eBook 1

Empower Your Workforce:

Unlock Productivity, Security, and IT Efficiency.

F12.net™

blackpoint Coalition® Lenovo WatchGuard®

Table of Contents

Executive **Summary**

Technology is no longer just a support function—it's the backbone of modern business performance. Yet, many mid-market enterprises face a growing challenge: IT systems that fail to keep up with the pace of business demands. Ageing infrastructure, outdated hardware, and fragmented IT management create operational bottlenecks, strain internal resources, and expose organisations to unnecessary risks.

For leadership teams, the consequences are felt across the organisation:

- **Productivity Loss:** Teams working on slow, outdated devices face frequent disruptions and reduced efficiency.
- **Security Gaps:** Disconnected systems and inconsistent security policies open the door to data breaches and compliance risks.
- **Escalating Costs:** Managing multiple vendors, hardware refresh cycles, and reactive IT support often leads to unpredictable expenses.

This isn't just an IT problem—it's a business risk. And with IT talent shortages and evolving cyber threats, the need for a more strategic approach has never been greater.

67% of IT leaders struggle with endpoint management across their workforce.

82% of breaches involve compromised credentials.

What's Holding Canadian Businesses Back?

A recent study from Gartner revealed that 67% of IT leaders struggle with endpoint management across their workforce, while 82% of breaches involve compromised credentials. These challenges persist as businesses expand remote work and hybrid models, increasing the complexity of securing and managing devices.

The result? Leadership teams spend more time reacting to IT issues than focusing on growth and innovation.

The Path Forward: Smarter IT with F12 Infinite.

F12 Infinite empowers Canadian businesses by unifying hardware, security, and IT management into a single, fully managed service. Built on partnerships with Lenovo, Blackpoint Cyber, WatchGuard, and Coalition, it simplifies complex IT environments and strengthens business resilience.

In this eBook, you'll discover how a proactive, integrated IT strategy can:

- **Empower Your Workforce:** Boost productivity with modern devices and seamless IT support.
- **Secure Your Organisation:** Mitigate risk with MDR and Zero Trust security framework.
- **Simplify IT Complexity:** Reduce vendor sprawl and operational noise with a unified platform and predictable pricing.

If your organisation is ready to reduce complexity, regain control, and focus on growth, this guide will help you explore the path forward.

The Hidden **Costs** of Outdated IT Infrastructure

Technology should drive business growth, not slow it down. Yet for many mid-market enterprises, outdated IT systems, fragmented hardware, and reactive support structures have become barriers to productivity, security, and financial efficiency.

Modern businesses face mounting pressure to stay competitive, secure their operations, and adapt to hybrid work environments. However, legacy IT systems often fail to keep pace with evolving needs. The result? Operational inefficiencies, increased risk exposure, and unpredictable expenses that directly impact business performance.

Productivity Loss from Aging Technology

Outdated hardware and inefficient IT systems lead to significant productivity challenges. Devices past their prime slow down employee workflows, cause downtime, and disrupt operations—especially in hybrid work environments where reliable, secure access is critical.

- 54% of employees cite outdated technology as a barrier to productivity, with disruptions like slow devices and connectivity issues (Source: Lenovo Future of Work Study 2023).
- The average mid-sized business loses $5,600 per minute of unplanned downtime due to outdated systems, costing businesses both revenue and productivity (Source: Gartner IT Cost Management Report, 2023).

Modern productivity hinges on reliable, secure devices paired with proactive IT support. However, without a streamlined IT management approach, companies often struggle to deliver the right tools for their teams.

Escalating IT Costs from Siloed Systems

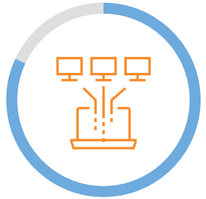
When IT operations are fragmented across multiple vendors and legacy contracts, financial waste becomes inevitable. Unmanaged hardware refresh cycles, multiple service contracts, and inconsistent support models can spiral into unpredictable costs.

- 67% of IT decision-makers report struggling to manage endpoint devices and their lifecycle effectively (Source: Gartner Endpoint Management Survey, 2023).
- 82% of businesses say they lack visibility into their full IT infrastructure, making cost management and forecasting difficult (Source: Forrester Business Technology Study, 2022).

