Sales Deck Pitch - Transcript 2026

Recorded by Ken Bagnall, Co-Founder and CEO

00:00:00:02 - 00:00:55:14 — INTRODUCTION

Silent Push is a Preemptive Cyber Defense platform. We deliver preemptive, precision driven data that empowers organizations to neutralize threats with confidence before compromise occurs. Everything is about pre breach detection. At the moment, attackers are much faster at setting up staging new infrastructure than enterprises are at detecting it and then sharing that information. We know from our past experience, running detection engineering and security companies, that the security industry is only aware on any given day of about 5% of attacker infrastructure that is about to hit in new campaigns.

00:00:56:00 - 00:01:24:03 — THE POST BREACH PROBLEM

The vast majority of attacker infrastructure is invisible to those security products. Generally, it is always reactive. The attacker infrastructure has to be *launched*, hit the customer before the security companies know to share it across all of their customers, and even a longer delay before that gets shared generally and it hits all security tools in order to block it for everybody.

00:01:24:04 - 00:01:56:14 — THE POST BREACH PROBLEM

So, you're always behind, the information is shared is always post-breach after campaign is launched and the vast majority of new infrastructure is not detected. And that problem has accelerated, with increased automation and the use of AI tools to generate attacker infrastructure. This is becoming a much larger problem. What's missing really — is people can't see the preparation phase.

00:01:56:15 - 00:02:33:05 — THE POST BREACH PROBLEM

All the work that goes in before launching a campaign and pre-breach, where actors are setting up that infrastructure, testing it, ageing it so that it doesn't get blocked just for being new — none of that is detectable from normal, security tools or security platforms. Generally, all that's visible is *post breach information*. So someone has to click on a link (etc.) before it becomes known.

00:02:33:09 - 00:03:04:06 — THE POST BREACH PROBLEM

When people talk about TTPs, they're always talking about *post-breach TTPs (tactics, techniques and procedures)*. After someone clicked the link, downloaded the malware — what happened? How did it move across the organization, how did it escalate privileges, etc.?

Our focus is on *pre attack TTPs*. How did they set up and manage their infrastructure to prepare the campaign and the attack? It's a very, very large difference between those two points of focus.

00:03:04:08 - 00:03:36:12 — PREEMPTIVE DEFENSE

The whole shift for us is to create this *preemptive* information so that we can let people know what is *about* to hit them. Therefore, they can prevent what's coming. And that's a that's a very big difference from the previous iteration of how people did things where they just shared Indicators of Compromise (IOCs) from campaigns that had already been launched and used.

00:03:36:13 - 00:04:59:00 — THE CONTEXT GRAPH

So how do we do this is critical, because you can't do this with traditional security platforms. What we have created is what we call the *Context Graph of the changing internet* — where we are measuring, monitoring, and mapping, the changing technical relationships on the internet every day.

[RELATIONSHIPS IN DNS] So, we are measuring changing relationships in DNS — we force re-resolutions of all DNS records on a daily basis.

We're then seeing when something has stood up on the end of those records — Does a mail server get set up? Does a server get set up on the end of an A record? What sort of header responses do we get from that in the preparation stage? When does that change?

[INFRASTRUCTURE CHANGES] Often, change detection is really the most important thing. Changing relationships and DNS let us know when they're moving infrastructure and things are about to be launched or the pattern of hosting before an attack.

Then we want to see: Do they set something up? Does it get set up?

[CONTENT CHANGES] And then finally we're looking at the content that they set up. Going into real detail about the JavaScript's on the page, logos, HTML titles, etc. But the combinations of these things give us the whole timeline up to the point of launch.

00:04:59:01 - 00:05:29:03 — CRIME GROUPS & APT GROUPS HAVE PROCESSES

It's a very exact science. This is not probabilistic. It's not predictive, saying "this infrastructure might be bad". We're following exact TTPs of how people manage their infrastructure because crime groups and APT groups are organizations with *processes*. Even if they change the underlying hosting providers or infrastructure they use, they will follow the same process.

