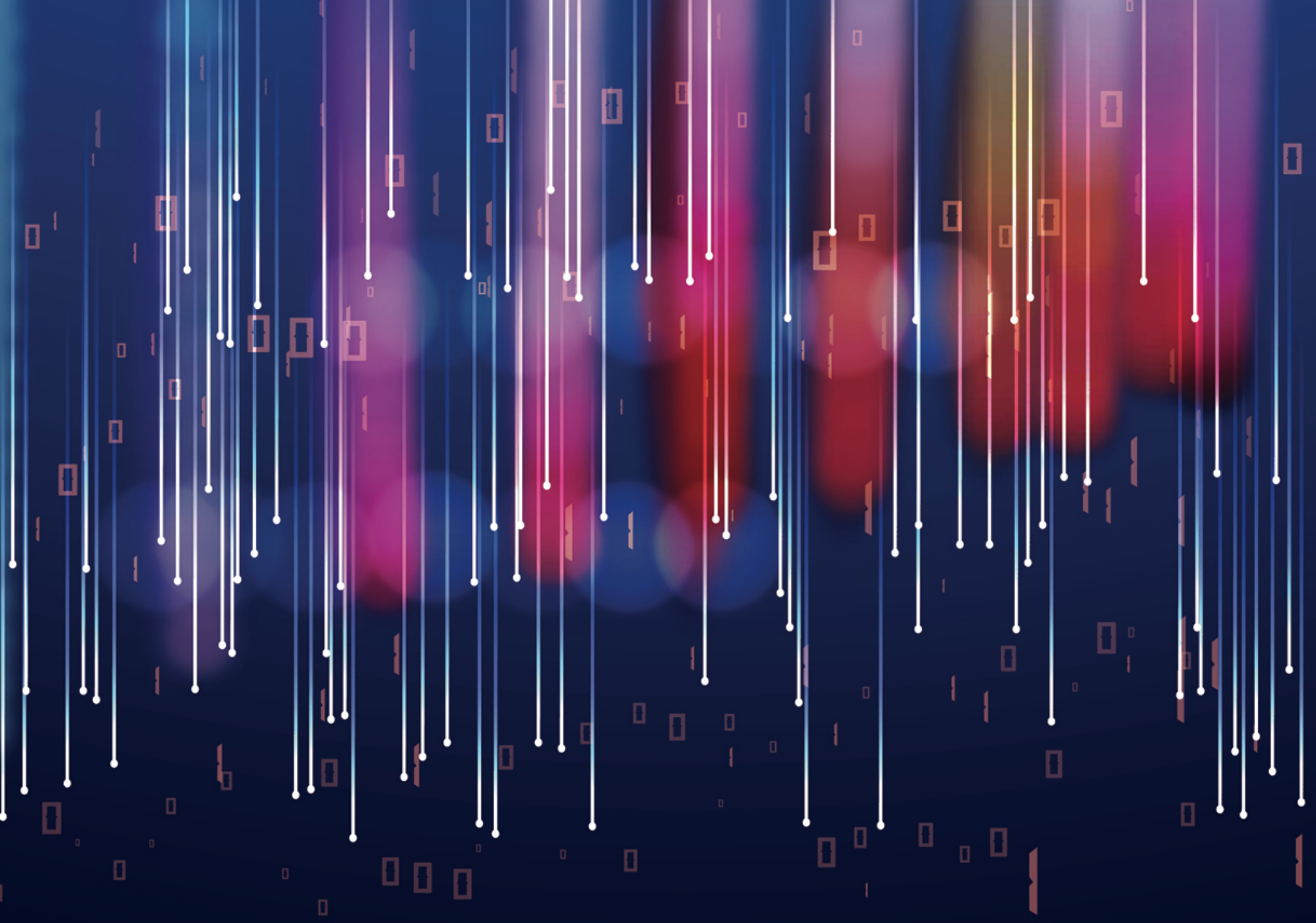


Healthcare IoT Security Operations Maturity

A Rationalized Approach to a New Normal

CROWDSTRIKE

MEDIGATE

Table of Contents

ABSTRACT 3

INTRODUCTION 3

THE THREAT TO HEALTHCARE -- REVISITED 5

To Pay or Not to Pay 6

A RECHARGED FOUNDATION 8

Orchestrated Visibility 8

Endpoint Detection and Response 9

Containment Capability..13

Effective Insurance Coverage 14

CROWDSTRIKE AND MEDIGATE 15

Business Value 17

CONCLUSION..19

About Medigate..21

About CrowdStrike..21

ABSTRACT

IoT cybersecurity management products are a key enabler of connected health. The global solution market is expected to expand at a compound annual growth rate (CAGR) of 28% over the next three years, and the healthcare sector is projected to experience the highest rate of growth.[1] Not surprisingly, healthcare delivery organizations (HDOs) are rapidly investing in these solutions, as they address the operational challenges to scalable, safe delivery. Interestingly, however, the adoption is occurring despite how hospital cultures still lag in their understanding of the real stakes and the capabilities that enable a desirable future state. This paper suggests that a more simplified approach to modernizing healthcare security operations is warranted. It suggests that a renewed focus on foundational enhancements presents a more rational path to maturity. The "blocking and tackling" sports analogy comes to mind, as only teams that effectively execute at this level can successfully move to the next.

INTRODUCTION

The explosion in connected health is driving a revolution in care delivery. To safely support this transformation, a blend of positive and negative pressures are driving HDOs to invest in security operations maturity. On the positive side, the shift to value-based reimbursement is in lockstep with the journey. And because healthcare operations research has never been well-funded, HDOs are learning that their investments in maturity are easily cost-justified. On the negative side, protections against cyber risk are rapidly becoming a matter of compliance. And, the COVID-19 pandemic has served as yet another catalyst, as it has created a perfect storm for adversaries. The volume of attacks following the first lockdown was staggering. Through June of 2021, 93% more ransomware attacks have been carried out than the same period last year.[2] The surge has given rise to “triple extortion” techniques whereby attackers, in addition to seeking payment from the HDO, also coerce payments from patients and business partners.

[1] https://www.marketsandmarkets.com/Market-Reports/iot-security-market-67064836.html

[2] https://pages.checkpoint.com/cyber-attack-2021-trends.html

Further complicating matters, healthcare's attack surface continues to expand and fragment. In short, if the goal is to monetize a successful breach, no other industry segment presents the bad actor with a more compelling target. In addition to new forms of ransomware, COVID-19 has unearthed unique opportunities to use lure content and social engineering techniques. Pandemic-related phishing aimed at staff searching for disease intelligence is now common, as are impersonations of health-focused organizations including the World Health Organization (WHO) and U.S. Centers for Disease Control and Prevention (CDC). Scams of all types targeting staff working from home have also emerged as a tactic. Regardless, 75% of all interactive healthcare intrusions observed and attributable in the first half of 2020 were identified as eCrimes.[3]

Although attacks aimed at vaccine-related intelligence gathering will likely persist, healthcare cybersecurity experts remain focused on ransomware attacks. CrowdStrike's *2021 Global Threat Report* confirmed this, as 71% of the cross-industry executives surveyed cited ransomware attack as their top worry. In fact, 56% reported they had suffered a ransomware attack, and 27% paid the ransom[4].

