

White Paper

Purchase to Pay for Healthcare



PROJECT HOSTS™
Security Compliant Clouds

Contents

- 1. Introduction and Scope
- 2. Healthcare Moves to the Cloud
- 3. SecureCloud P2P Product Features
- 4. The Palette User Experience
- 5. ERP Integration
- 6. Cloud Technology
- 7. Palette Software Accreditations
- 8. Project Hosts Accreditations

● → Executive Overview

● → For I.T. Executives



SecureCloud P2P

HEALTHCARE

● 1. Introduction and Scope

Healthcare organizations are looking to leverage technology to reduce the cost and inefficiency of their back office operations, and they need to ensure those solutions have the security standards the healthcare industry requires.

In April 2019 Palette and Project Hosts made available SecureCloud P2P, an ultra-secure AP automation and purchase to pay solution.

The two companies came together in 2017 to design and deploy both private and public cloud environments offering unparalleled uptime, infrastructure, security, compliance, and support.

SecureCloud P2P offers healthcare companies a secure platform for AP Automation and Purchase to Pay. The platform enables companies to capture vendor invoice data, process invoices with an approval workflow, automatically match POs, automate purchase requisitions and more.

This paper addresses both the features and security this industry-proven P2P platform provides.

● 2. Healthcare Moves to the Cloud

Today, many healthcare organizations are using cloud-based Software-as-a-Service (SaaS) applications for both critical and non-critical operations.

These include customer analytics, CRM, email, financial accounting, HR, and development and testing. At the edge, SaaS point solutions are commonly used for account verification, Know Your Customer (KYC), and security analytics.

However, as digital becomes mainstream and healthcare CxOs look for new ways to attract new clients, maximize retention, and slash costs, core services are moving to the cloud.

Fraudulent practices are driving healthcare organizations to be more diligent with the security of the SaaS software platforms they use.

Healthcare organizations are also digitally transforming their operations by deploying state-of-the-art technologies for fraud prevention, business processes improvement, regulatory compliance, and spend management.

There are good reasons why. The National Health Care Anti-Fraud Association® (NHCAA) estimates 3% of total health care expenditures are a result of fraudulent practices. Law enforcement agencies estimate the loss is closer to 10%, or \$300 billion.

One target of this trend is the elimination of paper processes and lengthy approval cycles with accounts payable automation and controlling indirect spend with purchasing automation, a task not typically handled by the ERP.



With the increasing collaboration between finance and procurement, Purchase to Pay platforms allow healthcare companies to control, regulate, and automate their purchasing policies.

By standardizing the ordering of goods and services, finance can reduce fraud, optimize expenditure, control indirect spend, negotiate discounts with key suppliers, and gain critical insights.

To do this, Healthcare organizations need a robust AP Automation and Purchase to Pay platform that has the highest security standards, operating procedures and best practices in place.

● 3. SecureCloud P2P Product Features

The SecureCloud P2P platform provides intelligent functionality for different accounts payable process areas:

Digital Capture • AP Automation • Purchase Automation • Document Archiving & Records Retention

SecureCloud P2P is a global solution for multiple ERPs, countries, currencies, and tax rules, with unlimited users, no user license costs, bulletproof compliance control, and minimal IT involvement. It's a modules-based cloud solution that grows with the healthcare organization.

Digital Capture

Companies in North America receive 90% of their supplier invoices by mail or email, and over 75% enter that invoice data into their systems manually.

Because it's labour intensive, error-prone and often requires hiring more people in order to manage growing invoice volumes, companies are looking to eliminate manual data entry completely.

The SecureCloud P2P Capture solution captures data from all invoice formats. Using AI and capture automation, data is extracted from both paper and emailed invoices.

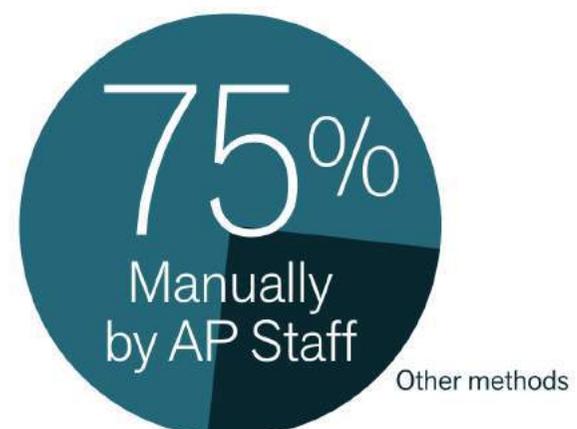
SecureCloud's capture solution intuitively detects and learns unique supplier invoices based on their respective layouts.

