SaaS Alerts™
Cover Your SaaS

VC3

MEET THE MSPs

Jonathan Whalley
Product Portfolio
and Marketing Manager

Cole Two-Bears
Vice President of Security Services

Location
Columbia, SC &
Edmonton, AB, Canada

By the Numbers

- 29 Years in Business
- 1,100+ municipalities
- 700+ businesses on client roster
- 11+ year average client tenure

Challenge

If the move to cloud-based data storage in the business world was a small, smoldering fire in the 2010s, then Covid was a can of gasoline. Post-2020, more workers and organizations than ever moved their operations and data to the cloud.

MSPs like VC3 had the job of shielding clients from any risk associated with that move. To add a layer of complexity, phishing attacks were on the rise. VC3 needed a layer of proactive protection in their workflow.

The stakes were high: VC3 is one of the largest MSPs in North America, with 1,800+ clients. Most of those clients are in critical sectors, like financial services organizations and municipalities. If VC3 allowed an IT incident, entire cities could be impacted.

Cloud companies like Microsoft weren't protecting these clients' data. So VC3 needed to be the hero — and they needed a tool to safeguard its wide portfolio of clients from costly damage.

Solution

VC3 immediately viewed SaaS Alerts as a must — not just a nice-to-have. They rolled out SaaS Alerts to all 1,800+ clients on an opt-out basis only.

VC3 communicated SaaS Alerts' importance to clients by outlining all the ways a security incident could threaten their organization:

- Reputation damage
- Financial costs
- Operational disruption

No business, municipality or organization wants any of those. And it turned out, they were all willing to pay a little extra to VC3 to protect against that risk.

Results

Now, SaaS Alerts is helping VC3:

Cover their clients' SaaS
Within a month of implementing SaaS Alerts, the VC3 team sat down for their regular security meeting. That meeting was soon "littered" with all the recent security threats that SaaS Alerts had helped them catch. VC3 now receives instant alerts any time an end user (allegedly) logs in from a strange place, like Russia. A password reset can happen quickly — and a crisis averted.

> **"If it weren't for SaaS Alerts, these organizations would never know until the threat actor was coming back and saying, 'Hey, we've exfiltrated all your data from your OneDrive, and we've deleted it, and we've deleted it from the 365 recycle bin.' So unless these clients have some type of SaaS backup, that data is now forever gone. SaaS Alerts notifies on the front end once that initial access has been made."**
>
> *— Cole Two-Bears, Vice President of Security Services at VC3*

Lay the groundwork for longer-term, strategic solutions
Having SaaS Alerts in place helps VC3 catch — and eliminate — security threats already in motion. But the tool also helps VC3 start conversations about more forward-looking solutions. For example, if VC3 notices multiple people trying to log into an end user's account from Russia, then it could be time to set up some Conditional Access policies.

When clients can clearly see incident data, they're grateful VC3 stopped the threat. But they can also see it might be time for stronger, more proactive policies. That increased security environment makes any MSP's job easier.

Better communicate with clients
Thanks to SaaS Alerts' reporting capabilities, VC3 can tell clients about an attack — then display the data proving it. That evidence can be the kick in the pants clients need to enact better security protocols.

> "We're able to say, 'Hey, this really happened. This is not a hypothetical situation. This is what transpired. And we were able to alert you.'"
>
> — *Cole Two-Bears, Vice President of Security Services at VC3*

Results (cont.)

Increase monthly recurring revenue (MRR)
VC3 announced that they would roll out SaaS Alerts to all of their clients. Folks could opt out of the service if they wanted. But to do so, they had to sign a waiver accepting responsibility for any future breaches to their SaaS environment. Nearly everyone was fine with the change because they wanted the peace of mind that came with the additional security.

> "There's probably a lot more expensive technologies out there. But for a lot of our client base, small-to medium-sized businesses with 15 to 50 users, this is a cost-effective and technically-effective solution that will protect them."
>
> — *Jonathan Whalley, Product Portfolio and Marketing Manager at VC3*

What VC3 Loves About SaaS Alerts

Proactive Protection	It's a workflow, not just a product.	Improved Communications
With SaaS Alerts, VC3 can stop attacks in their tracks — and not have to wait for a full crisis to manifest. Thanks to the 30,000-foot view over all their clients, VC3 can take proactive measures any time SaaS Alerts flags a suspicious behavior.	With seamless API integration, it's easy to fold SaaS Alerts into an MSP's entire workflow. VC3 saw that firsthand, thanks to the improved alerts and visibility SaaS Alerts brought to their daily workflow.	SaaS Alerts' reporting capabilities let VC3 move beyond hypothetical to deliver solid proof of breaches — and how those breaches were stopped — further building trust with customers.