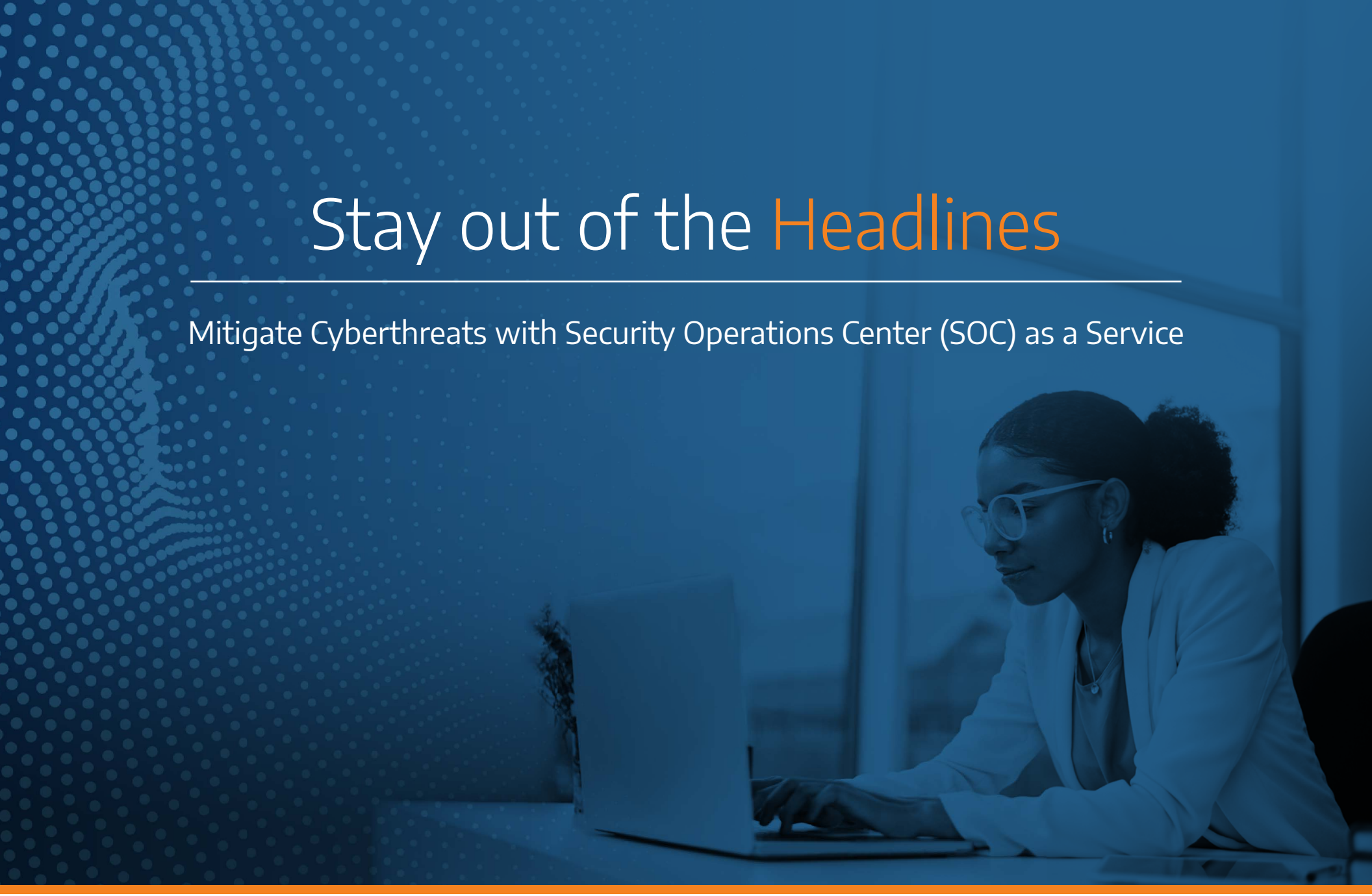
Stay out of the Headlines

Mitigate Cyberthreats with Security Operations Center (SOC) as a Service



ARCTIC WOLF | CIO DIVE

Custom content for Arctic Wolf
by **CIO Dive's Brand Studio**

Unprecedented advancements in technology continue to change our daily lives, so organizations must remake themselves into digital-first operations to ensure their futures. They must adapt to a dynamic business world that embraces innovative technologies, such as cloud computing, artificial intelligence (AI), and other breakthroughs.