Common cost-related challenges include:

- **Vendor Sprawl:** Juggling multiple service providers for hardware, security, and IT support.
- **Reactive Spending:** Increased spending on emergency IT fixes rather than proactive solutions.
- **Hidden Costs:** Licensing issues, unused software, and out-of-warranty devices.

67% of IT decision-makers report struggling to manage endpoint devices.



82% of businesses lack visibility into their full IT infrastructure.

Security Vulnerabilities and Compliance Risks

Outdated infrastructure isn't just a financial burden—it's a security risk. Legacy systems often lack modern security controls, leaving businesses vulnerable to cyber threats. Combined with a rise in hybrid work and endpoint expansion, the risks have never been higher.

- 74% of data breaches involve compromised privileged accounts or outdated security policies (Source: Verizon Data Breach Investigations Report, 2023).
- The average cost of a data breach in Canada reached $7.3 million CAD in 2023, largely due to delayed detection and outdated infrastructure (Source: IBM Cost of a Data Breach Report, 2023).

Security risks linked to outdated infrastructure:

- **Insufficient Endpoint Protection:** Lack of Zero Trust policies and multi-factor authentication (MFA).
- **Data Loss Exposure:** Unpatched systems and unsupported software increase breach risks.
- **Compliance Gaps:** Difficulty maintaining frameworks like SOC2 Type 2 and PIPEDA compliance without modern security protocols.

The IT Resource Strain: Limited Talent, Maximum Demand

Mid-market enterprises often face resource constraints, with limited in-house IT staff expected to manage complex infrastructures. As cyber threats grow and systems become more sophisticated, the skills gap continues to widen.

- 3.5 million cyber security roles remain unfilled globally, with Canada facing a 25,000+ professional gap (Source: ISC2 Cybersecurity Workforce Report, 2023).
- 68% of mid-sized businesses report being under-resourced for effective threat detection and response (Source: CyberEdge Group Report, 2023).

Without the bandwidth or expertise to manage infrastructure effectively, businesses risk both security gaps and operational inefficiencies.

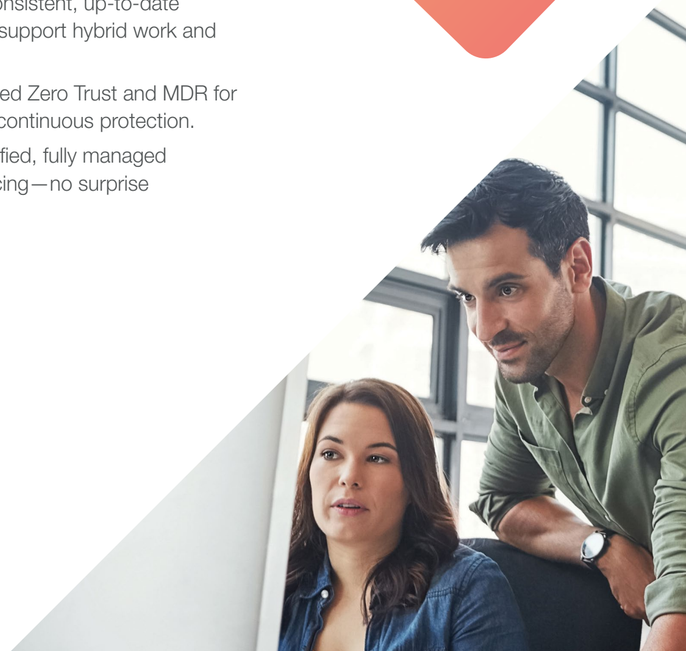
The Solution: Modernising IT with F12 Infinite

The hidden costs of outdated infrastructure can be controlled—but it requires a proactive, modern approach. F12 Infinite transforms mid-market IT management by:

- **Empowering Productivity:** Consistent, up-to-date hardware with Lenovo DaaS to support hybrid work and reduce downtime.
- **Securing Operations:** Integrated Zero Trust and MDR for advanced threat detection and continuous protection.
- **Simplifying Complexity:** A unified, fully managed service with flat, predictable pricing—no surprise costs or vendor confusion.

