INFOSEC GLOBAL

Cryptography Lifecycle Management

Threat Management | Agility Platform | Quantum Ready

A new Market is Emerging

Today, data and communications are hyper-connected and constantly in transit, moving in and out of trusted and un-trusted hardware, software, IoT devices and systems. Once deployed, connected devices can't change their cryptography or a digital identity, which means a single vulnerability in a critical layer, will stay forever. The current static security model will lead to a massive and devastating risk towards public safety, privacy, financial loss, health of individuals and more. Cryptographic Lifecycle Management is a new and disruptive market category that has emerged and transforms the cryptography market by securing current threats and dynamically preparing for future ones. Engaging with customers, partners and other industry stakeholders to raise awareness, drive adoption, and create a digital ecosystem to define and grow this market is the key to leading it. Cryptography is like our digital immune system, protecting and securing data, money, the health and safety of people and reputation. During the past few years, the explosive proliferation of digital connectivity—from smart phones to the widespread adoption of connected consumer products comprising the Internet of Things—has strained the most commonly used methods of encryption and authentication. For decades, cryptography has been launched piecemeal and without the agility to make necessary changes and updates. Although strong cryptography is as critical to protecting entire digital networks as it is to protecting the organizations that deploy it, there are no enforceable and accepted standards for its application and management.

Innovation in Cryptographic Lifecycle Management is a new market category that secures data and communications for all critical systems and IoT devices. Cryptographic Lifecycle Management automates threat management, enables crypto agility to make necessary changes and prepares for future threats, like quantum computing. The ability to manage the entire cryptographic lifecycle, and manage it as a service brings together a market that has been static and fragmented for years.

INFOSEC GLOBAL

Why do we need Cryptographic Lifecycle Management?

To date, cryptography has lacked the agility to make necessary changes once deployed. It has become so deeply entrenched across all the digital systems we access daily that it is almost impossible to release updates, patch vulnerabilities and conduct Cryptographic Lifecycle Management. The damage, severity and frequency of attacks are also increasing. Recently the fitness-wear giant Under Armour had a data breach that affected an estimated 150 million users of their food and nutrition application, MyFitnessPal. Shares of Under Armour fell as much as 4.6%, according to fortune.com. The breach was similar to other highly publicized hacks at LinkedIn, where more than 100 million users were affected, and Yahoo, where 1 billion accounts were compromised. In all these incidents, hackers stole customer information that included usernames, email addresses and "hashed passwords." The impact of weak crypto has cost companies like Equifax, Yahoo and Under Armour to lose millions in both equity and market cap.

