IDC

SPOTLIGHT

Sponsored by: Proofpoint

Threat actors are increasingly launching identity-based attacks to masquerade as legitimate users and target valuable healthcare IT resources. Many are going undetected until it is too late and the damage has already been done.

Identity Threat Defense: Protect the Latest Perimeter Exploited by Cybercriminals

May 2023

Written by: Lynne A. Dunbrack, Group Vice President, Public Sector

Introduction

Identity is not only the new perimeter to protect, but it is also becoming the new vulnerability that threat actors exploit to gain access to healthcare IT systems. Historically, security focused on blocking threat actors using technologies such as identity and access management (IAM) tools that provide single sign-on, multifactor authentication, and role-based access. Fast-forward to today. Cybercriminals are using sophisticated social engineering, phishing, smishing, and other exploits to steal credentials, which makes adopting identity threat defense (ITD) technology an imperative to make it harder for cybercriminals every step of the way should they breach the identity perimeter.

Multiple factors contribute to the challenges of protecting the identity perimeter in healthcare institutions, including:

- Fast access to patient information can be a matter of life and death. As such, there needs to be a careful balance between strict security protocols and secure but immediate access to healthcare IT systems.
- Evaporating perimeter security in the areas of Internet of Things (IoT)/connected medical devices. Traditional security approaches are challenged in this attack surface area, and attackers seek to exploit gaps in these systems.
- Data extortion is the crux of ransomware attacks, which presents a different type of risk category.
- Active Directory is a decades-old technology that is complex to manage at scale.

According to IDC's January 2022 *U.S. Healthcare Provider Technology and Connected Health Survey,* 32.6% of provider organizations are increasing their security budgets. Respondents indicated that the top 3 areas where they will increase spending are data security (34.7%), system monitoring (28.7%), and antimalware (26.7%). System access and identity management (23.8%) was in fourth place.

AT A GLANCE

KEY STATS

Healthcare providers that reported that their IT budgets would be increasing over the next 12 months indicated that the top 3 focus areas would be:

1. Data security — 34.7%
2. System monitoring — 28.7%
3. Antimalware — 26.7%

System access and identity management was fourth (23.8%).

(source: IDC's *U.S. Healthcare Provider Technology and Connected Health Survey*, January 2022)

KEY TAKEAWAYS

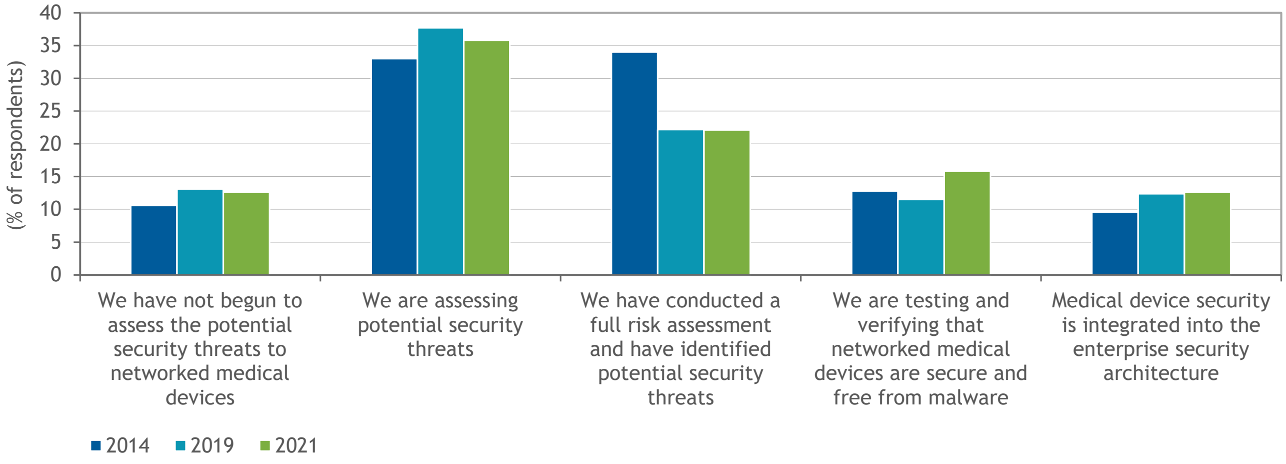
- Identity is the number 1 attack vector.
- Multiple factors contribute to the challenge of protecting the identity perimeter in healthcare institutions.
- Identity threat defense (ITD) is a discipline that combines security tools, processes, and best practices to protect identities.