74% of data breaches involve compromised privileged accounts or outdated security policies.

68% of mid-sized businesses report being under-resourced for effective threat detection and response.



The IT Resource Strain and Security Gaps Leaders Face

As Canadian businesses expand their digital operations and embrace hybrid work environments, the demand for skilled IT professionals has surged. However, a critical shortage of cyber security expertise, combined with increasingly complex technology stacks, has left many organisations struggling to keep pace with both innovation and protection.

The result? Overstretched IT teams, delayed threat response, and heightened exposure to cyber risks—factors that directly impact operational resilience and business continuity.

The Cyber Security Skills Gap: A Growing Crisis

The global cyber security talent shortage has placed significant strain on organisations of all sizes, but mid-market enterprises often feel the impact more acutely due to limited resources and hiring challenges.

- Canada faces a 25,000+ shortfall in skilled cyber security professionals, leaving businesses vulnerable to evolving threats. (Source: ISC2 Cybersecurity Workforce Report, 2023)
- 3.5 million unfilled roles in cyber security exist globally, with mid-sized businesses facing the largest talent gap. (Source: ISC2 Cybersecurity Workforce Report, 2023)
- 68% of IT decision-makers report their teams are under-resourced for proactive threat detection and response. (Source: CyberEdge Group 2023)

What this means for businesses:

- **Slower Threat Response:** Without adequate resources, threat detection and mitigation often fall behind, increasing the likelihood of prolonged breaches.
- **Higher Burnout Risk:** Overextended IT teams juggling operational tasks and security can lead to errors and overlooked vulnerabilities.
- **Increased Reliance on Reactive IT:** Limited bandwidth often forces teams to focus on damage control rather than proactive cyber resilience strategies.

68% of IT decision-makers report their teams are under-resourced for proactive threat detection and response.

Rising Threat Complexity Meets Resource Gaps

While internal IT teams face resourcing challenges, cyber threats have become more sophisticated. Ransomware, phishing attacks, and insider threats have surged, with mid-market businesses being a prime target due to often limited security layers.

- 51% of Canadian businesses reported a cyber attack in the last year, with 28% experiencing a ransomware event. (Source: Canadian Centre for Cyber Security, 2023)
- 74% of breaches involve human error or compromised credentials, a critical vulnerability tied to limited security education and endpoint protection. (Source: Verizon Data Breach Investigations Report, 2023)

The Compounding Risk Factors:

- **Unmanaged Endpoints:** Hybrid work has expanded the attack surface, with many companies struggling to secure remote devices.
- **Lack of Zero Trust Implementation:** Traditional perimeter security models are no longer effective, with insider threats and credential compromise now driving most breaches.
- **Compliance Challenges:** SOC2 Type 2 and PIPEDA standards demand continuous monitoring and reporting—capabilities many IT teams cannot manage alone.

The Impact: Increased Business Vulnerability

When internal IT resources are stretched thin, the business impact extends far beyond security risks. Gaps in coverage can lead to:

- **Longer Downtime During Incidents:** Without 24/7 monitoring, critical threats often go unnoticed until significant damage has occurred.
- **Financial Loss:** The average cost of a data breach in Canada is now $7.3M CAD, driven by slow detection and response times. (Source: IBM Cost of a Data Breach Report, 2023)
- **Missed Strategic Priorities:** IT teams consumed by security firefighting often lack the capacity to focus on digital transformation or business innovation.

The Solution: A Fully Managed Approach with F12 Infinite

Addressing both the talent shortage and rising security demands requires a different approach to IT management. F12 Infinite offers a proactive, fully managed IT ecosystem designed to eliminate resource strain while strengthening security.

- **Managed Detection & Response:** 24/7 threat monitoring and incident response, reducing the need for in-house expertise.
- **Zero Trust:** Ensures continuous verification of all access points to prevent unauthorised access.
- **Device-as-a-Service:** Modern hardware provisioning with full lifecycle management, reducing the IT workload.
- **F12 Managed IT Services:** Centralised IT management with flat-fee pricing, freeing internal teams to focus on strategic priorities.