Scanning and/or the importing of data from emailed or paper invoices is fast with accuracy rates of 95% for paper and 100% for emailed electronic formats such as data PDFs, EDI, XML, Word, Excel, and CSV.

How Companies Receive Invoices



How Companies Enter Invoice Data



● 3. SecureCloud P2P Product Features (cont'd)

AP Automation

SecureCloud P2P automates the processing of PO and Non PO invoices, and matches invoices to purchase orders, goods receipts and recurring contracts. A mobile approval workflow lets employees use email to make one-click approvals.

**Invoices get processed
3X faster with automation –
and with less cost**

Invoice Processing

SecureCloud P2P has an automated user-friendly invoice processing system, designed solely for the invoice approval process.

- Invoices are visible in a dashboard showing their status 24/7
- Exceptions are flagged
- Once approved invoices are sent to ERP for recording

Invoice Approval Workflow

Users can flag invoices or line items and send them to business users for review and approval. Bottlenecks can be immediately remedied.

- Approvers get a complete package to review including invoice, PO, goods receipt and messages
- Automatic notifications, reminders and escalation
- 1-click approval in email and mobile
- Intuitive interface with drag & drop workflows for ad-hoc rerouting

● 3. SecureCloud P2P Product Features (cont'd)

AP Automation (cont'd)

Intelligent PO Matching

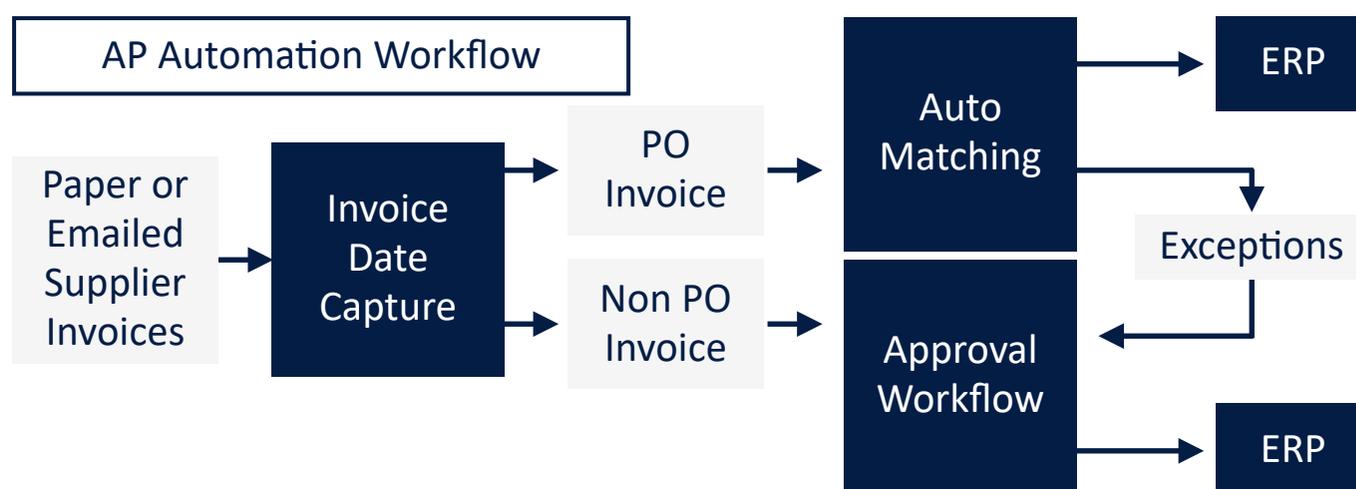
Automated purchase order matching shortens the approval cycle by matching invoices, purchase orders, goods receipts, and contract data.

One invoice can contain items from multiple purchase orders, and one purchase order can be matched to multiple invoices, whether they have been delivered in part or in full.