00:05:29:04 - 00:05:57:11 — EXAMPLE OF APT PROCESSES

So, we will always get used to seeing Gamaredon and GRU going through the same process — ageing their infrastructure by year, moving it across a range of 15 different subnets that they've rented in different places, etc. We know what these patterns are and we can follow them with an exact science. So, this *Context Graph of the changing internet* is incredibly important.

00:05:57:12 - 00:06:34:00 — WE ANALYZE BENIGN AND "BAD" INFRASTRUCTURE

The Context Graph is the source of truth, the *defined certainty* about what is happening. And we're analyzing *all infrastructure* — not just known bad infrastructure, *all known infrastructure*. This means infrastructure that people think is benign, infrastructure people think may become bad, and known bad infrastructure. It's all analyzed and measured by us at all times, because the *future threats will emerge from what is currently benign infrastructure.* So you can't just monitor known bad (infrastructure).

00:06:34:01 - 00:07:04:15 — COLLECTING AND CONTEXTUALIZING DATA

We have many, many different data types that we collect, such as our active collection of DNS records. That allows us to detect and measure changes before there is traffic. We measure each of the ASNs managing IP space. We are looking at all name servers, name server changes, name server patterns, WHOIS data for example.

We have traffic sensors globally. We are looking at the rate of change of domains across IP space, different types of proprietary hashes on all infrastructure. And then we make different types of measurements of change — density of infrastructure, diversity of

infrastructure, change frequency, etc. We make different types of reputation analysis on top of it.

00:07:39:08 - 00:08:12:00 — SEARCHING THE CONTEXT GRAPH

And all this can be queried and searched at any time. That definite certainty of the Context Graph is available to all our customers to search at any time as well as ourselves. And then obviously we operationalize that in the platform. So, we cluster that into determinations of different threat actor infrastructure, and we share it. But we also share all the underlying data all the way down to the raw data with our customer base.

00:08:12:01 - 00:08:51:00 — INTEGRATING THE CONTEXT GRAPH

So, the Context Graph is available to our customers to use in their integrations and across their security stack, across all different elements of their business.

So, all the different security teams — the SOC can use it for enrichment triage, the Incident Response Team can use it to find out what a threat is and whether that threat actor has more infrastructure set up that they should also be looking for.

Fraud teams can also use it to determine the provenance of an IP address and where the traffic is originally coming from.

00:08:51:01 - 00:09:20:00 — AGENTIC (AI) WORKFLOW EXAMPLE

It's all designed to be machine consumable. If someone is trying to build agentic workflows, they can obviously just consume the Context Graph into their agents in order to have a source of truth that they're actually putting into these workflows. It’s a really important, fundamental asset for all of the security industry to be able to build on top of.

00:09:20:01 - 00:09:48:04 — MODULES

The platform is then divided into three different core parts — Insight, Reconnaissance and Defender.

With Insight you can see *everything in one place, about any domain or IP address*. That will help you accelerate triage and see what something is likely to be straight away.

00:09:48:05 - 00:10:20:01 — MODULES CONTINUED

And you can spin out from that into Reconnaissance and find more of that type of infrastructure if you want.

Or, save (those searches) and push it into Defend for blocking, and create your own types of feeds for things that you're working on.

We also make Traffic Origin available in the Insight module. That gives you the upstream reality of where traffic is coming from, regardless of where the IP address is or says it is.

00:10:20:02 - 00:11:25:00 — TRAFFIC ORIGIN

For the example in this image, the IP address is in Ireland. So in historic workflows, people would have regarded this as connection from Ireland and worked off the reputation of that IP address. However, with our Traffic Origin capability and seeing the upstream traffic from our traffic sensors, we can see that this is actually Chinese traffic that is coming out from being proxied from an Irish IP address.

And that gives a completely different threat scenario to someone who is trying to assess Know your Customer (KYC) information, anti-money laundering, fraud investigations. Understanding where not just customers, but where your employees are logging on from.

So Traffic Origin is incredibly important part of the Insight module to give immediate context to security teams.