With F12 Infinite, Canadian businesses gain access to expert-level security and IT management without the complexity of hiring and managing a large in-house team.

51% of Canadian businesses reported a cyber attack in the last year, with **28%** experiencing a ransomware event.

The Solution:

Smarter IT with F12 and Lenovo

As Canadian businesses face increasing complexity in their IT environments, the demand for cost-efficient, scalable, and secure technology has never been higher. Outdated infrastructure, unpredictable spending, and the strain on internal resources often leave organisations struggling to keep up with the demands of a hybrid workforce.

F12 Infinite, in collaboration with Lenovo, transforms how businesses approach IT by providing a fully managed, integrated IT ecosystem designed for flexibility, security, and operational efficiency.

What Is Lenovo Device-as-a-Service (DaaS)?

Lenovo DaaS is a comprehensive solution that combines hardware, software, and lifecycle management services into a predictable, subscription-based model. This approach simplifies IT operations by bundling modern devices with proactive management, allowing businesses to scale with ease while controlling costs.

Key benefits of Lenovo TruScale DaaS include:

- **Predictable Costs:** A flat monthly subscription model that eliminates large capital expenses and simplifies budgeting.
- **Lifecycle Management:** Full device management from deployment to secure disposal, including asset tagging, imaging, and recovery.
- **Scalability:** The ability to adjust hardware capacity in line with business demands, such as seasonal workforce expansions.

Lenovo's TruScale DaaS empowers organisations to **avoid large upfront capital expenditures**, instead enabling cash flow management and a reduced total cost of ownership. (Source: Lenovo White Paper Contribution for F12)

The Problem: IT Complexity Is Holding Businesses Back

Many mid-market enterprises manage fragmented IT environments, balancing multiple service contracts, aging hardware, and siloed support models. This approach results in:

- **Inconsistent User Experience:** Employees working on outdated devices with varying performance levels.
- **IT Resource Strain:** Internal IT teams stretched thin managing hardware issues instead of focusing on strategic initiatives.
- **Security Gaps:** Inconsistent device management often leads to unpatched vulnerabilities and data exposure risks.

The Solution: F12 Infinite + Lenovo DaaS = Simplified IT Management

F12 Infinite integrates Lenovo DaaS as a core component of its fully managed IT ecosystem, offering a one-stop solution for endpoint management and infrastructure support.

- **Flexible Hardware Management:** Devices procured, managed, and retired seamlessly.
- **Security Built In:** ThinkShield security embedded in Lenovo devices for proactive endpoint protection.
- **Simplified IT Control:** One partner for hardware, IT management, and security—no vendor sprawl.
- **Scalable for Growth:** Easily expand or refresh devices without capital constraints.

This approach not only simplifies IT management but frees internal resources by shifting endpoint management from internal teams to a fully managed service.

Business Benefits of F12 Infinite with Lenovo DaaS:

1. **Increased Employee Productivity:** Modern, high-performance Lenovo Think-branded devices ensure employees have the tools needed for optimal productivity.
2. **Lower Total Cost of Ownership (TCO):** A subscription-based model reduces large capital expenditures while providing complete lifecycle services.
3. **Simplified Endpoint Security:** With ThinkShield protection and WatchGuard Zero Trust frameworks, endpoint security is embedded at the device level.
4. **Sustainability Built In:** Lenovo's CO2 Offset Service supports organisations in reducing their carbon footprint by offsetting emissions throughout the device lifecycle.

54% of employees cite outdated technology as a barrier to productivity.

(Source: Lenovo Future of Work Study, 2023)

Lenovo Asset Recovery Services help **reduce e-waste** while aligning with corporate sustainability goals.

(Source: Lenovo White Paper Contribution for F12)

Why Lenovo DaaS and F12 Together?

The power of F12 lies in the seamless integration of Lenovo's scalable hardware and lifecycle management with advanced cyber security and IT support from WatchGuard and Blackpoint Cyber.

