CONDOPLEX® systems

TECHNICAL WHITE PAPER · ENTRY PHONE SYSTEMS

The Entry Phone Decision

Why the front door is now a network decision — and what boards running MESH, Verex and other legacy platforms need to understand before they spend another dollar

The lobby entry phone is the single most-used piece of security equipment in a residential building, and the one most likely to be running on an architecture that no longer has a future. This paper examines what has actually changed in the underlying telephone network, documents the current support status of the legacy platforms still in service across the Canadian multi-residential market, and sets out the technical case for the Condoplex ELP1040 and the wider Condoplex entry phone range as the replacement standard.

Prepared by Condoplex Systems · **September 2026**

For condominium boards, property managers, consulting engineers and Condoplex dealers

Contents

Conclusion

Sources and Notes

Executive Summary

Every multi-residential building has one device that every resident, every visitor, every contractor and every delivery driver touches, and that no one thinks about until it fails. It is the entry phone at the front door. It is also, in a large proportion of the Canadian condominium stock, the piece of equipment running on the oldest and least defensible technology in the building.

This paper makes four arguments, in order.

First, the ground under traditional entry phones has moved, and it has moved permanently. Most legacy entry phone systems are dialers: they place a telephone call over a copper line to reach a resident. That copper is being decommissioned on both sides of the border, and in Canada it is being decommissioned with no meaningful regulatory oversight of the notice given to the people who depend on it. This is not a forecast. In March 2026 the United States Federal Communications Commission removed the filing requirement that would have told building owners their copper was going away. In Toronto, residents of one neighbourhood received written notice in August 2026 that their copper home phone service would end on 4 November 2026. An entry phone that depends on a dial tone is an asset with a defined and shortening life, regardless of how well the hardware is working today.

Second, the legacy platforms still in service are in materially worse condition than most boards realise, and the two most commonly cited — MESH and Verex — are in different conditions from one another. Verex is genuinely finished: production ended in 2019, all technical support ended on 31 December 2021, and the last release of its management software targets operating systems Microsoft stopped patching between 2014 and 2020. Enterphone MESH is a different case, and the honest version is more useful than the alarmist one: the product is still sold under a different name, but its original manufacturer became insolvent and its assets have changed hands twice in five years. Those two situations call for two different conversations.

Third, the replacement decision is no longer a choice between brands of door station. It is a choice between architectures: a device that dials a phone line, a device that depends on a vendor cloud and a per-suite subscription, and a device that is a native network endpoint on a platform the building owns. The contractual terms published by two of the best-known alternatives in this market state plainly that service may be terminated without notice or cause, and in one case that the entry system may be disabled for non-payment and the resident database permanently deleted after 120 days. Those are the vendors describing their own products.

Fourth, the Condoplex ELP1040 and the wider Condoplex entry phone range answer the specific failure modes documented in this paper: they are VoIP endpoints rather than dialers, they carry two-way audio and video to a resident’s phone and to the guard station simultaneously, they share one resident database with the suite panels, elevator control and access control in the same building, and they sit on a platform with a documented record of keeping twenty-year-old field devices connected to current servers rather than stranding them.

WHAT THIS PAPER IS, AND IS NOT

This is a technical and commercial analysis prepared by Condoplex. It argues a position, and it names competing products. Every factual claim about a third party in this document is sourced to that company's own published material, to a regulator, or to peer-reviewed research, and the source is listed in the final section so it can be checked.

Where the evidence is contested, thin, or comes from a party with a commercial interest, this paper says so rather than rounding it in Condoplex's favour. A board that catches one overstated claim will disbelieve the rest of the document, and it would be right to.

The evidence in one page

The nine findings below carry most of the argument. Each is drawn from a regulator, a manufacturer's own document, or peer-reviewed research, and each is cited in full in the final section.

Finding	Source and date
The FCC has removed the requirement for carriers to file copper retirement notices; public notice may now be a posting on the carrier's own website	FCC 26-19, adopted 26 March 2026, effective 20 May 2026
AT&T is approved to discontinue service across more than 30% of its copper footprint, beginning 15 November 2026	FCC discontinuance application granted 13 January 2026
Copper decommissioning in Canada is proceeding without active regulatory oversight; one Toronto neighbourhood received about three months' notice	CRTC commissioner's public comments; Bell notice of service end 4 November 2026
The most widely installed telephone entry system in Canada is, by its manufacturer's own manual, "designed to work only with POTS"	Mircom TX3 manual LT-969 v7, March 2023
A second legacy manufacturer states it "does not recommend using POTS as a connection option"	DoorKing Product Reference Guide, January 2026
All Interlogix technical support — covering the Verex platform — ended on 31 December 2021; production stopped at the end of 2019	Carrier Fire & Security wind-down announcement, September 2019; Interlogix support notice
The last Verex Director release targets Windows XP through Windows 7 and SQL Server 2005 — all unsupported by Microsoft since 2014–2020	Verex A&E specification v4.9.1; Microsoft Lifecycle Policy
Enterphone MESH's original manufacturer sold its assets in a distressed transaction and the line has changed hands twice since	Viscount Systems, 20 December 2018; Identiv 2019; Vitaprotech/Hirsch 2024
Legacy 125 kHz proximity fobs are commercially cloned for $20–$30 on site, using equipment costing under $200	ACMO CM Magazine, Fall 2021; CCI Condovoice, Summer 2017

PART 1 The Most Consequential Device in the Building

It is worth being precise about what an entry phone actually does, because the framing determines the budget it gets.

A lobby entry panel is usually procured as a communications convenience: a way for a visitor to reach a resident and be let in. In practice it is the enforcement point for the building's entire perimeter policy. It decides who crosses the line between the public street and the private residence. It is the device a resident interacts with when they are least equipped to make a good security decision — at the door, in a hurry, often remotely, frequently with a stranger on the other end claiming to be a delivery. And it is the device that generates, or fails to generate, the record of who came in and when.

Three consequences follow from that, and they set up everything else in this paper.

1.1 It is a life-safety adjacent system, not a convenience

The entry panel does not usually control life-safety functions itself, but it sits in the same chain as devices that do. In Ontario, where an electromagnetic lock is used on a door in an access-to-exit, the Building Code requires the locking device to release immediately on activation of the fire alarm, and to release on loss of power to the fire alarm control panel or to the locking mechanism itself, on a manual switch operated by authorised personnel, on an electrical circuit fault, and on operation of a manual pull station within 600 millimetres of the door.

The point for a board is narrower than it first appears, and it should not be overstated: a broken intercom does not by itself breach the fire code. What breaches the code is a door release chain whose fail-safe behaviour can no longer be verified. When the system controlling the door is a platform whose manufacturer no longer exists, whose documentation is out of print, and whose remaining integrator is working from memory and salvaged parts, the building has lost the ability to demonstrate that the interlock still behaves as the Code requires. That is a compliance exposure, and it is invisible until someone tests it or an incident forces the question.

1.2 It creates a duty once it exists

Community association guidance in North America is consistent and slightly counter-intuitive on this: installing a security measure can create a legal duty that did not exist before it was installed, because residents rely on it. The Community Associations Institute's published guidance on minimising liability is direct about what follows from that. Where a security feature is out of service, residents should be warned, and written logs should be kept.

> *If a feature is temporarily out of service, residents should be warned of the issue, and written logs should be kept.*
>
> Community Associations Institute, "Security measures: How communities can minimize liability," 13 March 2024

Read that sentence next to the reality of a legacy entry system that fails intermittently, is repaired with parts of unknown provenance, and is documented nowhere. A board operating that system is accumulating an exposure that grows every month, and the exposure is not the cost of the replacement — it is the record of having known and not acted.

1.3 It is a reserve fund component whose stated remaining life is probably wrong

This is the argument that is hardest for anyone to rebut, because it rests on statute rather than opinion.

Under section 94 of the Ontario Condominium Act, 1998, a condominium corporation must conduct reserve fund studies on a rotating cycle. The physical analysis is required to inventory every component expected to require major repair or replacement within thirty years where the replacement cost exceeds $500, and to record for each one its age, normal expected life, remaining life expectancy, estimated year of replacement and estimated cost. The financial analysis must project at least thirty years forward.

An entry phone system is unambiguously such a component. So the question a board should put to itself is not whether to think about the entry phone. It is what number currently appears in the reserve fund study against it, and on what basis. If the study assigns a remaining life of eight or ten years to a system whose manufacturer stopped supporting it in 2021, or whose transport the carrier intends to decommission, then the study is carrying a figure that the public record contradicts. Correcting it is not a purchasing decision. It is a fiduciary one.

THE REFRAME THAT CHANGES THE CONVERSATION

A board can argue indefinitely about whether the entry phone is "still working." It cannot argue with the fact that the reserve fund study is required to state a remaining life expectancy for it, and that a manufacturer’s end-of-support date is a matter of public record that any owner, purchaser, lender or status-certificate reviewer can look up.