CrowdStrike Intelligence continues to offer an unparalleled level of coverage. As of October 2021, the total number of adversaries tracked by CrowdStrike has increased to 164. And the number of activity clusters monitored has increased to 29. Specific to the healthcare sector, CrowdStrike Intelligence confirmed that 18 big game hunting (BGH) enterprise ransomware families infected 118 health care organizations. It also highlighted that new data extortion techniques will continue to accelerate through the introduction and rise of dedicated leak sites (DLSs).[5]

In October 2020, CrowdStrike also introduced a composite representation of the cybersecurity criminal threat. It is called the eCrime Index (ECX). The ECX exposes the strength, volume and sophistication of the cybercriminal market and is updated weekly based on 18 unique indicators of criminal activity. Notably, the ECX is up about 300% since its introduction last year.[6]

[3] CrowdStrike 2021 Global Threat Report: https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf

[4] CrowdStrike 2021 Global Threat Report: https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf

[5] CrowdStrike 2021 Global Threat Report: https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf

[6] https://www.crowdstrike.com/blog/how-big-game-hunting-ttps-shifted-after-darkside-pipeline-attack/

THE THREAT TO HEALTHCARE — REVISITED

Although dark web pricing varies, a health care record is typically valued 50 times more than a stolen credit card. Not only is personal health information (PHI) worth more, but there are more ways to monetize it, including ransoms, fraudulent medication prescriptions and phony claims for medical treatment.

Obviously, HDO spending on connected health is exacerbating the problem. Projections from industry analysts indicate spending on medical devices alone (IoMT) will continue at a CAGR of nearly 29.5% through 2028.[7] Although Medigate's experience indicates the rate is less, it is still explosive. Using device count increases and averaged costs as a proxy for spend, Medigate's study of nearly 1,000 healthcare facilities calculated the CAGR at 14.5%.[8]

Regardless of the increases in device spending, roughly 82% of health systems experienced some form of IoT cyberattack in 2020 [9], and the trend has not slowed in 2021. For example, while 34% of healthcare organizations globally reported being hit by ransomware through November 2020, the sector has experienced a 45% uptick since that time, according to *HealthITSecurity* [10]. For added perspective, 33% paid the ransom with knowledge that they may not get their data back. In fact, only 69% reported full restoration.[11]

A total of 92 ransomware attacks affected over 600 separate clinics, hospitals, and organizations and more than 18 million patient records in 2020. Although the average ransom paid by health systems in in the same year was $910,335 USD.,[12] attack restoration costs are highly variable. Nevertheless, the average cost of a successful attack on a health system is the highest reported across all industries. This has been the case for 11 consecutive years. Notably, these reported costs just increased by an average of 29.3% --from $7.13 million USD in 2020, to $9.23 million USD in 2021.[13]

[7] https://www.fortunebusinessinsights.com/industry-reports/internet-of-medical-things-iomt-market-101844

[8] Medigate original research presented August 2021; www.medigate.io

[9] https://www.aamc.org/news-insights/growing-threat-ransomware-attacks-hospitals

[10] https://www.aamc.org/news-insights/growing-threat-ransomware-attacks-hospitals

[11] https://www.aamc.org/news-insights/growing-threat-ransomware-attacks-hospitals

[12] https://healthtechmagazine.net/article/2021/06/how-minimize-risk-amid-rise-ransomware-attacks-healthcare-organizations

[13] https://www.upguard.com/blog/cost-of-data-breach (original research presented in Sept 2021 by IBM and Ponemon Institute)

Consider the $9.23 million USD restoration cost average cited above, and compare it to the example below:

- In mid-2020, a ransomware attack hit a U.S.-based university system (600 beds). For about 40 days, the hospital had to delay or cancel procedures and appointments, including regular treatments for cancer patients. While systems remained down, over 150 staff members who couldn't do their jobs were furloughed or reassigned. According to leadership, the shutdown costs rolled up to more than **$1.5 million USD per day** for a grand total of nearly **$64 million USD.**[14]

However, in terms of total cost, even the $64 million USD figure cited above is not comprehensive. Not included are unbudgeted advertising costs that HDOs report increase by an average of 64% to help repair reputational and patient loss to competitors in the two years following such incidents.[15] Unsettled liabilities were also not included, nor were other costs that are difficult to identify and measure until well after the fact.

That said, and considering all of the published statistics that describe the impact of cyberattacks to healthcare, perhaps the following summary statistics suffice:

- 82% of hospitals were successfully attacked between March 2020 and September 2021
- 34% of those attacks were ransomware
- 33% of hospitals that experienced a ransomware attack paid the ransom
- 31% of hospitals that paid the ransom did not get their data restored
- Breaches are a daily occurrence — some are more costly to fix than others
- **There is no total cost impact (TCI) standard for calculating restoration costs.**

To Pay or Not to Pay

HDOs are rethinking their ransomware payment policies. Naturally, many believe if HDOs removed the economic incentives, there would be less attacks. Some hospitals are even promoting legislation that outlaws ransom payments. Advocates of this position believe the move would force hackers to accept their efforts as pointless.

[14] https://www.beckershospitalreview.com/cybersecurity/inside-uvm-medical-center-s-ransomware-attack-11-details.html

[15] https://www.hipaajournal.com/advertising-expenditures-increase-64-following-a-healthcare-data-breach/

No legislation banning ransomware payments exists at the U.S. federal level. But the attitude at certain state levels is different. So far, four U.S. states have proposed laws that would stop or substantially restrict the practice. For example, in New York, Senate Bill S6806A "prohibits governmental entities, business entities, and health care entities from paying a ransom in the event of a cyber incident or a cyber ransom or ransomware attack."

Consider whether the following example makes a case for or against paying a ransom:

- A Massachusetts HDO now faces a class-action lawsuit after a ransomware attack in February 2021 put PHI at risk for more than 35,000 patients. While the class action is not unusual, in this case the provider admitted to paying the ransom. Despite how confident the hospital spokesperson was in explaining how its data and systems were quickly restored and secured after it paid the ransom, it didn't matter. Regardless of assurances that the stolen PHI had been destroyed, the plaintiffs' lawyers saw the ransom payment as an admission of guilt and were quick to point out that the promises of criminals were meaningless.

Is "to pay or not to pay" a Catch 22 for HDOs? While the debate is interesting, most experts continue to arrive at the same, simple conclusion:

- Giving any third party the power to decide which health systems survive and which do not is a Pandora's box that's tailor-made for cybercriminals. Said Ari Schwartz, managing director of cybersecurity services and policy at Venable LLP, "...**before the U.S. can explicitly outlaw paying a ransom, it first has to ensure the victimized HDO is capable of recovering from the cyberattack."**

Put simply, the debate is fast becoming a red herring. Regardless of ransom payment decisions, HDOs will be better served, if not soon required, to harden security infrastructures in ways that effectively deal with modern threats. In other words, HDOs must focus on preventing attacks in the first place. Whether it's the government and/or emerging cyber insurance coverages that will provide health systems a new way to rapidly recover from successful attacks, the conditions of any such potential relief will require that HDOs have modern defense protections in place.