This collaboration ensures:

- **One Point of Accountability:** F12 handles the entire IT stack, from device procurement to security management.
- **End-to-End Protection:** Built-in endpoint security and proactive threat detection safeguard against evolving threats.
- **IT Simplification:** Predictable costs, reduced vendor sprawl, and enhanced support services.

The Business Case for Modernising IT Now

Failing to modernise IT not only introduces operational inefficiencies but increases risk and hampers business growth.

By combining Lenovo DaaS with F12 Infinite, growing Canadian businesses can:

- **Empower Their Workforce:** Flexible, modern devices with proactive support.
- **Secure Their Organisation:** Advanced endpoint protection and 24/7 threat monitoring.
- **Simplify Complexity:** A single partner for all IT needs with a predictable pricing model.

Organisations using DaaS reduce hardware costs by up to **25%** over a device's lifecycle.

(Source: IDC DaaS Market Trends, 2023)

74% of data breaches are linked to compromised privileged credentials.

(Source: Verizon DBIR, 2023)

Protecting Productivity with **Proactive Cyber Security**

In today's digital-first business landscape, productivity is directly tied to how secure and resilient your IT environment is. For Canadian businesses, operational success depends on more than just having the right tools—it requires a proactive defence against cyber threats that can disrupt operations and drain resources.

Yet many businesses remain reactive when it comes to security, responding to threats only after damage has occurred. With cyber attacks becoming both more sophisticated and frequent, this approach leaves organisations vulnerable to costly downtime and data breaches.

Recent data highlights just how critical proactive security has become:

- Over 51% of Canadian businesses experienced a cyber attack in the past year, with 28% reporting ransomware incidents. (Source: Canadian Centre for Cyber Security, 2023)
- The average data breach in Canada now costs $7.3 million CAD, driven largely by slow detection and response times. (Source: IBM Cost of a Data Breach Report, 2023)

The message is clear: security gaps aren't just a technical issue—they're a business risk impacting productivity, financial stability, and trust.

The Resource Challenge: Cyber Threats Outpacing IT Capacity

The situation is further compounded by the ongoing cyber security skills shortage, which has left many organisations struggling to maintain adequate protection. Mid-market enterprises, in particular, face significant gaps in talent availability and security coverage.

- Canada is currently short 25,000+ qualified cyber security professionals. (Source: ISC2 Cybersecurity Workforce Report, 2023)
- 68% of IT leaders say their teams are under-resourced for proactive threat detection. (Source: CyberEdge Group Report, 2023)

Without the right expertise in place, many organisations are forced into reactive security models, responding to threats only after they occur—often too late to prevent operational disruption.

The F12 Approach: Proactive Security Without the Complexity

F12 Infinite delivers a fully managed IT and security solution that eliminates these gaps by integrating two powerful technologies:

1. **Managed Detection and Response**

   A 24/7 security operations centre (SOC) monitors your entire IT environment, identifying threats before they escalate into disruptions.

   - Real-time monitoring reduces the likelihood of prolonged breaches.
   - Security experts respond instantly, containing threats before they spread.

2. **Zero Trust Security**

   Zero Trust framework ensures that every access request is continuously verified—minimising the risk of compromised accounts or insider threats.

   - Multi-factor authentication secures endpoints and sensitive data.
   - Continuous verification ensures only authorised personnel gain access.

This proactive approach doesn't just reduce security risks—it safeguards productivity by keeping systems operational, reducing downtime, and ensuring threats don't disrupt the flow of business.

Proactive Security Means Greater Operational Efficiency

The benefits of proactive cyber security go far beyond data protection:

- **Minimised Downtime:** Faster threat detection prevents disruptions that could halt operations.
- **Stronger Compliance:** Meets standards like SOC2 Type 2 and PIPEDA with continuous security monitoring.
- **Increased IT Efficiency:** With F12 Infinite managing security operations, internal teams can focus on strategic growth, not fighting fires.

By embedding both MDR and Trust into F12 Infinite, businesses gain peace of mind—knowing their critical systems, data, and operations remain protected against both known and emerging threats.

