By Craig McDonald
Founder & CEO, MailGuard

Trusted Communications in the Age of AI

Why Communication Integrity Matters More as Organisations Move Faster

TRUSTED COMMUNICATIONS IN THE AGE OF AI

WHY COMMUNICATION INTEGRITY MATTERS MORE AS ORGANISATIONS MOVE FASTER

When communications are trusted, decisions are better. When decisions are better, businesses **move forward with confidence.**

Click to download **Visual 1**

Executive Summary

Artificial Intelligence is increasing the speed at which organisations make decisions and execute actions.

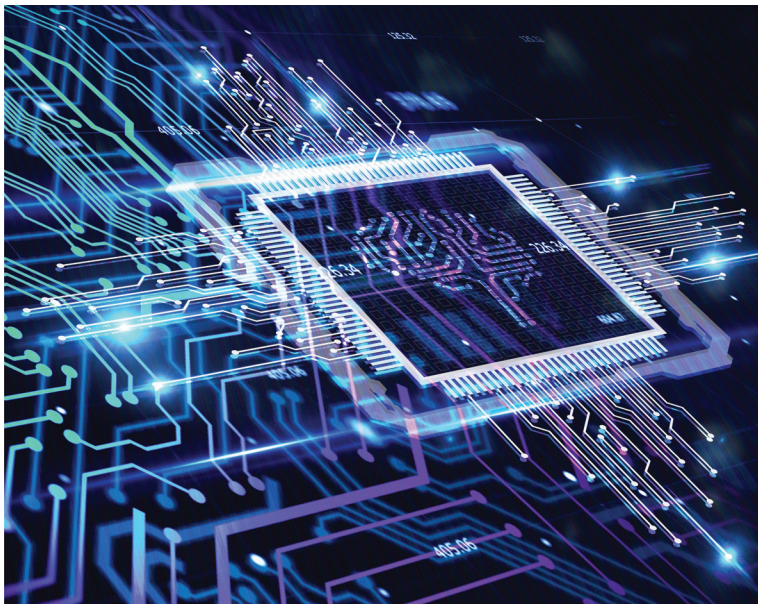
For the first time in history, business execution is accelerating faster than many organisations can verify the legitimacy of the information driving those actions.

This creates a new challenge.

As execution velocity increases, trust becomes a critical operational dependency.

Every business outcome begins with a communication.

Every communication must earn trust.



AI is Increasing Execution Velocity

Every major technology wave changes how organisations work. AI is no different.

Across every industry, organisations are exploring how AI can:

- Reduce manual effort
- Improve productivity
- Accelerate workflows
- Increase operational capacity
- Support decision making

The objective is simple. Do more with the same resources. Move faster, respond quicker, and execute better.

This creates significant opportunity. It also changes the importance of trust.

When decisions take days, there are often multiple opportunities to validate information.

When decisions take minutes, trust becomes increasingly important.

THE EXECUTION VELOCITY PRINCIPLE

AI ACCELERATES BUSINESS EXECUTION. VERIFICATION OFTEN DOES NOT ACCELERATE AT THE SAME RATE.

THE GAP CREATES EXECUTION RISK.

EXECUTION VELOCITY

ACCELERATING RAPIDLY

AI, automation and digital tools are driving execution speed to new levels.

THE GAP

Between execution and verification is widening.

VERIFICATION VELOCITY

INCREASING SLOWLY

Verification and trust processes often struggle to keep pace with execution.

THE CONSEQUENCE

The larger the gap, the greater the consequences of trusting the wrong information.

Fraudulent communications

Incorrect Payments

Operational Disruption

Financial Loss

Loss of Trust and Reputation

Close the gap. Build confidence. **Drive better outcomes.** Trusted communications are the foundation of **every confident decision.**

Click to download **Visual 2**

The Information Behind Every Decision

Every business decision begins with information...