A RECHARGED FOUNDATION

While healthcare spending on cybersecurity is increasing, it is important to note that HDOs have already made significant long-term investments in their security infrastructures. However, it's no secret that connected asset visibility has been especially poor in healthcare, and as a result, essential security enforcement systems have not been able to perform at required levels. The performance of existing infrastructure can be dramatically improved by addressing these long-standing data deficits and integrating capabilities that directly deal with the realities of modern threats. The recommendations made below are selected because they accomplish both. Importantly, they also enable the good performance of additional layered defense capabilities that are not listed:

- Orchestrated visibility
- Endpoint detection and response (EDR)
- Containment (network segmentation)
- Effective insurance coverage

Orchestrated Visibility

For CrowdStrike and Medigate, comprehensive visibility means knowing all there is to know about every connected endpoint. What's needed is a fully profiled, dynamically risk-scored inventory of all managed and unmanaged endpoints. To be clear, visibility means a moving picture of each device’s security posture, network status, location and device utilization. On a per-asset basis, that could mean as many as 100 unique and general identifiers, further detailed with images, maps, Manufacturer Disclosure Statements for Medical Device Security (MDS2s) and other specialized descriptors. Importantly, because the detection of unauthorized asset behavior requires detailed knowledge of authorized behavior, the operating requirements and workflows of each device-type must be incorporated into profiling details. This is what is meant by comprehensive visibility.

Making relevant "cuts" of the right data instantly available to the right systems and workflows is referred to as data orchestration. In this context, it is important to understand that Medigate data capture and orchestration is not limited to the device data that it passively captures from network traffic flows. It also includes the data actively captured and held in other networked systems, like the CrowdStrike Falcon® solution.

When the data are complete, the orchestration is thorough, and the underlying enrichment processes are continuous, a single source of truth can be shared across departments. Cross-functional workflows can then reference the same information, and the results of the efforts can be synchronized. “Effective orchestration delivers the payoff, as among other things, it breeds automation and accelerates convergence across the ecosystem,” said Jonathan Langer, Medigate’s CEO.

There aren't any chicken-and-egg questions here. Visibility must come first. To Mr. Langer's point, when the data is well-orchestrated, it becomes the security infrastructure Rosetta Stone. A common data foundation drives cross-departmental collaboration naturally, enabling operational leverage and productivity gains. A converged ecosystem delivers scale more safely and effectively.

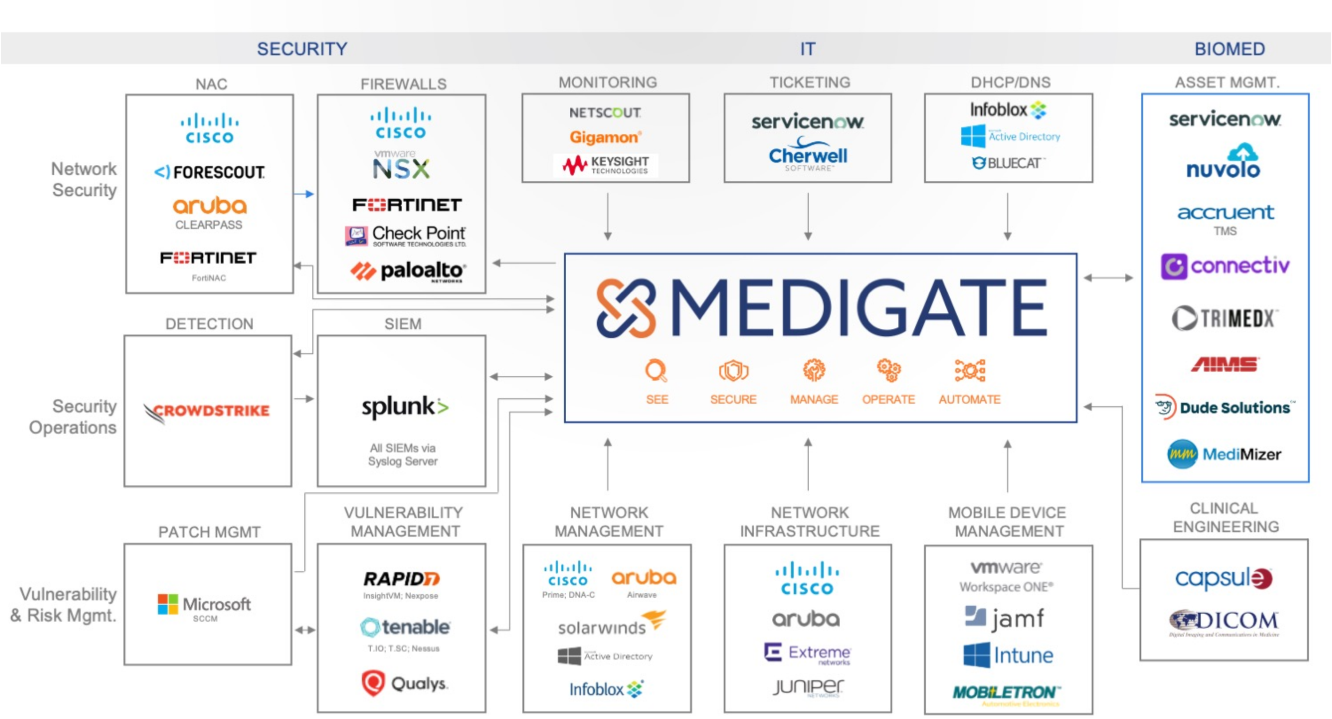


Figure 1. The many facets of Medigate's converged operations ecosystem.

Endpoint Detection and Response

EDR is a foundational capability, especially as care delivery continues to fragment. Connected health requires security practices that adapt to care delivery, regardless of where it executes, and not the other way around. Security must enable, not constrain. As pioneers of the space, CrowdStrike has spent the last decade expanding EDR capabilities by adding network visibility and telemetry from all workloads. The merger of this data with network and endpoint information allows users to understand which information is vital, when and where.

CrowdStrike's 2021 Global Threat Report analysis of Common Vulnerabilities and Exposures (CVEs) impacting IoT devices across the healthcare industry cites the following CVEs as most significant:

- DejaBlue (CVE-2019-1181/1182)
- BlueKeep (CVE-2019-0708)
- Netlogon (CVE-2020-1472)

An analysis of the health system clients shared by CrowdStrike and Medigate is revealed in the chart below. Interestingly, the most common CVEs were the same.

