with our familiarity association to successfully perpetuate their products in the marketplace.

Simply stated, it is better not to place a hologram, or any other layered technology in conjunction with a hologram, on a package at all to remove the problems of false association and false reassurance.

The next generation is here

It is undoubtedly true that holograms still maintain a robust presence on many packages, and this will likely continue for some time due to the branding caché that has been established. It is also true, as evidenced by the foregoing discussion, that many brand owners and governments are dropping further use of the hologram for purely security purposes and that the pace of new adoptions will continue to decline [12,13]. There is now widespread acceptance that holograms represent a low-hanging fruit – if not an actual invitation – to criminal enterprises that easily target hologram-embedded products.

Although there have been attempts to combine holograms with other layered technologies, their utility remains unclear in the face of consumer attitudes that the presence of such a tag is an assurance of authenticity. That is a dangerous allure to the counterfeiter who can take advantage of a natural naiveté in the lay population that is reassured by the mere presence of a hologram despite the inclusion of additional security layers[1].

The clear and compelling security deficits of holograms and other passive technologies has led to the development of an entirely new set of offerings that are characterized almost uniformly by their robust ability to withstand duplication. The recent advent of 3G solutions has ushered in a new era in the fight against counterfeit products. A 3G solution is one that can neither be successfully copied nor emulated. A few technologies can lay claim to these strict requirements. The two leading offerings include NFC tags [14] and fingerprinting technologies [15].

e-Fingerprinting® technology by Systech has drawn special acclaim because it is based on the barcode found on nearly all packaging, making it a non-additive, cost-effective solution [16]. It empowers consumers, complies with the zero tolerance for failure rule and allows unlimited authentications due to its uncompromising robustness.

Synthesis

We've entered a new era in the fight to protect consumers against the dangerous menace of counterfeiting. Holograms served their purpose at one time as a security tool, but no longer. They can however be very beautiful and offer the kind of visual appeal to a package that creates undeniable marketing sparkle. Any effort to extend their use beyond that into the product security realm would represent willful misuse, given what we now know about the futility of holograms, and therefore be an arguable abdication of corporate responsibility toward consumer safety.

Source: Avi Chaudhuri, PhD, Senior Global Partner, Systech International

[1] The introduction of a high-end security seal on a major drug brand in Asia suffered a similar fate, where authentication rates plummeted after the initial rollout due to consumer reassurance merely by the presence of the seal.

About the author

Avi Chaudhuri, PhD
Senior Global Partner, Systech International

Dr. Avi Chaudhuri has many years of experience in brand protection. His work in this field began in 2004 when he himself became the victim of a counterfeit drug. At that point, he began to research all available technologies that could not only defeat this problem, but also empower consumers to verify the genuineness of the drug right at the point of sale.

Dr. Chaudhuri became a strong public advocate of the need to protect consumers by evangelizing on the benefits of effective anti-counterfeiting technologies. He introduced the very concept of mass serialization to the Indian pharmaceutical industry ten years ago and helped to create a national SMS program that allowed consumers to verify their drug purchase.

Dr. Chaudhuri is now responsible for spearheading Systech's expansion in Asia and working with both pharmaceutical and consumer product companies to protect their brands and customers.

References

[1] Liquor tax stamps in India: Lessons NOT learnt by Uttar Pradesh as it follows in Delhi's footsteps. 2018.
https://www.reconnaissance.net/tax-stamp-news/issues/july-2018/

[2] Fake holograms: A 3-D crime wave. 2007.
https://www.wired.com/2007/02/2163064/

[3] How holograms can stop counterfeiting. 2008.
https://www.packagingdigest.com/smart-packaging/how-holograms-can-stop-counterfeiting

[4] New hologram technology adds anti-counterfeiting features. 2009.
https://www.secureidnews.com/news-item/new-hologram-technology-adds-anti-counterfeiting-features/

[5] Alibaba website of hologram suppliers. 2018.
https://www.alibaba.com/showroom/fake-id-hologram.html

[6] The hologram – still going strong! 2017.
https://www.itwsecuritydivision.com/Portals/0/documents/ITW%20White%20Paper%20-%20The%20Hologram%20Still%20Going%20Strong.pdf?ver=2017-09-06-081840-913

