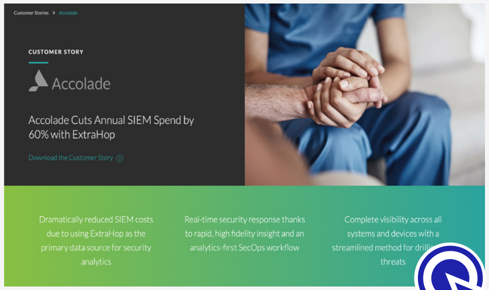
BUILDING RESILIENCY AT SCALE:

Securely Accelerating Digital Transformation



Customer Stories > Accolade

CUSTOMER STORY

Accolade

Accolade Cuts Annual SIEM Spend by 60% with ExtraHop

Download the Customer Story

Dramatically reduced SIEM costs due to using ExtraHop as the primary data source for security analytics

Real-time security response thanks to rapid, high fidelity insight and an analytics-first SecOps workflow

Complete visibility across all systems and devices with a streamlined method for drill threats

Read how a cybersecurity company helped client reduce annual SIEM spend by 60%

A new reality for healthcare cybersecurity

Healthcare's top priority has always been centered around patient outcomes – which is why it is so unfortunate their risk of a security or data breach remains so high.

Because of this patient focus, compared to other industries, hospitals and healthcare organizations have lagged both in their adoption of more secure technologies as well as more comprehensive cybersecurity practices. While the reasons for this are wide and varied, a combination of budget and personnel constraints are at the core.

"Unfortunately, what we see is that many of the technologies implemented in healthcare may not necessarily be adequate in detecting security incidents," said Lee Kim, Director of Privacy and Security for HIMSS. "In this day and age, healthcare IT teams must consider the resources that are required to keep them secure. As the tactics and techniques of threat actors evolve, it becomes a greater challenge for organizations to keep pace and keep patient health information (PHI) protected."

The emergence of COVID-19 has only exacerbated this issue. Charles Alessi, MD, Chief Clinical Officer at HIMSS, said the novel coronavirus pandemic has resulted in a "perfect storm" that has opened health systems up to increased cybersecurity threats. Many provider organizations have expanded their telehealth capabilities – and nonclinical staff may be connecting to the network from outside the four walls of the hospital. For all these reasons, many healthcare organizations are accelerating their move to the cloud.

"The pandemic has delivered a situation where we are relying on digital modalities to both give and receive care," he said. "As a result, we've seen an increased number of cyberattacks on healthcare organizations during this time, which makes it even more important that hospitals heighten their ability to detect and respond to potential threats before any data is compromised."

The Role Frameworks and Privacy Regulations Play in Healthcare Cybersecurity

Read this white paper to learn more about compliance issues and security best practices, featuring NIST, HIPAA and the MITRE Corp.

Healthcare compliance and security frameworks

A number of compliance mandates and frameworks offer help in meeting healthcare's stringent standards – the most notable of which is HIPAA.

Cybersecurity initiatives are vital to meeting HIPAA standards regarding the protection of patient medical records and other PHI. They also play a role in reducing overall security risks not only regarding data, but also threats that could directly affect patient care and patient outcomes. As more patients connect to care online – and as the healthcare internet of things (IoT) continues to grow – having a strong security plan in place not only safeguards patient information, but also patient safety.

A variety of cybersecurity frameworks can help provide guidance as hospitals design a comprehensive strategy to improve security across the enterprise. Many healthcare organizations have relied on best practices from organizations including the Health Information Trust Alliance (HITRUST), the National Institute of Standards and Technology (NIST), and the MITRE Corporation to reduce security risks and better manage security processes. Yet, while these frameworks can provide invaluable insights into how to assess and eliminate risks, they are not prescriptive – there is no one-size-fits-all security plan.

"There are a lot of overlapping areas between these different frameworks – there's quite a bit of commonality – but they don't tell you exactly what you need to do to protect your network," said Hakeem Abunada, Regional Sales Manager for ExtraHop. "There are many vendors out there who offer different security solutions. They don't all do the same things. But, to make sure you are actually getting the tools your organization will most benefit from, you need to first understand where you stand in terms of your framework and then determine what sorts of solutions will help you meet the different security controls or guidelines you've put in place."