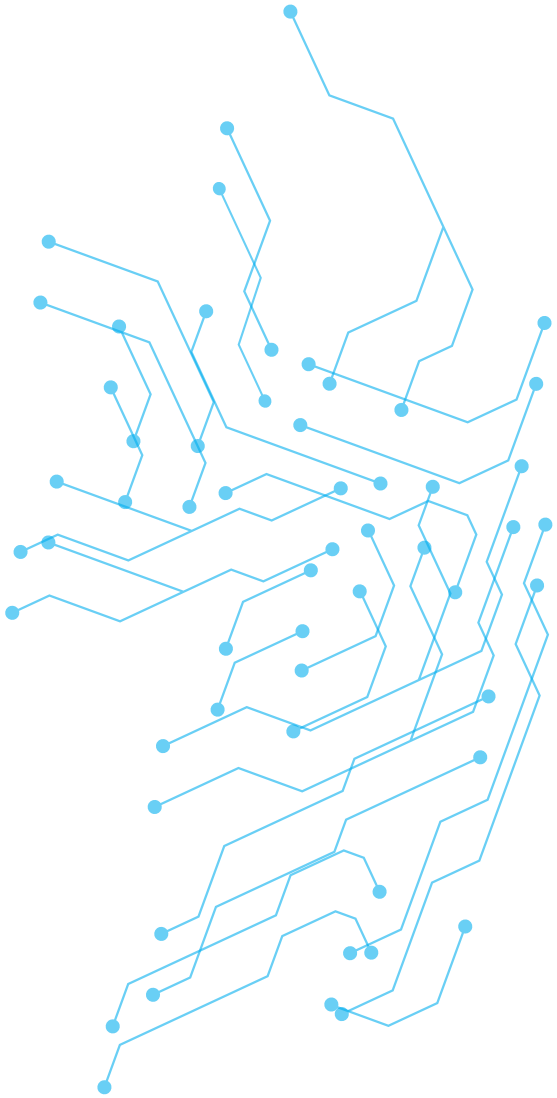
A customer request.
A supplier update.
An invoice.
A contract.
An approval.
A payment instruction.
An executive directive.

Before technology can automate a process, a person must first trust the information entering that process.

This principle does not change because AI is introduced. In many ways, it becomes more important.

AI can help organisations process information. It cannot guarantee that information is accurate, trustworthy, or legitimate.

The quality of outcomes remains dependent



Email Has Become Operational Infrastructure

Many organisations still think of email as a communication tool. In reality, email has become operational infrastructure.

It is often the mechanism through which organisations:

- Approve expenditure
- Manage suppliers
- Process invoices
- Communicate with customers
- Escalate issues
- Coordinate operations
- Authorise change

Many of the most important business decisions still begin with an email.

HOW BUSINESS EXECUTION ACTUALLY HAPPENS

FROM COMMUNICATION TO OUTCOME

01 TRUSTED COMMUNICATION

A message, request or instruction enters the organisation, typically via email or chat.

02 TRUST ASSESSMENT

Technology and human judgement assess the legitimacy and intent of the communication.

03 HUMAN DECISION

A person makes the decision to trust and act on the information.

04 EXECUTION

AI tools assist, automate and accelerate workflows to improve the speed of execution and efficiency.

05 BUSINESS OUTCOME

Value is created when the right action is taken. Risk is realised when the wrong information is trusted.

Every business outcome begins with a communication.
Every communication must **earn trust**.

Click to download **Visual 3**

When Trust is Manipulated

The communication is where trust begins, the decision is where trust is validated, the action is where value is created, and the outcome is where risk or reward is realised.

As organisations adopt AI assisted workflows, the speed of movement through this chain increases.

The underlying requirement for trust does not.

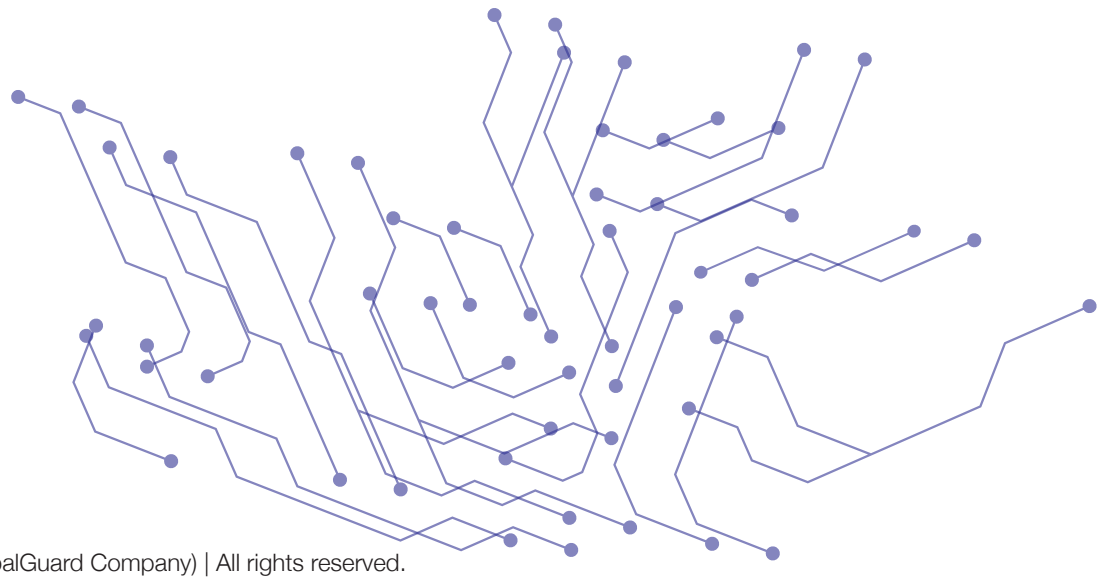
Historically, cybersecurity focused heavily on preventing unauthorised access. That remains important.