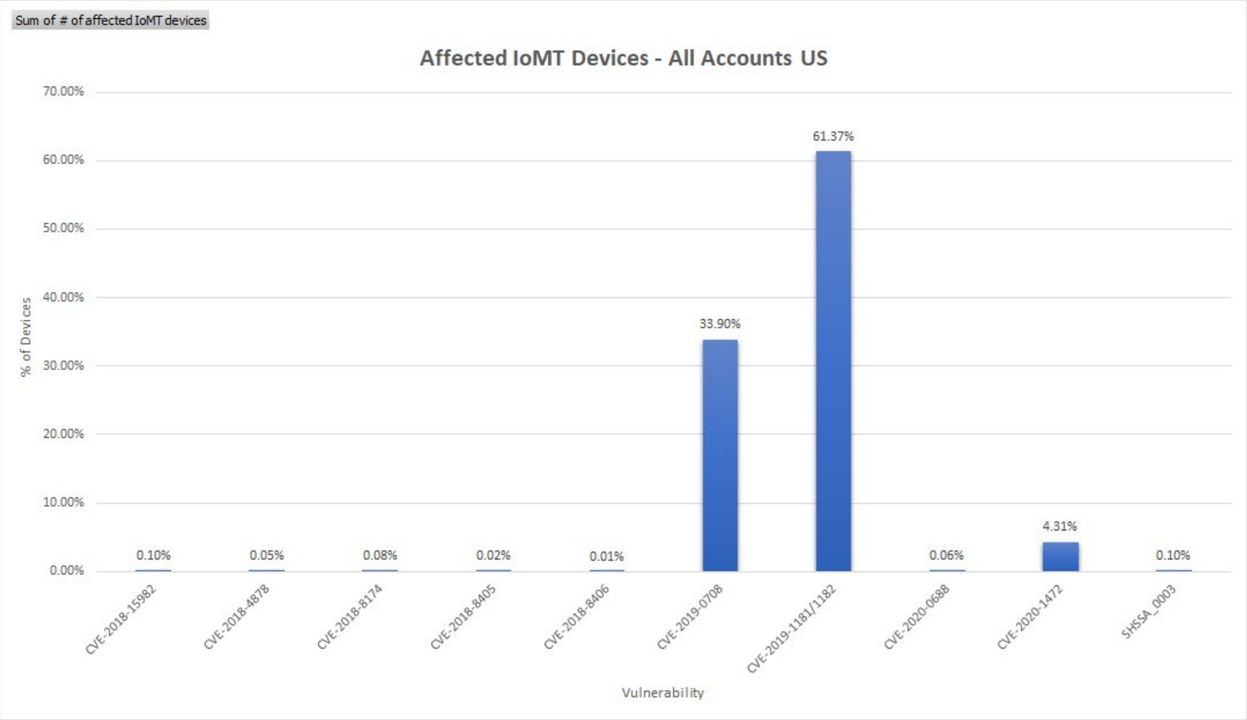
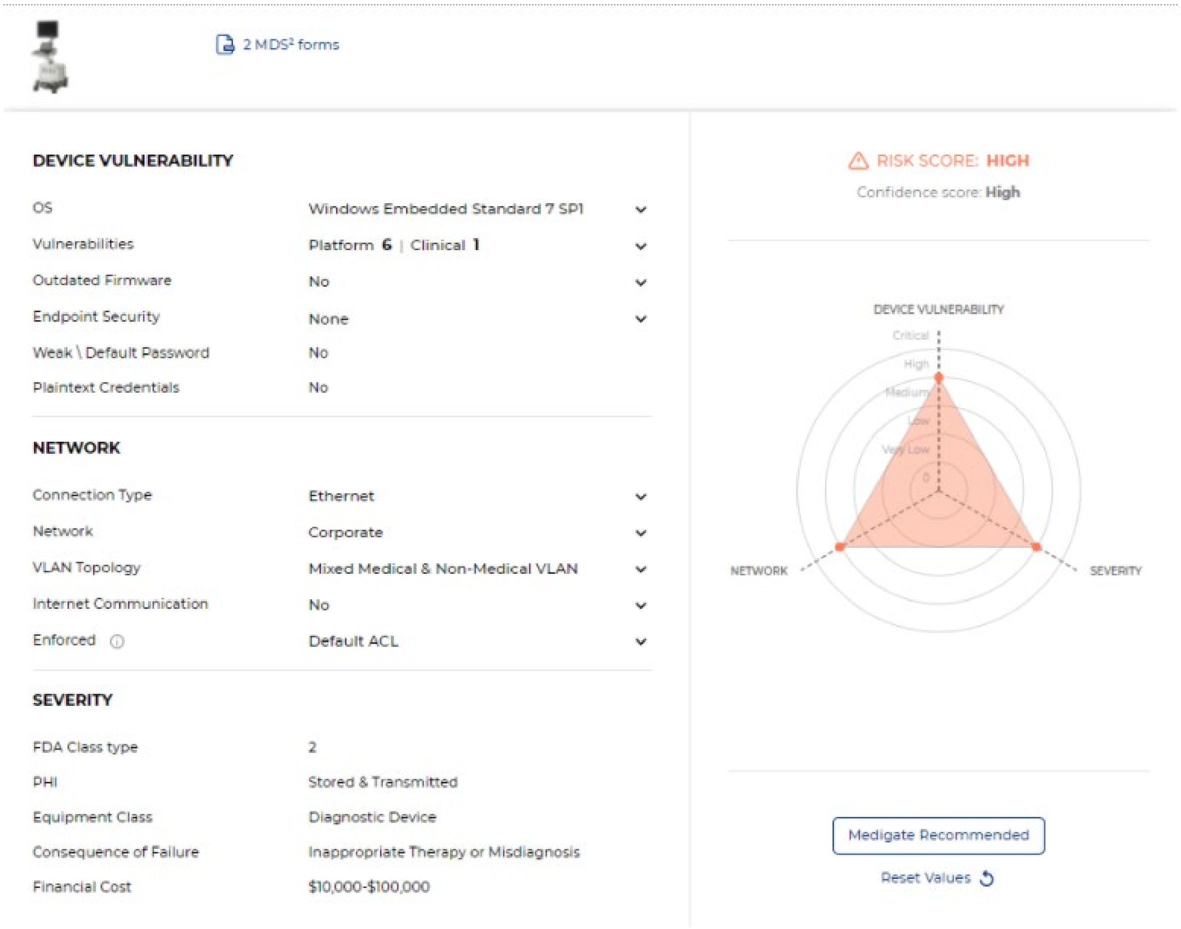


Figure 2. Percentage of IoMT devices affected by identified CVEs among health system clients shared by CrowdStrike and Medigate.

That said, Kobi Rubin, Medigate's Vice President, Data Science, revealed an irony. "The data speaks to a missed opportunity, as contrary to popular belief, 20% of IoMT [medical devices] actually do support installation of an EDR agent. Of that 20%, only 7% have an EDR agent installed, and 60% of them aren't even being patched. The same ‘miss’ holds true for common Windows Operating Systems (OS) vulnerabilities." For example, while 3% of the devices running vulnerable OSs can be safely patched and run antivirus (AV) software, 70% of them are not patched, and just 44% of that number have AV installed.[16] Mr. Rubin added, "The point here is, there are 'low hanging fruit' that a solid EDR foundation can resolve."

The "before EDR" example provided below reflects a risk assessment of an ultrasound device with six platform vulnerabilities and one clinical vulnerability. As seen, several considerations are factored into the “HIGH" risk score that is presented. Medigate allows each contributing risk factor's scoring significance to be modified, meaning the entire framework can be customized. This can be done globally, but more practically, it is done by specific device types or classes. In support of remediation and mitigation workflows, the user can simulate the effects of potential actions, including compensating controls. Essentially, device-, vulnerability- and threat-specific "what if" scenario-based analysis capability is provided.