- Match at the header or line level
- Match purchase orders with hundreds of lines
- Match internal or external POs
- Exceptions are sent to approvers to validate with one-click approval
- Line level color coding speeds identification and remediation of errors
- Provides a complete audit trail, including messages

Once an invoice is automatically matched to the PO and/or a goods receipt, it is passed on to the ERP for recording.

Automatic matching of POs within minutes of invoice receipt means approval cycle times are 3X shorter



● 3. SecureCloud P2P Product Features (cont'd)

Purchase Automation

With a user-friendly system for purchase-to-pay, your clients can steer the purchase towards selected suppliers, lowering both costs and time spent on the purchasing process.

Administration is reduced for the purchasing department, which can devote more time to negotiate favourable agreements and discounts.

Automated Purchase Requisitions

Requisitions can be routed automatically based on a company's business rules, ensuring the highest percentage of straight-through processing when an invoice arrives.

- Flexible workflows for navigating bottlenecks
- Authorizations based on amount
- Include approvers from various departments
- Reroute a workflow without coding or user licenses
- Permissions set who can purchase what and from which supplier

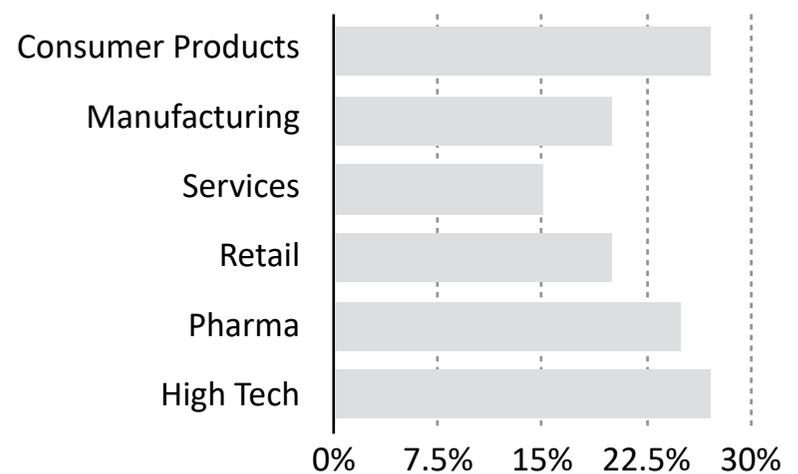
Approval Workflow for Purchasing

Purchase requisitions are available in a central dashboard where approvers have complete visibility to the expenditure request. Individual lines or entire requisitions can be rejected back to the requisitioner. Bottlenecks can be immediately remedied. Decision makers are aware of indirect spend in real time.

- Flexible workflows for navigating bottlenecks
- Authorizations based on amount
- Include approvers from various departments
- Users can make ad hoc changes to workflows

Clients get control of indirect spending – which can be up to 27% of total revenues

Percentage of revenues spent on indirect goods & services



Source: Accenture

● 3. SecureCloud P2P Product Features (cont'd)

Purchase Automation (cont'd)

Automated Purchase Orders

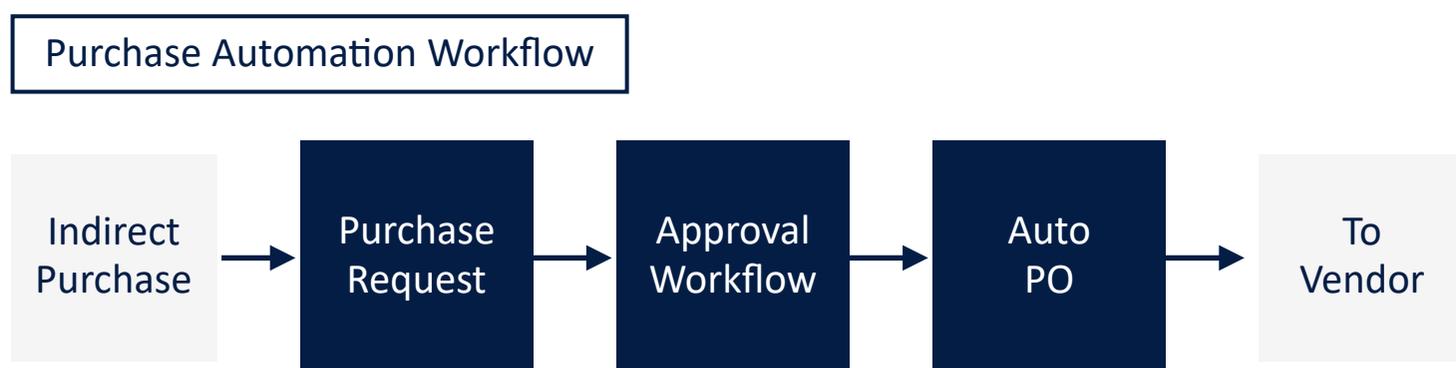
Purchase orders generated by SecureCloud P2P automated purchase requisitions are automatically delivered to vendors after they have been approved.