PART 2 The Dialer Is a Dead Architecture

Almost every entry phone installed in North America before roughly 2015, and a surprising number installed since, works the same way. A visitor selects a name. The panel seizes a telephone line and dials a number. The resident answers a telephone. The resident presses a digit, a relay closes, the door opens.

That architecture has a single point of dependency: the availability of a conventional telephone circuit. And that circuit is being withdrawn.

2.1 What the regulators have actually done

It is worth separating what regulators have done from what the intercom industry says they have done, because the marketing version is systematically overstated and a property manager who checks will find the discrepancy.

There is no single, day-precise "POTS shutdown deadline" in the United States. The date most often quoted in trade press derives from a wholesale unbundling transition in a 2019 FCC forbearance order, and that order explicitly did not require carriers to stop selling retail voice service over copper. Anyone citing it as a consumer cutoff is misreading it.

What has actually happened is more consequential and less widely understood. In March 2026 the FCC adopted its Network and Services Modernization Order, effective 20 May 2026. Among other things, it eliminated the requirement that carriers file copper retirement notices with the Commission. Reasonable public notice may now be given through industry fora, industry publications, or a posting on the carrier’s own website. Direct notice survives only for interconnecting carriers and 911 providers.

The practical translation for a building owner is worth stating plainly: the mechanism that would have told you your copper was being retired has been removed. Notice is now satisfied by something being published on a website you have no reason to visit.

The withdrawal itself is proceeding on a documented schedule. AT&T filed a discontinuance application on 1 December 2025 that was automatically granted on 13 January 2026, covering wire centres serving roughly 90,000 customers across eighteen states and bringing its approved discontinuances past thirty per cent of its copper footprint. Discontinuance under that grant begins on 15 November 2026. The company’s stated objective is to exit the large majority of its copper network outside California by the end of 2029. Separate applications covering approximately 184,000 residential and 15,000 business customers in California, filed in May 2026, propose discontinuance on or after 1 June 2027 and are being litigated.

2.2 Canada has less protection, not more

For a Canadian condominium audience this is the more important half, and the honest finding is uncomfortable.

There is no Canadian equivalent of the FCC’s discontinuance docket. The CRTC has a service-withdrawal procedure that applies to tariffed services, and it has been granting forbearance from regulating legacy access services on a case-by-case basis. In urban markets — which is to say, essentially every condominium market in the country — the framework does not bite. The result is that copper decommissioning in Canada is proceeding largely outside of regulatory supervision, a point a sitting CRTC commissioner has acknowledged publicly.

The concrete example is the one that should concentrate a board’s attention. Bell began decommissioning copper in 2022 and proceeds neighbourhood by neighbourhood. In Toronto’s Swansea area, residents received written notice in August 2026 that copper home phone service would end on 4 November 2026 — roughly three

months. Lifeline Canada, which provides medical alert services, reports that it receives no coordinated notice of copper shutdowns from carriers, and that approximately forty per cent of its customers use devices that plug into a copper phone jack.

WHY THE MEDICAL ALERT COMPARISON MATTERS

A personal medical alert device on a copper line is exactly the same class of asset as a lobby entry phone: a low-bandwidth, life-relevant device that quietly depends on a dial tone, owned by someone who was never told the dial tone was going away. If the sector serving vulnerable seniors gets roughly three months of notice and no coordination, a condominium corporation should not assume it will get more.

The underlying trend is confirmed by the regulator's own data rather than any vendor's assertion. The CRTC's Canadian Telecommunications Market Report 2026 records local and access revenues falling 4.8 per cent year over year from 2023 to 2024, a compound annual decline of 4.3 per cent across 2020 to 2024, with local and access falling from 11.0 per cent of total telecommunications revenues in 2020 to 8.3 per cent in 2024. Carriers are not maintaining a shrinking, unprofitable copper plant out of sentiment.

2.3 The vendors have conceded the point

The strongest evidence that the dialer architecture is finished does not come from Condoplex. It comes from the manufacturers who built the installed base.

Mircom's TX3 Telephone Access System is one of the most widely deployed multi-tenant entry systems in Canada. Its own installation and operation manual — current revision, version 7, March 2023 — describes two dial-out modes, ADC over dedicated subscriber lines and NSL intercepting existing building telephone lines, and states the position explicitly.

> *…designed to work only with POTS. Non-configurable PBX systems are not supported.*
>
> Mircom, TX3 Telephone Access System Installation and Operation Manual, LT-969 Version 7, March 2023

That is a current-revision manual for a mainstream product stating that it works only with the transport the carriers are actively retiring. Two years later, in May 2025, Mircom launched a cloud services platform whose published selling points include integrated VoIP to eliminate traditional phone lines. The company has conceded the argument in its own product roadmap.

DoorKing, another long-established telephone entry manufacturer, is blunter still. Its January 2026 product reference guide lists cellular and VoIP connectivity options alongside legacy POTS, with a plain recommendation attached.

> *DoorKing does not recommend using POTS (Plain Old Telephone Service) as a connection option.*
>
> DoorKing Product Reference Guide, Section 2, January 2026

When two legacy telephone entry manufacturers publicly disown the transport their own installed base runs on, the question for a board is no longer whether to migrate off it. It is whether to do so on a schedule of the building's choosing, or on the carrier's.

PART 3 What Buildings on Verex and MESH Actually Face

Two platform names come up repeatedly in the Canadian multi-residential market when the conversation turns to obsolete equipment: Verex and MESH. They are frequently mentioned in the same breath. They should not be. Their situations are materially different, and a board that treats them the same will either overspend or underestimate.

3.1 Verex: finished, and finished for longer than most owners realise

The corporate history matters here, because it explains why nobody is coming to help.

Verex was formerly Guardall North America, operating as a division of CSG Security Corp from 5201 Explorer Drive in Mississauga, Ontario. It reached United Technologies through Chubb, which UTC acquired in April 2003 — not, as is often repeated on resale listings, through GE. When UTC restructured its global security products business on 5 October 2010, Verex product began shipping under the Interlogix brand. The final Verex documentation carries a 2017 UTC Fire & Security copyright.

A CORRECTION WORTH MAKING IN FRONT OF A BOARD

Resale listings routinely describe this hardware as "GE Security Interlogix Verex." That is catalogue conflation from the period when UTC owned both GE Security and Chubb and folded them into one brand. It is not evidence that GE built or supported the product, and repeating it makes the rest of an assessment look unreliable.

On 19 September 2019 Carrier notified employees, and on 20 September distributors and the public, that it was winding down the Interlogix businesses in the United States and Canada.

> *After a thorough portfolio review of our security business, we have communicated our plans to wind down our Interlogix U.S. and Canada businesses. We plan to stop manufacturing new Interlogix products once final orders have been fulfilled, anticipated to be at the end of 2019.*
>
> Carrier Fire & Security Products, September 2019

Interlogix subsequently issued a product support announcement stating that technical support for its listed products would no longer be available after 31 December 2021. One point of precision is owed to the reader: Verex and Director are not named on that particular notice, whose product list covers other Interlogix lines. Given that the wind-down covered the entire Interlogix North American business and Verex was an Interlogix brand, the practical conclusion is not in doubt — but the defensible way to state it to a board is that Interlogix ended technical support for its product lines on 31 December 2021 and no Verex-specific support has been available since, rather than citing a Verex end-of-life bulletin that does not appear to exist publicly.

The head-end is the real problem

Hardware attrition is the obvious risk with any discontinued platform. With Verex it is not the most serious one. The management software is.

Verex Director is the software that holds the resident and credential database and administers the panels. The published A&E guide specification for version 4.9.1 lists its supported operating systems as Windows XP Professional, Windows Server 2003, Windows Vista Business or Ultimate, Windows 7 Professional, and Windows Server 2008 R2 Enterprise, with the database running on Microsoft SQL Server 2005 Express or SQL Server 2000/2005. The last release of Director that can be dated is version 5.0, from June 2017.

Set that against Microsoft's own lifecycle dates: Windows XP ended support on 8 April 2014, SQL Server 2005 on 12 April 2016, SQL Server 2008 and 2008 R2 on 9 July 2019, and both Windows 7 and Windows Server 2008 R2 on 14 January 2020.

The board-level translation is this. In a building still running Verex, there is very likely a computer in a service room, connected to the building network, running an operating system that has received no security patches for between five and twelve years, hosting an unpatched database that contains the access credentials of every resident. That machine cannot be replaced with a modern one, because the software will not install on a supported operating system. It cannot be patched. And when its hard drive fails — which is a question of when — the credential database goes with it.

And it may not be your entry phone at all

There is an important technical point here that is routinely missed, and getting it right immediately marks out a serious assessment from a superficial one.

The Verex 120-series catalogue is access control and intrusion equipment: two- and four-door controllers, switchplate and mullion proximity readers, keypads, power supplies, expansion modules and credentials. Extensive searching of Verex and Interlogix product documentation turns up no Verex telephone entry or lobby entry phone product.