And one "industry" that is booming as a result of all these advancements—and the disruptions they cause—is cybercrime.

"Cybercriminals are using more advanced and scalable tools to breach user privacy, and they are getting results," according to a World Economic Forum article. There's a reason bad actors leverage the same tools as sophisticated enterprises and governments. "AI systems are cheap, scalable, automated, anonymous, and they provide physical and psychological distance for the attacker, diminishing the immediate morality around cybercrime," the WEF writes. "With new advances in AI-driven technology, utilizing AI in cyberattacks will become an even more popular and dangerous trend."

No wonder cybersecurity professionals worldwide say the odds are better than 50-50 that their organizations will experience a cyberattack this year. For its State of Cybersecurity 2019 report, industry association ISACA polled more than 1,500 cybersecurity professionals around the world. With 46% of respondents seeing an increase in cyberattacks over the past year, 60% predicted it was likely (26%) or very likely (34%) that their enterprises would experience a cyberattack in 2019.

What's at Stake?

The effects of security breaches and cyberattacks span the financial, reputational, and personal realms. Here are a few data points to consider:

- According to the latest data breach cost report from the Ponemon Institute and IBM, the average cost to an organization of a data breach is $3.9 million globally, which is 12% higher than five years ago, but in the United States, the average cost is more than twice that: $8.2 million.

- Organizations in regulated industries, such as healthcare and financial services, are more likely to lose customers and clients after a breach. Customer loss averages 7.0% at healthcare organizations and 5.9% at financial services companies; the overall average is 3.9%, the institute found.

- Security leaders are increasingly worried about potential damage to customer retention and their brand reputation. The 2019 CISO Benchmark Study from Cisco was based on a survey of 3,200 security leaders in 18 countries. In 2019, one-third of respondents agreed they were concerned that "continued negative sentiment around data breaches and the prevalence of malware … makes consumers wary," up from 26% in 2018. Thirty-two percent agreed in 2019 that "household names become synonymous with a large attack for years," up from 27% a year earlier.

- Those concerns are not unfounded. In an IBM-Harris Poll Survey of consumers conducted in August 2019, an astounding 94% of respondents agreed strongly (64%) or somewhat agreed (29%) that "businesses should be doing more to actively protect consumers against cybersecurity threats."

- Finally, cyberattacks have an often unrecognized effect on the well-being of employees, from security teams on the front lines all the way up to top leadership, according to reports in CIO Dive. In one study, 56% of CTOs and CIOs with security responsibilities reported stress-related conditions, as did 51% of other tech executives. There's reason for this; after major security breaches, 23% of CEOs leave their companies. In another report, 12% of CISOs feared they would be fired after a breach, even though only 1% actually were dismissed.