Both internal purchase orders generated by SecureCloud P2P and external purchase orders are located in one place—taking advantage of reporting and PO matching.

Tracking supplier performance such as commodity purchases, matching statistics, and vendor spend can all be facilitated in the reporting system.

- Employees purchase goods and services within a set budget
- Purchases can be limited to preferred and properly approved suppliers
- Generate better information for price and contract negotiations

Compliance control reduces the risk of fraudulent activity in the purchasing process



4. The Palette User Experience



User Satisfaction

With over 4,000 customers worldwide and over 250,000 users Palette has considerable market presence and experience. Customers have provided the following feedback:

- **96%** feel that Palette fulfills expectations
- **95%** consider Palette to be a worthwhile investment

What Customers Say

Per Sunnermark is CEO at Encare, a Swedish growth company with fewer than ten employees. Previously he was the CEO of a listed company with 2,700 employees and a revenue of over \$2 billion. He has used solutions from Palette Software in both companies to free up time for his organization and enable growth.

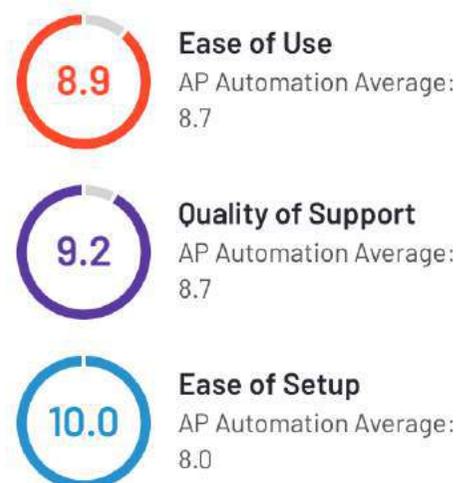
“It doesn’t matter what your organization looks like, its size or what you offer. As a CEO I enable my organizations growth and profitability which makes digitalization equally important no matter the size of the company.”

– Per Sunnermark, CEO – Encare

Minimal I.T. Involvement

The intuitive interface and ease of use has meant IT gets very few calls for support. Installation, technical support and customizations are handled by Palette support staff.

Palette User Ratings G2 Crowd



● 5. ERP Integration

SecureCloud P2P integrates with over 50 ERPs

The data integration process can often seem overwhelming. SecureCloud P2P's industry standard middleware alleviates the burden with powerful integration capabilities built into an easy to use graphical user interface.

It gives the ability to connect multi-company, distributed, or group finance applications in any enterprise, web-based, or cloud architecture.

Seamless integration with popular ERPs such as NetSuite, Oracle E Business Suite, Sage 200, SAP Business One, SAP R/3, Dynamics AX, NAV, and 365

SecureCloud P2P has a range of ready-to-use connections to the most common ERP systems on the market such as NetSuite, SAP Business One, Sage, Dynamics and more. Healthcare organizations get a proven integration methodology that enables a standard configuration and seamless data flow between SecureCloud P2P and their ERP.

The SecureCloud P2P integration interface offers several options to facilitate communications and data sharing between SecureCloud P2P and your client's business system.

SecureCloud P2P API and integration technologies products and services create flexible opportunities to implement secure, efficient and transparent system connectivity, with high business and user value.

Whether they use the SecureCloud P2P standard API to integrate or one of our many connectors, SecureCloud P2P Integrated Solutions supports Stored Procedures, Web Service or Files, XML and/or text files and tab-delimited integrations.

