Pioneer Telephone Cooperative

Partners with Rapid7 to Secure Critical Communications Services

Products

InsightVM

InsightIDR

InsightAppSec

Industry

Communications & Media

Size

Mid-Market

RAPID7
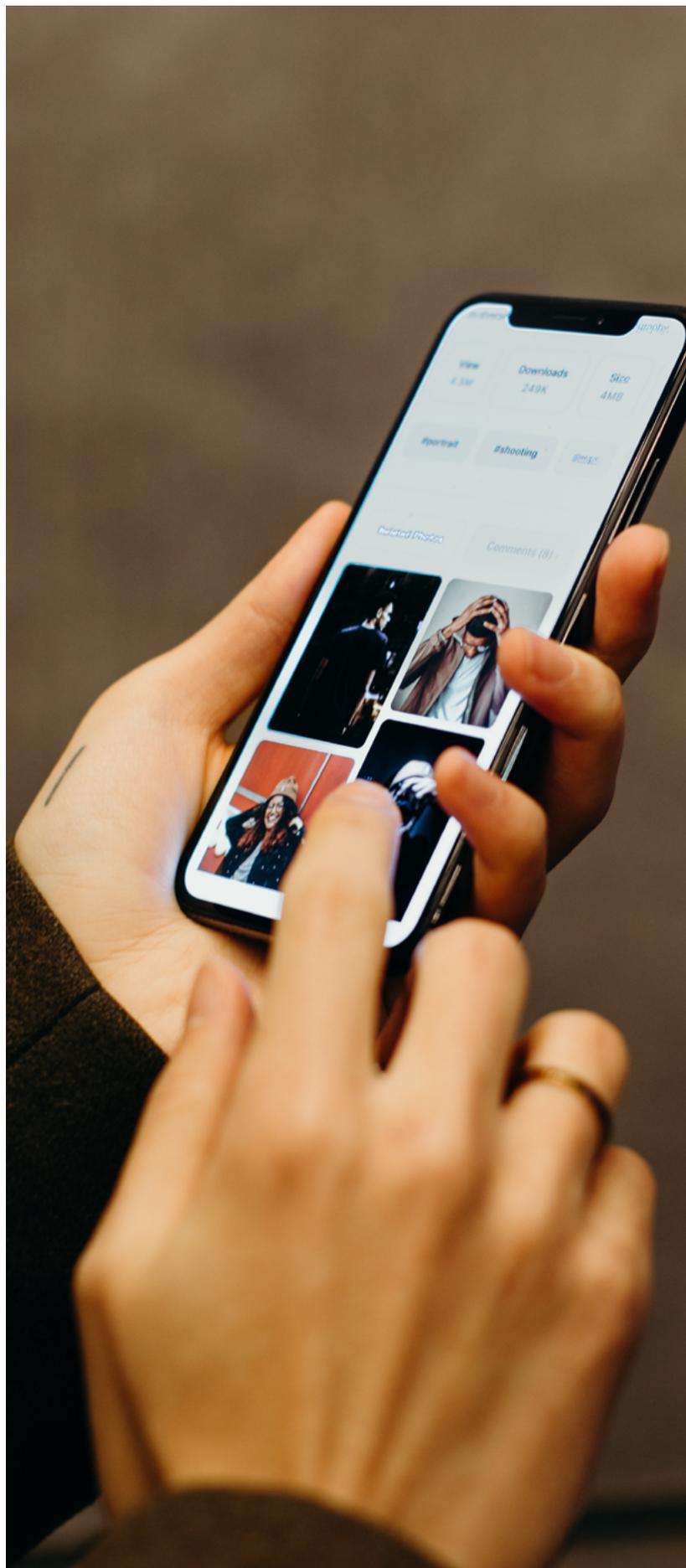
Overview

The Company

Pioneer Telephone Cooperative is the third largest telecommunications cooperative in the United States. The company provides more than 150,000 residential & business customers in Western Oklahoma with advanced telecommunications services, including high-speed/fiber Internet, cellular, and iVideo. Over the years they have adapted to numerous changes in the business environment. Today the company has more DSL or fiber internet customers than traditional telephone customers.

Daniel Hernandez, Information Security Analyst III, leads Pioneer's three-person team handling security across a cluster of networks that include more than 5,000 devices, 1,700 users, a large mobile workforce and a corporate structure with multiple business groups.

The Challenge

The biggest cybersecurity challenge facing Pioneer is the ability to manage increasing levels of vulnerabilities with a small team. Their challenge is compounded by new types of high profile, yet deeply embedded, vulnerabilities, such as Log4Shell. "It's a lot tougher for us to ask our developers and system admins if they use a specific type of sub-component of software because they only know about the top-level software that they purchased. And so, it's a lot harder to have that visibility, to understand what's being used under the hood in all these applications," Hernandez says.

RAPID7

The Solution

Pioneer uses the NIST Cybersecurity Framework (NIST-CSF) to benchmark their security program.

