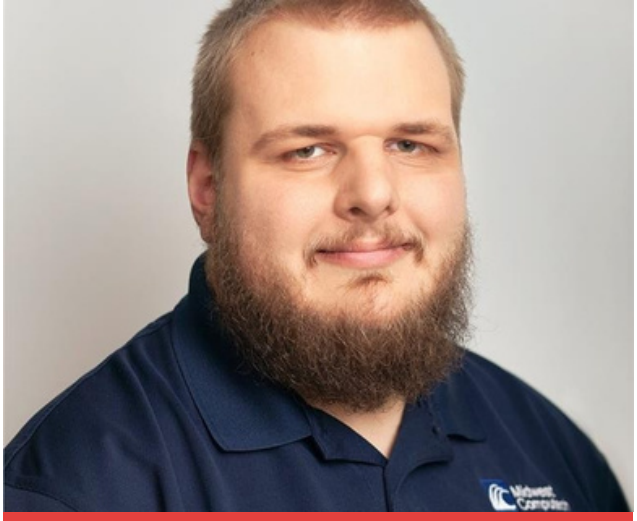
SaaS Alerts
A Kaseya COMPANY

Heartland Business Systems

How Heartland Business Systems (HBS) uses SaaS Alerts to protect their customers, grow their business and make more money.

AWARD-WINNING MSP

- Cisco Partner of the Year
- Microsoft's Midwest Partner of the Year



Cody Brandow
Security Engineer

Located

- Headquartered in Little Chute, Wis.
- 13 offices in eight states

Challenge

For MSPs, clients in the education sector — like school districts — are practically Petri dishes of cybersecurity risk.

There are thousands of end users, including minors. They log on every day to potentially dozens of SaaS apps. Permission settings vary widely for teachers, students and administrators — making management even more complex.

If an administrator's account is breached, important files, data and even money are at risk.

If a student's account is breached, a minor's personal data could be at risk.

This could lead to legal ramifications for the district. Hackers could also use the student's email to send adult content to other classmates.

Imagine a classroom of high schoolers opening THAT email.

+1 (910) 887-3352
sales@saasalerts.com
www.saasalerts.com

To make things even more complex, Cody Brandow, Security Engineer at Heartland Business Systems (HBS), also knows that staff members at the school districts he serves use OAuth to log into their personal apps.

After all, it's easy to just use the same login for everything, right?

Cody's team had no visibility over which users were on which apps. He knew this created a big cybersecurity hole for his education clients.

> **"None of the schools I talked to could answer the question, 'If an account's been compromised, how do we know, and how soon can we take action?'"**
>
> *— Cody Brandow, Security Engineer at HBS*

Solution

Cody knew he needed a SaaS monitoring and remediation tool that could help him track the steady flow of his education clients' SaaS activity — and stop breaches fast.

He found SaaS Alerts (and its automated remediation features!) and was immediately intrigued.

SaaS Alerts' Respond module uses machine learning pattern detection to identify breaches and create instant alerts. This feature runs in the background 24/7, so Cody and his team don't lose sleep trying to keep an eye on all user behavior by themselves.

Using Respond, Cody set up remediation rules that automatically shut down accounts that exhibit suspicious behavior. He also customized those rules for each school district based on their lists of approved apps.

Results

SaaS Alerts has helped Cody and his team:

Log Out at the End of the Day (For Real!)

Outside of nine-to-five business hours, MSPs are (ideally) eating dinner, hanging out with their families or binging reality TV. Those hours, though, are also prime time for hackers — because they know most MSPs are offline.

But thanks to SaaS Alerts' 24/7 monitoring and automated remediation, Cody's team can truly unplug after logging out.

Take this story: At 5:54 one evening, the HBS team received a SaaS Alerts notification about potential suspicious account activity. Ordinarily, this would have been a big "uh-oh" — and an after-hours scramble to grab a laptop.

But SaaS Alerts' Respond module was there to automatically handle the drama. Remediation rules kicked in, and the account was locked by 6:10 pm. *Phew.*

> "This breach happened at a time when nobody was really watching. Without SaaS Alerts, the hacker would have been in there all night."
>
> — *Cody Brandow, Security Engineer at HBS*

Offer More Tailored Cybersecurity Services to Clients

Within SaaS Alerts, Cody can build customized Respond rules based on which apps particular districts have deemed "safe." For example, if Quizlet is approved in District A, then there won't be a Respond rule triggered when a staff member accesses it.

But across town in District B, maybe Quizlet is *not* on the approved list.

If a user starts making flash cards in the app, the Respond rule will kick in and automatically shut it down.

Sign Their Biggest Client

SaaS Alerts doesn't just keep HBS clients safe. It's also a powerful prospecting tool that helped them gain new customers and increase MRR.

In fact, HBS signed its most *lucrative client* — a school district with more than 7,000 end users — thanks to SaaS Alerts.

During a demo, Cody connected the district to SaaS Alerts and quickly noticed something was awry.

The district used Square to process payments at concession stands. But SaaS Alerts showed that those funds were being rerouted to somewhere other than the district's bank account. In total, Cody identified $6,000 of missing funds.

But it wasn't just missing hot dog money. Cody also noticed an account at the district's Central Office was accessing files from multiple locations. School administrators are certainly multitaskers, but they can't be in two places at once.

The district called their cyber insurance company — then promptly hired Cody.

> "When SaaS Alerts identified financial theft *and* a breach at Central Office, it immediately convinced the district it needed to hire us."
>
> — *Cody Brandow, Security Engineer at HBS*

Gain Visibility Over Unauthorized App Usage

Cody's team can also use SaaS Alerts to monitor when staff log into unapproved apps using their professional credentials.

He even identified one teacher who used their official login to access the (wait for it) … Wendy's app.

Ordering a Frosty during lunch is important, sure. But not important enough to risk the entire district's cybersecurity.

On top of identifying unapproved app usage, the team also uses SaaS Alerts data to offer better vetting of districts' approved apps. For example, a seemingly innocuous app used by one client actually had a server outside the U.S.

With SaaS Alerts on their side, Cody's team helps clients design more proactive access policies, protect district data and users, and (crucially) cut down how many chicken nuggets are ordered using official district credentials.