00:11:25:01 - 00:11:53:09 — RECONNAISSANCE

The next part is Reconnaissance. And this is where we enable you to access all of our searches and queries across all of our different datasets, and across all the different patterns we've created in the Context Graph. So you can map adversary campaigns, you can search for the different pre-attack TTPs of how they set up and manage their infrastructure.

00:11:53:10 - 00:12:28:07 — RECONNAISSANCE CONTINUED

You can find phishing infrastructure before it gets used, in a whole different number of ways. Not just from domain similarity but also from contents — looking for five icons, different JavaScripts on pages, etc. But the important thing is that we're trying to give parity to the analysts in any customer environment to get access to the same tools as we make available to our own analysts.

00:12:28:08 - 00:13:11:00 — DEFEND MODULE

Then the last part of the platform is Defend. This is all focused on anything that integrates with your security stack. So, making things available for immediate action within your security environment. That includes integrations into your SIEM, SOAR or your firewall, and also includes our fast lookup Threat Check service for immediate determinations of “good, bad”. Or to run a Threat Check against our Traffic Origin data to quickly let you know countries of origin of the traffic from behind an IP address.

All of this is available in the Defend module to give you an idea about *how clearly* and *how much earlier* we see malicious infrastructure that enables you to defend your organization.

00:13:11:01 - 00:14:16:07 — PROOF OF VISION: SALT TYPHOON CASE STUDY

The Salt Typhoon case study is a good example where in May, we saw them setting up infrastructure.

In June, we published a TLP Amber report based on the feeds that we'd already made in May.

Then in July, competitors started to see that infrastructure that we identified in May hitting telecommunications companies, as Salt Typhoon tried to breach those environments.

And then third parties and other security companies publicly confirmed and validated our information, that indeed the infrastructure that we had seen earlier was what was trying to break into those telecommunications companies later on.

00:14:16:08 - 00:14:50:03 — Visibility and IOFA™ Feeds

We have constant monitoring of that government organization, or the contractor involved setting up that infrastructure. We always have it available. We know what the TTPs are. We constantly have Indicator of Future Attack ™ (IOFA™) feeds of what they've set up and are ready to use against global telecommunications companies. All they (telecommunications companies) have to do is use Silent Push to be defended from that threat group.

00:14:50:04 - 00:15:18:09 — FIN7, LAZARUS EXAMPLES

And we have this functionality available across multiple APT groups and international crime groups. For example, FIN7 set up their infrastructure well in advance. We have all

of that and a lot of it. Different North Korean groups such as Lazarus, for example. We always have that infrastructure tracked well in advance. We have good visibility of what they do and where they're operating from.

00:15:18:11 - 00:15:35:05 — EARLY DETECTION METRICS

So, we have lots of examples of this. We have an average of 104 days early detection before customers start seeing this in traffic.

00:15:35:06 - 00:16:03:50 — WHO USES SILENT PUSH?

The world's largest organizations use us. So, we are across currently eight governments, security agencies, different armies. Largest companies all the critical categories would use us. Anyone with a mature security organization would definitely use us. We give them insight that is impossible to obtain elsewhere.

00:16:03:51 - 00:16:45:00 – WE'RE NOT A BLACK BOX SCENARIO.

We are not a black box scenario. As well as providing the finished intelligence of the Indicator of Future Attack ™ (IOFA™), we provide TLP Reports which explain how we monitor and query on the underlying Context Graph for that crime group and how they manage their infrastructure. We give clear insight into how we do what we do, plus a working tutorial of how we do what we do, and give you access to all the underlying queries on the underlying data.

We can really be broadly used across security organizations and different teams.

00:16:45:01 - 00:17:17:07 — WE DON'T PARTICPATE IN INDVIDIUAL TAKEDOWNS

We don't really participate in individual takedowns because it's clear from what we see that the scale of the crime infrastructure makes it farcical to try and take down pages one at a time. So, for example, the Chinese Triads crime infrastructure operating out of Southeast Asia has about 1.4 million live hostnames and pages going any day.