"To make sure you are actually getting the tools your organization will most benefit from, you need to first understand where you stand in terms of your framework and then determine what sorts of solutions will help you meet the different security controls or guidelines you've put in place."

Hakeem Abunada | Regional Sales Manager | ExtraHop

Stopping threats before the breach

Take one look at the U.S. Department of Health and Human Services (HHS) Office for Civil Rights' "Wall of Shame," the web page that lists healthcare organizations that have reported breaches of unsecured PHI, and it soon becomes clear breaches are close to inevitable. One of the biggest challenges of effective cybersecurity is that it isn't always clear when your network has been compromised, according to Alessi.

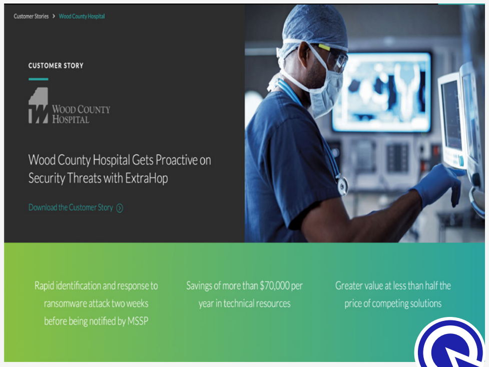
"This isn't like when a thief takes a jewel from the safe and you can see that it's gone. The data doesn't necessarily disappear when a malicious actor gains entry to your network," he said. "Threat detection is very challenging work. You may not notice that you have been compromised unless you have the right systems in place – the trick is to stop it before you are breached."

Guy Raz, a Sales Engineer at ExtraHop, said that cyberthreats can be difficult to identify because it's hard, if not impossible, to deploy agents on every endpoint. This is especially true when you look at the devices that are increasingly more common in healthcare, like IoT and connected medical devices. As for collecting and analyzing logs to detect issues, many organizations turn them off when they are too "noisy," and cyber criminals are quite good at deleting logs to cover their tracks.

"It goes beyond the perimeter north-south communications on your network. Without visibility inside your network, that east-west corridor, you won't see unusual activity that could indicate a malicious actor is present," Raz explained. "If you can't see a potential threat, you can't stop it."

Unfortunately, by hook or by crook, attackers will always find a way inside the network by using the latest phishing schemes, social engineering techniques, or brute force. But, while you may not be able to keep every bad actor out, having the right solutions in place can help you quickly identify that an adversary has infiltrated the network. They can also help you manage the threat before he or she has extracted sensitive data or deployed the ransomware that can affect your organization's ability to deliver care.

> *"Threat detection is very challenging work. You may not notice that you have been compromised unless you have the right systems in place – the trick is to stop it before you are breached."*
>
> **Charles Alessi, MD** | Chief Clinical Officer | HIMSS



Customer Stories > Wood County Hospital

CUSTOMER STORY

WOOD COUNTY HOSPITAL

Wood County Hospital Gets Proactive on Security Threats with ExtraHop

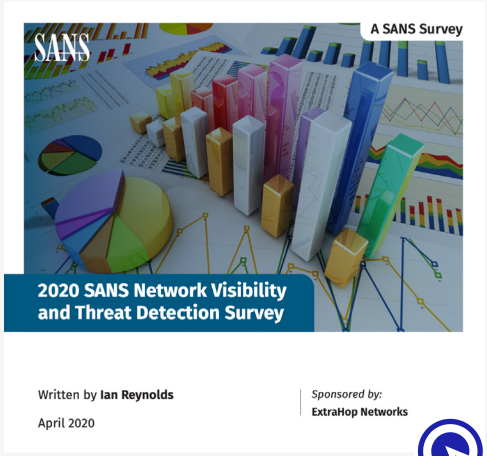
Download the Customer Story

Rapid identification and response to ransomware attack two weeks before being notified by MSSP

Savings of more than $70,000 per year in technical resources

Greater value at less than half the price of competing solutions

Learn how a hospital quickly neutralized a ransomware threat in this case study



SANS

A SANS Survey

2020 SANS Network Visibility and Threat Detection Survey

Written by **Ian Reynolds**

April 2020

Sponsored by:
ExtraHop Networks

Learn how cybersecurity professionals are protecting their organizations' ecosystems in this in-depth survey

Network visibility challenges

The recent pressures on healthcare organizations, namely the COVID-19 pandemic, have led many healthcare organizations to accelerate their move to the cloud to gain the agility needed to support initiatives like telehealth, remote patient monitoring and work-from-home employees.

