A PARALLO EBOOK

Further, faster, safer: a security roadmap for SaaS creators and ISVs

How to put some security guard-rails around your march to application maturity

August 2020

by Blair Corbett, Parallo Security Services Manager

Contents

Introduction 3
Protecting your security and compliance posture in Microsoft Azure 5
Constantly monitor, alert and respond to security incidents 6
Protect your product with continuous auditing and reporting 8
Bringing strategic insight and oversight to your security challenges 9
Security Services Summary 11
Focus on building great software, fast (but safely) 12
Parallo: SaaS and ISV specialist services 12

Introduction

The cloud has transformed the ISV industry and customer expectations, mostly for the better. For any organisation leveraging cloud technology, security is a key consideration. Gartner certainly thinks so – they predict spending on cloud security generally to increase 33% in 2020 over 2019. They see specific areas such as data security (7% growth), application security (6%) and identity access management and infrastructure protection (6%) all getting more focus.

SaaStr Founder Jason Lemkin also agrees. In his blog post, 'It's Time For You To Make Security a Core Feature — Not a Tax' he argues that "If these Public Unicorns have these basic application-level security issues, what else is lurking beneath the surface? You know when you see one flag, there's another 10 to follow…"

His recommendation? "Security. It's a big and broad topic. And the more you learn, the scarier it can be.

Just do this to start. Make it a core part of the roadmap for every single release, for every SCRUM, for every discussion.

And you'll come out way, way, way ahead in the medium and long term."

All this means that you need to develop software products and deliver them to the market as fast as possible, while also ensuring yourproduct is secure - and that you can prove it is . As an ISV you are not only responsible for your own security, but the safety of your client's data – and more

Maximising growth while managing security

In our experience of working with many ISVs, they tend to fall into two camps. Some have established procedures and processes within their development cycles, treating security holistically. They know and understand it, and it's something that's managed from the beginning. The rest are perhaps more in "start-up mode", where they are mindful of security, however as a focus point it competes with a raft of other existential priorities.

What happens then is that the bugs and other security problems within their application aren't being addressed or identified, which poses significant risk down the track. This second camp – especially when they find product-market fit and are accelerating – often don't realise that they have grown to the point of needing to zero in on security, or if they have realised it, it's perceived to be too expensive or difficult to achieve.

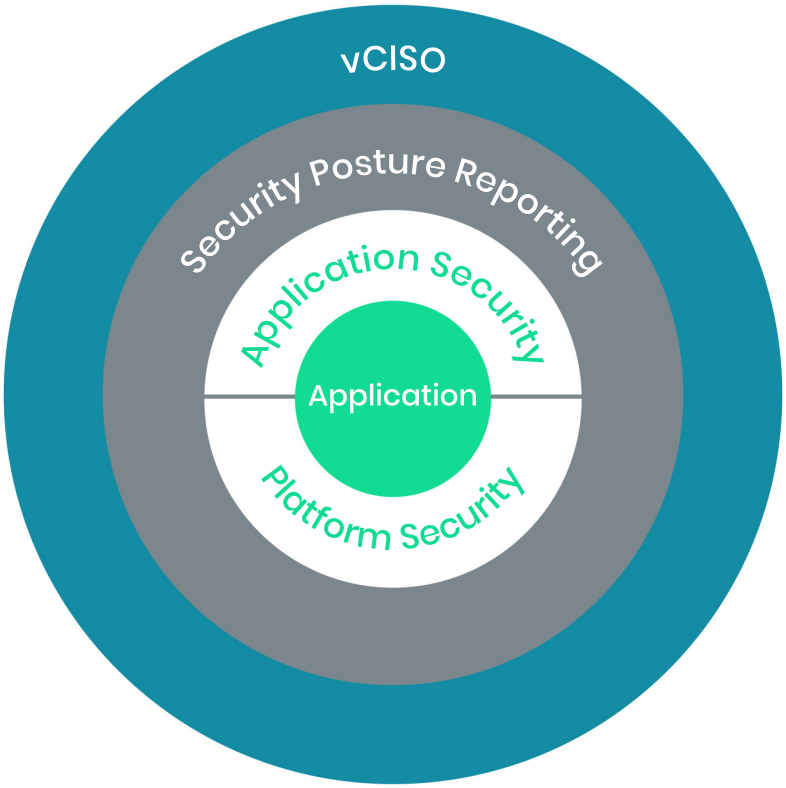
A comprehensive security ecosystem that allows ISVs to get smarter, go faster and be better