[7] Here's how to spot the difference between real and fake designer bags. 2017
https://www.racked.com/2017/1/2/14149614/fake-handbags

[8] Warning: Counterfeits – Illegal imitations of Yonex badminton equipment can be found anywhere! 2019
http://www.yonex.com/products/badminton/warning-counterfeits

[9] Don't be fooled by fakes. 2018.
https://printerpoint.co.in/real-vs-fake/

[10] Money and our minds: can neuroscience stop counterfeiting? 2017
https://www.ft.com/content/a4b295ca-fe07-11e6-96f8-3700c5664d30

[11] The evolution of brand protection. 2018.
https://cdn2.hubspot.net/hubfs/3844090/UniSecure-WP_Evolution-Brand-Protection_10-2018.pdf

[12] Are holograms really helpful against counterfeits? 2017.
https://knowfakes.com/corp/Hologram_Failure.html

[13] Why do credit cards have holograms?
http://creditcorner.net/why-do-credit-cards-have-holograms/

[14] QR codes and anti-counterfeiting: The false sense of consumer security and why NFC is the most appealing alternative (2018).
https://selinko.com/blog/qr-codes-and-anti-counterfeiting/

[15] Arjo Solutions launches Safe app for authentication based on Signoptic technology (2016).
http://www.labelsandlabeling.com/news/new-products/arjo-solutions-launches-safe-app-authentication-based-signoptic-technology

[16] Systech launches UniSecure™: The ultimate anti-counterfeiting tool (2015).
https://www.businesswire.com/news/home/20150928006053/en/Systech-International-Launches-UniSecure™

Blockchain

Making the cryptocurrency foundation really work as a physical product protection solution

Why Blockchain is Important

Building a better “mousetrap” has been the goal in brand protection solutions for decades. Despite the billions being invested in protecting products and securing the supply chain, we are not seeing a material decrease in issues. The gray market is strong, and seemingly getting stronger. If you have a great product, someone is likely counterfeiting it. If you have a well-planned distribution and channel strategy, someone is looking to divert goods from it and impact your revenue flow.

Many in the industry are looking toward blockchain as the latest “mousetrap” to truly solve global brand protection issues. Why? Blockchain has so many characteristics that are required in this battle, including:

- Trusted chain of possession
- Known ownership and title transfer
- Notarization and time stamping of all events
- Notion of smart contracts
- System of warranties

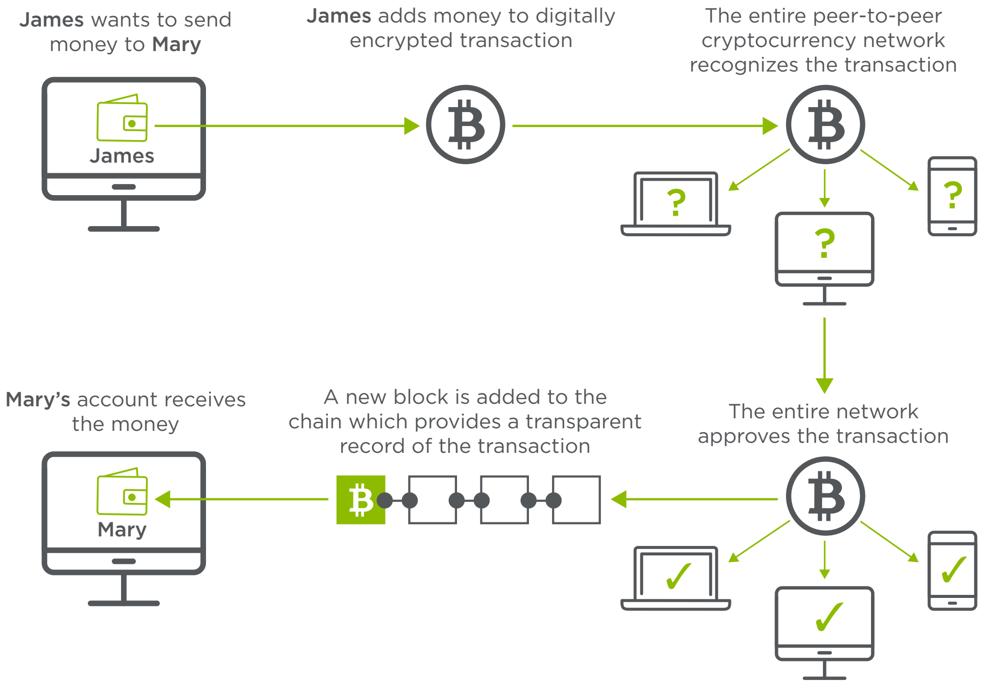
These are essential requirements for a trusted supply chain, enabled by blockchain.