Connected medical and IoT devices, which cannot be instrumented in traditional ways and are rarely built with security in mind, go largely unseen on the network. Encrypted traffic is another area where organizations continue to struggle with network traffic visibility. Such blind spots put healthcare organizations at a great disadvantage.

"Visibility into network traffic is needed for healthcare organizations to detect if there is unusual activity," said Kim. "Healthcare organizations too often may not have the visibility they need to understand what the threat actor may be doing once inside the network and thus not appreciate the potential impact and consequences of the infiltration."

Raz added that a compromise doesn't have to lead to a breach. When there is complete network visibility into all devices and all communications, healthcare organizations are in a position to stop an attack before any damage is done. The use of machine learning algorithms that learn normal network behavior can monitor activity across a hybrid network, alerting provider organizations that there is unusual behavior that requires further investigation.

"A compromise means an asset is no longer operating in the state we want it to be in," explained Raz. "Maybe someone downloaded malware or clicked a phishing message. Historically, there wasn't a great solution to cover the entire visibility spectrum. If there is a visibility gap, it means you may miss that compromised device – and that's a problem."

Network detection and response solutions provide complete visibility to monitor activity across the entire network. When combined with machine learning, you can detect unusual behavior – if your domain controller starts talking to your accounting server for example – and then investigate and respond to quickly shut an incident down before it can move laterally, escalate privileges and steal personally identifiable information or PHI.

"Network data is the richest source of truth out of all the data sources," Raz said. "And when you are looking at what data is traversing the network, essentially anything associated with an IP address, you can see what's happening at the network level. Many healthcare organizations will address their perimeter first and then their endpoints for point detection and response. But that's not enough – without network data you are still blind to activity inside the network."

"Visibility into network traffic is needed for healthcare organizations to detect if there is unusual activity. Healthcare organizations too often may not have the visibility they need to understand what the threat actor may be doing once inside the network and thus not appreciate the potential impact and consequences of the infiltration."

Lee Kim | Director of Privacy and Security | HIMSS

Healthcare IT News

TOPICS SUBSCRIBE MAIN MENU

Asia Pacific EMEA Global Edition

Global Edition HIMSS20 Digital Coverage

A security success story: Using cloud migration to improve data protection

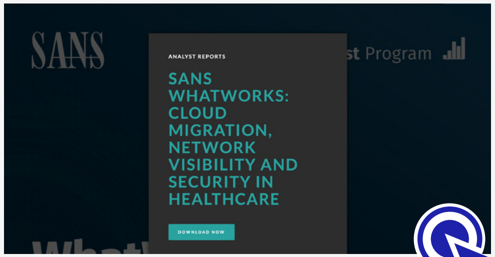
Big transitions can present an opportunity to enact security improvements, but they can also make a complicated process even more complex.

By Kat Jercich | June 05, 2020 | 11:05 AM

Watch what happens

cisco The bridge to possible

Read a success story that shows it is possible to maintain security and network performance while migrating to the cloud in Healthcare IT News



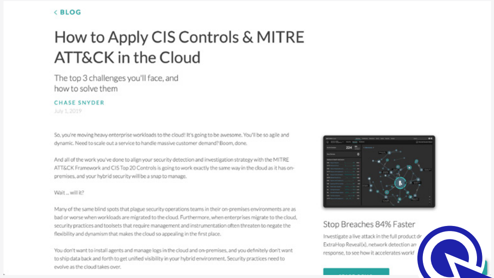
SANS

ANALYST REPORTS

SANS WHATWORKS: CLOUD MIGRATION, NETWORK VISIBILITY AND SECURITY IN HEALTHCARE

DOWNLOAD NOW

Read how a hospital group became an early-adopter of enterprise cybersecurity SaaS as the medical group migrated to a cloud-based infrastructure – and beyond



