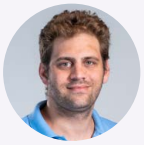
vorlon

SPLITIT CASE STUDY

Splitit cuts the time to detect and respond to third-party security incidents by 93%

"We started seeing integrations sharing data that we never knew existed."



Ran Landau
Chief Technology Officer
Splitit

splitit

INDUSTRY
Financial Services

CHAMPION
Ran Landau, CTO

Security challenges

- Took hours or days to "connect the dots" to detect and resolve security incidents
- Hard to track and manage unauthorized third-party application access
- Tedious point-in-time audit evidence collection meant "taking 100s of screenshots"

Results with Vorlon

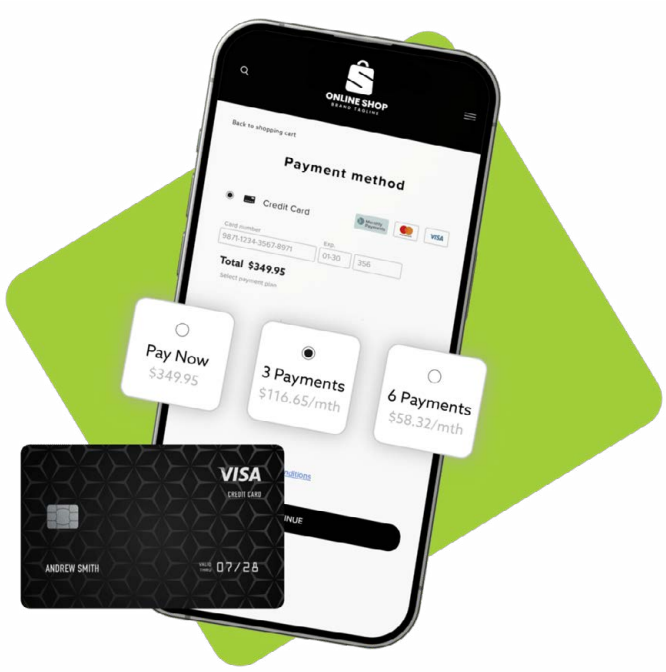
- 93% reduction in time to investigate phishing and other security incidents
- Effective management of secrets, access, and data sharing across third-party app ecosystem
- Automated real-time reporting of compliance evidence, eliminating days of manual audit prep work

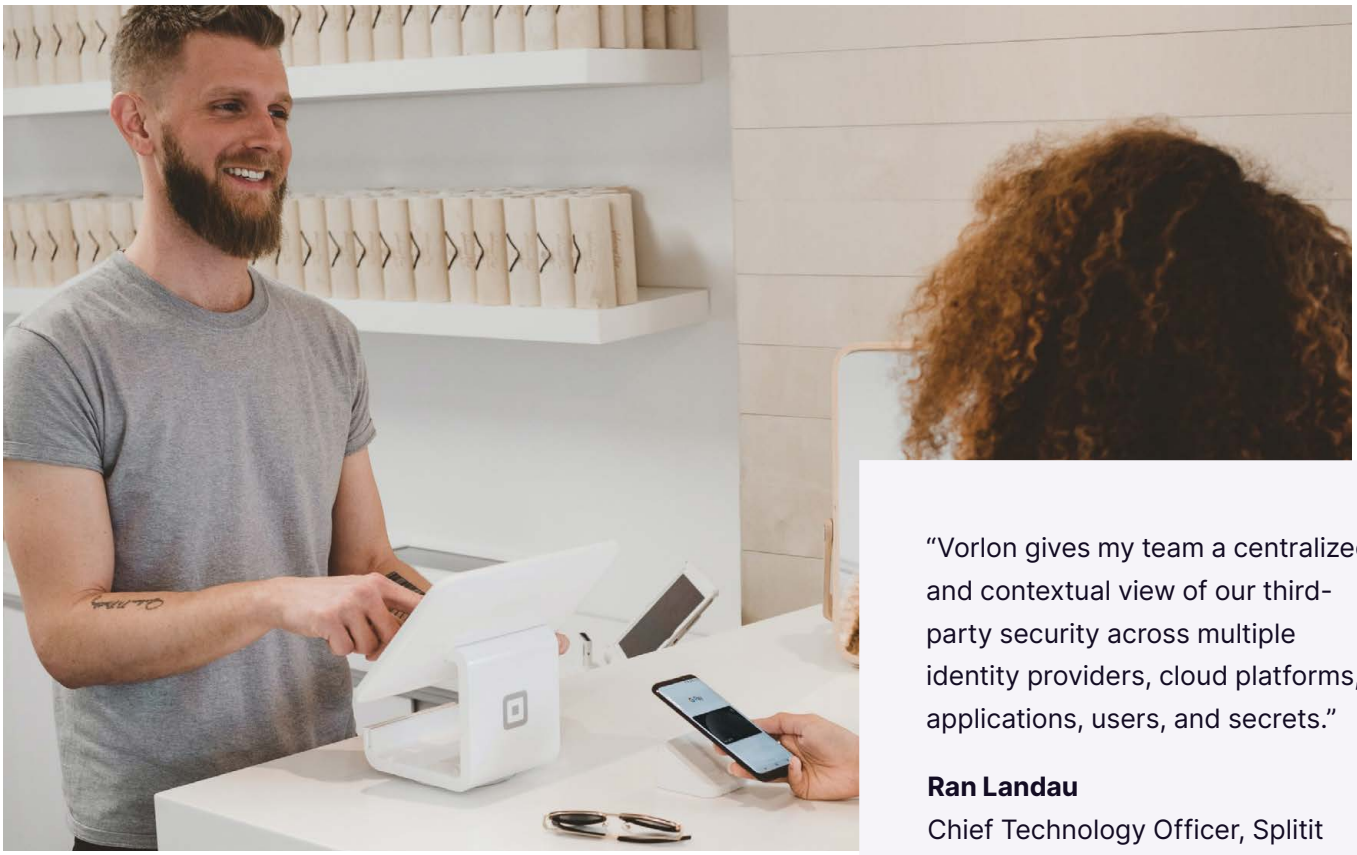
Third-party application ecosystems are under attack