"The number one step is to proactively identify the vulnerability," says Hernandez. "You've got to be able to identify what you've got and where you've got it. That is where Rapid7 InsightVM helps. The next thing is to detect potential attacks and threats. And detection is where Rapid7 InsightIDR comes into play. Whether it's happening in real-time or in the past. That's the biggest step."

Another important part of the Pioneer approach is using Rapid7 InsightAppSec to bridge the security gap for applications developed internally. "Our primary goal was to look at apps coded by our internal programmers and available to outside users," states Hernandez. "And I'll tell you, we found a lot of things that were easy to fix but they could have been really dangerous."

Identify Critical Assets And Prioritize Vulnerabilities with InsightVM

It is difficult to overstate how important visibility is for the Pioneer security team. "For me, it's about identifying the critical assets and workloads. Even though I know I can't fix 100% of all the vulnerabilities that are out there, just knowing what and where those issues are, and which of those issues impact critical assets and workloads, is the first step to fixing things in the future," explains Hernandez. With InsightVM the Pioneer security team can prioritize and manage vulnerabilities much more effectively; they can see clearly what needs to be tackled first.

For example, InsightVM enables Hernandez to evaluate the weekly emails he gets from CISA (Cybersecurity and Infrastructure Security Agency). "I see the vulnerabilities and ask: 'Do we have this stuff?' That's where InsightVM comes in, it helps me know what we really have and what we don't have, so we know which of the vulnerabilities apply to us. That is one of the things we value most about InsightVM; it has the capacity to pinpoint actively-exploited vulnerabilities, so we can prioritize and direct our attention where it's needed most."

> **"**
>
> **We like how InsightVM and InsightIDR communicate with each other so you can identify a detection and see what vulnerabilities are affecting a specific user or asset.**
>
> Daniel Hernandez, Information Security Analyst III

RAPID7

InsightIDR Provides Critical Alerts

"We get alerts within the IDR platform that we do have to work on," add Hernandez. "We identify the threat if there is one. Once we've identified it, we contact those who are affected by it and go from there on our response. We can decide to isolate the machine, or to wipe it completely. It just depends on what we're seeing."

One security event that the Pioneer security team will not soon forget was the highly-publicized SolarWinds attack. "We were one of the original 26 organizations hit by the attack a couple of years ago," Hernandez says. "But we had InsightIDR in place so we knew at that time what those indicators were, so we could go back and look at those indicators in a historical context and tell conclusively from the logs that our data was not exfiltrated." InsightIDR was absolutely priceless in knowing that there was nothing else affected. Otherwise, we would've spent thousands of dollars to bring in forensics folks to find out that nothing actually happened".

For Hernandez, the historical information they get from IDR is a huge benefit. "Knowing that I've got all of those logs, that I can go back and look at any time I need to, to go back and look at an incident after the fact and know that I've got sufficient logging in place to understand what had happened, if anything, is critical."

Nurturing Developer Relationship with InsightAppSec

Hernandez is working closely with his IT colleagues to bring an integrated approach to security and InsightApppSec is an important component of this strategy. "A lot of our developers did not have the security background to really understand potential problems. And our security team does not have in-depth developer knowledge," he adds. "But all the evidence provided by InsightAppSec gives us real talking points so we can explain the issues that we're seeing based on evidence provided by InsightAppSec. And then identify the solutions available. This is very helpful."

Hernandez and his security team now meet regularly with their in-house developers to cover any issues that arise with new internal applications. "That's really our way of having an open, ongoing dialogue with our programmers. Instead of just saying to them: 'Hey, please go fix your stuff.' InsightAppSec has helped us bridge the communication gap between our programmers and our security team."
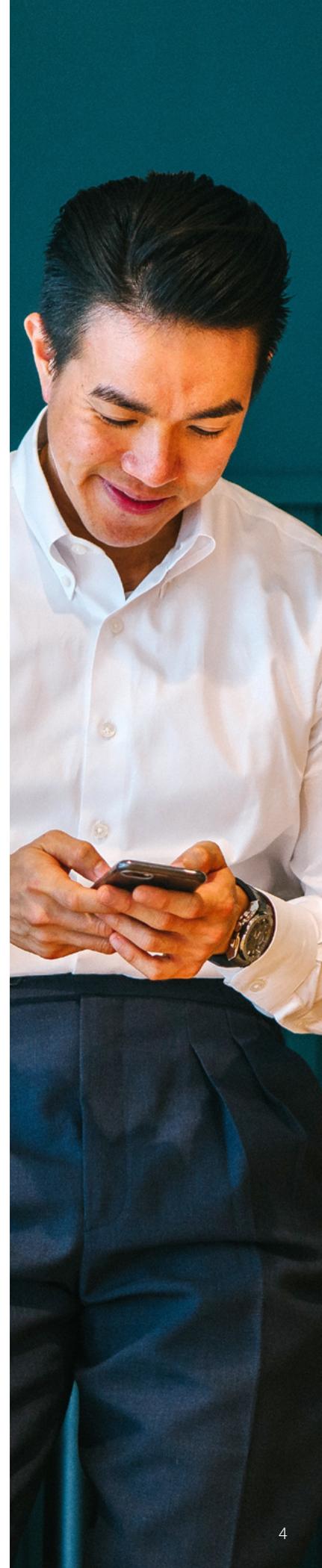
RAPID7

The security team is doing the same with InsightVM; opening those doors and having those conversations on a regular basis with the system admins. "The Rapid7 products will continue to help bridge the gap and nurture those relationships and bring them up-to-speed on the security aspects of things. That's going to help all the way around."