2 MDS² forms

DEVICE VULNERABILITY

OS	Windows Embedded Standard 7 SP1
Vulnerabilities	Platform **6** | Clinical **1**
Outdated Firmware	No
Endpoint Security	None
Weak \ Default Password	No
Plaintext Credentials	No

NETWORK

Connection Type	Ethernet
Network	Corporate
VLAN Topology	Mixed Medical & Non-Medical VLAN
Internet Communication	No
Enforced	Default ACL

SEVERITY

FDA Class type	2
PHI	Stored & Transmitted
Equipment Class	Diagnostic Device
Consequence of Failure	Inappropriate Therapy or Misdiagnosis
Financial Cost	$10,000-$100,000

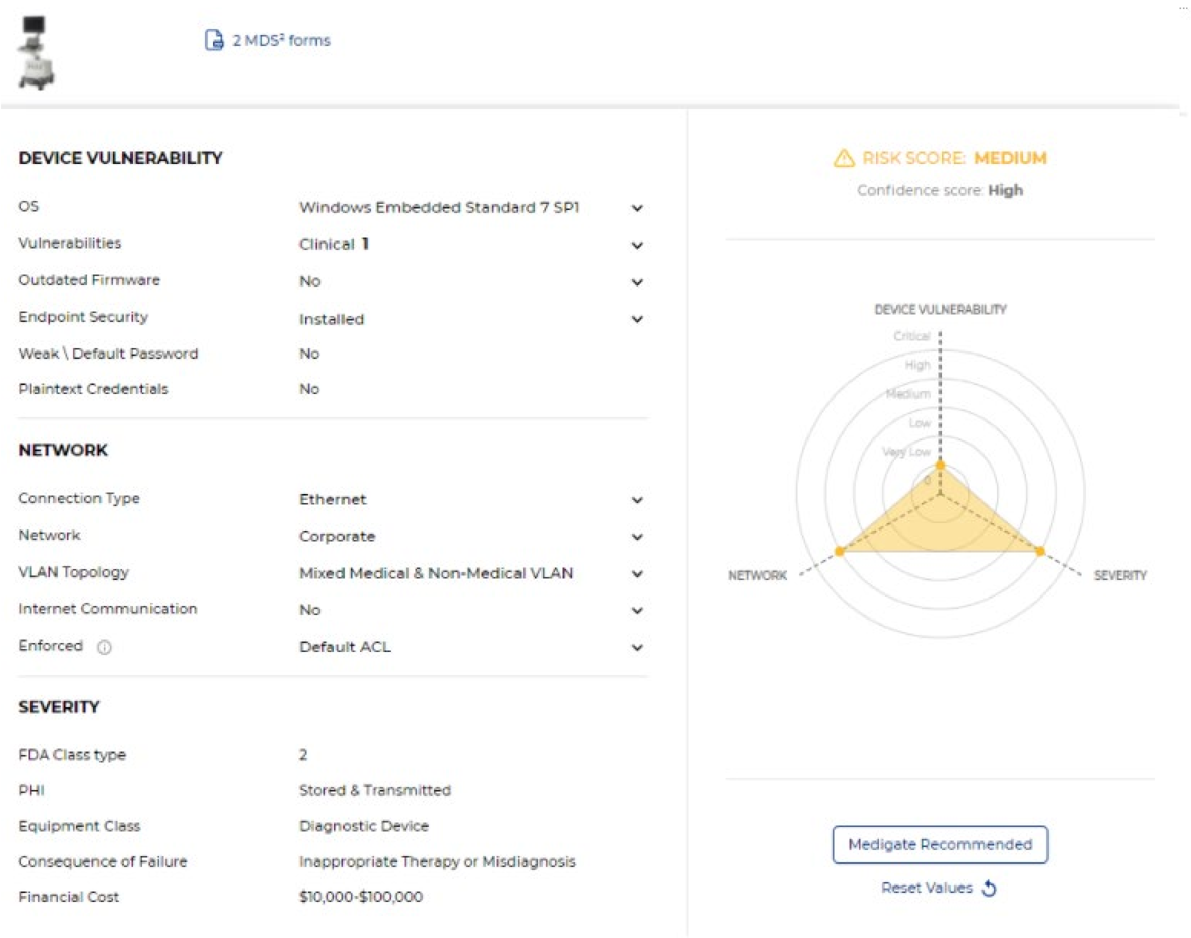
RISK SCORE: **HIGH**

Confidence score: **High**

Figure 3. Medigate dashboard showing device vulnerability, network information for the device, severity of the vulnerability and a composite risk score before installation of EDR.

[16] Medigate original research presented August 2021; www.medigate.io

The "after EDR" case on the same device presented below is also interesting, as it clearly demonstrates the impact of endpoint security. It confirms that the installation of AV on all endpoints, including the relatively small percentage of medical devices that permit it, combined with available patching, results in significant security posture improvements, which confirms Mr. Rubin's point.



2 MDS^2 forms

DEVICE VULNERABILITY

OS	Windows Embedded Standard 7 SP1
Vulnerabilities	Clinical **1**
Outdated Firmware	No
Endpoint Security	Installed
Weak \ Default Password	No
Plaintext Credentials	No

NETWORK

Connection Type	Ethernet
Network	Corporate
VLAN Topology	Mixed Medical & Non-Medical VLAN
Internet Communication	No
Enforced	Default ACL

SEVERITY

FDA Class type	2
PHI	Stored & Transmitted
Equipment Class	Diagnostic Device
Consequence of Failure	Inappropriate Therapy or Misdiagnosis
Financial Cost	$10,000-$100,000

RISK SCORE: **MEDIUM**

Confidence score: **High**

Figure 4. Medigate dashboard showing device vulnerability, network information for the device, severity of the vulnerability and a composite risk score after installation of EDR.

Extended Detection and Response (XDR) is the next advance in cybersecurity protection. According to analyst firm Gartner, "XDR is a SaaS-based, security threat detection and incident response capability that integrates multiple security products into a security operations system that unifies all licensed components." In short, XDR's objective is to enable a more holistic and simpler view of threats.

The governing philosophy is also appropriately simple: **only when superior threat intelligence can be matched with superior visibility can threat processing be optimized.** A unified view of risk is hard to achieve in a mixed bag of managed and unmanaged device types and classifications. This is a key reason why the integration of CrowdStrike and Medigate is so timely and valuable.

XDR represents the natural evolution of EDR, so CrowdStrike's recently announced first release of Falcon XDR at Fal.Con 2021 was anticipated. CrowdStrike was already correlating telemetry from all types of workloads, now including agentless device identities and anomalous behavior detection from Medigate, so the release of Falcon XDR makes sense. Said Todd Felker, former Director, Information Security at Torrance Memorial Medical Center and now a Senior Healthcare Strategist with CrowdStrike, "Medigate not only quickly identified and profiled all of the clinical devices on my network, but in partnership with CrowdStrike, a natural evolution toward XDR that provides a game-changing level of sophistication was revealed, as was a realistic path to comprehensive NAC [Network Access Control]."

Containment Capability

It was only a few years ago when failed attempts at implementing NAC led to publicity that caused many health systems to put critical, high-profile NAC projects on hold. It was a visibility problem, with deficits in IoMT discovery and identification specifically called out as the culprit. Many firewalling and NAC projects still languish to this day for the same reasons.

Whether the goal is to layer sophisticated firewalling defenses or Access Control List (ACL) deployments for NAC, comprehensive and detailed visibility must come first. Or, if the goal is to effectively cloak devices from prospective hackers, then awareness of what’s being hidden is required. If the objective is to contain breaches to a network segment, then there must be a process that expedites the creation of appropriate security policies and allows them to be validated before deployment.