In practice, that means a building described as "running Verex" almost certainly has a lobby entry panel from an entirely different manufacturer — Mircom, Enterphone, Cornell, DoorKing, Lee-Dan, Aiphone or similar — interfaced to a Verex access control head-end. Which means the building has two obsolescence problems, from two vendors, with two different remediation paths and two different costs. Any proposal that does not distinguish between them has not surveyed the building properly.

The credentials are the quiet emergency

Verex credentials are G-Prox II proximity cards and fobs, supplied in 26-bit industry standard or 36-bit Verex format. This is the unencrypted low-frequency proximity technology class, and its weakness is not a theoretical concern raised by a vendor trying to sell an upgrade. It is documented by the condominium industry's own associations.

The Association of Condominium Managers of Ontario published an analysis in its magazine in 2021 describing standard fobs of this class as transmitting an unencrypted facility code and card number continuously, with no encryption in the communication between card and reader, and reporting commercial cloning available at twenty to thirty dollars per fob, performed on site, with blank fobs costing as little as ten. The Canadian Condominium Institute had already described commercial fob duplication as a growing and disturbing business trend in 2017, noting cloning equipment available for under two hundred dollars and operators advertising the ability to clone seventy-five formats across thirty-five countries.

In 2024 a director at HID, the largest credential manufacturer in the industry, publicly described 125 kHz proximity cards and readers in the era of consumer cloning tools as not just obsolete but actually dangerous. The statement was subsequently softened, which is itself informative.

WHAT THIS MEANS IN PRACTICE

A building running legacy proximity credentials cannot know how many working copies of its fobs exist. There is no audit that reveals it, because a cloned credential presents as the original. Every departed resident, contractor, and former staff member is a potential holder. This is not a reason to panic; it is a reason to stop treating credential technology as a component that can be deferred to the next reserve cycle.

3.2 MESH: the honest version is more useful than the alarming one

MESH is Enterphone MESH, and its history is the history of its manufacturer.

Viscount Systems Inc. of Burnaby, British Columbia announced field trials of MESH in March 2003, describing an integrated platform converging voice, data and video — intercom and emergency communications, card access, elevator control and alarms, and CCTV. The company had been a research and development affiliate of Telus from 1969 to 1997 and claimed roughly 35,000 sites in more than thirty countries. The architecture comprised MESH panels at doors and gates, MESHguard consoles for visitor management, and IP-addressable panels networked to MESH servers.

What happened next is a matter of public record. Viscount voluntarily deregistered with the United States Securities and Exchange Commission in November 2016. In December 2018 it agreed to sell substantially all of its assets to Identiv for approximately one million dollars in cash and two million in stock plus earn-outs. The announcement was candid.

> *Over the last few years, Viscount has faced significant hurdles in delivering its product.*
>
> Scott Sieracki, Chief Executive Officer, Viscount Systems Inc., 20 December 2018

The same release warned that the company's previously filed financial statements should not be relied upon, and that no assurance could be given that shareholders would ever receive any recovery following satisfaction of Viscount's remaining obligations to creditors. Identiv completed the acquisition of the Freedom, Liberty, Enterphone MESH and Services business lines on 3 January 2019. In April 2024 Identiv agreed to sell its physical security business to Vitaprotech for $145 million; the transaction completed on 9 September 2024 and the combined entity was relaunched under the Hirsch brand, headquartered in Lyon, France.

What that means today — stated accurately

It would be convenient for this paper to assert that MESH is discontinued and unsupported. It is not, and a board that was told so and then checked would be entitled to discount everything else in the document.

The Enterphone product family is still actively sold. The current Hirsch catalogue lists Enterphone iQ, Enterphone 19, Enterphone Kiosk, Enterphone Microserver and Enterphone Mobile, and the current overview brochure does not use the MESH name at all. The MESH 19, MESH IQ and MESH Kiosk hardware maps onto that current line, so an upgrade path plausibly exists. No end-of-life or end-of-support notice for Enterphone MESH appears to have been published, and MESH is not listed on Hirsch's legacy product support page.

The accurate case is therefore different, and stronger for being accurate:

- The original manufacturer no longer exists. Viscount was, by its own account, unable to deliver its product, and sold its assets in a distressed transaction.

- The product has passed through two ownership changes in five years — Viscount to Identiv in 2019, Identiv to Vitaprotech in 2024 — and is now supported from a corporate structure two acquisitions removed from the engineers who designed it.
- The brand name the building knows its system by has been retired from the current catalogue.
- The Enterphone MESH installation guide still lists technical support at the original Burnaby telephone number and an email address at a misspelled legacy domain, which is a reasonable proxy for how much attention the documentation has received since 2019.
- The architecture is a browser-managed Linux appliance whose published default administrative username is a single well-known word, which is a question worth putting to whoever maintains it.

THE ACTION A BOARD SHOULD TAKE ON MESH

Not "replace it immediately." Ask Hirsch, in writing, for a support-status letter covering your specific panel model and firmware revision: is it supported, for how long, what is the security update commitment, and what is the upgrade path and its cost. Then compare that letter with what a replacement platform will commit to in writing. If the letter does not arrive, or arrives without dates, that is the answer.

3.3 The life-support option, and why it usually fails

Faced with an obsolete system, the first instinct is to keep it running with salvaged parts. It is a legitimate short-term tactic and it deserves a fair hearing rather than a dismissal.

Refurbished Verex and Interlogix hardware is genuinely available on secondary marketplaces, and many long-established commercial integrators keep pulled parts from upgraded buildings. For a board that needs to get through a fiscal year before funding a capital project, buying a spare controller as a shelf spare is a rational hedge.

What it is not is a strategy, for four reasons that compound.

1. A salvaged part carries no warranty from anyone. Carrier's commitment covered product purchased through its dealer channel; a board buying a panel from a marketplace listing has no recourse of any kind if it fails on installation.
2. There is no firmware. Interlogix technical support closed at the end of 2021. If a salvaged board is at a different firmware revision than the system it is joining, there is no source for the version that would make them compatible and no one to ask.
3. Provenance is unverifiable. A unit pulled from another building may have been removed because it was faulty. Nothing in a marketplace listing distinguishes a working spare from the reason a previous building gave up.
4. It does not address the head-end, the credentials, or the transport. Keeping the field hardware alive does nothing about an unpatchable Windows 7 management computer, cloneable proximity fobs, or a telephone line the carrier intends to decommission. The building spends money and ends the year in the same position.

The wider risk category is well recognised. The United States Cybersecurity and Infrastructure Security Agency published two fact sheets on grey market components in critical manufacturing supply chains in August 2024, addressing precisely the class of risk that arises when critical infrastructure depends on components acquired outside authorised channels.

PART 4 The Condoplex Answer: the ELP1040 and the Entry Phone Range

Everything above describes the problem. This part describes what Condoplex builds and why its architecture answers each of the specific failure modes documented so far.

4.1 It is a VoIP endpoint, not a dialer — this is the whole argument

The single most important thing to understand about the ELP1040 is architectural rather than cosmetic. It does not seize a telephone line and dial a number. It is a network device that places SIP-based voice and video calls over the building's Ethernet infrastructure. Its published connectivity is Ethernet, VoIP, and RS-485 to slave devices at 100 megabit.

Consider what that removes from the risk register in Part 2. There is no subscriber line for a carrier to decommission. There is no dependency on a dial tone whose withdrawal is now notified by a posting on a website. There is no recurring per-line telephone charge rising at a rate the building cannot control, and no exposure to the phase-out that both Mircom's and DoorKing's own documentation acknowledges.

This also reframes the cost conversation in the building's favour. A building running a traditional dialer is paying a carrier every month for lines that exist solely to serve the front door. A VoIP entry system runs on network infrastructure the building already has and already pays for. Condoplex extends this deliberately across the wider platform through its VoIP services — A/V calling, PBX and SIP trunk integration, call escalation and text messaging — with the explicit objective of reducing or eliminating the building's dependence on traditional phone lines rather than merely working around them.

THE ONE-SENTENCE VERSION

Every competitor discussed in this paper is either migrating off the telephone line, charging a subscription to escape it, or recommending against it in their own manual. Condoplex was architected without it.

4.2 Two-way audio and video, to the resident's phone and the guard screen at once

The second differentiator is what actually happens when a visitor presses a button, and it is where the gap between a dialer and a platform becomes visible to residents rather than to engineers.

On a traditional system, a visitor is a voice. The resident hears someone claiming to be a courier and makes a security decision with no information beyond an audio channel of indifferent quality. On the Condoplex platform the resident sees the visitor. The ELP1040 carries a built-in ONVIF-compliant IP camera, and the Condoplex mobile application — available for both iOS and Android, for residents and for guards — supports two-way audio and video calling. A resident can answer the front door from a phone anywhere, see who is standing there, speak with them, and release the door.

What distinguishes this from the app-based intercoms discussed in Part 6 is that it is not an either/or. The same call is available to the guard or concierge station simultaneously. Condoplex describes the guard screen as consolidating entry calls, suite alarms, elevator activity, panic alerts and water leak notifications onto a single display, with two-way audio and video to residents, entry phones and suite panels without a separate telephone. Events are prioritised and queued so nothing is lost during a busy period, and every guard action is logged automatically with a timestamp.