All these capabilities evolved from building the necessary infrastructure to facilitate cryptocurrency, namely Bitcoin. It works because blockchain uses a decentralized ledger (chain) of all transactions (blocks) across a peer-to-peer network. All participants confirm transactions without the need for a centralized certification authority. Everyone sees and agrees to the truth, and this process replicates as transactions occur and new blocks get added to the chain.

Blockchain was architected to be the backbone of cryptocurrency and it is important to differentiate the two concepts. This digitally created, blockchain-based exchange medium leverages advanced encryption techniques to control the creation of monetary units and verify the exchange and ownership of funds. It does this for all parties and transactions within the cryptocurrency network. Meaning, if James wants to transact with Mary, both parties must be members of the currency network with both public and private keys to their personal "wallet".

All cryptocurrency for both James and Mary are tied to the same blockchain. So, when James wants to send money to Mary, James adds money to a digitally encrypted transaction to be sent to Mary. The entire peer-to-peer cryptocurrency network recognizes the transaction, as they see it with all their public keys, the transaction is recognized, recorded in a new block on the chain, everyone agrees that James has transferred money to Mary and Mary's account receives the money.

Figure 1


James wants to send money to **Mary**
James
James adds money to digitally encrypted transaction
The entire peer-to-peer cryptocurrency network recognizes the transaction
?
?
?
The entire network approves the transaction
✓
✓
✓
A new block is added to the chain which provides a transparent record of the transaction
Mary's account receives the money
Mary

Source: Systech

What does cryptocurrency have to do with the brand protection of physical products?

The trusted chain of possession, known ownership and title transfer, plus notarization and time stamping of all events that is required to establish a cryptocurrency is exactly in line with trusted supply chain requirements. When you add the immutability of the encrypted blockchain ledger that contains all the events and transactions, you have a trusted platform that could be adapted for supply chain use.

We can easily see the applicability of blockchain in financial transactions amongst supply chain partners. It can enable the streamlining of payments processing with highly efficient, fast and secure transactions in a closed blockchain network. Plus, blockchain can empower global transactions – tearing down national currency borders and facilitating trade.

But how?

The very things that are necessary for safety and honesty in the supply chain are delivered by blockchain.

- Blockchain provides **consensus**—there is no dispute in the chain regarding transactions because all participants on the chain agree to the same version of the ledger.
- Everyone on the blockchain can see the **chain of ownership** for an asset on the blockchain.
- Records on the blockchain cannot be erased which is critical for a **secure** and safe supply chain.
- Blockchain provides **attestation**—there is no dispute in the chain regarding the ownership or the integrity of the data.

How about physical product and brand protection using blockchain? We need to make a leap here to take a purely digital technology and somehow apply it to the physical world.

There have been some well publicized initiatives in gemstones, food and other physical goods that have blockchain as the underpinnings of “protection”. These involve data entry at various points along the supply chain, with participants getting product transaction updates

> *Combining bulletproof digital identity with authenticated and trusted physical product identity makes the use of blockchain truly a viable resource in the fight brand protection.*

(blocks) into the ledger history (chain) by a variety of methods. There are some special reader devices that identify the unique item, in gemstones for example. Each trade partner would need to be equipped with this specialized device to have the capacity to participate and update the provenance of the item.

More commonly, we see barcodes being used throughout the supply chain as the vehicle to identify items and upload that data to the shared blockchain. There is an inherent gap here, as barcodes on packages, pallets or containers are disconnected, and decidedly non-digital. Additionally, barcodes are easily replicated, so the trust in mass barcode utilization in concert with blockchain limits the real faith we can put in the system.