Creating reasonable security policies that aren’t overly complex has always been a challenge in healthcare, so Medigate now generates the policy baselines automatically. Because Medigate knows each device's operating requirements (e.g., internal/external connection requirements, intended workflows, etc.), the automation is highly effective.

Through meaningful integrations with all firewalling and NAC enforcement products, administrators can:

- Understand device identities and existing relationships
- Virtually simulate the impact of security policies
- Test the impact of underlying policy rules and modify them as required
- Study segmentation effects without disruption to clinical operations

The availability of device profiles, policy automation and simulation/virtual testing are recent and important innovations. In retrospect, it's hard to understand how east-west firewalling and NAC-based segmentation projects were viable without such capabilities.

The state-of-the-art just described has powered a relative flood of successfully operationalized deployments. According to Kierk Sanderlin, Medigate's Vice President, Customer Success, "Nearly 38% of Medigate's clients are now engaged in NAC projects covering more than 600,000 medical devices. We fully expect this trend to pick up, as containment capability is widely recognized as foundational, and it's now achievable."

Effective Insurance Coverage

Cyber insurance should exist to help the impacted HDO recover quickly. In theory, the more mature the HDO’s cybersecurity ecosystem, the lower its premium costs should be. Remarkably, when cyber insurance was first introduced to healthcare, the underwriters had no tables to reference, and yet they still sold products. The losses they suffered were significant, resulting in coverage pullbacks and premium increases that undermined what should have been a vibrant market. Necessity is the mother of invention, and no truer words serve to describe the transformation currently underway in healthcare cyber insurance underwriting.

To determine premium costs, the newest generation of cyber insurers are now insisting on comprehensive Security Risk Assessments (SRAs). Security posture is now being evaluated in a broader, more modern context that includes how well-orchestrated the underlying connected asset visibility data are, and how well-integrated the HDO’s medical device management and security practices are. A more fluid premium arrangement is in the offing, as insurance carriers will monitor their clients' developing maturity. In other words, premium costs may soon be raised or lowered based on the HDO’s compliance to the recommendations made in the SRA. Added Felker, "Cyber insurance underwriters are keenly aware of the impacts of attacks that start on these vulnerable devices and may be willing to offer better terms to organizations that have this level of maturity and integration between their tools."

In terms of coverage, if containment capability exists, then coverage can be scoped more intelligently. Pixel Health, a diversified healthcare consultancy, is a leader in the underwriting transformation that is currently underway. Mike Machulsky, a senior Pixel executive, added the following: "We have developed a cyber risk rating engine that is 100% tailored to the HDO market. It is comprehensive and continuously updated, as we are constantly reassessing risk factors that impact the HDO's cybersecurity risk posture. Our evaluations include people, processes, supply chain, the organization's change management culture and, of course, security infrastructure deficiencies."

The impact that security operations maturity is now having on **HDO credit ratings** is yet another reason for HDOs to harden security infrastructure. In addition to insurance providers, credit bureaus are well aware of best security practices, as they are also integrating modern SRAs into their rating frameworks. They are evaluating HDO security postures, scoring them and making decisions that have significant financial consequences. Bottomline, the costs and benefits directly tied to the assessed maturity of a HDO's security and connected asset management ecosystem are multiplying.

CROWDSTRIKE AND MEDIGATE

Medigate and CrowdStrike have partnered because healthcare's co-mingling of agent and agentless endpoints presents unique security and asset management challenges that are not being properly addressed. The solution synergies are easily understood. It's an obvious "better together" story:

- The CrowdStrike Falcon platform has revolutionized endpoint security by being the first cloud-delivered endpoint protection solution to unify next-generation antivirus and EDR. CrowdStrike Falcon delivers a 24/7 threat hunting service, all via a single lightweight agent that integrates antivirus, endpoint protection and artificial intelligence-powered threat hunting.

- Separately, Medigate pioneered a passive, agentless approach that delivers detailed visibility to unmanaged medical devices. In addition to correlating device-specific vulnerabilities and threats, Medigate continuously hunts for unauthorized traffic flows.

- Medigate ingests telemetry provided by CrowdStrike Falcon and adds it to the unmanaged device profiling information it collects and manages. Given these data enhancements, Medigate's coverage of IoMT, inclusive of inter-device communications, results in more comprehensive detections of anomalous IoT/IoMT network behavior. The combined solution delivers more comprehensive and accurate real-time detection and response capabilities and maintains a unified history of all responses/actions.

- Most importantly, not only is the combined data valuable to both CrowdStrike and Medigate, but it can be orchestrated to the benefit of the entire ecosystem (e.g., VM, SIEM, CMMS, CMDB, ERP, etc.). In addition, the threat intelligence gathered by both companies is aggregated, processed and accurately correlated to the right assets and supporting workflows. A higher level of intelligence is created that delivers improvements to existing infrastructure and ensures that future investments in layered defense capabilities can perform.

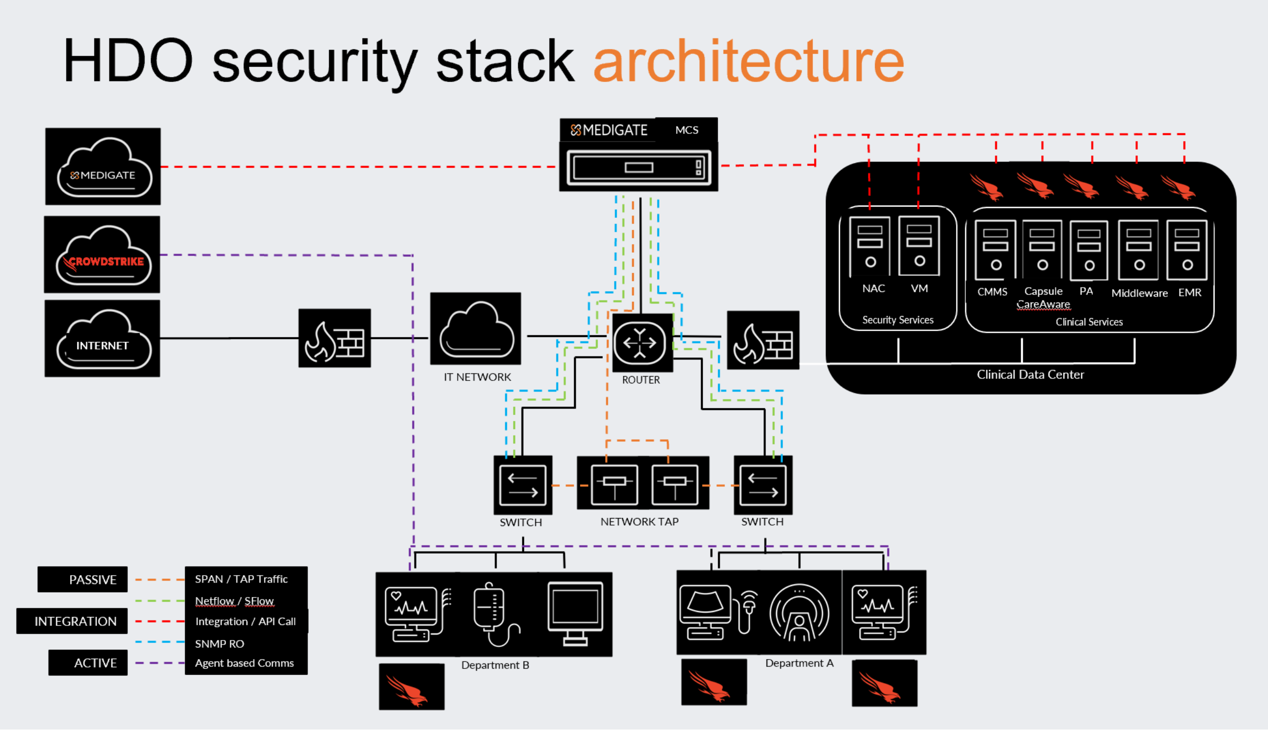


Figure 5. How CrowdStrike and Medigate's solutions work together to protect HDOs.