‹ BLOG

How to Apply CIS Controls & MITRE ATT&CK in the Cloud

The top 3 challenges you'll face, and how to solve them

CHASE SNYDER

July 1, 2019

So, you're moving heavy enterprise workloads to the cloud! It's going to be awesome. You'll be so agile and dynamic. Need to scale out a service to handle massive customer demand? Boom, done.

And all of the work you've done to align your security detection and investigation strategy with the MITRE ATT&CK Framework and CIS Top 20 Controls is going to work exactly the same way in the cloud as it has on-premises, and your hybrid security will be a snap to manage.

Wait ... will it?

Many of the same blind spots that plague security operations teams in their on-premises environments are as bad or worse when workloads are migrated to the cloud. Furthermore, when enterprises migrate to the cloud, security practices and toolsets that require management and instrumentation often threaten to negate the flexibility and dynamism that makes the cloud so appealing in the first place.

You don't want to install agents and manage logs in the cloud and on-premises, and you definitely don't want to ship data back and forth to get unified visibility in your hybrid environment. Security practices need to evolve as the cloud takes over.

Stop Breaches 84% Faster

Investigate a live attack in the full product d ExtraHop Reveal(x), network detection an response, to see how it accelerates workf

Read this blog post to learn how to protect your assets in the cloud

Accelerating the move to the cloud

While cloud adoption had been lagging in healthcare, COVID-19 has pushed greater acceleration across organizations of all shapes and sizes. The cloud provides healthcare delivery organizations (HDOs) with a more agile infrastructure to adapt to changes and scale operations faster than before – telemedicine and temporary remote clinics are two great examples. But, migrating to the cloud also brings new security concerns.

"Misconfigurations are the primary cause of breaches in the cloud," said Kim. "Visibility into cloud workloads remains a challenge for detecting a compromise and protecting the expanding attack surface."

While security associated within individual cloud applications is quite good, it's providing oversight across the number of cloud-based technologies to deliver care that will inevitably put pressure on the system, Alessi said. And, when push comes to shove, it's really up to healthcare organizations to take the lead in securing their assets. Kim said there are often misunderstandings about who is responsible for the security of the cloud and what kind of monitoring is actually occurring.

"Unfortunately, too often, organizations don't realize this until something major has happened," she said. "It's important to understand that the responsibility for protecting patient data lies with the healthcare organization, and that includes all traffic traversing the network."

Many healthcare organizations made the decision to move to the cloud to lessen the burden of security requirements, yet still need to comply with standards like HIPAA, HITRUST or payment card industry data security standard (PCI DSS), according to Raz. With shared responsibility models, he argued healthcare organizations must continue to be active participants in any and all security efforts.

"Cyberthreats in the cloud have been challenging to identify," Raz said. "Luckily, many organizations are starting to think security first when they make these moves. They are thinking about how to operationalize and optimize cloud platforms with complete visibility that will allow for quick detection and quick remediation."

> *"Misconfigurations are the primary cause of breaches in the cloud. Visibility into cloud workloads remains a challenge for detecting a compromise and protecting the expanding attack surface."*
>
> **Lee Kim**

Teamwork: SecOps + ITOps + CloudOps working together

Too often, Raz said, healthcare organizations look at cybersecurity as an old-fashioned perimeter surrounding the network – the old castle and moat approach to security. Yet, as organizations move to the cloud, a successful strategy really requires having a handful of different fortifications – this means that IT, Security and Cloud teams must work in cohesion.

“Organizational and data silos can delay the response to an incident on the network: Without a lightning-quick reaction to an event, security is going to fail,” said Raz. “Early detection of breaches largely depends on how fast you can identify, investigate and respond to any potential compromise so you can minimize threats before the worst happens. Identifying an application slow down for instance, could be a security problem, a network problem or a cloud responsibility. Security is everyone’s problem – and healthcare organizations need to recognize that.”