In food, for example, consumers are increasingly interested in the sustainability and ethical sourcing of their products. Solid records are required to prove the lineage and provenance of sourced ingredients, as well as characteristics like organic. Basic track and trace systems can handle the traditional supply chain movement recordkeeping here. In this case, blockchain is being implemented as a solution because it can handle the track and trace data as well as surrounding metadata of the item, such as region, farm, processing dates and locations, etc.

Making the transition to the real world

For blockchain to work credibly to create safety and brand protection in the supply chain, we need not just assurance that the item is authentic, but a seamless and direct digital connectivity path for that product's data. With its strong encryption, immutability and peer-to-peer visibility, blockchain provides a strong system to create and manage digital identity. Combining bulletproof digital identity with authenticated and trusted physical product identity makes the use of blockchain truly a viable resource in the fight brand protection.

In a barcode-enabled, physical product blockchain solution, we need the capacity to not just read the barcode, but authenticate it as legitimate, and connect it digitally. Creating this closed loop of trust is necessary because these are not digital entities we are talking about here.

There are several methods being looked at today to add a packaging element that tightens the link between the digital blockchain and the physical item. Serialized barcodes are being added to complement static UPC codes. Holograms, security inks, fluorescent patterns, taggants and other additive methods are being used to create a trusted link between the physical and the digital. While all these technologies and approaches reduce the risk of counterfeits connecting to the blockchain, they can still be replicated by sophisticated counterfeiters. Furthermore, these solutions require physically adding a stamp or sticker to the packaging, taking up valuable real estate on product packaging and adding significant cost and complexity to the manufacturing process.

The barcodes on the packages themselves have the untapped potential to be the critical link to connect the product to the digital world – closing the loop for blockchain. In the printing process, environmental conditions such as line speed, humidity, ink level, substrate variances and others create micro-differentiations in the printed barcode. Though millions of the same UPC code are printed and read without issue, they are inherently unique. This can be leveraged to create a unique identifier for each individual product.

Systech makes blockchain-enabled brand protection real with UniSecure.

UniSecure transforms the existing barcode on packaging into a cutting-edge brand protection and diversion detection/mitigation solution. This is typically achieved with a standard point-of-sale UPC barcode but could be one of several different flavors of barcodes such as 2D Data Matrix and QR Codes. Though there may be millions of the exact same barcode out there, UniSecure's patented technology is able to leverage the micro-variances in printing to derive a unique digital signature, or e-Fingerprint®, for each and every package.

This unique identity allows an ostensibly static barcode to be brought to life and linked to critical production and supply chain metadata. Again, connecting a physical product to the digital world, closing the gap for blockchain.

UniSecure's methodology and delivery of a unique e-Fingerprint is bank-safe secure and cannot be reverse engineered or duplicated in any manner. Systech retained the Salt Hill Statistical Consulting Co. to provide independent, expert statistical analysis to design and conduct a test that determines the probability of a counterfeit passing as a genuine e-Fingerprinted item using a barcode.

> *If the solution is using simple bin and case barcodes, then the system is open to fraud by replicated barcodes entering and/or exiting the supply chain. Downstream scans will never detect fraud, or diversion of legitimate product out of the supply chain because a fake barcode reads just like the original.*

The results:

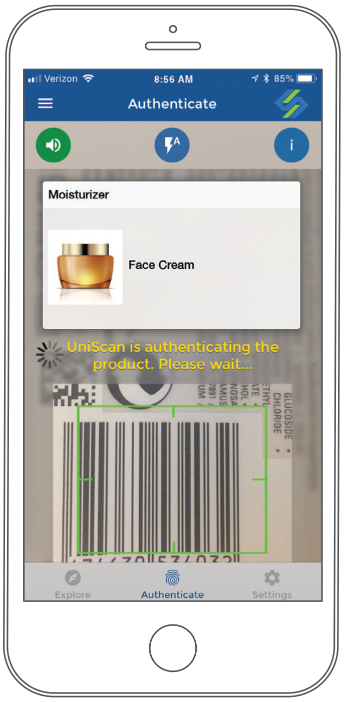
No fake products would be authenticated as legitimate in the more than

21 million samples

Scoring indicated that chance of a fake product authenticating as legitimate was less than

1 in 55 quadrillion

In addition to these statistical realities, there is a practical reality. The UniSecure Cloud that stores all legitimate e-Fingerprints boasts enterprise-class data security and protection. In addition to the fact that a counterfeiter could never derive an e-Fingerprint, that fake data could never get into the UniSecure Cloud to be subsequently authenticated in the field.