Identity Threats Are on the Rise

Identity has become a top attack vector in healthcare. As healthcare organizations strengthen security in one area, cybercriminals move on to the next to exploit a new vulnerability. Among the vulnerabilities are the following:

- **Identity sprawl.** The proliferation of human and nonhuman accounts and the use of disparate identity systems to manage them increase the risk of identity-based attacks. The widespread adoption of SaaS applications and line of businesses developing their own applications exacerbates identity sprawl, making it difficult to determine the actual edge of the network.
- **Healthcare workforce flexibility.** Workforce hiring and outsourcing plus staff turnover create their own challenges in provisioning and decommissioning credentials. For example, many healthcare organizations have outsourced certain functions to third parties located across the globe that have no loyalty to the entities they are supporting.
- **Insider risk.** In fact, insider risk is higher in healthcare than in other industries. According to Verizon's 2022 *Data Breach Investigations Report*, threat actors in healthcare are 61% external and 39% internal, nearly twice the percentage of internal threat actors across all industries. If staff believe that there are no consequences to breaches, they may be tempted to sell information about VIP patients or disclose other sensitive data to pay their bills during economically challenging times. That said, most internal breaches are due to human errors such as misconfiguration or unintended exposure of data rather than malicious behavior.
- **Medical device vulnerability.** Securing connected medical devices is inherently complex because of the scale of the problem and their vulnerability is exacerbated by poor security practices. Progress on securing connected medical devices by fully integrating them into the security architecture has been painfully slow as demonstrated by comparing three IDC surveys that span seven years (see Figure 1). It is not uncommon for medical devices to still have their default passwords and settings, which can be easily discovered in manuals posted online by threat actors.

FIGURE 1: ***Progress Healthcare Organizations Have Made in Security-Connected Medical Devices in the Past Seven Years***



n = 95

Source: IDC's U.S. IoT Decision Maker Survey, 2014, 2019, and 2021

What Is Identity Threat Defense?

The term identity threat defense (ITD) is often used as if it were referring to a class or category of security tools. ITD is more than that. It's a discipline that combines security tools, processes, and best practices to protect identities. ITD spans the entire life cycle of the attack — before, during, and after. It's a comprehensive solution that includes both prevention and detection capabilities. Attractive deception targets can be deployed to draw a bad actor away from real targets, thus creating bottlenecks that make traversing the network more difficult. When a compromise is detected by ITD — whether from internal or external sources — remediation is initiated via actionable recommendations and alerts and monitored by dashboards.

Anatomy of an Identity Threat Attack

To build a robust ITD strategy, healthcare organizations need to understand the following fundamental steps in an identity threat attack:

- **Discover credentials.** Typically, threat actors steal users' credentials through social engineering tactics or by compromising Active Directory, or they buy the credentials on the dark web through access brokers.
- **Breach identity perimeter.** Once threat actors have credentials, they can breach the identity perimeter, compromise other user credentials, and move about the network undetected.
- **Escalate privileges.** Once inside the network, threat actors will often take advantage of configuration oversights, poor security hygiene, or application design flaws to gain unauthorized elevated access to resources that are generally inaccessible to most users.
- **Move laterally to more valuable targets.** Once threat actors have obtained higher privileges, they can traverse the network in search of sensitive data and more valuable assets while also obtaining increased privileges using various tools to continue deeper into the network.
- **Attack.** Threat actors have plenty of time to explore the network; collect more information about systems, applications, and accounts; identify security systems; obtain more credentials; and escalate privileges. So, it's no surprise that data theft, system compromises, or ransomware extortions might occur weeks or months after the original breach.

Thwarting Identity Attacks

Here's how ITD prevents small breaches from becoming catastrophic:

- **Protects the new perimeter.** ITD identifies vulnerabilities in identity and access management systems. This information helps with mounting a response in the event of a breach.
- **Places obstacles to limit or prevent lateral movement.** If threat actors breach the identity perimeter, ITD makes it difficult for them to traverse the network to gain further access or escalate privileges. Deception targets lure threat actors away from real targets. Unlike honeypots, these targets monitor and collect information to identify identity attackers as well as their tactics and their technologies. Thus they provide threat intelligence to help with an effective defense.
- **Monitors data handling.** ITD monitors how data is handled by all users to identify any anomaly that suggests data exfiltration is occurring. For example, are files being chopped up into smaller sizes to make them easier to upload to another system or application? Is this user commonly online at this hour and accessing this IT resource?