Clients improve business processes through integration of:

- Master data such as General Ledger and other account coding, supplier, and payment data is brought into SecureCloud P2P for validation and workflows.
- Business transaction data, e.g., purchase order, delivery receipts (full or partial), supplier invoice data and more, are regularly synchronized between SecureCloud P2P and the client's business system(s).
- Transfer of approved/matched supplier invoices, employee expense forms and other optional transactions such as purchase requisitions are sent for further processing by the client's system for further processing and/or vouchering.

● 6. Cloud Technology

SecureCloud P2P features secure access and leverages a healthcare organization's remote key authentication services.

SecureCloud P2P Cloud Technology

Project Hosts ensures that encryption of all data, including Personally Identifiable Information (PII) and protected health information (PHI) is handled in transit and at rest in both production and disaster recovery (DR) instances.

Production and DR environments are located in separate centers on unique power grids, backup power, and fuel sources. Uptime service level agreements meet the most rigid client requirements.

Project Hosts set of Azure managed services extend compliance beyond the infrastructure (IaaS) and platform (PaaS) level to protect entire applications at the Software (SaaS) level, implementing controls related to access, authentication, encryption, auditing, scanning, business continuity and change management.

Project Hosts SecureCloud P2P Service Implements and Manages:

- ISO 27001 Security Controls
- Azure subnets with their NSG "firewall" access controls
- Active Directory Domain to manage servers and group policy
- Web Application Proxy (WAP) servers as the controlled front door to the Deployment
- McAfee Host Intrusion Prevention System (HIPS) on every server
- EndPoint Protection centrally managed by McAfee ePolicy Orchestrator
- Remote Desktop Gateway servers for secure remote administration

- Logging configuration, collection, alerting, and review
- OS, DB and application software patching
- Project Hosts' Centralized inventory tracking and alerting system
- (Admin Center)
- Incident response system with periodic tests.

Project Hosts Also Manages:

- Single sign-on (SSO) from other authentication systems
- Quarterly web app vulnerability scanning
- Monthly cloning of servers in the deployment for scanning (where scanning production servers would cause disruption)
- Coordination with customer to patch web applications or modify configurations
- 24/7 support of applications on Project Hosts' approved application list
- Project Hosts' user authorization and administration tool (PH Portal)

Production and DR environments are located in separate centers on unique power grids, backup power, and fuel sources

● 6. Cloud Technology (cont'd)

Microsoft Azure and Security Standards

Project Hosts implements security on top of Microsoft Azure (both PaaS and SaaS) by way of “security envelopes” that are pre-audited and managed for various compliance standards.

Applications deployed in Azure and protected by these security envelopes inherit their compliance, removing a key barrier to migrating from on-premises or AWS deployments into Microsoft Azure.

Healthcare organizations have to assess the adequacy of the cloud service provider’s processes and controls that help to assure the confidentiality, integrity, and availability of data that is stored in the cloud.

When stored in Microsoft Azure, customer data inherits the benefits of multiple layers of security and governance technologies, operational practices, and compliance policies to enforce data privacy and integrity at very specific levels.

Project Hosts implements a set of operating procedures and practices, which ensures the implementation of the following security controls that cover most if not all information security standards:

- AC: Access Control Policy
- AT: Awareness and Training
- AU: Audit and Accountability
- CA: Security Assessment and Authorization
- CM: Configuration Management
- CP: Contingency Planning
- IA: Identification and Authentication

Healthcare organizations institutions have to assess the adequacy of their cloud service provider’s processes

- IR: Incident Response
- MP: Media Protection
- PE: Physical and Environmental Protection
- PL: Planning
- PS: Personnel Security
- RA: Risk Assessment
- SA: System and Services Acquisition
- SC: System and Communications Protection
- SI: System and Information Integrity

Seamless Upgrades

SecureCloud P2P is a cloud-based SaaS model, which means your clients always get access to the latest upgrades and releases of new functionality. Updates are included in the subscription and take place without any time-consuming and expensive upgrade projects.

● 7. Palette Software Accreditations

SOC 1

A SOC 1 Report (System and Organization Controls Report) is a report on Controls at a Service Organization which are relevant to user entities' internal control over financial reporting. The SOC1 Report is what you would have previously considered to be the standard SAS70 (or SSAE 16), complete with a Type I and Type II reports, but falls under the SSAE 18 guidance (as of May 1, 2017).

