VECTRA®

How medical device companies can safeguard vital IP

Real-time, automated threat detection and response finds attackers before damage is done

Intellectual property (IP) is the lifeblood of medical device companies. An analysis of the top 10 medical device manufacturers indicates that intangible assets – R&D, trade secrets, designs, manufacturing processes, clinical trials management systems, and customer relationships – constitute 20-30% of their market value.

Beyond the accounting, IP is the engine of growth, the future of the company.

Unfortunately, IP theft is a growing problem for the medical device industry, as well as other IP-intensive industries. The economic damage of IP theft to U.S. companies is estimated at over $300 billion per year, according to an IP Commission Report, issued by the Commission on the Theft of American Intellectual Property.

Stolen IP represents a significant subsidy since the thieves don't have to bear the costs of developing or licensing that technology or manufacturing process. If a competitor steals a company's product-related trade secrets, it can beat that company to market with a new and innovative product, undercutting the victim company's market share.

The IP Commission concluded that IP theft hinders the development of new inventions and industries, putting the U.S. economy and security at risk. Negative impacts to business include:

- Lost sales
- Lost brand value
- Reduced scope of operations
- Lost jobs and reduced ability to provide employee benefits
- Reduced incentive to innovate
- Reduced ability to conduct R&D
- Increased IP protection expenses for prevention, remediation, and enforcement

Cyber attacks are a key and growing vector for IP theft. Understanding the nature and scope of these cyber threats—and how to combat them – is critical to protecting IP.

The Cognito™ automated threat detection and response platform from Vectra® helps medical device makers protect their IP by providing continuous, automated threat surveillance and detection across the entire enterprise. By automating threat detection and enabling faster incident response, Cognito condenses weeks or months of work into minutes, enabling security teams to take action to prevent theft or damage to vital assets.

The what and why of IP theft

Medical device manufacturers have a significant amount of IP to protect. Consequently, they've been the target of numerous attacks, which fall into two broad categories:

Insider trading and market manipulation

This includes stealing information such as trial results, non-public earnings information, and acquisition targets to profit in equity markets. This manipulation impacts all legitimate shareholders, including executives, employees and public shareholders.

Theft of trade secrets for competitive advantage

This enables perpetrators to accelerate time-to-market and reduce costs, especially R&D expenses. Corporate espionage may come from any competitor, but is especially likely from emerging economies with substantial funding and support from governments.

In its report, the IP Commission notes that the scale of economic impacts from IP theft is unprecedented due to national security ramifications, international dimensions, significant foreign-state involvement, and inadequate legal and policy remedies and deterrents. It cites China, Russia, and India as the countries most often implicated in the theft of IP from U.S. companies.

These countries all share a poor legal environment for IP, protectionist industrial policies, and a sense that IP theft is justified by helping level a playing field that benefits developed countries. Unfortunately, the risk of getting caught or prosecuted for IP theft is almost zero as there are few mechanisms to hold anyone accountable.

China leads in IP theft

The IP Commission estimates that China is responsible for 50-80% of international IP theft, and is the No. 1 perpetrator of cyber attacks designed to steal IP. One reason is that China's industrial policy goals encourage IP theft, and an extraordinary number of Chinese business and government entities are engaged in this practice.

The Chinese government's sponsorship of cyber attacks on IP has been well documented. Such attacks have largely targeted strategic emerging industries that China has identified in five-year plans.

Currently the Chinese government, in coordination with state-owned enterprises, is funding a new program dubbed "Made in China 2025," whose goals include capturing substantial global market-share over time. Advanced medical devices are among the 10 targeted sectors in this plan.

Given China's past behavior, it's likely that the country will use corporate espionage, both through cyber attacks and insider theft, to obtain the necessary technology to grow the targeted industries.

For example, in 2006, China approved an "indigenous innovation policy." Subsequently, the People's Liberation Army (PLA) began targeted cyber attacks against industries considered strategic by the Chinese government, with the goal of committing espionage and stealing data.

According to the IP Commission report, the PLA accessed victim networks over months and years, and stole broad categories of IP, including technology blueprints, proprietary manufacturing processes, test results, business plans, pricing documents, partnership agreements, and emails and contact lists from victim organizations' leadership.

The American renewable energy industry was one such target. In 2011, SolarWorld Americas filed a trade case against China as a flood of cheap Chinese solar panels was pushing several U.S. manufacturers into bankruptcy.