The business impact from a single security breach can lead to disruption, reputational damage, loss of revenue and erosion of customer trust. Security breaches can have serious consequences to other organisations that you partner with or that utilise your products .

To address these security challenges, Parallo has created a Managed Security Service, comprising of a suite of four security service components, created to strengthen your Microsoft Azure infrastructure and Web Application security posture. Our security service will enhance your overall cybersecurity strength and how well it can predict, prevent and respond to evolving and emerging cyberthreats. We've also solved the problem of how to cost-effectively establish a disciplined approach to continual security posture improvement, as well as strategic advice and governance support for the CEO.

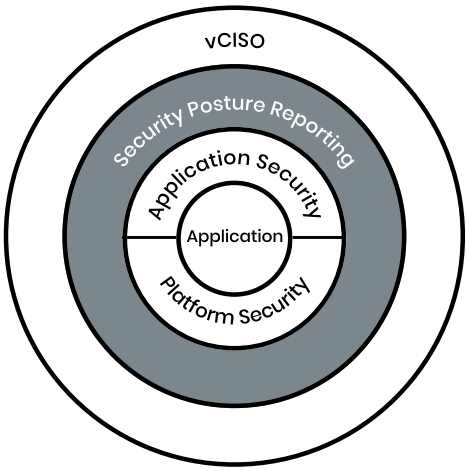
In this eBook we cover these services, the tools we employ to do this, and introduce the concept of a virtual CISO.

Parallo Managed Security Service



1 Protecting your security and compliance posture in Microsoft Azure

This is **Phase One** of our approach, known as the Security Posture Reporting Service. This focuses on an ISV's cloud platform, and highlights the services that are available to mitigate threats and incidents such as data breaches or denial of service. ISVs need to implement a continuous security improvement process, and to actively audit their platform for security vulnerabilities. Monitoring for security attacks and breaches in real-time with a swift response is key.



Our approach to the visibility, reporting, and management of your Security Posture.

We first aggregate all the Azure infrastructure security issues on a dashboard to gain visibility. From this, we then establish the current security and compliance baselines by leveraging Azure's Secure Score as the relative metric for continual improvement.

Your Secure Score is represented on a scale from 0-100 in regards to how secure your infrastructure is. We present a 'Current State Assessment' to document baselines and threats and the state of your security posture, as compared to peers. This gathered data serves to proactively surface any pressing security issues and drive remediation activities.The service includes an on-going status report where we review and update security baselines to monitor improvement over time. The monthly check-in itemises new threats that may crop up, and prioritises actions based on risk. The Executive Summary at the start of the report provides board report content to inform key risk owners.

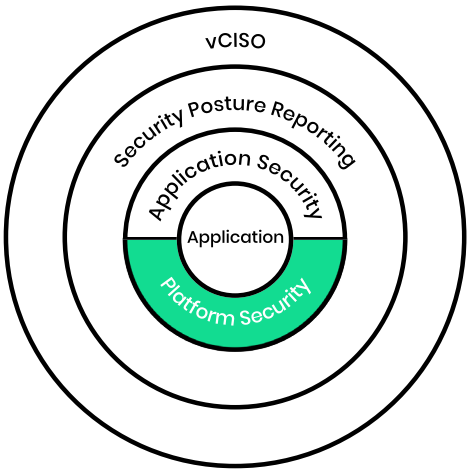
Our Security Posture Reporting Service ensures the necessary continuous improvement process for Azure infrastructure security is in place, and a conscious course of action is also established.