Third-party applications and the underlying services they rely on are constantly in flux. Vendors change their APIs without notice, engineers provision secrets with too much access (then leave the company), and API endpoints share more data than needed to complete the task at hand. Most enterprises lack visibility into their third-party application ecosystem. Attackers have caught on. According to the Verizon DBIR, third-party breaches are growing 68% yearly.

Splitit helps shoppers finance purchases in over 100 countries

Splitit is a global payment solution provider that lets shoppers use the credit they've earned by breaking up purchases into monthly interest-free installments using their existing credit card. It serves many Internet Retailer top 500 merchants and shoppers in over 100 countries. A strong security program has helped drive rapid growth and earned the trust of global brands such as Google, TikTok, Amazon, and AliExpress. Ran Landau is Splitit's CTO; "I have a strong appetite for seeking innovative solutions to improve my total security posture, and Vorlon appeared to be doing something I hadn't seen before. Vorlon gives us insights into our API data flows to see connections across our applications," explains Landau.





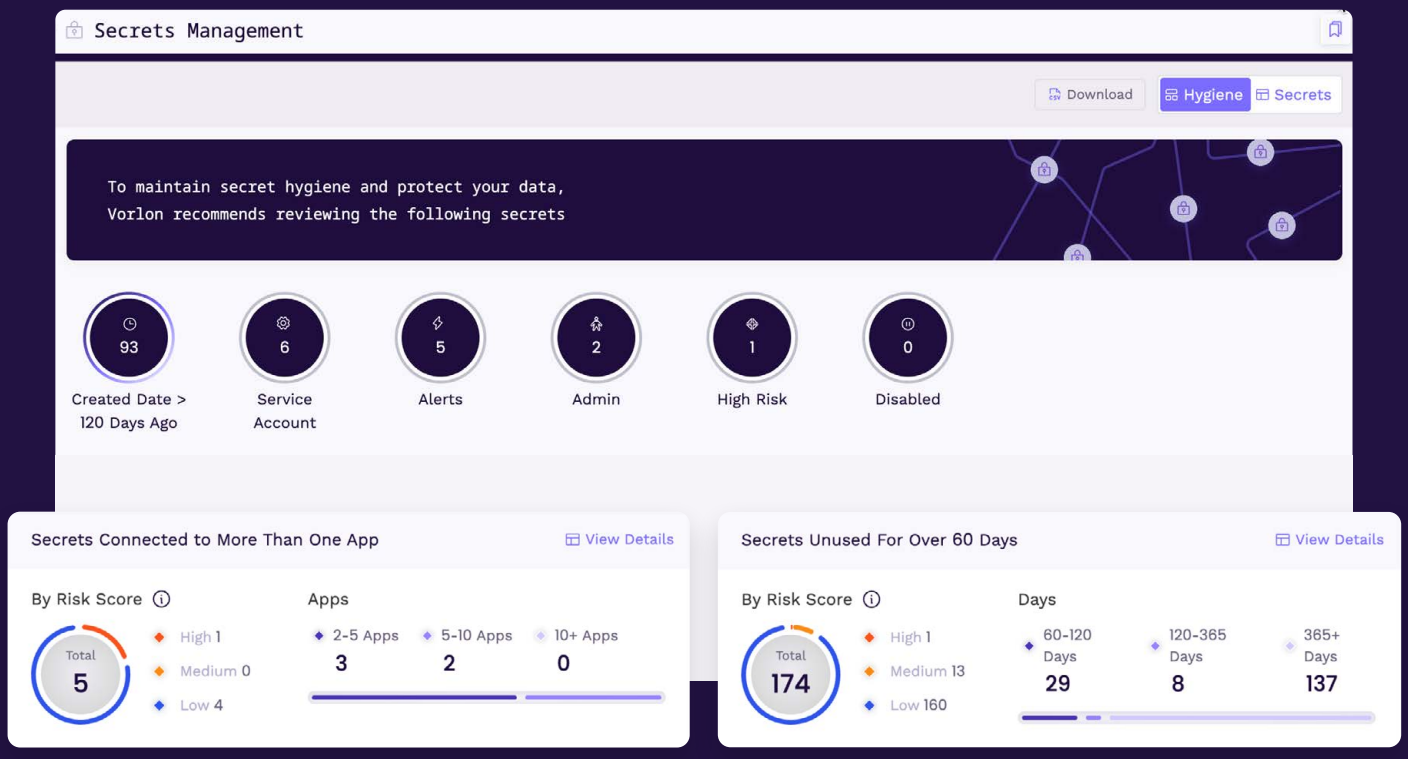
"Vorlon gives my team a centralized and contextual view of our third-party security across multiple identity providers, cloud platforms, applications, users, and secrets."

Ran Landau
Chief Technology Officer, Splitit

A more effective way to manage secrets and sensitive data flows

Managing secrets is difficult, especially with an ever-expanding number of interlocking applications and services. Vorlon automatically tracks secrets, their permissions, history, and associated sensitive data flows. “We can now quickly see which secrets have gone unused for 60 days or more and react quickly to protect them,” Landau said.

Another challenge is potential data exfiltration. If there’s ever a breach, understanding what data was exposed requires collecting and analyzing logs from numerous inter-connected applications, which can be a complex and time-consuming process. Landau explains, “We’re talking about 40 different applications which means a lot of work to understand if the various access permissions have been correctly scoped and set.