After the U.S. Commerce Department imposed tariffs on imports of Chinese solar panels in May 2012, hackers tied to the Chinese military broke into SolarWorld Americas' computers and stole business documents, including cash-flow records and details of proprietary technology, as well as records pertaining to its trade dispute.

In a similar incident, American Superconductor Corp. had its wind-energy software code stolen by a major customer in China. The company not only lost that customer, but also 90% of its stock value, according to the IP Commission report.

In the crosshairs

Cyber attacks against medical device manufacturers have been in the news for years, as the following examples illustrate. With China setting its sights on the medical device industry, U.S. companies have a lot to lose.

In 2015, the FBI indicted a man for stealing secrets from Covidien and Edwards Life Sciences while employed by the companies. According to MDDI Online, he allegedly stole more than 10 trade secrets on medical devices, representing millions of dollars of R&D, by downloading documents from a work computer and sending them to his personal email account. The man intended to use the trade secrets to establish his own company in China, MDDI Online reported.

In a similar case in 2014 cited by MDDI Online, an Indian national who worked first for CR Bard and then for Becton, Dickinson (BD) and Company stole information related to the companies' products by downloading information from company computers and forwarding it to his personal email accounts. While at BD, MDDI Online reported, he downloaded approximately 8,000 files, collecting enough information to mass produce BD's new disposable pen injector.

In 2014, medical device giants Medtronic, St. Jude, and Boston Scientific were all victims of cyber attacks. According to MDDI Online, since no patient information was compromised, it was concluded that the attackers were trying to steal IP.

Unfortunately, medical device makers are often targeted repeatedly. For example, following an earlier IP theft, a division of St. Jude was awarded a $2.3 billion verdict against a former employee and the Chinese medical device company he started after allegedly stealing St. Jude trade secrets, the website Law360 reported.

New approaches for protecting IP

Medical device companies face a very competitive environment, increasing the incentive for IP theft as well as damage to victims. While traditional industrial espionage techniques have been used extensively, cyber methods for stealing IP have become more widespread and harmful due to low costs, difficult attribution, and the ability to perpetrate crimes remotely to remain immune from extradition.

And whereas it typically takes months to discover a breach of credit cards or consumer identities – usually when the thief tries to use the stolen data to perpetrate fraud – IP theft may never be definitively discovered; victims are just left with an insidious disbelief at a competitor seeming to be just one step ahead.

It's imperative that medical manufacturers take precautions to defend themselves from all types of IP theft, including both opportunistic and targeted cyber attacks. Experts offer a number of key recommendations to help enterprises fend off advanced cyber threats.

For example, the IP Commission recommends companies continue to deploy what it terms "prudent vulnerability-mitigation measures," which try to "strengthen one's existing network security by pursuing the newest and best software, network appliances, regular updates, updated firewalls, most recent patches to software weaknesses, and so forth."

However, the report authors note that such measures place a high burden on network administrators. In addition, vulnerability-mitigation measures "have proved largely ineffective in defending against targeted hackers, who are hired specifically to pursue American corporations' IP."

To protect trade secrets and other IP, the IP Commission notes that enterprises need security systems that are capable of rapidly analyzing the behavior of unknown files and links, and that provide advanced, real-time network analysis.

Analysts at Gartner agree: Prevention is not enough. In fact, Gartner analysts have been saying for several years that advanced targeted attacks make prevention-centric strategies obsolete.

Gartner notes that "comprehensive protection requires an adaptive protection process integrating predictive, preventive, detective and response capabilities," and that information security architects should shift their mindset from incident response to continuous response, wherein systems are assumed to be compromised and require continuous monitoring and remediation.[1]

Vectra believes that prevention-centric products such as firewalls, intrusion prevention systems (IPS), web security proxies, payload analysis tools, and antivirus software have a place in the enterprise security tool box, providing a first line of defense. But once attackers gain a foothold inside the network, they are free to begin their exploitation, to which perimeter defenses are blind.

To combat advanced threats, security professionals need automated real-time detection and reporting capabilities that provide multiple opportunities to stop an attack. The Cognito automated threat detection and response platform provides such capabilities.

Cognito detects attacks in progress, streamlines security operations

Automated threat hunting and detection is central to the Cognito platform. Cognito enables medical device manufacturers to detect and respond rapidly to threats, finding attackers before critical IP is stolen.