2 Constantly monitor, alert and respond to security incidents

To respond to security threats in real-time, and to prove that security is an essential part of their product infrastructure, ISVs should implement a Security Information and Event Management (SIEM) and Security Orchestration, Automation and Response (SOAR) system. This is **Phase Two** of our approach – a Monitored Security Service.

In addition to management services, a SIEM & SOAR system provides a log of activity as well as insights into IT environments. The objective is to identify potential threats and vulnerabilities, as well as resolve security incidents 24/7.

More than just logging, a SIEM platform maintains a record of 'digital footprints' – a collection of systems logs and activity information to help pinpoint unusual activity and report on suspicious behaviour – a bird's-eye view of your IT security.



The 24/7 Azure Sentinel Security Service

We've developed a real-time monitoring and alerting and response service to protect your Azure and Office 365 components from security threats before they happen. We leverage the proactive cloud-native Azure Sentinel Service to simplify security operations and protect against external and internal hazards.

Azure Sentinel continually monitors and reports on your cloud platform. With regular monthly reviews scheduled, Sentinel highlights security events, alerts, and shadow IT subscriptions.

Sentinel also:

- Collects data at cloud scale – across all users, devices, applications, and infrastructure, both on-premise and from multiple clouds.
- Detects previously uncovered threats and minimises false positives using AI powered analytics and unparalleled threat intelligence from Microsoft.
- Investigates threats with AI, and hunts suspicious activities at scale, tapping into decades of cybersecurity work at Microsoft.
- Responds to incidents rapidly with built-in orchestration and automation of common tasks.

During the Azure Sentinel onboarding process, we audit your Azure and Office 365 infrastructure and document all components to be monitored. Following this audit, we understand the current state of your security policies and any special rules to be noted.

Once Azure Sentinel is implemented and configured to your system, we set our Monitored Security Service into place. The service ensures regular reporting and assessment of threats on a daily, weekly and monthly basis. There's also a 24/7 alert response and threat investigation procedure.

In case of a security breach, we perform the following crucial remediation steps:

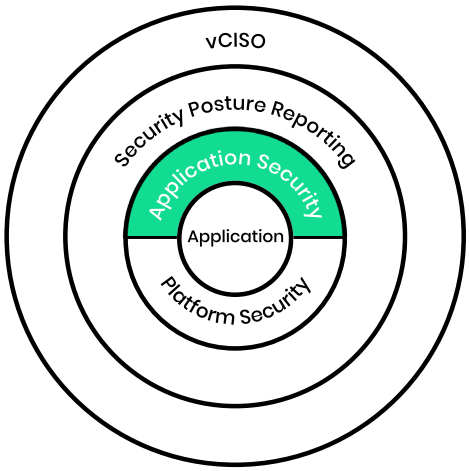
- Document the incident timeline, resources in jeopardy and the business risk. Incident mitigation and next steps are identified and actioned.
- A root case analysis is performed and corrective actions are executed to strengthen security.

SIEMs can involve a complicated implementation, often need constant tuning, and require dedicated specialist resources.

Wouldn't you rather invest this time and effort in developing paid product features for your customers?

3 Protect your product with continuous auditing and reporting

Phase Three of our plan is known as Application Security Testing (AST). These are tools and services aimed at improving Web Application security through continuous auditing and reporting. In order to mitigate risk and address your software's compliance requirements, AST is an essential component of your software security initiative.



If you don't perform regular AST, you'll be unaware of security issues within your Web Applications. This gives attackers a potential window to access sensitive data, which will endanger your reputation and revenue.

Rather than purchase a costly automated AST product, we recommend the option of letting a trusted third-party perform and manage this service for you.

The Application Security Service

Based on our years of experience supporting ISVs with their security needs, we've developed a tailored AST service using a top-tier Web Application Scanning application. We run this application over your product, which will bring to the surface any code related issues.

Setting up the Web Application Security Testing services involves an initial discussion to document the applications that need scanning, and the cadence that these scans are performed. Key stakeholders from the DevOps and Executive teams are involved in the kick-off application deployment process to ensure an efficient long-term relationship.