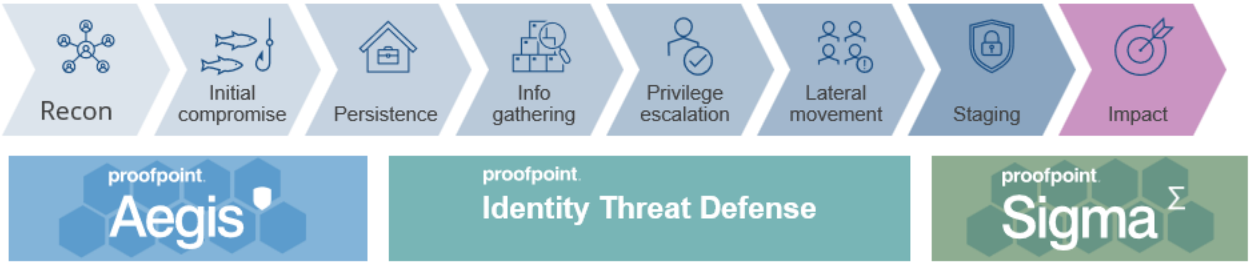
Considering Proofpoint

Founded in 2002, Proofpoint Inc. is a leading cybersecurity company serving more than 13,000 enterprise customers worldwide. On average, Proofpoint analyzes 2 billion emails, 26 billion URLs, and 17 million attachments and monitors 17 million cloud accounts per day using advanced artificial intelligence (AI) and machine learning (ML). It uses these insights to improve the security posture of its clients. Proofpoint's largest customer segments are financial services and healthcare.

Proofpoint has three platforms that are designed to break the attack chain (see Figure 2):

- **Aegis Threat Protection Platform** provides AI/ML-powered threat protection against business email compromise, phishing, ransomware, supply chain threats, and advanced threats.
- **Identity Threat Defense Platform** was part of the Illusive Networks acquisition and includes Illusive Spotlight and Illusive Shadow.
- **Sigma Information Protection Platform** protects information from external and internal threats and secures access to web and cloud services.

FIGURE 2: ***Proofpoint — Protecting Against Advanced Email Attacks and Identity-Based Threats Across the Attack Chain***



Source: Proofpoint, 2023

In addition, Proofpoint provides a fourth platform — Intelligence Compliance Platform — that enables corporate and regulatory compliance while protecting a healthcare organization's digital engagement channels. The company also offers a full complement of premium managed services for email threat protection, information protection, and security awareness.

In December 2022, Proofpoint acquired Tel Aviv–based Illusive Networks. Illusive provides ITD and strong post-breach defense capabilities to prevent ransomware and identity-based data breaches across the attack chain. Illusive identity risk management helps organizations prevent, detect, and respond to cyberthreats:

- **Illusive Spotlight** provides continuous discovery of identity vulnerabilities by inspecting Active Directory for misconfigurations, privileged access management gaps, and exposed endpoints and servers. Spotlight automatically purges identity risks from endpoints and servers. The Illusive Identity Intelligence Dashboard highlights and prioritizes identity risks, thus providing security and risk management teams greater visibility into identity vulnerabilities and threats.

- **Illusive Shadow** deploys agentless deceptions that mimic artifacts such as credentials, data, and connections that would be useful to attackers in their quest to escalate privileges and move unfettered across the network. Shadow immediately issues alerts should an intruder take the bait while capturing forensic data about the attacker that the healthcare organization's security team can use to stop the attack. A deterministic approach to detection based on how the intruder interacts with the deceptions greatly reduces the high false positives typically found in probabilistic approaches that rely on signatures or behavior analysis, thus freeing up security operations center staff to focus on higher-priority incidents. The Shadow management console provides visibility in how close intruders are to critical assets and intelligence on the attacker's activity.

Identity Threat Defense Use Cases

Deployed together — along with Proofpoint's extensive offerings — Illusive Spotlight and Illusive Shadow address the following high-priority use cases:

- **Detect advanced persistent threats (APTs) and targeted ransomware attacks early.** Successful intervention and remediation start with detecting breaches early, before threat actors wreak havoc. Proofpoint Aegis Threat Protection Platform helps healthcare organizations protect themselves against APT attackers.
- **Impose barriers to prevent threat actors from gaining unfettered access to data.** Illusive Spotlight makes it more difficult for the attacker to "live off the land" by continuously and automatically identifying and cleaning up credentials and pathway information that are the fuel for the attacker. Illusive Shadow deploys deceptions that mimic data that threat actors need to advance toward more critical assets. Real-time alerts are issued when these deceptions are accessed, enabling healthcare organizations to react and stop lateral movement and privilege.
- **Identify data traffic anomalies and understand how data is being manipulated.** The challenge with compromised credentials is determining whether the threat actor is acting with malicious intent or is a legitimate user simply mishandling the data inadvertently. Proofpoint combines artificial intelligence and machine learning with behavioral analytics in its Supernova Behavioral Engine to discern the difference so healthcare organizations can take the appropriate action.
- **Prevent data exfiltration.** Proofpoint Sigma Information Protection Platform delivers risk-aware data security that can perform data loss prevention (DLP) in real time. Proofpoint protects sensitive data in cloud apps and blocks sensitive content from being exfiltrated via command and control, downloaded to unmanaged devices, and being emailed out.
- **Secure IoT and medical devices.** Illusive Shadow's deceptions can emulate medical devices and appear real to threat actors traversing the network looking for vulnerable devices to exploit.
- **Prevent data extortion.** At the heart of the ransomware attack is data extortion because of the inherent value of healthcare information not only to the healthcare organization and its patients but also to cybercriminals who sell it on the dark web. In addition to its identity threat defense products, Proofpoint Aegis Threat Protection Platform stops the ransomware attack by blocking malicious email and shifting defenses further up the ransomware attack chain.

Challenges

The market challenges that Proofpoint and its customers face can also present opportunities for a company with strong healthcare experience and a broad product portfolio:

- **Cybercriminals are constantly evolving their craft to exploit new vulnerabilities such as identity.** Threat actors are highly responsive to new opportunities to exploit healthcare organizations. Identity-based attacks are increasing across industries. However, they are particularly pernicious in healthcare because of the need for immediate access to sensitive health information to deliver optimal healthcare services to patients.
- **Heightened demand for security products and professionals.** The growing volume of phishing and other cybercriminal attacks inside and outside the healthcare industry increases the demand for security products and professionals. This increased demand also makes it harder for healthcare organizations to attract and retain highly skilled IT security talent. As such, they lean on their security vendors to provide managed security services. A vicious cycle ensues.
- **Balancing robust security and user access to IT systems and data.** There is a constant struggle between IT security teams that want to lock down access to IT systems and line-of-business executives who want ready access to data in those systems. If security protocols are too strict, end users will find ways around them, often making end users more vulnerable to social engineering and IT systems more prone to attack.
- **Navigating acquisitions**. Thoma Bravo, a private equity firm active in the cybersecurity market, took Proofpoint private in a $12.3 billion deal in April 2021. Proofpoint is no stranger to acquisitions, having spent more than $1 billion to acquire 17 companies. Illusive Networks, its latest acquisition, was completed in December 2022.

Conclusion

Healthcare security professionals must stay hypervigilant to escalating identity threats to defend the identity perimeter and protect valuable and sensitive IT assets. The key to protecting healthcare IT against identity-based attacks is to take a three-pronged approach:

1. Protect identities from being compromised in the first place.
2. If identities are compromised, impose barriers to lateral movement and privilege escalation.
3. Use deceptions to collect forensic data that helps with response and remediation.

It should also be noted that people and identities are the common link across the attack chain. Teach users how to properly handle data. Explain what will happen if they don't protect data. Users will continue to be careless or take shortcuts — or even behave maliciously — if they believe there are no repercussions for their actions.

Healthcare security professionals must stay hypervigilant to escalating identity threats to defend the identity perimeter and protect valuable and sensitive IT assets.

IDC believes that the identity threat defense market will be important for healthcare cybersecurity. To the extent that Proofpoint can address the challenges described in this paper, the company has a significant opportunity for success.

About the Analyst

Lynne A. Dunbrack, *Group Vice President, Public Sector*

Lynne Dunbrack is Group Vice President for Public Sector, which includes IDC Government Insights and IDC Health Insights. She manages a group of analysts who provide research-based advisory and consulting services for payers, providers, accountable care organizations, IT service providers, and the IT suppliers that serve those markets. Lynne also leads the IDC Health Insights Connected Health IT Strategies program.

MESSAGE FROM THE SPONSOR

More About Proofpoint

Proofpoint, Inc is a leading cybersecurity and compliance company that provides health institutions protection and visibility for their greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps healthcare stop targeted threats, safeguard their patient data and intellectual property, and make their users more resilient against cyberattacks. Leading healthcare organizations of all sizes, including more than three-fourths of the Fortune 500 healthcare institutions, rely on Proofpoint for people-centric security solutions that mitigate their most critical risks across email, the cloud, social media, and the web before they cause lasting harm. More information is available at www.proofpoint.com/healthcare.

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.