Picking up where perimeter security leaves off, Cognito provides deep, continuous analysis of internal and internet network traffic and detects the fundamental actions and behaviors that attackers must perform when they spy and spread across an organization's networks, and steal valuable assets.

Cognito also monitors and detects suspicious access to critical assets by authorized employees, as well as policy violations related to use of cloud storage, USB storage, and other means of moving data out of the network.

Leveraging a unique combination of data science, machine learning and behavioral analysis, Cognito detects all phases of a cyber attack, including command and control (C&C) and other hidden communications, internal reconnaissance, lateral movement, abuse of account credentials, data exfiltration, ransomware activity, and botnet monetization.

In addition, by automating the manual, time-consuming Tier 1 analysis of security events, Cognito dramatically reduces the time spent on threat investigations by 75-90%, enabling security teams to focus on data loss prevention and mitigation.

[1] "Designing an Adaptive Security Architecture for Protection from Advanced Attacks," by Neil MacDonald and Peter Firstbrook, 12 February 2014, ID G00259490, https://www.gartner.com/doc/2665515/designing-adaptive-security-architecture-protection

Cognito highlights

Key capabilities of the Cognito platform include:

- Continuous monitoring and analysis of all network traffic, including internal (east-west) network traffic, internet-bound (north-south) traffic and internal traffic between physical and virtual hosts with an IP address – for example, laptops, servers, printers, BYOD/personal smart-devices, and IoT devices – regardless of the operating system or application, including traffic between virtual workloads in the data center and in the public cloud.
- Real-time visibility into network traffic by extracting metadata from packets rather than performing deep packet inspection, enabling protection without prying.
- Analysis of metadata from captured packets with behavioral detection algorithms that spot hidden and unknown attackers, whether traffic is encrypted or not.
- Deterministic identification of attack behaviors, including the use of remote access Trojans, encrypted tunnels, reconnaissance tools, and use of stolen credentials. Cognito persistently tracks threats over time and across all phases of an attack, ranging from C&C, internal reconnaissance, lateral movement, and data exfiltration behaviors.
- Tracks the internal Kerberos infrastructure to understand normal usage behaviors and detect when trusted user credentials are compromised by an attacker, including the misuse of administrative credentials and abuse of administrative protocols (e.g., IPMI). Detects lateral movement using common tools such as PsExec and MSRPC.
- Automatic correlation of threats with host devices under attack and threat detection details that include host context, packet captures, the seriousness of the threat, and certainty scores.
- Delivers real-time notifications to security teams, with one-page explanations of each attack detection, including underlying events and historical context that led to the detection, possible triggers, root causes, business impacts, and steps to verify.
- Drives dynamic response rules or automatically triggers a response from supported security enforcement solutions, including:
  - Cognito integrates with the Cisco Identity Services Engine (ISE) to immediately isolate or quarantine a host.
  - Cognito works with Carbon Black to rapidly isolate or quarantine a host device when a threat is detected and to kill a malicious process.
  - Cognito integrates with next-generation firewalls from Palo Alto Networks, Cisco and Juniper Networks to block a compromised host device.
  - Cognito integrates with SIEMs such as HPE ArcSight and IBM QRadar to automate security operations workflows.
- Supports adaptive cybersecurity through an ongoing process of improvement that leverages the work of the Vectra Threat Labs™, a group of highly-skilled security researchers, as well as behavioral detection algorithms that constantly learn from the local environment and from global trends.

With Cognito, medical device makers gain the advanced, real-time network analysis and detection needed to protect valuable IP assets.

Staying a step ahead

Theft of IP will continue to be a major threat for the medical device industry. Vectra arms security teams with an automated solution that works in real time to rapidly detect known and unknown cyber attacks across the constantly evolving threat landscape.

With the unique ability to detect and mitigate cyber attacks while they are happening, Cognito enables security teams to respond with unprecedented speed, accuracy and efficiency – well before the bad guys compromise IP or cause irreparable damage.

Likewise, Cognito gives security teams unparalleled network visibility into malicious attack behaviors and automates the hunt for cyber threats, which lets organizations focus on keeping target assets safe.

VECTRA®
Security that thinks®

Email info@vectra.ai **Phone** +1 408-326-2020
vectra.ai