That last point deserves emphasis in the context of Part 1. The audit trail is not an add-on module or a paid analytics tier. It is a property of the architecture: because every device is on one platform reporting to one server, the record of who called, who answered, what the guard did and when the door opened exists by default.

- For the resident — see and speak to the visitor from anywhere, release the door from the app, arm and disarm the suite panel, and receive parcel and alarm notifications through one application rather than several.
- For the guard — answer entry calls with live video, release doors and elevators, and reach any resident directly from the same screen that is already showing building alarms.
- For management — visibility into building events and system health remotely, with a single record rather than a reconstruction across separate systems.

4.3 The ELP1040 itself

The ELP1040 is Condoplex's flagship lobby entry panel. It is built around a large-format portrait touchscreen with gesture control, capable of displaying a resident directory of up to 25,000 names — a capacity that matters less for a single tower than for a multi-building campus administered as one estate.

The panel runs an embedded Linux operating system rather than depending on an obsolete desktop Windows installation. This distinction is worth stating carefully, because it is frequently overstated by vendors who should know better. Linux is not maintenance-free. It requires security patching, and its releases reach end of support like any other operating system. Condoplex is no exception, and this paper would fail its own test if it pretended otherwise.

The difference is not that the exposure disappears. It is that it is dated, scoped, communicated in advance, and survivable — which is precisely what the platforms in Part 3 could not offer. The current Condoplex platform release is CPLX Linux 6, and the position on both releases is set out below without softening.

Condoplex platform lifecycle	Position
Current release	CPLX Linux 6. Supported for the foreseeable future.
How updates are delivered on Linux 6	Continuous delivery. Security and feature updates are applied as software, several times a year, without hardware replacement.
Previous release	CPLX Linux 5, retiring February 2027.
What the 5 to 6 migration requires	A head-end upgrade with new controllers. This is a planned capital item, not a remote software push, and boards on Linux 5 should be budgeting for it now.
What is retained through that migration	Field devices. Entry panels, suite panels and readers carry across — the upgrade is to the head end, not the building.
Dealer readiness	Condoplex is retraining its dealer network ahead of the February 2027 date.

That table is included deliberately, because it is the honest version and the honest version makes the argument better than a claim of permanence would. A building on CPLX Linux 5 has a dated event ahead of it, a defined scope, a vendor that has published the date in advance, a dealer network being retrained to deliver it, and — critically — field hardware that carries across rather than being scrapped. Compare that with the position of a

Verex building, whose vendor stopped manufacturing at the end of 2019 and ended support on 31 December 2021, and whose management software still runs on Windows 7. Both are operating-system end-of-life events. Only one of them was managed.

The forward-looking half matters too. Linux 5 was installed software; Linux 6 is delivered continuously. The migration a Linux 5 building faces in 2027 is a transition off the old model and into the one where capability arrives as software on hardware already installed. It is the last upgrade of that kind, not the first of a recurring series.

ASK THIS OF CONDOPLEX, AND OF EVERYONE ELSE

Which operating-system release is my system on, what is its supported life, how is the upgrade to the next release delivered, what does it cost, and is it included in what I already pay? Condoplex's answers to those five questions are in the table above. A vendor who cannot answer them about their own product is describing the same risk as the platform you are replacing.

The housing is high-grade 316 stainless steel and vandal resistant, with all components flush mounted. It is available in indoor and outdoor recessed variants and in indoor and outdoor pedestal configurations in both straight and angled forms.

The ELP1040 in pedestal configuration. The panel is finished to specification rather than supplied in a fixed housing colour, so the lobby is designed first and the hardware matched to it.

That last point is not a cosmetic footnote. In a competitive tender, the specifying architect or interior designer usually has a lobby scheme before they have a security package, and most entry panels arrive in a single industrial finish that has to be designed around. A panel finished to the building's specification removes an objection that has nothing to do with security and everything to do with who signs the cheque.

Published specification

Specification	ELP1040

Models	ELP1040VTS indoor recessed; ELP1040VTO outdoor recessed; ELP1040IPA / IPS indoor pedestal (straight / angled); ELP1040OPA / OPS outdoor pedestal (straight / angled)
Display	Large-format portrait gesture-controlled colour touchscreen; directory capacity up to 25,000 names
Camera	Built-in ONVIF IP camera; reads temporary 2D barcode passes; detects proximity of a caller
Operating system	Linux
Housing	High-grade 316 stainless steel, vandal-resistant, flush-mounted components
Audio	Adjustable 2.0 watts; hands-free to suite panel, telephone system, guard station and guard phone
Connectivity	Ethernet; VoIP; RS-485 to slave devices; 100 Mb
Access functions	Lobby door and/or elevator floor restriction; 12-digit keypad; internal card reader; Wiegand output for integration with third-party access control
Relay output	2 × 3 A for maglocks, door strikes or external camera lock
Power	12 VDC or 120 VAC @ 3 A UPS
Physical	Recessed fascia 16⅜″ W × 29 3⁄16″ H × 5″ D; back box 15 7⁄16″ W × 25 3⁄16″ H × 4 11⁄16″ D; weight 30 lb (12 kg)
Other	Multi-lingual voice prompts; messaging; automated software updates; security audit record of visitor calls; postal lock switch; automatic/accessible door push button (pedestal mount)

A SPECIFICATION NOTE THAT SHOULD BE MADE EXPLICITLY, NOT BURIED

The ELP1040's built-in card reader is published as HID-compatible 125 kHz. For the reasons set out in Part 3.4, no building should standardise on 125 kHz proximity credentials in 2026. Specify encrypted 13.56 MHz credentials on the Condoplex access control platform, and treat the panel's built-in reader as a compatibility path for an existing credential population during a phased migration rather than as the end state. Any vendor — including this one — who lets a board buy new hardware and re-issue the same cloneable fobs has not done the job.

4.4 The rest of the range

A building is not one door, and a range that only addresses the main lobby forces a building into multiple vendors — which is the condition Part 3 describes as the root cause of the problem.

ELP770 — the compact VoIP panel

The ELP770 is a VoIP entry panel for multi-residential and office towers built around a seven-inch portrait gesture-controlled touchscreen at 250 to 400 nits, with a two-megapixel camera and LED illumination. It supports SIP VoIP communications, works with the iOS and Android application, and adds video capture for

missed calls, interactive texting and hot buttons. It is available in indoor and outdoor models, surface or recessed with hood, and — a practical detail for retrofit work — supports either 12 VDC or Power over Ethernet, which can remove a power run from the installation entirely. Two further models, the ELP780 and the lower-cost ELP520, extend the range downward for secondary entrances and smaller properties.

Intercom and panic stations

For parking levels, stairwells, change rooms and other areas of isolation, the RPI-C, RPI-WP, RPIN-C and RPS-1 network intercom and panic stations put audited communication throughout the building. The audio channel is opened automatically to the security desk, and the server records acknowledgement time, guard actions and call termination.

One feature of these stations deserves particular attention from any board that has ever wondered whether the panic button in the garage actually works. The units are fully interrogated: the system polls them each cycle and signals the security desk if a unit becomes defective or goes off-line. Nobody has to walk the building pressing buttons to discover that an emergency device has been dead for three months.

4.5 Condoplex's own answer to the outage question

Part 7 of this paper tells boards to ask every bidder which functions survive a loss of internet connectivity, function by function, and to insist on the answer in writing. It would be indefensible to set that test and then not sit it. This is the Condoplex answer.

The architectural reason the answer looks the way it does is that the Condoplex server is on the building's own network, not in a data centre. Entry panels, readers, suite panels, the guard station and elevator interfaces all talk to that local server. A loss of the building's internet link therefore severs the building from the outside world, not from itself.

Function	During a loss of building internet
Credential authentication at readers	Continues — authenticated locally against the on-site server
Door release from the entry panel	Continues
Visitor call to the guard or concierge station	Continues, with audio and video
Guard door and elevator release	Continues
Suite panel arm and disarm	Continues
Suite alarms and panic stations reporting to the guard	Continues
Elevator floor control	Continues
Audit logging	Continues — written locally and synchronised when the link returns
Resident SIP calls to telephones	Depends on configuration — continues where the SIP trunk or PBX is on premise; stops where resident calling is routed through a hosted service
Mobile app calling from outside the building	Stops until the link returns

Function	During a loss of building internet
Push notifications to residents	Stops until the link returns
Cloud backup of configuration and audit logs	Pauses; resumes automatically on reconnection
Remote factory technical support	Unavailable until the link returns
Software and security updates	Deferred until the link returns

Two honest qualifications belong with that table. The first is the SIP row: whether a resident's telephone still rings during an outage depends on how the building's calling is configured, and that is a design decision to settle at specification rather than a property of the panel. The second is that "no cloud required to function" — a claim made in the comparison later in this paper — means precisely what the table says and no more. Cloud services are used for backup, for remote support, for updates and for reaching residents' phones when they are away from the building. What is not cloud-dependent is the operation of the building's own security: the doors, the credentials, the guard station and the record of what happened.