However, many modern attacks do not begin with technical compromise. They begin with communication. A supplier banking update, an executive request, a payment instruction, a request for information, or a message that appears legitimate.

The objective is not necessarily to compromise a system. The objective is to influence a decision.

As execution accelerates, verification becomes increasingly important. Trust is not a feeling. Trust is the outcome of verification. The organisations best positioned for the AI era will be those capable of verifying critical communications before business actions occur.

As organisations accelerate business processes, the consequences of trusting the wrong instruction can increase significantly.



Building Confidence in Trusted Communications

Most organisations adopt multiple layers of protection across critical business systems.

This reflects a simple reality. Different technologies identify different risks, different controls provide different forms of visibility, and different approaches contribute to resilience in different ways.

Email security is no exception.

As communication driven attacks continue to evolve, many organisations choose to maintain specialised protection focused on identifying malicious intent before users engage.

For most organisations, effective protection operates quietly in the background. Business continues uninterrupted, and decisions continue to be made on trusted information.

The value often becomes visible only when organisations review what was prevented from reaching their users.

"Cybercrime is not just about the data, it's about disruption, distraction, and erosion of trust."

Donald Good
Former Deputy Assistant Director, FBI Cyber Division

Why This Matters for MailGuard Customers

For more than two decades, MailGuard has helped organisations identify sophisticated impersonation attacks, business email compromise campaigns, credential harvesting attempts, QR code phishing campaigns, and emerging social engineering techniques before users engaged with them.

For many organisations, the value of protection is easiest to see in what did not happen.

- The payment that was not processed.
- The credentials that were not stolen.
- The impersonation attempt that did not succeed.
- The operational disruption that never occurred.

As AI becomes more deeply embedded into business operations, the role of trusted communications becomes increasingly important.

MailGuard's role remains simple. To help organisations identify malicious intent before user engagement and support confidence in the trusted communications that drive business decisions.

"Threats were still getting through Microsoft. MailGuard picked them up."

IT Manager
Porsche

"We've seen email-based attacks surge. MailGuard and Defender 365 together have helped us stay protected."

CISO
Silk Logistics Holdings

MailGuard protects more than:

- **5,500+** organisations protected
- Available in **141** countries
- Supporting operations across **17** currencies
- Supporting operations across **52** tax jurisdictions

Across these environments we continue to see:

- **Business Email Compromise**
- **Supplier Fraud**
- **Invoice Manipulation**
- **Executive Impersonation**
- **Credential Harvesting**

All designed to influence business decisions.

Independent Industry Perspectives

"It's the type of innovation that we want to see."

Satya Nadella
Chairman & CEO, Microsoft

"I support MailGuard's mission, as a solution designed to intercept threats before user engagement. It's fast, focused, and built with intent in mind."

Donald Good
Former Deputy Assistant Director, FBI Cyber Division

"You are being led by what I see as one of the world's best, at protecting secure infrastructure, securing your people, and securing your business."

Steve Miller
VP, Microsoft Australia & New Zealand

THE TECHNOLOGY CHANGED. THE TRUST CHALLENGE REMAINS.

DIFFERENT TOOLS. FASTER EXECUTION.
SAME FUNDAMENTAL REQUIREMENT.

THEN

TRADITIONAL BUSINESS OPERATIONS

PHONE CALLS
Conversations and verbal approvals

FAX & PAPER
Signed documents and physical delivery

EMAIL
Messages, approvals and attachments.