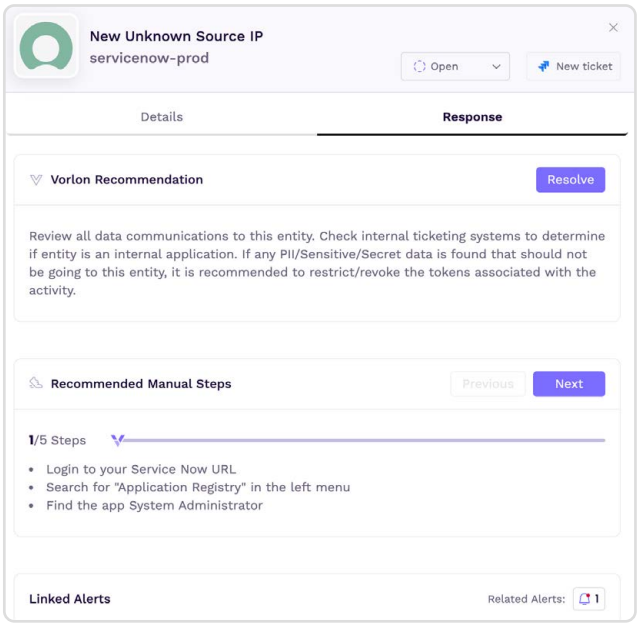


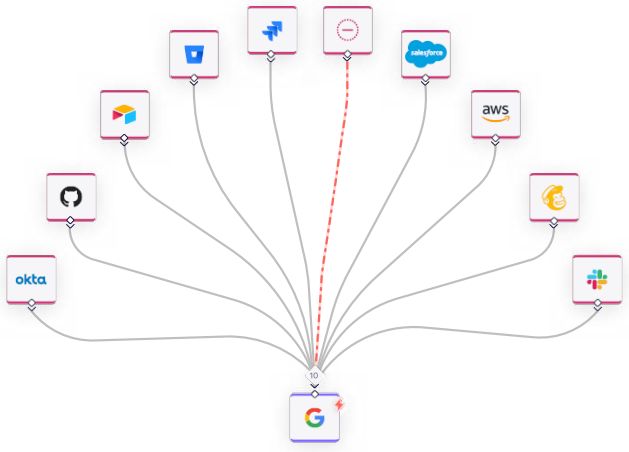
"The default settings on Snowflake left us with overly permissive administrative rights and sensitive data sharing. We were able to track and remove this permission thanks to Vorlon."

Ran Landau
Chief Technology Officer, Splitit

Faster resolution of third-party security incidents

"Alerts tend to pile up and require too many investigative steps to resolve," says Landau. "This makes it hard to find something suspicious and challenging to connect the dots when examining multiple application dashboards or log files to figure out what happened. Vorlon connects those dots for me. What used to take my SOC hours to resolve now just takes a few minutes. Vorlon helps us make more sense out of the many sources of alerts. We can close these cases more quickly."

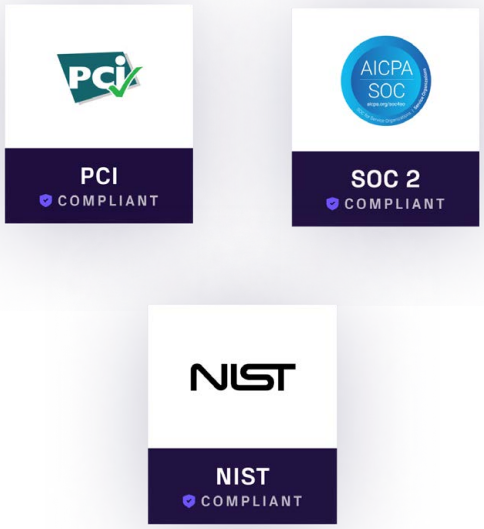




Faster investigation of phishing attempts

Splitit, like all global businesses, was being targeted by phishing attacks. "Some phishing attempts look like they're coming from an app we own. Vorlon helps us investigate their source and correlate the various events for faster resolution," says Landau. "This isn't a field well covered by other tools, but it's a big security risk."

Collecting evidence for PCI DSS4, SOC 2, and NIST



Another challenge was collecting the evidence Splitit needed to show auditors they had effective controls to manage third-party application risk. For example, PCI DSS 4 requires:

- An inventory of all trusted keys and certificates
- Automated audit log reviews
- The ability to detect and prevent phishing attacks
- Regular reviews of access rights

Vorlon has enabled Splitit to strengthen its security posture and better deploy resources, enabling them to be more productive in finding and stopping potential third-party application attacks.

> "A lot of controls are about showing visibility around PII data flows. Before Vorlon, the team spent days collecting over 100 screenshots of Vanta dashboards and other systems. Now, Vorlon does that work for us, continuously monitoring our environment and providing evidence and answers for multiple certification and regulation checkpoints for PCI, SOC2, and NIST."
>
> **Ran Landau**
> Chief Technology Officer, Splitit

About Vorlon

Vorlon is the first easy way to detect and respond to third-party breaches. With Vorlon Third-Party Application Detection and Response (TADR), your vendor app ecosystem finally gets proactive security coverage like you have for your endpoints and cloud. After an agentless, proxy-free setup, you can monitor sensitive data flows, manage secrets, detect anomalies, and revoke access. Powered by patent-pending DataMatrix® technology, Vorlon creates an algorithmic model of your applications and connected services for faster, AI-driven remediation. Backed by Accel and SOC 2 Type 2 Certified, Vorlon is trusted by Fortune 500 companies and startups. Learn more at vorlonsecurity.com.