The same distinction applies to the statement that Condoplex hardware keeps working if the commercial relationship ends. The equipment is owned by the corporation and the server is on site, so the building continues to admit residents, release doors and log events. What lapses with the service agreement is what the service agreement provides — software and security updates, cloud backup, factory technical support and the extended warranty. That is a materially different position from a platform whose published terms permit the service itself to be suspended, but it is not a claim of perpetual immortality and should not be sold as one.

4.6 One platform, one database — why integration is a security property

The recurring theme of Part 3 is not that individual products failed. It is that buildings ended up operating several disconnected systems from several vendors, and the seams between them became the vulnerability.

Condoplex's architectural position is that resident information is entered once and propagates to every device — entry phones, suite panels, guard screens and the mobile app — from a single database. The consequences are practical:

- A resident who moves out is removed once. There is no scenario in which a name persists on the lobby directory, or a credential remains live, because a second system was not updated.
- The guard sees one prioritised queue rather than three screens. Incident response does not depend on which monitor someone happened to be facing.
- Elevator control is part of the same conversation. A resident releases their floor from the lobby panel, the suite panel or the app; floor access can vary by time of day; and inter-floor guest release and private child-lock elevator control are available on compatible panels.
- Suite panels across generations coexist. SP2300, SP2660 and SP2800 panels connect to the same building-wide server, so a building retrofits at its own pace rather than in one capital event.
- A suite smoke alarm can notify the guard before the building fire system trips — which, beyond the safety benefit, is a direct avoided cost in false-alarm charges.

The audit trail argument from Part 1 lands here. A building with one platform can produce a single exportable record for an insurer or a police investigation. A building with four vendors produces four partial records with mismatched clocks, assembled by hand after the fact.

4.7 Backward compatibility: the argument no cloud vendor can make

This is the differentiator that matters most to a board with an existing Condoplex installation, and it is the direct answer to the stranded-asset problem that Part 3 documents.

> *If your building already has a Condoplex system, a full replacement is rarely necessary. Condoplex's backward-compatible design means that devices installed 20 — or even 25 years ago — can still connect to a modern server and benefit from current software.*
>
> Condoplex Customer Guide 2026

Taken component by component, the published position is that access control requires replacing the control unit only; intercoms require upgrading the head end only; suite alarms require a software upgrade; the resident database is converted automatically; staff learn new features rather than a new system; and service downtime is minimal.

The contrast with everything in Part 3 is the point. Verex owners are being told their platform is finished and everything must go. The value of a vendor that has demonstrably kept two-decade-old field devices connected to current servers is not sentimental — it is the expected lifetime cost of the next twenty years of ownership.

The forward-looking version of the same argument is the software update model. Condoplex delivers new capability through dynamic software updates applied several times a year rather than through hardware replacement, with roadmap features including mobile guest check-in, QR code and time-limited PIN access, NFC tap-to-enter, contactless entry with AI-assisted identity matching, parcel lockers, EV charging integration and camera analytics — all intended to reach compatible buildings through updates without core hardware replacement. Whether every roadmap item ships on schedule is a fair question for any vendor; the architectural claim, that capability arrives as software on hardware the building already owns, is verifiable against the twenty-year track record above.

4.8 Designed and made in Canada, and why that is now a security specification

Condoplex is a Canadian manufacturer, operating from Toronto, and describes its products as designed and made in Canada. For most of the last twenty years that was a procurement preference. It has become a security specification.

In the United States, section 889 of the 2019 National Defense Authorization Act prohibits federal agencies from procuring or using covered telecommunications and video surveillance equipment from a named list of manufacturers including Hikvision and Dahua, and from contracting with entities that use it.

In Canada, following a national security review, the federal government ordered Hikvision's Canadian operations to cease at the end of June 2025, banned federal departments and government-owned corporations from purchasing or using its products, and began reviewing its own properties to remove legacy equipment. The responsible minister went further than the order itself required.

> *The Government of Canada welcomes foreign investment — but will never compromise on Canada's national security. [Canadians should] take note of this decision and make their own decisions accordingly.*
>
> Hon. Mélanie Joly, June 2025

The honest framing matters here, because overstating it would be easy and would be caught. Canada has no statutory equivalent of section 889 binding private buildings. A condominium corporation is not prohibited from buying equipment from these manufacturers. What can be said accurately is that the federal government

reviewed this vendor class, concluded it was unacceptable in its own facilities, and publicly invited Canadians to reach the same conclusion. For a board weighing a device that has a camera and a microphone in the lobby and a network connection to the outside world, that is a material input.

The wider point is that the entry panel is an internet-connected device and should be assessed as one. The relevant baseline is published: NIST's IoT device cybersecurity core baseline sets six capabilities — device identification, device configuration, data protection, logical access to interfaces, software update, and cybersecurity state awareness. It is a fair checklist to hold any intercom vendor against, and most legacy entry phones fail the software update criterion outright, because there is no mechanism to update them at all.

That this is not hypothetical is a matter of public record in this exact product category. In March 2023 the US Cybersecurity and Infrastructure Security Agency published an advisory covering thirteen vulnerabilities in a smart intercom — including hard-coded SSH credentials rated 9.8, a hidden SSH server, and missing authentication for a critical function — affecting all versions of the product, and recommended that operators disconnect the device from the internet. In a separate case, a vulnerability disclosed in 2022 in a mainstream multi-tenant intercom allowed an attacker with an NFC-capable phone to brute-force a four-digit administrator passcode and open the building; it could not be fixed by software update and required hardware replacement. A lobby door station is an attack surface, and the update mechanism behind it is part of the specification.

PART 5 Why Condoplex Is the Right Replacement for a MESH or Verex Building

The general case for a platform is one thing. The specific case for replacing these two systems is where a board actually makes its decision, because the question is never "what is the best entry phone" in the abstract. It is "what happens to my building, my wiring, my residents and my budget between now and the day this is finished."

5.1 The migration problems these buildings actually have

A MESH or Verex building presents a recognisable set of constraints. They are worth naming before claiming to solve them.

- Existing riser wiring that runs from the lobby to a service room and, in many buildings, to every suite. Replacing it is the single largest cost variable in any intercom project and the one most likely to trigger a special assessment.
- A resident database of several hundred records that currently exists inside an obsolete head-end, in a proprietary format, on a machine nobody wants to reboot.
- A live credential population — hundreds or thousands of fobs in circulation — that cannot be re-issued overnight without a resident-relations problem.
- Suite hardware of mixed vintage, and residents who did not ask for a project and will judge it entirely by whether the front door works on the day of the cutover.
- A board that needs the work staged across fiscal years rather than delivered as one capital event.

5.2 How the Condoplex approach maps onto each

Wiring and staged cutover

The Condoplex upgrade position is that intercoms are addressed by upgrading the head end, with existing field devices retained where possible, rather than by replacing every station. For a building whose risers are sound, that is the difference between a manageable project and a special assessment. The panel range supports this directly: recessed, surface and pedestal mounting on the ELP1040, and PoE support on the ELP770, which in a retrofit can eliminate a separate power run to a secondary door.

Where a building is coming off a third-party legacy panel — which, per Part 3.1, is what most "Verex" buildings actually have — the ELP1040's Wiegand output allows the new panel to interoperate with an existing access control system during the transition, so the entry phone and the access control head-end do not have to be replaced in the same weekend.

The database

The resident database is the part boards worry about least and should worry about most, because it is the part that cannot be re-purchased. Condoplex's published upgrade position on its own platform is that the resident database is converted automatically rather than re-keyed. For a building migrating from a foreign platform, the equivalent commitment — that the data is extracted, converted and verified as part of the project rather than typed in by a site administrator over a fortnight — is a question that belongs in the tender, and it is one a board should ask every bidder to answer in writing.

Credentials

The recommended path is the phased one: bring the existing credential population across through the panel's compatible reader so that no resident is locked out on day one, then migrate to encrypted 13.56 MHz credentials on a published schedule, deactivating rather than deleting old credentials so the audit record survives. This is exactly the approach the condominium management literature recommends, and it converts the credential problem from an emergency into a planned line item.

Coexistence across generations

The suite panel range is the clearest expression of the philosophy: SP2300, SP2660 and SP2800 panels connect to the same building-wide server, so old and new coexist and the building retrofits at its own pace. A board can replace the lobby panel this year, the guard station next year, and suites over three years, with a working, supported system at every point in between. No architecture that requires a flag-day cutover can offer that.

5.3 The comparison a board should actually make

Verex and Enterphone MESH are frequently presented as a single "legacy" category. They are not, and a table that treats them as one would be making exactly the error this paper warned against in Part 3. The columns below are separated deliberately. Note how many of the MESH entries are conditional: that is the accurate position, and a board should treat any supplier who fills those cells with confident absolutes as having guessed.