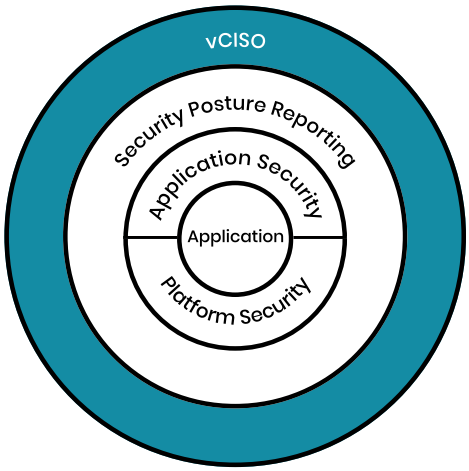
Once the AST service and schedule are in place, ISVs receive the following security outputs:

- A high-level executive summary report to provide a product security snapshot for board-level assurance, documenting continuous improvement over time.
- Deep technical reporting highlighting application vulnerabilities, how these vulnerabilities can be exploited and detailed remediation activities.
- Additional issues reported on and surfaced, in line with new releases.

This essential application protection service provides a form of continuous compliance designed to give you increased visibility into vulnerabilities within your product. It implements a recurring process for identifying and resolving application issues as well as a plan to address the findings.

4 Bringing strategic insight and oversight to your security challenges

The critical importance of cybersecurity to ISV and SaaS success is increasingly putting the focus on having a strategic role within ISVs to drive this area. For many ISVs, funding this sort of position, which requires high level expertise and strong strategic skills, or finding someone with the right skills, can be difficult as a fulltime role.



Parallo offer a Virtual Chief Information Security Officer (vCISO) as a part-time professional working with your organisation to provide cybersecurity leadership. Typically, it's more efficient and cost-effective than bringing in an in-house senior executive. A Virtual CISO is a highly qualified and trained security expert who drives your program. Working alongside your management and IT teams, they're capable of examining and refining the big security picture of your organisation.

A virtual CISO (also known as CISO-as-a-service or fractional CISO) is an on-demand executive-level cybersecurity professional who helps to:

- Identify key risks.
- Align cybersecurity efforts to business priorities.
- Ensure that legal, regulatory, and contractual requirements for cybersecurity are understood and managed.
- Respond to prospect and customer security questions and RFPs.
- Implement and Manage Security Policy.

The role is strategic. They take a holistic view of your security, and work with you to build internal processes, so that there are robust policies in place to reduce your vulnerability. This includes on-and-off-boarding for users, and a solid understanding of the regulatory processes that your customers need to work within. Where you have vulnerabilities, they come up with a strategy to deal with them.

A Virtual CISO will typically conduct a cybersecurity risk assessment based on your business assets; establish a cybersecurity strategy based on your business needs; build a cybersecurity plan and program; build a Governance, Risk and Compliance (GRC) program; and focus on people – including potentially managing personnel, contractors and/or vendors.

By engaging a virtual CISO, you can:

- Gain immediate access to an experienced senior cybersecurity professional.
- Get independent advice from a trusted expert to validate the cybersecurity controls proposed by IT suppliers and internal teams.
- Build a cost-effective, scalable, and flexible cybersecurity function.

Building and executing a training strategy

Preparing a vCISO program for your ISV:

- Look for a partner who understands your business, your goals and your customers
- They should be able to liaise effectively with high-level management teams, mid-level IT analysts and product engineers
- They need to be capable of developing a long-term security and compliance vision for your business
- Have a proven ability to monitor, evaluate and stay on top of threats and security incidents

The Parallo vCISO service provides specific expertise with demonstrable experience, specifically aligned to your business. With advice on-demand and access to expert guidance to address any cybersecurity issues, including control improvements, compliance issues, and customer queries, our vCISO service provides complete security leadership.