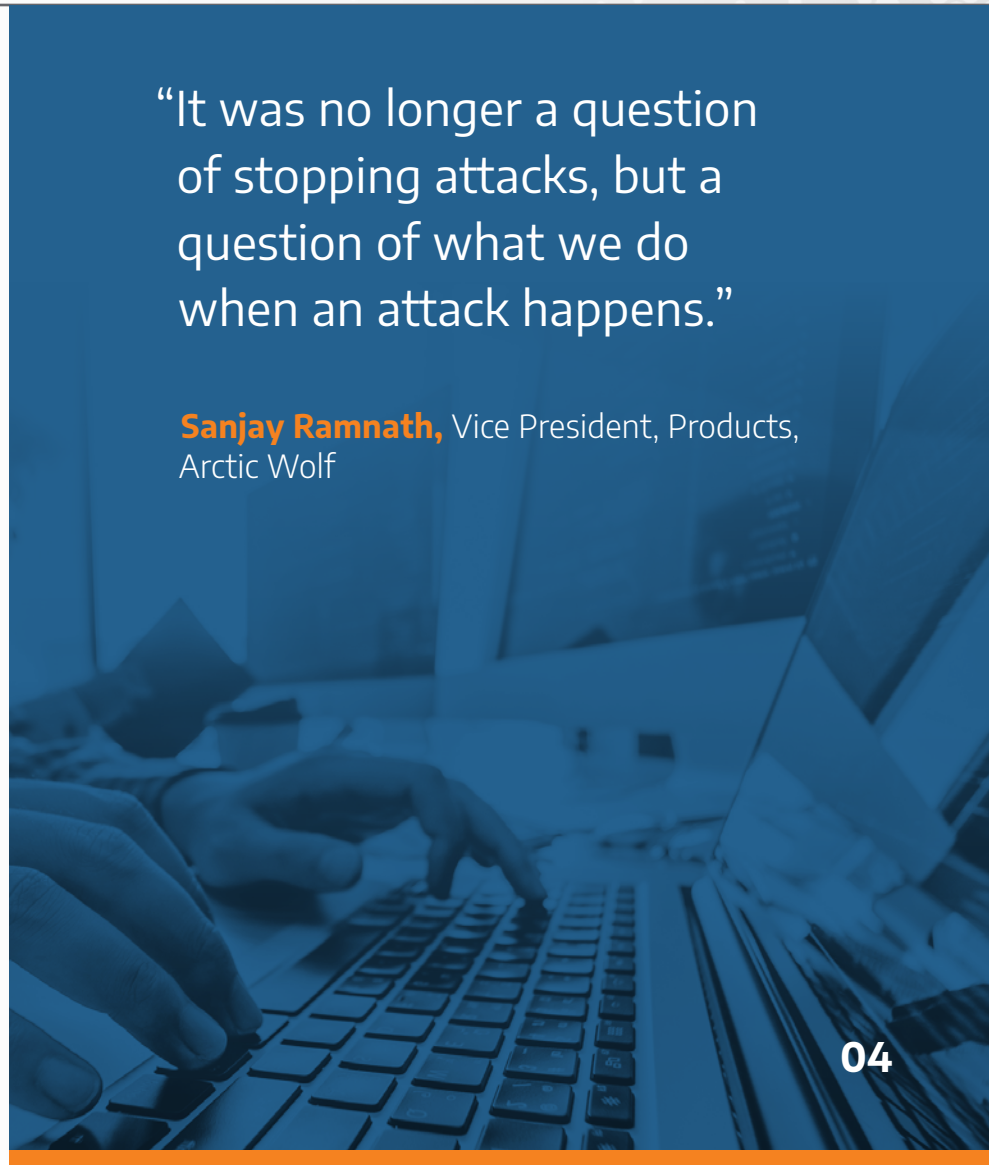
Cybersecurity Solutions
Pivot on Tactics

Along with the explosion in the number and types of cybersecurity threats, providers of security solutions are growing rapidly. Gartner projects global spending on information security products and services will increase 9% over 2018 to reach $124 billion in 2019. And the way threats are addressed has taken a 180-degree turn.

"If you go back a decade or so, security was all about blocking threats," said Sanjay Ramnath, Vice President, Products at Arctic Wolf. "The principle was that we could stop bad actors from coming into our network with anti-virus solutions, firewalls, web proxies, email security, and the like."

Over time, however, attacks became more prevalent and more sophisticated. "It got to the point where we had to change that fundamental hypothesis. It was no longer a question of stopping attacks, but a question of what we do when an attack happens," Ramnath added.

Organizations often deploy their own technology yet also look to outside services to avoid the headlines and other negative effects of cyberattacks.



ARCTIC WOLF

> "The most important thing is to quickly identify when there is an intrusion and to take action before something catastrophic happens."

Sanjay Ramnath, Vice President, Products, Arctic Wolf

An example of this is Roper Technologies, a diversified company operating dozens of businesses that design and develop software and engineered products and solutions for a variety of niche B2B markets. Roper uses Arctic Wolf™ Managed Detection and Response, which is part of the Arctic Wolf security operations center (SOC)-as-a-service.

"Anybody can put in a tool that scans, essentially, the same kinds of data," said Karine Thibault, Director, Cybersecurity at Roper Technologies. "What Arctic Wolf does for us is triage. They use human analysis to tell us when we have an issue that's really important."

"What makes Arctic Wolf unique is that we've integrated people, process, and technology," Ramnath said. "We have our own technology stack, a cloud infrastructure, and the ability to collect massive amounts of data across multiple environments, including our customers' third-party solutions," he said. "On top of that, we provide what few other managed-security providers can, and that is a concierge experience."