Issue	Verex	Enterphone MESH	Condoplex
Manufacturer status	Wound down 2019; brand extinct	Original manufacturer insolvent 2018; line owned by Hirsch after two changes of ownership	Current Canadian manufacturer, direct factory support
Current support	Ended. No technical support since 31 December 2021	Model-specific status must be confirmed in writing with Hirsch	Current product, supported release
Head-end	Legacy Windows and SQL Server, unsupported by Microsoft since 2014–2020	Browser-managed Linux appliance; revision dependent	Maintained Linux platform with managed OS and software updates
Upgrade path	No manufacturer path exists	Potential path to the current Enterphone line; confirm cost and scope	Staged migration; existing field devices retained where possible
Credentials	Commonly legacy unencrypted proximity	Installation dependent — audit before assuming	Encrypted 13.56 MHz credentials available; phased migration
Transport	Interfaced entry panel typically dials a telephone line	IP-based; confirm the resident calling path	Native VoIP; no subscriber line to withdraw
Resident experience	Audio call; no visual verification	Varies by panel model and app entitlement	Two-way audio and video to the resident's phone
Guard and suite integration	Separate systems, separate screens	Confirm what integrates with your concierge and suite panels	One database across entry, suite panels, elevator and access control

Issue	Verex	Enterphone MESH	Condoplex
What to do first	Plan replacement; it is an end-of-life asset	Request a written support-status letter before spending anything	Site survey and staged proposal

THE DISTINCTION THAT PROTECTS YOU

If a bidder tells a MESH building that its system is discontinued and unsupported, ask them to produce the end-of-life notice. There does not appear to be one, and the current owner still sells the successor line. A supplier who overstates the urgency on the way in is telling you something about how they will behave on the way through the project.

PART 6 The Alternatives, Named and Compared

A board replacing a legacy system will be shown four other names. Each is a real product with real strengths, and this section states them before stating the limitations. Every factual claim below is drawn from the manufacturer's own published material — manuals, price lists and contracts — rather than from third-party commentary, because a vendor's own documentation is the one source a board cannot be told is biased.

6.1 Mircom TX3

Mircom is a Canadian manufacturer headquartered in Vaughan, Ontario, and the TX3 is among the most widely installed multi-tenant entry systems in the country. It is a genuinely capable, well-supported product line, and one fair point should be conceded immediately: the classic TX3 telephone access system is standalone. It does not require a subscription, and it does not stop working if a commercial relationship ends. That is a real advantage over the cloud-native platforms below and it should not be glossed over.

The limitation is architectural and is stated in Mircom's own current manual: the TX3 telephone access system is designed to work only with POTS, and non-configurable PBX systems are not supported. Everything in Part 2 applies. Mircom's own answer to this is Mircom Cloud Services, launched in May 2025 on subscription plans, whose published benefits include integrated VoIP to eliminate traditional phone lines — which means the escape route from the transport problem is a subscription the classic product did not require.

For a condominium specifically, the further question is integration depth: whether the entry system, the suite panels, the elevator control and the guard station are one platform with one database or several products interfaced together. That is the distinction Part 4.6 describes, and it is the question to put to any bidder.

6.2 ButterflyMX

ButterflyMX is the best-known cloud-native video intercom in North America and it is a genuinely good product at what it does. The industrial design is excellent, the resident app experience is polished, and it publishes its pricing openly — 8-inch surface-mount panels at $3,995 and 12-inch at $5,995, with recessed variants — which is more transparency than most of this industry offers.

Three things should nevertheless be understood before a board signs.

The recurring cost is unclear by an order of magnitude

ButterflyMX publishes an annual software fee of $30 to $42 per apartment unit per year. Integrators who install the product publish figures of $10 to $30 per unit per month — that is, $120 to $360 per unit per year. That is a discrepancy of between three and twelve times, and this paper will not pretend to reconcile it. The correct response for a board is not to pick a number but to require a written total-cost quotation over five and ten years before signing anything.

The terms of service are the real specification

The most important document a cloud intercom vendor publishes is not its brochure. ButterflyMX's terms of service state that it may suspend, disable or delete an account and access to the services with or without notice, for any or no reason. The services are provided as is, with all faults, and as available, with warranties disclaimed as to completeness, accuracy, availability, timeliness, security and reliability, and with no warranty of operation or compatibility with any other system or device. No uptime guarantee or service level agreement is offered. The terms are silent on what happens to the installed hardware if the service ends.

THE QUESTION THIS RAISES

A board is being asked to make the front door of a residential building dependent on a service that is contractually not warranted to be available, may be discontinued without notice or cause, and carries no stated commitment about what the hardware does afterwards. That may still be an acceptable trade for the resident experience. It should be an informed trade.

Connectivity and building-systems integration

ButterflyMX's own installer network requirements specify wired Ethernet, stating that wireless networks do not meet its stability needs, with a minimum of two megabits per second in each direction per touchscreen and ideally a dedicated connection or VLAN. It offers elevator control, including zoned control. What could not be found in its published material is any documented integration with an in-building guard or concierge station or with in-suite security panels of the kind standard in Canadian condominiums — the architecture is app-first and cloud-first, and the concierge equivalent is a paid add-on dashboard. That is a legitimate question to put to the vendor rather than an assertion, but it is the central question for a staffed building.

6.3 2N

2N, part of the Axis Communications group, deserves more credit than it usually gets in competitive comparisons, and this paper will give it. It is SIP-native, so it does not share the transport problem. Its licensing has been simplified in the customer's favour: the former enhanced video, enhanced audio, enhanced integration and NFC licences were discontinued, several capabilities including the HTTP API became free, and what remains is a one-time Gold licence rather than a subscription. Its My2N cloud platform is optional and openly priced at around €40 per apartment per year, or €225 per apartment for ten years. It supports both 125 kHz and 13.56 MHz credentials, PIN, Bluetooth, NFC, QR codes and fingerprint, and has documented integrations with several major access control platforms.

It is a serious product. The distinctions for a Canadian condominium are two. First, no documented integration with in-suite condominium security panels or a Canadian-style concierge station could be found in its published material — 2N is an intercom and access endpoint, not a building platform, and the surrounding systems have to be assembled from other vendors and interfaced. Second, and more subtly, that assembly is precisely the multi-vendor condition that Part 3 identifies as the origin of the obsolescence problem in the first place. A building that solves its intercom problem by adding a fourth vendor has improved its front door and left its architecture unchanged.

6.4 DoorKing

DoorKing is a long-established and mechanically rugged telephone entry manufacturer with a large installed base, particularly on gated and perimeter applications. Its January 2026 product reference guide sets out its current position clearly, and two elements of it are directly relevant.

First, on transport, DoorKing now offers cellular and VoIP connectivity and explicitly does not recommend POTS. Its published subscription schedule prices cellular voice and data between $49.95 and $97.95 per month by tier with a $45 activation per control box, and internet VoIP at $38.95 per month for voice and data. That is real, published, per-door recurring cost from a legacy vendor, and it is the clearest evidence available that the subscription model is arriving across the whole category, not only at cloud-native companies.

Second, on credentials, the readers listed in the current catalogue are 26-bit Wiegand proximity — which is the same unencrypted low-frequency technology class discussed in Part 3.4. A board replacing a legacy system in 2026 in order to fix a credential-cloning exposure should look closely at whether the replacement fixes it.

The contractual terms are the sharpest point of all, and they are DoorKing's own words.

> *If credit card payment is refused by your bank, or if there is not sufficient funds in your bank account, your use of the Product may be disabled until payment in full is received. […] If your account is classified (at DoorKing's sole discretion) as inactive for over 120 days, DoorKing has the right to permanently delete your subscriber data.*
>
> DoorKing Connection Services Terms, sections 4.1 and 6

The scope of that clause should be stated precisely rather than stretched, because the precise version is damaging enough. What the terms establish is that DoorKing's connected calling service may be disabled for non-payment, and that subscriber data held by that service may be permanently deleted after prolonged inactivity. They do not, on their face, establish that every local door or access function stops, or that a locally held resident database is erased — a board should ask DoorKing directly which functions survive a suspension, and get the answer in writing.

Even read narrowly, it matters. A condominium corporation changes property managers, changes bank accounts, changes signing authorities, and occasionally misses an invoice during a transition. The scenario in which an administrative lapse suspends the service that lets visitors call residents, and four months later removes the subscriber data behind it, is not exotic. It is a Tuesday in the life of a self-managed board.

6.5 Summary comparison

Read down the final row of the table below before anything else. It is the row that Part 3 of this paper is about. Every building described in that section is in difficulty today because of a decision made a decade or two ago about which vendor to depend on, made without asking what that dependency would mean if the vendor changed course. Boards buying entry systems in 2026 are making the same decision — and this time the contractual answers are published in advance.