The F12 Infinite Advantage: Productivity, Security, and Simplicity Combined

A fragmented approach to IT and security often creates operational blind spots—leaving IT teams overwhelmed and productivity impacted by reactive fixes. F12 Infinite simplifies security and productivity into a single, unified service with:

- 24/7 Threat Monitoring and Rapid Response
- Fully Managed Endpoint Protection with Lenovo DaaS and WatchGuard security.
- A Single Partner for Security, IT, and Risk Management.

By removing complexity and addressing both security gaps and resource strain, F12 Infinite ensures your organisation stays operational, secure, and focused on business growth.

Why IT Integration **Matters** for Business Resilience

Many Canadian businesses operate with a patchwork of IT systems—different hardware providers, multiple security tools, and various service contracts managed separately. This fragmented approach often leads to operational blind spots, security gaps, and rising costs, making it harder for businesses to maintain stability when disruptions occur.

Yet resilient businesses know that growth, security, and efficiency aren't separate goals—they're connected. IT integration isn't just about simplifying operations; it strengthens an organisation's ability to adapt, respond, and stay productive, even when challenges arise.

The Cost of Fragmented IT Management

A disconnected IT ecosystem—where endpoint management, security, and infrastructure operate in silos—creates operational friction and introduces hidden risks:

- **Visibility Gaps:** 82% of IT leaders report challenges in gaining full visibility across their entire technology stack, making it difficult to manage threats and performance. (Source: Forrester Business Technology Study, 2022)
- **Inconsistent Security Controls:** Multiple vendors and unaligned policies often lead to security gaps and unpatched vulnerabilities.
- **Operational Inefficiency:** 67% of IT managers cite vendor sprawl as a key driver of increased operational complexity. (Source: Gartner Endpoint Management Report, 2023)
- **Higher Costs:** Managing multiple tools and contracts often leads to redundant services and unpredictable expenses.

The impact? Increased downtime, security vulnerabilities, and strained IT resources—all while leadership loses control over IT performance.

The Case for Integration: Why Resilient Businesses Centralise IT

A fully integrated IT strategy bridges the gaps between security, infrastructure, and operational support—eliminating fragmentation while ensuring every layer of the business is protected and optimised.

What Does IT Integration Deliver?

- **Unified Security Posture:** Consistent policies across all endpoints, applications, and networks—reducing the risk of cyber threats.
- **Operational Continuity:** Centralised monitoring and proactive management prevent downtime and ensure business continuity.
- **Simplified Vendor Management:** A single service provider simplifies contracts, renewals, and support channels.
- **Cost Predictability:** Integrated pricing models reduce surprise costs while offering flat, per-user fees.

Real-World Benefits: A Data-Backed Approach

Organisations adopting integrated IT solutions experience measurable business improvements:

- **Reduced Downtime:** Companies with integrated IT models report 50% fewer outages linked to infrastructure mismanagement. (Source: Uptime Institute Outage Analysis, 2023)
- **Enhanced Security:** Businesses with unified security strategies experience 30% lower breach risks. (Source: Ponemon Institute, 2023)
- **Lower IT Costs:** Consolidating IT tools reduces operational spending by up to 25%. (Source: Gartner IT Cost Optimization Guide, 2023)

These results show that IT resilience directly correlates with business resilience, keeping operations secure, stable, and scalable.

The F12 Infinite Solution: IT Integration Without the Complexity

F12 Infinite simplifies IT integration by combining hardware, security, and IT management into a single, fully managed service. By partnering with Lenovo, WatchGuard, Blackpoint Cyber, and Coalition, F12 Infinite offers:

1. **Unified Security and Endpoint Management**
   - **Zero Trust:** Continuous verification of all network activity to reduce insider threats and credential misuse.
   - **MDR:** 24/7 threat detection and response, ensuring proactive protection against emerging threats.
   - **DaaS:** Fully managed endpoint hardware lifecycle services, keeping devices modern and secure.
2. **Consistent Compliance and Risk Management**
   - **SOC2 Type 2 & PIPEDA Compliance:** Continuous monitoring to meet Canadian data protection standards.
   - **Coalition CRA:** A free Cyber Risk Assessment that identifies security gaps and supports insurance readiness.
3. **Simplified IT Operations**
   - **Single Partner Management:** One contract, one service provider, full IT coverage.
   - **Flat Monthly Pricing:** No surprise costs—predictable, per-user pricing simplifies budgeting.