Integrated Security Solutions

Another big plus for Hernandez is the efficiency of the integrated Insight Platform. "Having a single point of contact for support so you don't have to open up tickets for different vendors saves us a lot of time. Also, we like how InsightVM and InsightIDR communicate with each other so you can identify a detection and see what vulnerabilities are affecting a specific user or asset."

Having a single Agent for InsightVM and InsightIDR is also really beneficial by eliminating potential compatibility issues,saving time in installation and maintenance, and receiving detailed vulnerability and threat information directly from our assets. "A single unified Agent has also allowed Pioneer to extend coverage across various parts of their infrastructure. "We do have a lot of folks out in the field," Hernandez says. "Having those ties back to the agent, having those agents report over the internet, not having to be connected to the corporate network, that was a huge gain for us."

A True Cybersecurity Partnership

For Hernandez and his Pioneer team, the goal is steady improvement in risk reduction across the infrastructure landscape they protect. "In cybersecurity, you don't get to check a box very often. Being able to show progress towards that goal is important. That's a big value Rapid7 provides us."

Above all else, Hernandez values the partnership with Rapid7. "The best thing is the partnership and conversations with Rapid7 product managers, and the knowledge that Rapid7 really wants to improve their products and make them useful for customers," concludes Hernandez. That's the first thing that attracted me to Rapid7, and it still does today. That partnership is the number one thing that I've really appreciated."

> **The best thing is the partnership and conversations with Rapid7 product managers, and the knowledge that Rapid7 really wants to improve their products and make them useful for customers.**
>
> Daniel Hernandez, Information Security Analyst III

RAPID7

About Rapid7

Rapid7 is creating a more secure digital future for all by helping organizations strengthen their security programs in the face of accelerating digital transformation. Our portfolio of best-in-class solutions empowers security professionals to manage risk and eliminate threats across the entire threat landscape from apps to the cloud to traditional infrastructure to the dark web. We foster open source communities and cutting-edge research–using these insights to optimize our products and arm the global security community with the latest in attackers methods. Trusted by more than 10,000 customers worldwide, our industry-leading solutions and services help businesses stay ahead of attackers, ahead of the competition, and future-ready for what's next.
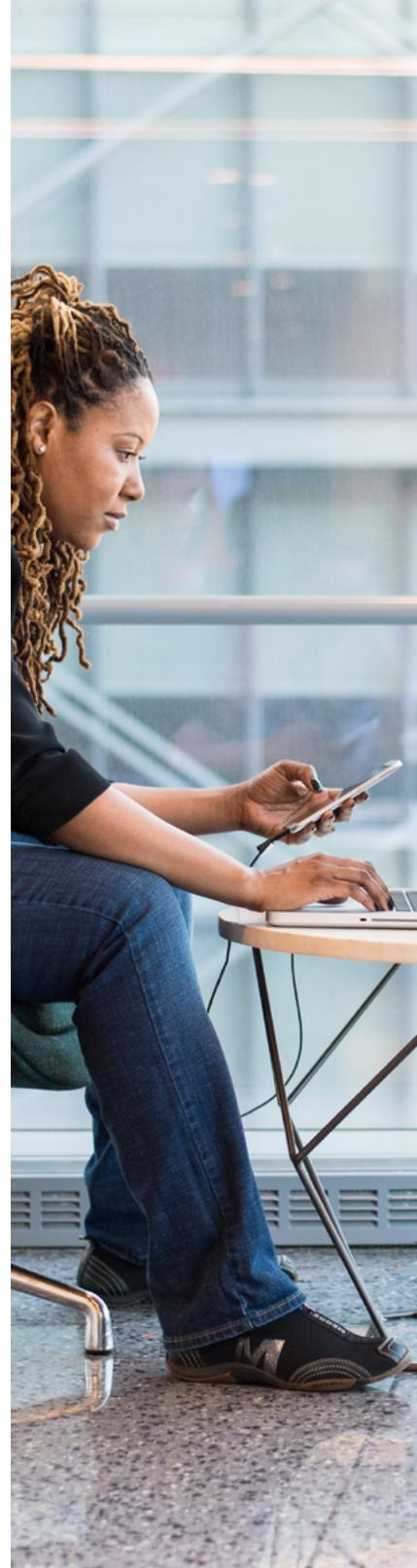
RAPID7

PRODUCTS

Cloud Security

XDR & SIEM

Threat Intelligence

Vulnerability Risk Management

Application Security

Orchestration & Automation

Managed Services

CUSTOMER SUPPORT

Call +1.866.380.8113

To learn more or start a free trial, visit: **https://www.rapid7.com/try/insight/**