SOC 2

The Service and Organization Controls (SOC) 2 Report will be performed in accordance with AT-C 205 and based upon the Trust Services Criteria, with the ability to test and report on the design (Type I) and operating (Type II) effectiveness of a service organization's controls (just like SOC 1 / SSAE 18). The SOC 2 report focuses on a business's non-financial reporting controls as they relate to security, availability, processing integrity, confidentiality, and privacy of a system, as opposed to SOC 1/SSAE 18 which is focused on the financial reporting controls.

HIPAA

Health Insurance Portability and Accountability Act of 1996 is United States legislation that provides data privacy and security provisions for safeguarding medical information. Protected health information (PHI) under the US law is any information about health status, provision of health care, or payment for health care that is created or collected by a Covered Entity (or a Business Associate of a Covered Entity), and can be linked to a specific individual.

GDPR Ready

The General Data Protection Regulation 2016/679 is a regulation in EU law on data protection and privacy for all individuals within the European Union and the European Economic Area. It also addresses the export of personal data outside the EU and EEA areas.

PEPPOL

PEPPOL is an EDI protocol that enables public entities and their suppliers to exchange electronic procurement documents over its network.

8. Project Host Accreditations

HITRUST

The Health Information Trust Alliance, or HITRUST, is a privately held company located in the United States that, in collaboration with healthcare, technology and information security leaders, has established a Common Security Framework (CSF) that can be used by all organizations that create, access, store or exchange sensitive and/or regulated data. The CSF includes a prescriptive set of controls that seek to harmonize the requirements of multiple regulations and standards.

HIPAA

Health Insurance Portability and Accountability Act of 1996 is United States legislation that provides data privacy and security provisions for safeguarding medical information. Protected health information (PHI) under the US law is any information about health status, provision of health care, or payment for health care that is created or collected by a Covered Entity (or a Business Associate of a Covered Entity), and can be linked to a specific individual.

ISO 27001

ISO/IEC 27001 is an information security standard, part of the ISO/IEC 27000 family of standards, of which the last version was published in 2013, with a few minor updates since then. [1] It is published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) under the joint ISO and IEC subcommittee, ISO/IEC JTC 1/SC 27.[2]

FedRAMP

FedRAMP provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services used by the US government. Because its goal is to protect US citizen data in the cloud, it is government's most rigorous security compliance framework.

DoD IL5

With their PaaS-level PATO built on Microsoft Azure, Project Hosts is able to offer DoD Mission Owners and ISVs the ability to place their applications in a DISA validated cloud environment that satisfies 87% of the IL5 controls out of the box, along with services to manage the remaining application-level controls. Mission Partners access their environment directly from the DoD network (DODIN) over the DISA BCAP without ever having to traverse the Internet.

Project Hosts secures, manages and provides continuous monitoring for customer applications deployed on their platform. Project Hosts also develops application-specific System Security Plans (SSPs), manages annual 3PAO scanning and penetration testing of customer-provided applications, and provides monthly application-level POA&Ms.

About Palette Software

Palette Software is a market-leading vendor of financial process automation for domestic and global corporations.

Palette solutions automate the connecting and matching of purchase orders, invoices and contracts, on-premise or in the cloud.

Customers experience significant and measurable cost savings, productivity gains and operational excellence. Palette solutions are GDPR compliant and optimize financial management for more than 3,500 customers in 50+ countries.

With 25 years of experience, Palette and its partners offer automation solutions for organizations of all sizes worldwide.

palettesoftware.com

About Project Hosts

Project Hosts implements security and compliance on Azure for US Federal government, healthcare organizations and commercial enterprise. Project Hosts' pre-audited environments give organizations turnkey compliance for their applications, removing a key barrier to migration from on-premise deployments into Azure.

Project Hosts environments hold certifications and authorizations from ISO 27001, HIPAA, HITRUST, FedRAMP, and the DoD, including a DoD IL5 PATO, just 1 of 7 companies to achieve this authorization.

Healthcare organizations, federal, state and local government agencies, and enterprises rely on Project Hosts to ensure they have a cloud solution that meets their business needs, their budget and most importantly, protects their organization, employees and data from unauthorized access or theft.

projecthosts.com

Palette is now

rillion

rillion.com