Moisturizer

Face Cream

UniScan is authenticating the product. Please wait...

Authentication is achieved with a simple smartphone application. It captures an image of the barcode to be matched in the cloud with its derived e-Fingerprint. Trusted authentication of the item is that simple – all based on the original barcode.

Imagine establishing this unique personality for each and every item coming off a packaging line. As mentioned, you could immediately authenticate that package in the marketplace. Next, metadata about that product could be associated with its unique identifier. This allows the user to discover rich detail about that product which is not physically able to fit on the package's printed label. Finally, the user could communicate back to the brand with information about their experience and share individual comments and reviews. Uniqueness enables a strong anti-counterfeiting solution as well as a data-driven enriched customer experience.

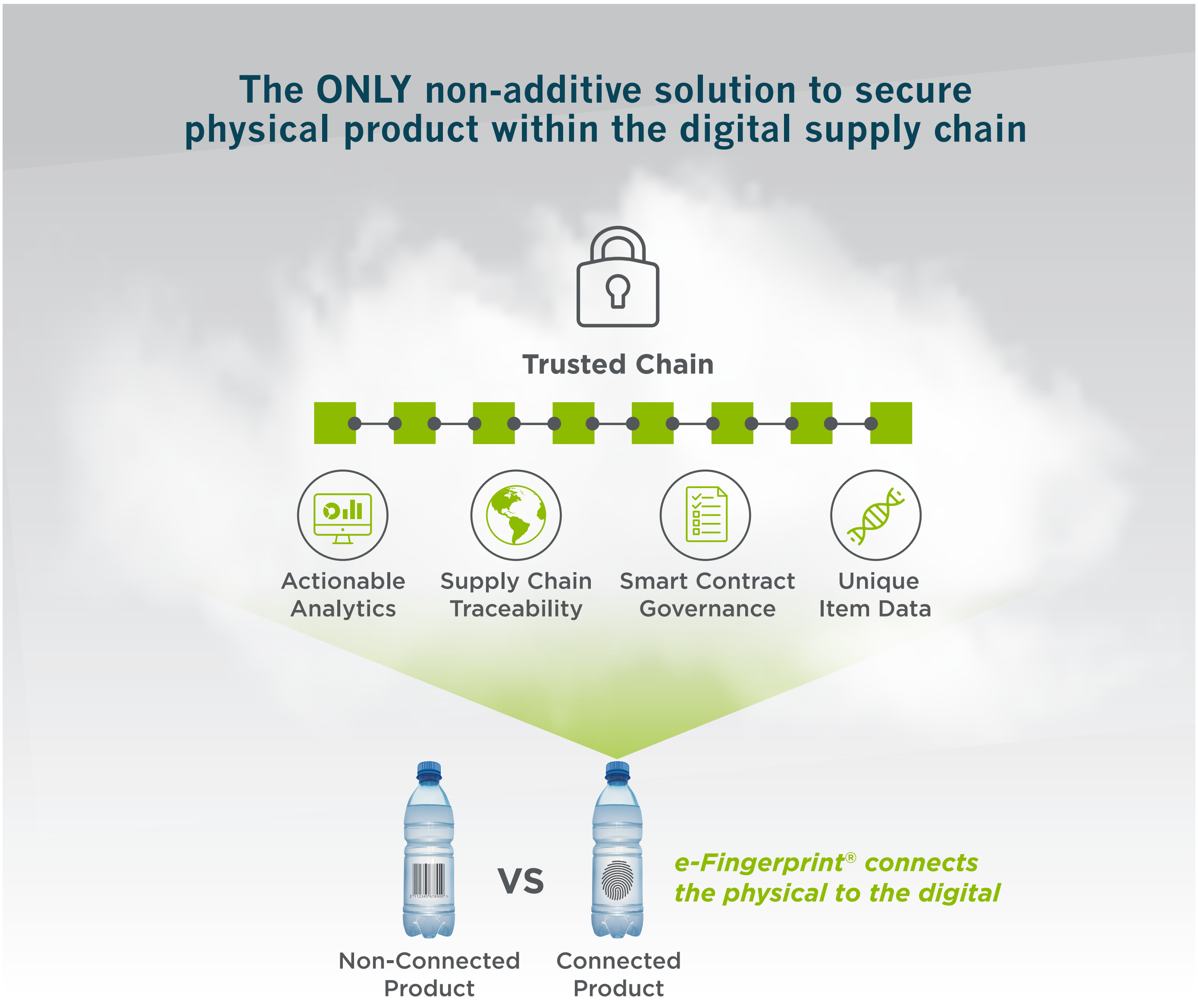
Now combine this with blockchain.