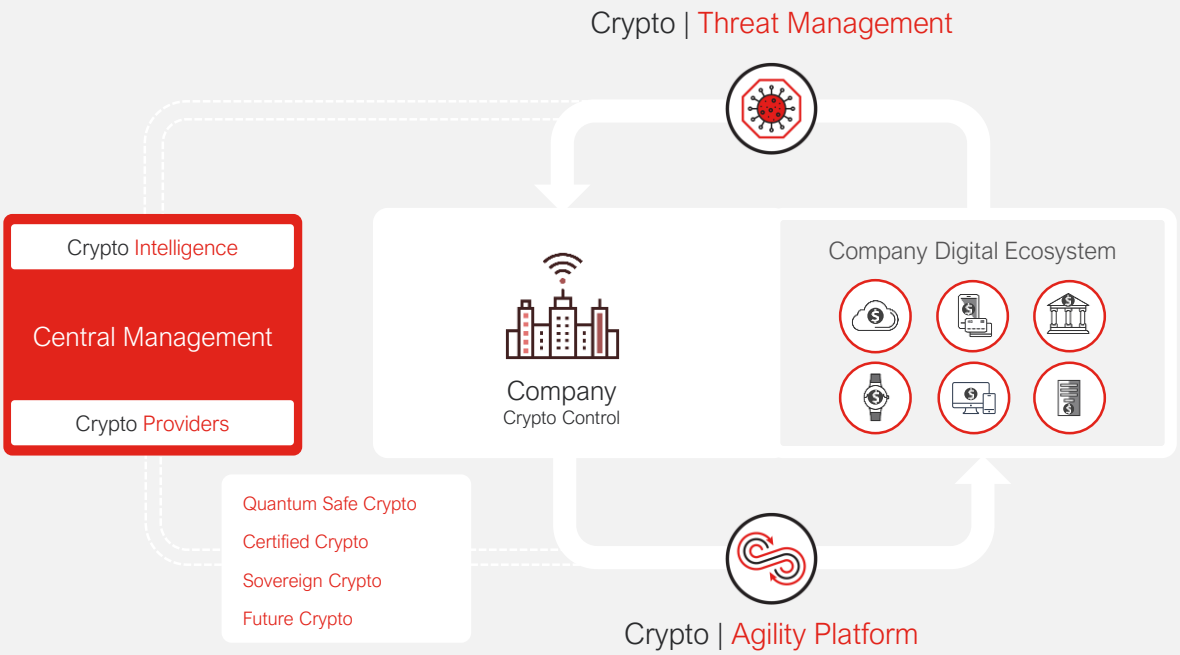
There is no shortage of cryptographic vulnerabilities to site; "MD5" is a cryptographic hash function that was published in 1992 and was broken in 2004. Although several practical attacks have been demonstrated based on MD5, it still occurs in some use cases and was one of the main reasons malware Flame was able to infect systems. SHA-1 is a cryptographic hash function that was broken in 2005 with the first practical attack presented in 2017. Since 2005 cryptographers have urged the industry to switch to safe standards. Today major browser providers mark any website showing a SHA-1 certificate as untrusted. WEP, the Wired Equivalent Privacy Algorithm was blamed for the theft of 45 million credit card numbers in 2007. Recently, the much stronger WPA standard was under attack as well - and the list goes on. In addition to crypto vulnerabilities, the use of cryptography in malware is also rising. In 2014 Cisco observed that about 10% to 12% of malware was using encryption in the form of SSL/TLS. However, in Cisco's new research published in February of 2018 the number was revised to 50% of malware using SSL/TLS, indicating 70% of malware using some form of encryption. Again, the biggest challenge here is that there is no multinational, organizational body enforcing standards for its application and management. A basic building block that justifies the need for Cryptographic Lifecycle Management is the plain reality of just how many organizations don't know in any detail what suite of encryption standards they have deployed across their IT infrastructure. A next generation cryptography solution should provide organizations with a means of comprehensively scanning their IT infrastructure. They need this to generate an accurate audit of exactly what cryptography they have implemented across their digital eco-system, this includes cryptographic keys and certificates.

In addition, global crypto standards are among the casualties arising from greater economic nationalism. More and more countries are deviating from global standards and moving to mandating their own. This makes the crypto environment even more dynamic than it was in the past. Meantime the criminal and nation state attackers are ramping up their spending on finding flaws in crypto standards that they can exploit. Enterprises need next generation cryptographic solutions that help them dynamically monitor and update these standards to protect them against the latest vulnerabilities. Finally, Cryptographic compliance, regulations and policies are becoming stricter for the private sector and the fines associated to companies with things like PCI, HIPPA, GDPR (General Data Protection Regulation) will push enterprises to prepare for stronger data protection.

INFOSEC GLOBAL

What is Cryptographic Lifecycle Management?

What differentiates next generation cryptography solutions is the ability to deliver Cryptographic Lifecycle Management. This includes three critical market components:



Threat Management

Pro-active inventory and detection of cryptographic vulnerabilities and applications using cryptography

Agility Platform

Enabling updates, fixes and interoperability of cryptography, keys and certificates, without having to upgrade software and hardware

Central Management

Enabling migration for new implementations of cryptography and towards quantum safety and ensure Path to Future

Crypto agility should also be wedded to interoperability and viewed as a means to a number of clearly defined benefits for organizations. Crypto agility can be too narrowly defined as a way of reducing the cost of swapping out legacy cryptographic primitives. Establishing partnerships that implement crypto agility at every stage of the digital ecosystem and supply chain will help developers secure their high-value IoT environments. This should also support migration to new implementations of cryptography and quantum-safe cryptographic primitives. Regardless of when quantum computers become a reality and are able to break popular cryptography standards, today's current cryptographic algorithms will need to be upgraded. Some large organizations will have the resources, including the in-house cryptographic expertise, to piece together the components of Cryptographic Lifecycle Management themselves. But we also recognize that this expertise is in such short supply worldwide that most organizations can't do this. Driving market awareness and adoption for Cryptographic Lifecycle Management and building a digital ecosystem of partners to deliver on it - is the key to leading this emerging market. Bottom line: If you don't manage your cryptography you are vulnerable to current threats and aren't preparing for future ones.