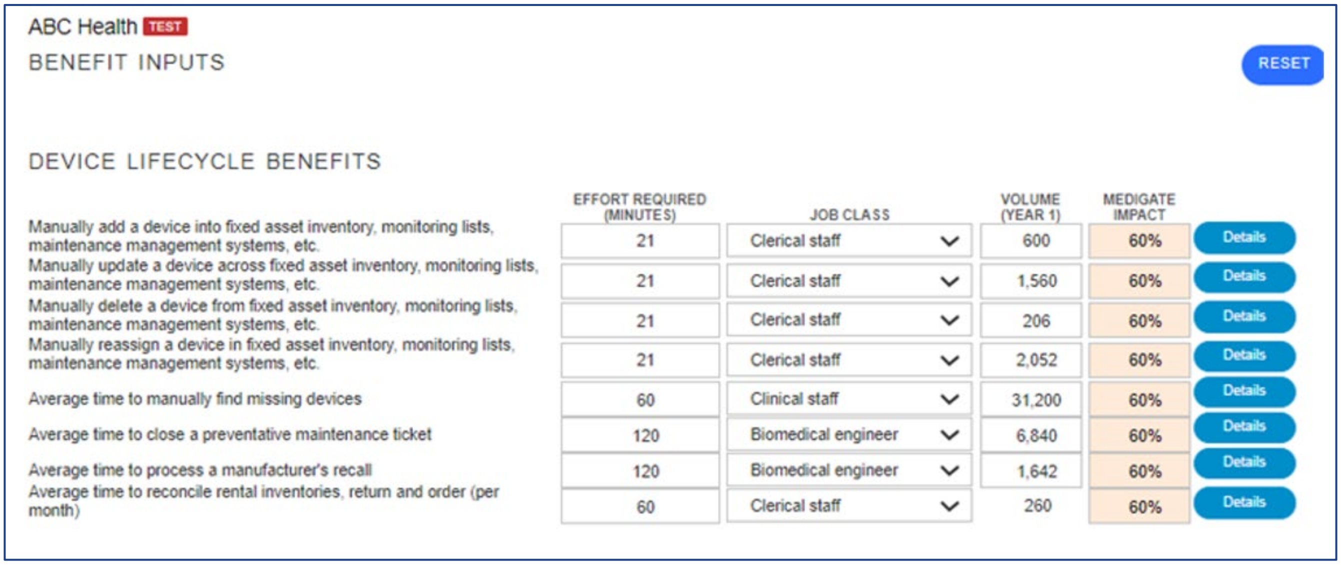
Both CrowdStrike and Medigate have dominated their respective cybersecurity solution markets. For example, Forrester named CrowdStrike as a Leader in “The Forrester Wave™: Endpoint Security Software As A Service, Q2 2021”. Like CrowdStrike, Medigate was named a "Leader" in the report, *The Forrester New Wave™: Connected Medical Device Security, Q2, 2020*, an evaluation of current offering, strategy, and market presence. Medigate is healthcare-specialized and has already received seven different industry awards in 2021, including *Best in KLAS* for *Healthcare IoT Security*.

Business Value

Security operations maturity gains do not intuitively bridge to business value. In large part, this is due to an understandable focus on mitigating the disruptive costs associated with a breach. But as health systems are learning, a successfully executed, integrated approach to security and asset management is a silo-busting affair that creates operational leverage. And translating that leverage to business value is not a fuzzy process, provided there is agreement on value estimation procedures and acceptable levels of accuracy.

As stated throughout this paper, having an accurate inventory of all of the devices attaching to clinical networks must be considered a foundational capability. From there, security-infused operational efficiencies can be achieved and/or the security risks associated with existing operational inefficiencies can be largely reduced. The risk of a breach and associated costs are naturally lessened. Among other things, savings based on eliminating redundant cybersecurity tools can be realized. Savings based on reductions in cybersecurity insurance premium costs are also now available. And the savings connection between a strong security posture and good credit standing is also directly linked and consequential. Of course, there are many other benefits that are more difficult to quantify. For example, the value of reassigning staff to more valuable work is notable, especially given the healthcare industry's technology management and cybersecurity talent recruitment and retention challenges.

Both CrowdStrike and Medigate have a great deal of experience articulating the business cases that support investments in security infrastructure. The value analyses that can be provided jointly and separately articulate a detailed, cost-justified roadmap. These business cases not only address the benefits mentioned above, but zero in on the time-value of workflows by job class and the operational savings based on delivered automation. While the value of alternative equipment maintenance (AEM) program enablement is not yet available, capital equipment spend reductions based on improved asset utilization is now being effectively assessed, as access to validated asset utilization data is now available.



ABC Health TEST

BENEFIT INPUTS

DEVICE LIFECYCLE BENEFITS

	EFFORT REQUIRED (MINUTES)	JOB CLASS	VOLUME (YEAR 1)	MEDIGATE IMPACT	
Manually add a device into fixed asset inventory, monitoring lists, maintenance management systems, etc.	21	Clerical staff	600	60%	Details
Manually update a device across fixed asset inventory, monitoring lists, maintenance management systems, etc.	21	Clerical staff	1,560	60%	Details
Manually delete a device from fixed asset inventory, monitoring lists, maintenance management systems, etc.	21	Clerical staff	206	60%	Details
Manually reassign a device in fixed asset inventory, monitoring lists, maintenance management systems, etc.	21	Clerical staff	2,052	60%	Details
Average time to manually find missing devices	60	Clinical staff	31,200	60%	Details
Average time to close a preventative maintenance ticket	120	Biomedical engineer	6,840	60%	Details
Average time to process a manufacturer's recall	120	Biomedical engineer	1,642	60%	Details
Average time to reconcile rental inventories, return and order (per month)	60	Clerical staff	260	60%	Details

