Case Study

Healthcare

AT&T Cybersecurity

# A winning combination of always-on support and flexibility

**Solutions**

- AT&T Managed Threat Detection and Response
- AT&T Managed Endpoint Security with SentinelOne
- AT&T Managed Vulnerability Program with Tenable
- Penetration testing services with AT&T Cybersecurity Consulting
- Private fiber connectivity between multiple sites, internet service, MPLS

**Highlights**

- Access to support that is always just a phone call away
- A true 24/7/365 extension of the in-house team
- Customization and flexibility for proactive security
- Reaping the cost benefits of consolidation with an integrated suite of managed services

## Overview

This mid-sized healthcare and manufacturing company is one of the largest manufacturers of biomedical devices in the United States. The company has been in business for several decades and is headquartered in Fort Lauderdale, Florida, with additional presence elsewhere in the US and globally.

## A longstanding customer

The company has been a customer of AT&T for the last decade or so, initially engaging for bundled internet and fiber optics services and then adding various cybersecurity services over time as the cost advantages of consolidating to one vendor became apparent.

The AT&T Cybersecurity and local AT&T fiber teams work together to assist the company in achieving its goal of maintaining the key principles of information security: confidentiality, integrity, and availability. The AT&T fiber service delivers more than 99.9% uptime, and the company's suite of AT&T Cybersecurity services helps keep its business environment secured with minimal downtime.

AT&T Business

## Lower costs and less complexity

Managing solutions from multiple vendors can lead to increased cost and complexity. As this healthcare manufacturer has continued to invest in a growing portfolio of services from AT&T, it has reaped the benefits that consolidation offers. Its status as a longtime customer has been an advantage during pricing negotiations on additional services.

> "For us, having one vendor to partner with and one hand to shake is of great value."
>
> – Director, Infrastructure and Security

## Balancing budget needs and staying agile

Prior to moving to AT&T Cybersecurity, the healthcare manufacturer worked with other providers such as IBM Security QRadar and ArcSight for its managed detection and response (MDR) needs. However, the company's IT decision-makers sought an alternative after pricing doubled.

With AT&T, the company found flexibility that is atypical for a Fortune 500 company. Not only was AT&T willing to adjust pricing to fit within the company's budget, but it has also been willing to adapt to its changing needs, and this has been crucial in helping the company stay agile and secure.

Initially, the company's IT decision-makers deployed the AT&T USM Anywhere platform, which is the technology that underpins the AT&T MDR service, AT&T Managed Threat Detection and Response[1]. They selected the platform because of its large customer base and because they found its ease of deployment and ease of use to be a good fit for their mid-sized business and IT systems.

## An extension of the in-house team

The company has a small IT and security team but a big security mindset—security is everyone's responsibility—from the help desk to the security engineers. Even with this approach, company leadership recognized the need to outsource their security operations and bring on a team that could provide them with the 24/7/365 dedicated cybersecurity coverage that they did not have the resources for. At the same time though, they did not want to completely relinquish control. They needed a team that would function as an extension of their own team rather than as its replacement, and this is what they got when they upgraded to AT&T Managed Threat Detection and Response.

The company had used endpoint protection products from other vendors such as Symantec and Cylance but wanted an option with more focus on innovation and better support. The decision to go with AT&T Managed Endpoint Security with SentinelOne[2] was a logical next step, not only because of its smooth integration with MTDR but also because of the cost benefits that attend consolidation. And later on—for similar reasons, the company chose to add Tenable through the AT&T Managed Vulnerability Program[3]. The company has also commissioned several penetration tests[4] through AT&T Cybersecurity Consulting.

## Support that is always available

For the company's IT and security leadership, their strong relationship with the AT&T sales and SOC teams is key. When asked what they consider to be the biggest differentiator in the services provided by AT&T, the answer was unequivocal: the high level of support they receive from these two teams.

> "When problems arise, these teams are always just a phone call away. For me, that's important. When we have challenges, they can quickly escalate and help us resolve any problems we encounter."
>
> – Director, Infrastructure and Security

> "Sometimes sellers make a sale and then move on to the next one, right? That doesn't happen with this sales team. They are around if there are issues—and they don't really let go, which is great."
>
> – Director, Infrastructure and Security

In any service, issues will come up that need to addressed, and these can range from challenges with process to personnel or technology issues, and everything in between. However, the issues themselves are not as important as the speed at which they are escalated and resolved, and this is where the "always-on" mindset of the AT&T sales and SOC teams makes a big difference for the company. Its IT and security leadership depends on and indeed expects 24/7/365 availability and support—and they are not disappointed.

When the company encounters challenges, they are able to quickly escalate to their sales team and get help resolving them. As the company's Director of Infrastructure and Security says, "I call my salespeople on the weekends—and they pick up."

The AT&T SOC team is similarly highly responsive.  As with every AT&T MDR customer, the company has a Customer Experience Manager (CEM) who is the primary point of contact between the company's IT and security team and various members of the

AT&T SOC team including the company's designated threat hunter and its incident responders. The CEM coordinates weekly meetings with the AT&T SOC team and company personnel to review findings and determine whether issues require escalation or investigation.

## Finding flexibility

Not every environment is the same and not every security team is the same. The AT&T team has guided the company's IT and security staff through deployment and implementation of the various products and services it has purchased, but what has been most important for the company is that the AT&T team is willing to work with it on customizing aspects of the service and technology to fit its specific needs.

The company has a highly mature staff that prefers to take a more hands-on approach, and at times this has required pushing for adjustments and improvements, such as requesting broader access to the technology. The AT&T SOC team has been flexible and has worked to accommodate these requests, whether this be to adjust tuning or to work with AT&T developer teams to give the company the access it needs to be proactively involved in improving its cybersecurity posture.

## Technology and support that evolve with the business

As cybersecurity products and services evolve to meet the challenges of a constantly shifting threat landscape, it is critical that organizations have in place the resources and support they need to address these challenges. The company's Director of Infrastructure and Security noted the benefits that AT&T Cybersecurity's suite of managed services provides in this area: "Having the right team, the right technology, and the right support has helped us throughout the years. We are always looking for new technologies that can protect the business, and I am confident that the AT&T Cybersecurity team will continue to help us integrate and implement solutions that can keep the company secured."

[1] https://cybersecurity.att.com/products/managed-threat-detection-and-response

[2] https://cybersecurity.att.com/products/sentinel-one

[3] https://cybersecurity.att.com/products/managed-vulnerability-program

[4] https://cybersecurity.att.com/products/penetration-testing-services