Given the relatively high likelihood that an attack or breach of some kind will happen, "the most important thing is to quickly identify when there is an intrusion and to take action before something catastrophic happens," Ramnath said. That's where engineers dedicated to individual accounts—who know the typical patterns in those enterprises—are the first line of defense.

"There's so much data, and networks are so distributed, that it's not enough to have a platform that aggregates and correlates data," he said. "You have to manage the data and convert it into actionable outcomes."

Indeed, speed is of the essence when an intrusion or security abnormality is detected. According to the Ponemon Institute/IBM research, "the cost of a breach with a life cycle of more than 200 days is $1.2 million higher than a breach with a life cycle of less than 200 days." Further, because of legal and regulatory costs, as well as customer attrition, almost half (47%) of the costs don't occur until more than a year after the incident.

Turning Down the Noise

From an industry perspective, "vendor overload is a massive problem in cybersecurity," Thibault said. "Whenever there's a problem, all sorts of vendors pop up to try to fix that problem, but each of those options fixes different parts of the problem." Not only do security tools that mitigate one specific problem, called point solutions, have limited utility, but they also don't work well with other vendors' products. Therefore, one root cause can set off alerts in numerous siloed tools.

According to the CISO Benchmark Study, 41% of organizations see more than 10,000 alerts every day, and the report notes that a best practice for managing alerts is to reduce the number of point solutions in favor of more robust systems. Enterprises are heeding that advice. "In 2018, there were 54% of respondents with 10 or fewer vendors in their environment, whereas now this number has risen to 63%," according to the report. "More than one-third (36%) have only 1 to 5 vendors." Those organizations are seeing a significant drop in alert noise, with the report noting that "63% of organizations with only 1 to 5 vendors and 42% of organizations with 6 to 10 vendors saw fewer than 5,000 alerts per day."

Since Roper Technologies began using SOC-as-a-service, Thibault no longer worries about alerts until they reach a high threshold of importance. "Instead of getting notifications every five seconds that something is popping up, Arctic Wolf only contacts me when they vetted something as a potential issue that really requires my attention," she explained.

Arctic Wolf uses machine learning to filter the data, but "our team of security engineers ultimately makes the decision on whether something is a real threat or not for the customer. That requires a certain level of expertise and security knowledge, as well as the ability to correlate multiple pieces of data," Ramnath said.

> "Whenever there's a problem, all sorts of vendors pop up to try to fix that problem, but each of those options fixes different parts of the problem."
>
> **Karine Thibault,** Director of Cybersecurity, Roper Technologies

Cautionary Tales of Cybercrime

What can security professionals learn from recent security breaches and malware attacks that have put well-known organizations in the headlines? Let's briefly review what happened in four incidents, all of which fall into highly regulated business categories—banking/financial services, healthcare, legal, and government.

Capital One: Intruder exploits misconfigured firewall

On July 29, 2019, Capital One Financial Corp. issued the type of press release companies dread—an announcement that "unauthorized access by an outside individual" compromised data involving approximately 100 million U.S. individuals and 6 million Canadians. The alleged hacker, whom the FBI arrested, exploited a misconfigured firewall in Capital One's infrastructure in the Amazon Web Services (AWS) public cloud. Although the accused was a former AWS employee, Capital One said that "this type of vulnerability is not specific to the cloud."

Capital One said it expected incremental costs of approximately $100 million to $150 million from the incident, including customer notifications, credit monitoring, technology costs, and legal support. That estimate did not include potential lawsuit verdicts or settlements. Within days of Capital One's announcement, the first major class-action lawsuit was filed, accusing Capital One of "failing to appreciate the security requirements of any business that manages sensitive personal electronic data."

LabCorp and Quest Diagnostics: Third party exposes data from multiple clients

In June 2019, the two largest health-diagnostics companies in the United States, LabCorp and Quest Diagnostics, were dragged into the headlines after the collections agency and billings vendor they both used, American Medical Collection Agency (AMCA), acknowledged it suffered an eight-month-long security breach. An intruder hacked into AMCA's web-payment system to access Social Security numbers, payment-card details, and bank account information, along with basic personal information, involving 11.9 million Quest Diagnostics patients and 7.7 million LabCorp patients. It was subsequently revealed that smaller labs were also affected, meaning that more than 20 million records were exposed, all told. Before the end of June, AMCA's parent company had filed for Chapter 11 bankruptcy protection.