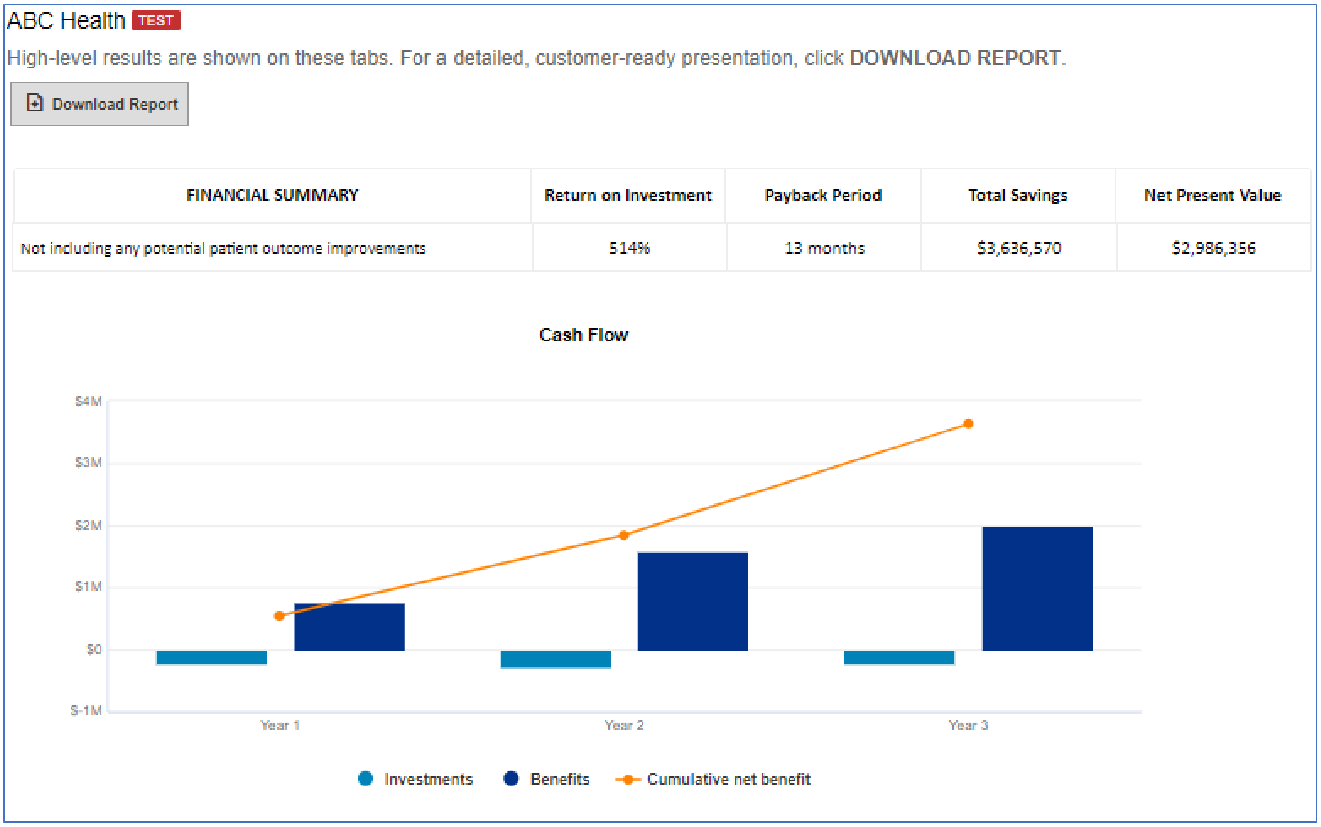
Figure 6. This is a partial screen shot of the Business Value Analysis format that Medigate uses to help reveal the value of delivered automation in device lifecycle management. As a user scrolls down, tasks associated with Network Policy Creation and Network Management workflows are deconstructed the same way.

CrowdStrike commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) that enterprises may realize by deploying the CrowdStrike Falcon Complete™ fully managed endpoint protection service. Over the three-year period, the TEI model found that a composite HDO realizes benefits of $7.25 million USD versus costs of $1.44 million USD, adding up to a Net Present Value (NPV) of $5.81 million USD and an ROI of 403%.[17]

Medigate's Business Value Analysis (BVA) model is solely based on customer inputs and actual values derived from the client's network. The model deconstructs workflows by job class, time-value and total potential savings impact (as determined by a cross-section of appropriate HDO staff). The model also allows the HDO to determine, by facility, how long it will take identified savings to be achieved. In Medigate's experience, customers report original investment payback periods of 10 to 14 months and ~550% ROI over the three-year term of typical analyses.[18]

[17] CrowdStrike Research: https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf

[18] Medigate original research presented in September 2021; www.medigate.io



ABC Health TEST

High-level results are shown on these tabs. For a detailed, customer-ready presentation, click DOWNLOAD REPORT.

FINANCIAL SUMMARY	Return on Investment	Payback Period	Total Savings	Net Present Value
Not including any potential patient outcome improvements	514%	13 months	$3,636,570	$2,986,356

Figure 7. This payback and ROI 3-year analysis represents a HDO composite average.

CONCLUSION

This paper asserts that HDOs must have an intimate understanding of their entire connected landscapes, otherwise, threat intelligence cannot be accurately processed or correlated to the right devices, and remediations will not deliver the desired impact. Although this paper did not detail the myriad possibilities associated with building a sophisticated multi-layered defense, it is not suggesting that other tools of the trade (e.g., SIEM, CMMS, ITAM, VM, etc.) are not needed. Rather, it argues that processes that continuously improve visibility and its orchestration, EDR, and containment capability must be in place, or these additional defense layers cannot perform at their highest intended levels.

- Comprehensive clinical network visibility is “must have” capability, and recent advances can now deliver it. HDOs cannot afford to accept the tradeoffs typical of inferior and/or legacy solutions. The state-of-the-art is the minimum requirement.

- An effective EDR capability is also essential. Because the capability is rapidly evolving to XDR, HDO evaluations must be mindful. Regardless of the acronym (EDR vs. XDR), unified capability that integrates intelligence from all relevant security components is foundational.

- An attack containment strategy (e.g., NAC) provides the HDO a way to control damage and rationalize recovery costs. Insurers know this. Although IoMT data deficits stalled NAC projects in the past, Medigate and CrowdStrike have resolved these problems.

- When premium costs and the coverage available are reasonable, cyber insurance is a solid investment. A new breed of cybersecurity underwriting is rapidly developing and should be investigated, as the approach now taken by the market's newest entrants is setting a standard that will be emulated.

To safely scale the delivery of connected health, security and asset management practices must converge. It’s the only way that individual contributions of limited healthcare staff and systems can become greater than the sum of their respective roles and parts. A common reference foundation must be created, not only to modernize existing infrastructure where possible, but to ensure the performance of future investments in layered capabilities.

About Medigate

Medigate is a healthcare-dedicated medical device security, asset management and operational analytics company. We deliver integrated solutions that break traditional IT, Technology Management and Supply Chain operational silos to eliminate long-standing workflow inefficiencies that manifest as unnecessary costs and risks. Medigate solutions deliver superior clinical network visibility and power workflow automations spanning preventative maintenance to the remediation of threats to security policy enforcement. As further evidenced by its being selected as *Best in KLAS 2021 for Healthcare IoT Security*, the company is widely recognized as the solution market leader. Learn more: https://www.medigate.io/

About CrowdStrike

CrowdStrike, a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates upward of 1 trillion endpoint-related events per day in real time from across the globe, fueling one of the world's most advanced data platforms for security. There's only one thing to remember about CrowdStrike: We stop breaches. Learn more: https://www.crowdstrike.com/

Email: **ContactCrowdstrike-Medigate@medigate.io**

MEDIGATE

CROWDSTRIKE