	Condoplex	Mircom TX3 classic telephone access configuration	ButterflyMX	2N	DoorKing
Transport	VoIP / SIP native	POTS only, per the manufacturer's manual	IP / cloud	SIP native	Cellular or VoIP; POTS not recommended
Two-way video to resident app	Yes	No — audio telephone entry	Yes	Yes	Limited
Cloud required to function	No	No	Yes	No (My2N optional)	Yes for cellular / VoIP modes
Mandatory recurring fee	No — services optional	None	Yes, per unit	One-time licence	Yes, per door
Guard / concierge station	Native, single queue	Building systems integration	Not found in published material	Not found in published material	Not found in published material
In-suite security panels	Native, multi-generation	Separate product line	Not found	Not found	Not found
Elevator control	Native, incl. inter-floor and child lock	Via access control	Yes, incl. zoned	Via access platform plugins	Via expansion points
If the vendor relationship ends	Hardware is owned and keeps working	Keeps working — no subscription to lapse	Terms silent on hardware; no SLA	SIP endpoint continues locally	Connected calling service may be suspended; subscriber data deleted after 120 days
Manufacturing origin	Canada	Canada	United States	Czech Republic (Axis group)	United States

WHAT THIS TABLE DOES AND DOES NOT COVER

The Mircom column describes the classic TX3 telephone access configuration specifically — the product in the largest number of Canadian buildings today, and the one a board on a legacy system is most likely to be replacing or extending. It is not the whole Mircom catalogue.

Mircom also offers the TX3 Touch video intercom line and, since May 2025, Mircom Cloud Services, which adds remote management, tenant administration and integrated VoIP on subscription plans. Those change the transport and video rows materially, and they move Mircom into the same recurring-fee category as the cloud-native vendors. A board comparing current products should ask Mircom for that configuration and price it over five and ten years alongside everything else.

PART 7 What a Board Should Ask Before It Signs Anything

The following questions are not weighted toward any manufacturer. They are the questions that, asked of every bidder in writing and answered in writing, will surface the differences that matter. Condoplex is content to be assessed on them.

On architecture and transport

1. Does this system require a telephone line to place a call to a resident? If yes, what is the plan when the carrier decommissions copper in this neighbourhood, and who bears that cost?
2. Is the panel a native SIP/VoIP endpoint, or is VoIP delivered through an adapter or a cloud service? What happens if that service is unavailable?
3. Which functions continue to work if the building's internet connection fails for 24 hours? Answer function by function: door release, resident call, guard call, credential authentication, audit logging.

On commercial terms

1. What is the total cost of ownership over five and ten years, itemised into hardware, installation, cabling, licences and recurring fees? Provide it as a written schedule, not a monthly rate.
2. Is any recurring payment required for the system to continue functioning? What specifically stops working if a payment is missed, and after how long?
3. What are your published terms of service, and what do they say about suspension, termination, uptime and the status of the installed hardware if the agreement ends? Provide the document, not a summary.
4. If your company is acquired, restructured or discontinues this product line, what is the contractual commitment to this building?

On integration and the building as a whole

1. Is the resident database shared with the suite panels, the guard station, elevator control and access control, or does each system hold its own copy?
2. Can a guard answer an entry call with live video from the same screen that displays suite alarms and panic events, without a separate telephone?
3. What audit record is produced automatically, where is it stored, how is it backed up, and can it be exported in a form usable by an insurer or the police?
4. Which credential technologies does the system support, and are you proposing encrypted 13.56 MHz credentials or 125 kHz proximity? If the latter, explain why.

On the vendor and the equipment itself

1. Where is this equipment manufactured, and does it contain components from manufacturers subject to government security restrictions in Canada or the United States?
2. What is the software update mechanism, how often are updates issued, and what is the committed support horizon for this specific model and firmware revision? Provide it in writing.
3. What is the oldest field device from your company still operating on a current server today? This single question separates platform vendors from product vendors.

7.5 Reading the answers

The questions matter less than what a bidder does when asked them. The pattern below is consistent enough to be useful.

If a bidder…	What it usually means
Answers the outage question function by function, in writing	They have tested it. This is the single best signal of engineering maturity in the whole list.
Says "it works offline" without qualifying which functions	Nobody has tested it, or the answer is uncomfortable. Ask again in writing.
Will not provide a five- and ten-year cost schedule	The recurring cost is material enough that showing it would lose them the bid.
Points to a brochure when asked for terms of service	Read the terms yourself. The brochure is the marketing document; the terms are the product.
Cannot name an oldest field device still running on a current server	They are a product vendor, not a platform vendor. Price the next replacement into this decision.
Proposes 125 kHz proximity credentials in 2026	They are re-installing the vulnerability you are paying to remove.
Quotes the entry panel without surveying the access control head-end	They have not understood the building, and the change order is already written.

FOR BOARDS CURRENTLY ON MESH OR VEREX SPECIFICALLY

Before evaluating any replacement, do two things. First, establish what you actually have: a Verex head-end is access control, and your lobby panel is probably a different manufacturer’s product, which means two assessments, not one.

Second, write to the current owner of your platform — Hirsch for Enterphone MESH — and request a written support-status letter for your specific model and firmware, including the security update commitment and the published upgrade path. What comes back, or does not, is the most useful single piece of evidence you will gather in this process, and it costs nothing.

PART 8 What Condoplex Commits To, in Writing

A paper that spends seven parts telling boards to demand written commitments from their suppliers has an obligation to put its own on the record. Everything in this section is a Condoplex commitment that can be attached to a quotation and held to.

8.1 Product support and lifecycle

Commitment	Condoplex position
Current platform release	CPLX Linux 6, supported for the foreseeable future, with updates delivered continuously as software
Previous release	CPLX Linux 5 retires February 2027; migration requires a head-end upgrade with new controllers, with field devices retained
Standard hardware warranty	1 year
Extended warranty	Optional 5-year term, as a paid service level agreement including software updates, cybersecurity patching and factory technical support
Product support horizon	Condoplex supports products for as long as spare parts remain obtainable. This is stated as it is: a commitment of intent and practice, not a contractual date. A board should ask for the current spares position on the specific model it is buying.
Support hours	08:00–20:00 Eastern, Monday to Friday
Out-of-hours support	Available for urgent issues, including weekends

WHY THAT SUPPORT-HORIZON WORDING IS NOT DRESSED UP

It would be easy to write "long-term support commitment" here. What Condoplex actually does is support products for as long as spares can be obtained, and saying so plainly is worth more than a phrase that sounds like a guarantee and is not one. Ask every other bidder the same question and compare the specificity of the answers, not their confidence.

8.2 The backward-compatibility claim, evidenced

Part 4.7 states that Condoplex field devices installed twenty to twenty-five years ago still connect to current servers. That is the most consequential claim in this paper, because it is the only real evidence any vendor can offer about what will happen to equipment a building buys today.

The specific evidence: Condoplex has suite panels in service today that are more than twenty-five years old, still operating, still connected to current servers. Not maintained as museum pieces on an isolated legacy system — connected to the same platform sold to new buildings this year.

Set that beside the Part 3 record. Verex buildings are being told that a platform sold as recently as the 2010s is finished and everything must be replaced. Condoplex has hardware from the late 1990s still doing its job. Whatever else a board weighs, that is the difference between buying a product and buying into a platform, and it is measurable rather than rhetorical.

Evidence	Detail
Oldest Condoplex field devices still operating on a current server	Suite panels in excess of 25 years old, in service and connected today
Buildings operating mixed-generation panels on one server	[To be supplied by Condoplex]
Reference buildings available to speak to a board	[To be supplied by Condoplex, with the owner's consent]

8.3 Data location, backup and security policy

Question a board should ask	Condoplex answer
Where does cloud backup physically reside	Canadian servers
What is backed up	System configuration, site data and audit logs, on an automated schedule
What happens to the building's data if the agreement ends	[Retention, export and deletion policy — to be supplied]
Published cybersecurity and update policy	[Policy document reference — to be supplied]

8.4 Cost over five and ten years

Part 7 tells boards to require a five- and ten-year cost schedule from every bidder, including all recurring charges. The comparison only means something if Condoplex supplies the same schedule, in the same format, for the same building. The figures below are completed against the specific quotation — this is the only section of this paper that is building-specific rather than general.

Cost element	Condoplex, for this building
Hardware	[Quoted]
Installation and cabling	[Quoted]
Recurring services, annual	[Extended warranty and remote services, itemised]
Five-year total cost of ownership	[Total]
Ten-year total cost of ownership	[Total]
Mandatory per-suite or per-door fee	None. Recurring services are optional and quoted separately.

Set that schedule beside the published figures in Part 6: a per-apartment annual software fee at one vendor, and a per-door monthly subscription between roughly $39 and $98 at another. Over ten years, in a building of any size, the recurring line is not a rounding difference. It is frequently the largest number in the comparison, and it is the one least likely to appear in a headline quotation.

Conclusion

The entry phone decision has quietly changed character. For thirty years it was a question about a device: which panel, which finish, how many buttons. It is now a question about an architecture, and the three available architectures carry very different long-term obligations.

A dialer is tied to a transport that both regulators and its own manufacturers have moved on from, on a timetable set by a carrier rather than by the building. A cloud subscription platform delivers an excellent resident experience in exchange for a dependency whose terms — published by the vendors themselves — include suspension without notice, no warranty of availability, and in one documented case the disabling of the entry system and deletion of the resident database for non-payment. An owned, integrated, network-native platform costs more thought at specification time and less for the following two decades.