NOW

AI-POWERED BUSINESS OPERATIONS

AI & COPILOT ASSISTANCE
Intelligent support for faster decisions, emails and insights.

AUTOMATION & WORKFLOWS
Automated processes, email & chat replies, and approvals.

CLOUD & COLLABORATION
Real-time information sharing across teams.

ADVANCED ANALYTICS
Data-driven insights at speed and scale.

CONNECTED ECOSYSTEMS
Systems and partners integrated seamlessly.

TRUST

Assessing legitimacy.
Understanding intent.
Making confident decisions.

The technology is changing.
The **trust challenge** remains the same.

Click to download **Visual 4**

Final Thought

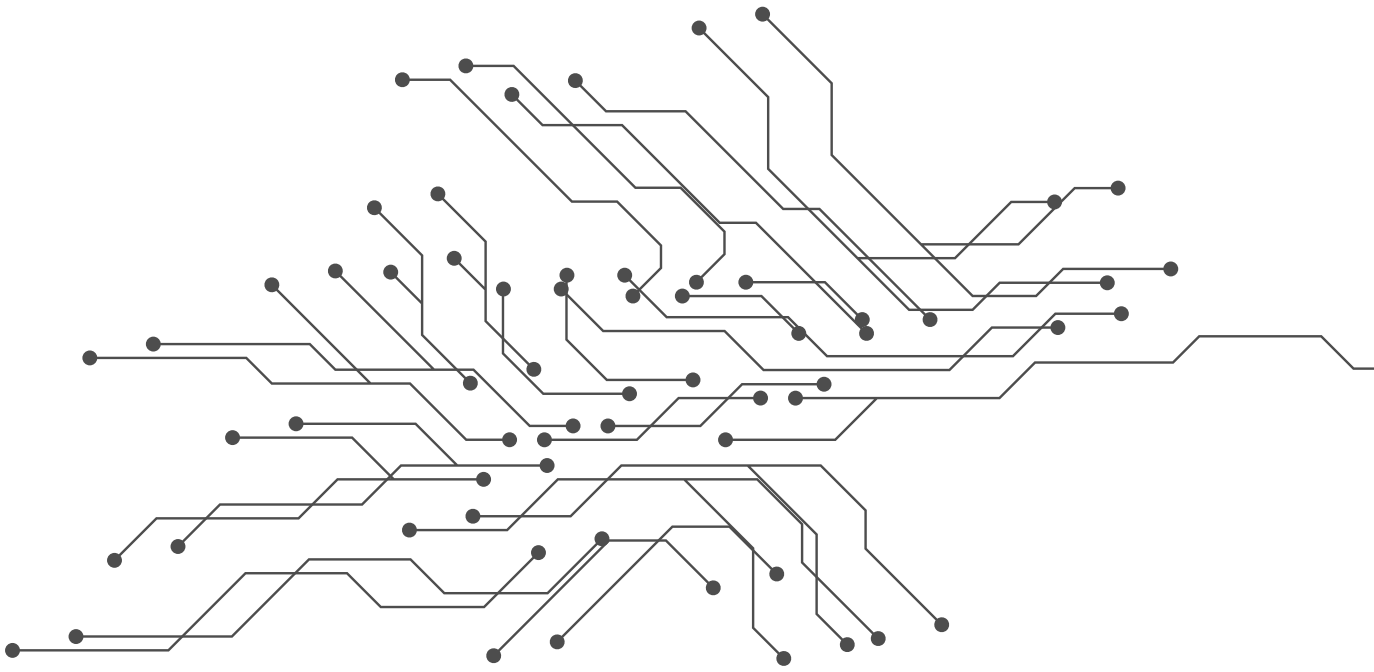
The AI era will not be defined by how quickly organisations can automate.

It will be defined by how confidently organisations can verify the information driving execution.

Because before any decision is made, any workflow is automated, or any action is taken, a communication must first be trusted.

And trust must be earned before execution.

Craig McDonald
CEO & Founder, MailGuard



Let's Connect

Craig McDonald
CEO & Founder
craig@mailguard.com.au

Author of:

- Surviving the Rise of Cybercrime
- Bulletproof Your Business
- Email: The Silent Business Assassin
- Execution Trust: Why The Next Era of Business Risk Will Be Defined By What Machines Are Allowed To Do (forthcoming)