If your supply chain challenge demands comprehensive visibility and trust, consider this:

Connecting the physical product with the digital e-Fingerprint, ensuring authenticity when an event is recorded and managing all the transactions by a blockchain network delivers the closed loop required for absolute security.

This blockchain would likely be private, with known, subscribed entities. When an entity joins the permissioned blockchain network they are granted a private key – that they control – and it represents them on the network for posting and unlocking transactions. This is another barrier for gray market infiltration or diversion, as all the players and assets are known in the blockchain. However, Systech's unique e-Fingerprint is encrypted and "blockchain-ready" so it could be stored in a public blockchain without the risk of divulging competitive intelligence to potential data miners.

Basic barcodes combined with blockchain are not secure. Barcodes that are e-Fingerprinted, authenticated and then connected to a blockchain are not just secure, but trusted and visible.


The ONLY non-additive solution to secure physical product within the digital supply chain
Trusted Chain
Actionable Analytics
Supply Chain Traceability
Smart Contract Governance
Unique Item Data
VS
Non-Connected Product
Connected Product
e-Fingerprint® connects the physical to the digital

Source: Systech

Conclusion

The market is advancing with pure digital non-cryptocurrency uses of blockchain. The dynamics and requirements of the supply chain make blockchain something that leaders must investigate. Closing the loop of physical world to digital world is a critical issue when evaluating blockchain for supply chain use. Systech's ability to connect the once non-connected to ensure authenticity is a critical step to achieving ultimate brand safety and protection.

About US

Systech is revolutionizing brand protection. For over 30 years, global brands have relied on us to combat counterfeiters, prevent product diversion and meet regulatory compliance. Innovation is deeply engrained in our DNA – from our start-up roots in advanced machine vision to pioneering pharmaceutical serialization and transforming traceability and non-additive authentication. Our software solutions ensure products are authentic, safe and connected across the supply chain – from manufacturing to the consumer's hands.

US Headquarters: +1 800 847 7123
UK Office: +44 1482 225118
EU Office: +32 2 467 03 30
India Office: +91 22 4541 1400
China Office: +86 21 51798418

SystechOne.com/UniSecure
Sales@SystechOne.com

SYSTECH®
ONLY ONE

Systech: Combating Supply Chain Threats with Digital Brand Protection is published by Systech. Editorial content supplied by Systech is independent of Gartner analysis. All Gartner research is used with Gartner's permission, and was originally published as part of Gartner's syndicated research service available to all entitled Gartner clients. © 2019 Gartner, Inc. and/or its affiliates. All rights reserved. The use of Gartner research in this publication does not indicate Gartner's endorsement of Systech's products and/or strategies. Reproduction or distribution of this publication in any form without Gartner's prior written permission is forbidden. The information contained herein has been obtained from sources believed to be reliable. Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. The opinions expressed herein are subject to change without notice. Although Gartner research may include a discussion of related legal issues, Gartner does not provide legal advice or services and its research should not be construed or used as such. Gartner is a public company, and its shareholders may include firms and funds that have financial interests in entities covered in Gartner research. Gartner's Board of Directors may include senior managers of these firms or funds. Gartner research is produced independently by its research organization without input or influence from these firms, funds or their managers. For further information on the independence and integrity of Gartner research, see "Guiding Principles on Independence and Objectivity" on its website.