Having the right solutions and processes in place is required to quickly find answers about what’s happening on the network. If teams are working with the same network data it will improve analyst efficiency which is key to keeping up with evolving threats and bad actors. Healthcare organizations need to look beyond their endpoints and make sure they have full visibility into the devices and communication traversing the entire hybrid network to protect PHI and other valuable data, according to Raz. Network detection and response solutions with embedded machine learning algorithms provide a way to do that.

Abunada added that SecOps, ITOps and CloudOps need to all work together to provide the kind of fast response that leads to true protection. “Organizational silos and data silos mean that your teams are wasting time trying to figure out who is responsible. That is time that should be spent getting to the root cause of a problem. The lag is also providing attackers more time to move around the network to get to your crown jewels.”

> *“Without a lightning-quick reaction to an event, security is going to fail. Early detection of breaches largely depends on how fast you can identify, investigate and respond to any potential compromise so you can minimize threats before the worst happens.”*
>
> **Guy Raz** | Sales Engineer | ExtraHop

RESEARCH REPORT APRIL 2020 | $499

Interop NETWORKComputing InformationWeek DARKReading

NEXT

The State of IT Operations and Cybersecurity Operations 2020

This year’s survey found that organizations are becoming more aware of their security needs and assigning more responsibilities to the security team. However, those changes are resulting in some increasing tension between the teams.

sponsored by ExtraHop

Get this in-depth research report that surveyed IT professionals about the state of IT operations and cybersecurity operations in 2020

ExtraHop

BETTER TOGETHER

An Executive’s Guide to Integrating SecOps and NetOps

Read how synergy drives better results and keeps your organization safer in this white paper about bringing NetOps and SecOps together

The missing link – network, endpoint, logs

To successfully protect the enterprise – and your patients – from potential breaches, Kim said healthcare organizations need to detect and respond to incidents faster.

"It is important to understand your traffic and be able to quickly and efficiently investigate when you come across something that is anomalous," she said. "Too often, healthcare organizations don't even realize that something bad is occurring on the network. And, when you can't quickly block and tackle those threats, the consequences are likely to be severe."

While there is no magic, one-size-fits-all solution to cybersecurity, it starts with shoring up people, processes and technology across the enterprise. It's vital to have a strong strategy in place to make sure your organization is prepared to effectively manage the "inevitable" post-compromise situation, according to Abunada.

"Comprehensive detection and response requires cooperation among security tools – correlating data across endpoint, log and the network solutions is necessary to see everything across the hybrid landscape," he said. "When you apply machine learning to the network data to understand normal vs. unusual network behavior, you gain the situational awareness needed to detect and stop threats before they become a breach.

"It's up to every healthcare organization to come up with their own success criteria because different organizations will find success differently," Abunada continued. "But meeting those goals really does require being able to understand what is happening at every level of your network and then rapidly and effectively responding to any potential threats."

Raz agreed. "What works for financial services or retail might not be the best fit for healthcare," he said. "You want to take a comprehensive approach to gain cross-tier visibility so you can understand what's happening on the network in real time across the entire spectrum. When you have those three data sources working together, you are in a much better position to not just mitigate risks, but also be more efficient from a security operations perspective. That's what you need to keep your network safe."

To learn more about how ExtraHop can help your organization deliver cloud-native network detection and response capabilities to better secure the hybrid enterprise, visit www.extrahop.com/demo/cloud.

ExtraHop

About ExtraHop

ExtraHop delivers cloud-native network detection and response to secure the hybrid enterprise. Our breakthrough approach applies advanced machine learning to all cloud and network traffic to provide complete visibility, real-time threat detection, and intelligent response. With this approach, we give the world's leading enterprises including The Home Depot, Credit Suisse, Liberty Global and Caesars Entertainment the perspective they need to rise above the noise to detect threats, ensure the availability of critical applications, and secure their investment in cloud. To experience the power of ExtraHop, explore our interactive online demo or connect with us on LinkedIn and Twitter.

HIMSS™
Produced by HIMSS
©2020
www.himss.org