For the buildings this paper is principally about — those running Verex, Enterphone MESH, and the other platforms of that generation — the situation is not identical and should not be described as though it were. Verex is finished, and has been since technical support ended on 31 December 2021. MESH is not discontinued, but its original manufacturer is gone, its assets have changed hands twice, and the name the building knows it by has been retired from the catalogue. Different facts, different urgency, the same underlying question: how much longer does the board want the front door of the building to depend on a decision someone else will make without consulting them?

The Condoplex case rests on four things that can be checked rather than asserted. The panel is a VoIP endpoint, so there is no phone line to lose. It carries two-way video to the resident's phone and to the guard station on the same call, so the visitor is seen rather than merely heard. It shares one database with the suite panels, elevator control and access control, so the seams that produced the current problem do not exist. And the platform has a documented record of connecting twenty- and twenty-five-year-old field devices to current servers, which is the only meaningful evidence any vendor can offer about what it will do with the equipment a building buys today.

The front door is the most-used security device in the building. It should not be the least-considered line in the reserve fund study.

NEXT STEP

Condoplex and its authorised dealers will conduct a site survey documenting exactly what is installed, distinguish the entry panel from the access control head-end, identify what can be retained, and provide a staged replacement proposal priced over ten years including all recurring costs. For buildings currently on MESH or Verex, that survey also includes helping the board request a written support-status letter from the current owner of their platform — whatever they decide to do next.

Sources and Notes

Every third-party factual claim in this paper is listed below. Claims about Condoplex products are drawn from Condoplex published specifications and the Condoplex Customer Guide 2026 and are identified as manufacturer statements. Where the evidence base is thin or contested, the relevant section says so in the body text rather than here.

Telecommunications and copper retirement

Federal Communications Commission, Reducing Barriers to Network Improvements and Service Changes; Accelerating Network Modernization ("Network and Services Modernization Order"), FCC 26-19, WC Docket Nos. 25-208 and 25-209, adopted 26 March 2026, published 91 FR 20913 (20 April 2026), effective 20 May 2026. docs.fcc.gov/public/attachments/FCC-26-19A1.pdf

Federal Communications Commission, Petition of USTelecom for Forbearance, FCC 19-72, WC Docket No. 18-141, adopted 26 July 2019 — cited here for the point that it did not require discontinuance of retail TDM voice service. docs.fcc.gov/public/attachments/FCC-19-72A1.pdf

AT&T discontinuance application filed 1 December 2025, automatically granted 13 January 2026; discontinuance from 15 November 2026. Broadband Breakfast, "AT&T Approved to Discontinue Service at More than 30% of Copper Footprint This Year." California applications WC Dockets 26-121 and 26-122, filed 20 May 2026. California Public Utilities Commission, federal applications to discontinue landline voice service.

Canadian Radio-television and Telecommunications Commission, Canadian Telecommunications Market Report 2026, local and access revenue data. crtc.gc.ca/eng/publications/reports/PolicyMonitoring/2026/ctmr.htm

Telecom Regulatory Policy CRTC 2016-496; Telecom Decision CRTC 2008-22 (service withdrawal and destandardization); Telecom Decision CRTC 2025-310 (Bell forbearance, Digital Exchange Access Service).

Reporting on Bell copper decommissioning, the Swansea (Toronto) notice of 4 November 2026 service end, CRTC Commissioner Bram Abramson's comments on the absence of active regulatory oversight, and Lifeline Canada's statements on medical alert devices, 1 September 2026.

Legacy platforms: Verex and Enterphone MESH

Carrier Fire & Security Products statements on the Interlogix wind-down, 19–20 September 2019, as reported by SecurityInfoWatch, Security Sales & Integration and SDM Magazine. Interlogix product support announcement, technical support ending 31 December 2021 (distributor reproduction, Group One).

Verex corporate lineage: Guardall North America rebranded as Verex (Security Systems News); FCC grantee record X78, Guardall, a division of CSG Security Corp, 5201 Explorer Drive, Mississauga, Ontario; VEREX Technology company record (SecurityInformed); UTC acquisition of Chubb, April 2003; UTC Fire & Security re-introduction of the Interlogix brand, 5 October 2010 (PR Newswire); final Verex documentation, © 2017 UTC Fire & Security Americas.

Verex Director software: A&E Guide Specification v4.9.1 (supported operating systems and SQL Server versions); Verex Director v5.0 Quick Start Guide, P/N 466-2442F, 30 June 2017; Director licence tiers and panel capacities (Interlogix product page). Verex 120-series catalogue and G-Prox II proximity credential datasheet (SecurityInformed).

Microsoft Lifecycle Policy end-of-support dates: Windows XP, 8 April 2014; SQL Server 2005, 12 April 2016; SQL Server 2008 and 2008 R2, 9 July 2019; Windows 7 and Windows Server 2008 R2, 14 January 2020.

Viscount Systems Inc.: MESH field trials announcement, 17 March 2003 (GlobeNewswire); asset sale agreement and Scott Sieracki statement, 20 December 2018 (SecurityInfoWatch); Identiv completion of acquisition, 3 January 2019 (GlobeNewswire); Identiv sale to Vitaprotech announced 3 April 2024 and completed 9 September 2024, relaunched as Hirsch (BusinessWire).

Enterphone MESH Installation Guide (Identiv), including hardware models, browser management, default credentials and listed support contact. Current Enterphone overview brochure and Hirsch product pages for Enterphone iQ, 19, Kiosk, Microserver and Mobile; Hirsch support page (legacy product listing).

Credentials and cybersecurity

Garcia, de Koning Gans, Muijrers, van Rossum, Verdult, Wichers Schreur and Jacobs, "Dismantling MIFARE Classic," ESORICS 2008. Teuwen (Quarkslab), "MIFARE Classic: exposing the static encrypted nonce variant and hardware backdoors," IACR ePrint 2024/1275, August 2024. Oswald and Paar, "Breaking Mifare DESFire MF3ICD40," CHES 2011 — cited for the honest limits of the DESFire comparison.

Michel Lauzon, "Fob Cloning in Condominiums," CM Magazine (Association of Condominium Managers of Ontario), Fall 2021. Quintin Johnstone, "Access Fob Counterfeiting," Condovoice (Canadian Condominium Institute, Toronto), Summer 2017. IPVM, "Flipper Zero Makes 125 kHz Prox Cards 'Actually Dangerous,' Says HID Director," 10 May 2024.

CISA ICS Advisory ICSA-23-068-01, Akuvox E11 smart intercom, March 2023, thirteen CVEs including CVE-2023-0345 (CVSS 9.8). CVE-2022-40903, Aiphone GT series, disclosed by Promon, published 8 November 2022. NISTIR 8259A, IoT Device Cybersecurity Capability Core Baseline, May 2020.

NDAA FY2019 section 889 (Congressional Research Service overview LSB10895). Government of Canada order requiring Hikvision to cease Canadian operations, June 2025, and the statement of the Hon. Mélanie Joly (CBC News; The Record). Canadian Centre for Cyber Security, Technology Supply Chain Guidelines TSCG-01.

CISA, Critical Manufacturing Sector: Introduction to the Gray Market, and Supply Chain Security and the Gray Market, August 2024 — cited for the existence and subject of the guidance.

Competing products — all from manufacturers' own published material

Mircom, TX3 Telephone Access System Installation and Operation Manual, LT-969 Version 7, March 2023 (POTS-only statement, ADC and NSL modes, RS-485 and TCP/IP networking). Mircom Cloud Services launch, 8 May 2025 (PR Newswire; mircom.com/mcs).

ButterflyMX published pricing (butterflymx.com/cost); ButterflyMX Terms of Service (suspension, disclaimer of warranties, absence of SLA); ButterflyMX installer network requirements document; ButterflyMX elevator controls product material. Integrator-published subscription figures from Alarm New England and Safe and Sound Security, cited to illustrate the discrepancy rather than to establish a figure.

2N IP Verso 2.0 product specification; 2N licensing FAQ (discontinuation of enhanced licences, one-time Gold licence); My2N Management Platform published pricing.

DoorKing Product Reference Guide, Section 2, January 2026 (connectivity options, POTS recommendation, 26-bit Wiegand readers); DoorKing subscription schedule, January 2026; DoorKing Connection Services Terms, sections 4, 4.1, 6 and 8.

Governance, liability and reserve funds

Condominium Act, 1998 (Ontario), sections 93(4), 94 and 115(2); Condominium Authority of Ontario, Guide on Condo Reserve Funds (component inventory requirements, thirty-year projection, $500 threshold).

Ontario Building Code, article 3.4.6.16, Door Release Hardware (fail-safe release conditions for electromagnetic locks in an access to exit).

Community Associations Institute, "Security measures: How communities can minimize liability," 13 March 2024.

Published intercom replacement cost ranges (Swiftlane, 2026; BAS-IP) — cited in the body only to establish that no independent benchmark exists and that a written multi-year total-cost quotation is the appropriate response.