00:17:17:07 - 00:18:23:00 – TAKEDOWNS AT SCALE

Trying to chase those down one page at a time is ridiculous. So, we try and do this at scale. We share our information with Law Enforcement, Treasury, etc., to try and get sanctions taken and pressure put on infrastructure providers *not to host this*

infrastructure and to do work to make sure that they don't participate unbeknownst to themselves in the crimes that are being perpetrated through their infrastructure.

So, we operate at that level of scale. We share, the platform with the Cybercrime Atlas which is hosted by the World Economic Forum. And that has led to over 2000 arrests so far just in the last year. We also share analyst time with those organizations to make sure that we really deal with crime at scale.

00:18:23:01 - 00:18:55:13 – SOC ROI

For the enterprise using us, it almost sounds too obvious to say, but the advantages to them are quite stark. The return on investment for a SOC team to immediately get the type of context that we provide for them to see what matters or what doesn't matter, is pretty dramatic.

00:18:55:15 - 00:20:00:00 — SOC ROI CONTINUED + TRAFFIC ORIGIN EXAMPLE

If you take a look at something like Traffic Origin. Before we provided this context as to where traffic was coming from, you could buy lists of IP addresses that were supposed to belong to anonymization networks, but they would have too many false positives for you to be able to action them.

Us adding the Traffic Origin context means that you have something very firm to make decisions based on. So, you've got an employee says they're logging in from a US IP address. The traffic is actually coming from Iran. Huge red flag, something very serious. You can take action on it.

While if you just have “coming from an IP address in the US, appears to be a proxy”. Well, that applies to so many IP addresses in the US both good and bad, that it's impossible to make a decision based on that.

00:20:00:01 - 00:20:28:10 — IR ROI

It’s really important for us to add this context to make information actionable. And really that's the Silent Push difference — that suddenly you can actually *do* things with the information.

For Incident Response teams, where they are looking at complete unknowns, and supposed to be able to take action on them... They can come into Silent Push, hit our Context Similarity search, find out about this infrastructure you're looking at. Find out that this domain or IP is managed in a similar way to all of this other infrastructure, and

here is everything that group or campaign is setting up at the minute that you also need to look for in your logs.

00:20:50:13 - 00:21:01:00 — DIFFERENT SECURITY TEAMS (CTI, FRAUD)

We can also work across all the different security teams. All the way from CTI teams to Fraud teams, we can help them hunt for what's *about* to affect their organization.

00:21:01:01 - 00:21:52:07 — INTEGRATIONS: “API FIRST”

We make sure that we integrate with all of your security stack, and we have built in integrations, native integrations and Splunk apps, playbooks etc., into hopefully everything that you need.

But also, the whole platform is API first and built on top of APIs, which are all available to our customers. So, there is nothing that we can do that you can't automatically do, within your environment.

00:21:52:09 - 00:22:21:02 — SHAREABILITY AND INTEGRATIONS

Critically, the information that we make is preemptive. We are certain that it is crime or APT infrastructure and that this is being managed in a very particular way. And we can share that information out with our customers. We make sure that we can share it in critical, actionable ways that fit in with your security stack. It enables you to neutralize the activity as far as your organization is concerned as soon as it is set up. You can choose which type of crime or APT infrastructure matters to you.

00:22:21:03 - 00:22:43:08 — DETERMINISTIC RULES

And focus on having rules in place for that particular type (of infrastructure), whether that's initial access brokers or particular APT groups. If you’re a Telecommunications company, you might want Salt Typhoon etc. And you can have that particular (APT) group neutralized in your environment all the time because, we will let you know exactly what they're doing as they do it.

00:22:43:09 - 00:23:11:01 — DETERMINISTIC ACCURACY

Everything is deterministic. So, we don't have any kind of probability type information in here. It is all, clear this is a particular campaign or threat actor and we are mapping

them this exact way and we share all of that. There's no black box determinations where we don't tell you how things work. Everything is fully shared all the way down.

00:23:11:02 - 00:23:42:09 — CONCLUSION

So critically, we save your organization time. We give you early detections that you wouldn't be able to do otherwise. You don't have to try and glue together lots of different types of information from different places. We make all the data from scratch. We've correlated it all. We're monitoring all the changing, technical relationships on the internet to give you the final outcome that you need. It's all done for you.