Besides the usual effects of a security breach, LabCorp and Quest face repercussions unique to healthcare. These include investigations from two state attorneys general and inquiries by New Jersey's U.S. senators, as well as possible fines for HIPAA violations. Class-action lawsuits have also been filed.

The AMCA incident is an example of the growing risk of third-party breaches. "A lot of sensitive information goes across organizational boundaries," Ramnath said. Rather than going after a firm with solid security practices, attackers look for loopholes they can exploit with less secure third-party partners.

Public sector: More ransomware attacks on local governments

City and local governments, police departments, and schools appear to have become more frequent targets of ransomware attacks. So Allan Liska, threat intelligence analyst at Recorded Future, decided to find out if that impression was correct. He went through local newspapers and websites nationwide to do a count.

"It does appear that ransomware attacks on state and local governments are on the rise," he writes. Although the number of incidents in 2016 and 2017 reflected the same up and down pattern as ransomware attacks across all sectors, attacks on state and local governments were slightly higher than the general trend for 2018 and the first four months of 2019, the cutoff point in Liska's study. For 2018, Liska found reports of 53 ransomware attacks in local government bodies. The 21 incidents reported through the end of April put 2019 on track for a record-high total.

The uptick is surprising because cybercriminals are much less likely to get money from them, Liska wrote. Seventy percent of the organizations he reached denied paying any ransom.

DLA Piper: Global malware attack envelops law firm

On June 27, 2017, DLA Piper, one of the largest business law firms in the world, was a victim of a malware attack known as NotPetya. Pushed out through an update of Ukrainian accounting software M.E.Doc, the malware swept quickly across the globe through the networks of multinational companies such as Maersk, Merck, and Mondelez.

Although NotPetya first appeared to be ransomware, its "ransom messages were only a ruse: The malware's goal was purely destructive," according to a Wired article. "It irreversibly encrypted computers' master boot records … Any ransom payment that victims tried to make was futile. No key even existed to reorder the scrambled noise of their computer's contents." A White House source told Wired that the worldwide impact of NotPetya exceeded $10 billion.

Spreading from DLA Piper's Ukrainian office, the malware took down 1,500 of the firm's 1,800 servers, infected more than 6,500 PCs and laptops, and crashed all primary communications systems—email, phones, voicemail, video, TelePresence, and Skype/Lync.

The immediate effect was an extra 15,000 hours of overtime for IT teams, but the total cost is estimated in the millions of dollars. On a fortunate note, no client or confidential data were compromised, because everything was wiped away by NotPetya, and DLA Piper said it retrieved all of it from backups.

Conclusion

Although industrywide statistics and details of cybercrimes paint a grim picture of the cyberthreat landscape, organizations can take many actions—alone or with a trusted partner—to improve security and improve detection and response.

The fast growth and changing nature of cyberthreats inform every decision a cybersecurity professional makes today.

"There has been a drastic change in the tactics attackers use. They aren't necessarily going after big companies or well-known companies. Everyone is a potential target," Thibault said. "And there is no perfect technology solution. We can add all the tools in the world, but—at the end of the day—bad actors might find a way in."

In this environment, Thibault added, "prevention is critical, but detection and remediation are a must."

"Prevention is critical, but detection and remediation are a must."

Karine Thibault, Director of Cybersecurity, Roper Technologies

Through the industry's original Concierge Security™ Team, Arctic Wolf provides the scalable managed cybersecurity protection IT-constrained companies need to keep their critical data, network, web-based applications, and devices safe. Working as an extension of your internal team, highly-trained and coveted security experts deliver 24x7 cloud-based monitoring, risk management, threat detection, and response services that protect you from ever-evolving methods of cyber attack. By escalating only the issues that require action, Arctic Wolf eliminates noise, enabling your limited IT resources to focus on other priority initiatives. Personal, predictable protection—it's the Arctic Wolf difference.

Learn More

Custom Content. Targeted Results.

Industry Dive's Brand Studio collaborates with clients to create impactful and insightful custom content. Our clients benefit from aligning with the highly-regarded editorial voice of our industry expert writers coupled with the credibility our editorial brands deliver. When we connect your brand to our sophisticated and engaged audience while associating them with the leading trends and respected editorial experts, **we get results.**

LEARN MORE