Security Services Summary

Focus Area	Security Posture Reporting Service	Azure Sentinel Security Service	Application Security Service	vCISO Service
Outcome	• Visibility, reporting, and Management of Security Posture. • Improving Azure Infrastructure security posture through continuous auditing and reporting.	• Real-time monitoring and alerting of Microsoft Azure and Office 365 components.	• Improving Web Application security through continuous auditing and reporting.	• Gain immediate access to an experienced senior cybersecurity professional. • Build a cost-effective, scalable, and flexible cybersecurity function. • Develop and align internal and customer aligned security strategies.
The business problem being solved?	• Provides a continuous improvement process for Azure Infrastructure security vulnerabilities and a process to address these findings.	• Proactive cloud-native SIEM to simplify security operations and protect against external and internal security threats before they happen.	• Provides a recurring process for surfacing Web Application security vulnerabilities and a process to address these findings.	• vCISO — an experienced cybersecurity executive that your organisation can name is your CISO in sales collateral and audit responses.
Service Outputs	• Azure Infrastructure security issues are summarised in a detailed report with remediation efforts and costs clearly articulated. • Remediation activities are tracked through to completion. • Azure Infrastructure security issues will be surfaced as new Security Center features are released or as the customer's infrastructure landscape changes. • A simple Executive Summary provides a snapshot for board level assurance. • The process is executed on a recurring schedule.	• Reduce security incident response times with automated responses. • Ensures immediate focus on Security risks as they are found. • Security coverage scales seamlessly with customer growth. • Aligns to customer need to react • The process is continually executed 24/7.	• Web Application security issues are summarised in a detailed report. • Remediation activities are tracked through to completion. • New Web Application security issues will be surfaced as releases are deployed. • A simple Executive Summary provides a snapshot for board level assurance. • The process is executed on a recurring schedule.	• Advice on demand (up to 4 hours per month) —access to expert advice ad hoc to address cybersecurity issues, including control improvements, compliance issues, and customer queries • Monthly reporting—a cybersecurity report tailored to your needs.
Schedule	• Monthly and/or as required	• Real-time	• Monthly and/or as required	• Monthly and/or T&M
Costs	Contact Parallo for costs	Contact Parallo for costs	Contact Parallo for costs	Contact Parallo for costs

Focus on building great software, fast (but safely)

We understand how important it is for ISVs to focus their time and resources on application development an degrowing your customer base. However, our extensive experience has shown us that all too often, the issue of security gets moved down the list of priorities, to make way for rapid delivery. Speed is, of course, essential for ISVs to remain relevant and competitive, which is why you need to stay focused on your product and your customers.

From risk to opportunity: security is your opportunity to build trust and loyalty. Our security solutions enable you to get the complete picture of your security and compliance, while continuing to focus on what you do best.

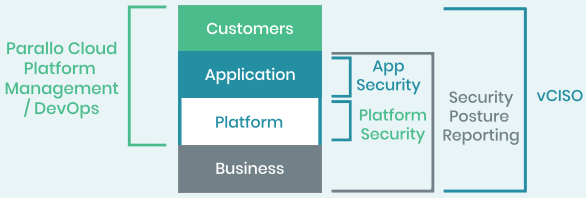
Read more about ISV security at www.parallo.com, or schedule a consultation with one of our security experts.

Parallo: SaaS and ISV specialist services

Free Your Focus: Parallo enables ISVs and SaaS creators to focus on what really matters; your product, new features, building your customer base and accelerating revenue growth.

As a Microsoft Azure Expert for ISVs, we've chosen to go deep and develop a unique understanding of the technology that enables SaaS and ISVs and what drives them; we know that you strive to differentiate from your competitors, gain new customers, and maximise net revenue retention through rapid feature release and adoption. If you're looking for expertise across the tech domains and services to help you do that, we're the specialists, with specific services for the ISV and SaaS segment of Azure consumers.

We enable you to meet the key challenges around the security, compliance and IP protection of your offering. We look after your data and ensure its availability, via secure cloud infrastructure. We also understand the consequences of a lapse in security; in a nutshell, we know how crucial it is to be always available and reliable, with predictable costs. Find out more about our solutions for ISVs and SaaS creators here.



Microsoft Partner
Microsoft

Gold DevOps
Gold Application Development
Gold Cloud Platform
Silver Security