Why IT Integration Drives Business Resilience

Resilient businesses can withstand disruption, adapt to change, and maintain operational excellence even under pressure. F12 Infinite ensures your IT systems contribute to that resilience by:

- **Minimising Disruption:** Centralised threat monitoring and endpoint security ensure systems stay operational.
- **Driving Productivity:** Modern devices paired with Lenovo DaaS reduce downtime and empower teams.
- **Reducing Risk Exposure:** WatchGuard and Blackpoint Cyber safeguard critical systems with proactive security.

Take Control of Your IT Future with F12 Infinite

A fragmented IT strategy can leave your business exposed. F12 Infinite offers a proven path to secure, simplified, and integrated IT management—so your business stays protected and focused on growth.

Ready to Strengthen Your Business Resilience?

Book Your Free Cyber Risk Assessment Today

Use Case: **Preventing Ransomware Disruption** in Agriculture with F12 Infinite

The Challenge: A Ransomware Attack Disrupted Operations and Productivity

A mid-sized dairy and crop farm in Canada, with 120 employees, faced a ransomware attack that halted critical farm operations. The business relied on a mix of automated feeding, milking, and crop irrigation systems to keep operations running across its three sites. However, the attack encrypted operational systems, preventing automated schedules from running and leaving both livestock care and crop maintenance at risk.

The IT setup was a mix of outdated hardware and off-the-shelf antivirus software spread across 30 administrative computer users and 90 non-computer staff who relied on automated equipment to complete essential tasks.

- **No Automated Task Execution:** Feeding and milking operations were suspended for 18 hours, impacting livestock welfare.
- **Operational Chaos:** Manual scheduling was impossible due to system lockouts, and livestock care became fully reliant on paper records.
- **Untrained Staff:** Employees lacked cyber security awareness training, increasing vulnerability to phishing and malware attacks.
- **Inconsistent Support:** The farm relied on calling laptop manufacturers' help desks for technical support and had no centralised IT expertise.
- **Disjointed SaaS Management:** The business struggled to manage multiple third-party SaaS platforms (e.g., farm management software, accounting tools) without proper security oversight or integration.

What Made the Farm Vulnerable?

- **No 24/7 Monitoring:** Antivirus software detected the attack too late to stop data encryption.
- **Relying on Consumer-Grade Tools:** Off-the-shelf antivirus software lacked the sophistication for proactive threat detection.
- **Poor Endpoint Management:** Devices were outdated, unpatched, and lacked proper encryption settings.
- **Lack of Network Segmentation:** Critical automation systems shared the same network as office computers, allowing the ransomware to spread across the entire infrastructure.
- **No Incident Response Plan:** The IT staff had no playbook for handling security incidents, leading to delays in response.

The Solution: F12 Infinite's Comprehensive IT Integration for Agriculture

To prevent future attacks and secure operational continuity, the farm partnered with F12 Infinite for a fully managed IT and cyber security solution, combining:

MDR (Managed Detection & Response):

- 24/7 threat detection and monitoring across all systems, including automated milking and feeding equipment.
- Proactive ransomware containment, automatically isolating infected devices.
- Real-time alerts sent to F12 security teams for immediate action.

Zero Trust Security:

- Network segmentation to isolate critical automation systems from administrative IT resources.
- Multi-Factor Authentication (MFA) on all remote access points.
- Least-Privilege Access ensuring non-computer staff could only access operational tools.

Device-as-a-Service (DaaS):

- Hardware standardisation with modern, secure Lenovo Think-branded devices.
- Lifecycle Management: Automatic updates, patching, and encryption for all 30 administrative workstations.
- Consolidated Vendor Support: Replacing multiple manufacturer help desks with a single, dedicated support through F12.

Cyber Risk Assessment (CRA):

- Full IT risk assessment that exposed outdated device vulnerabilities and software misconfigurations.
- Cyber Insurance Qualification: The CRA identified risks and helped the farm qualify for a reduced cyber insurance premium.

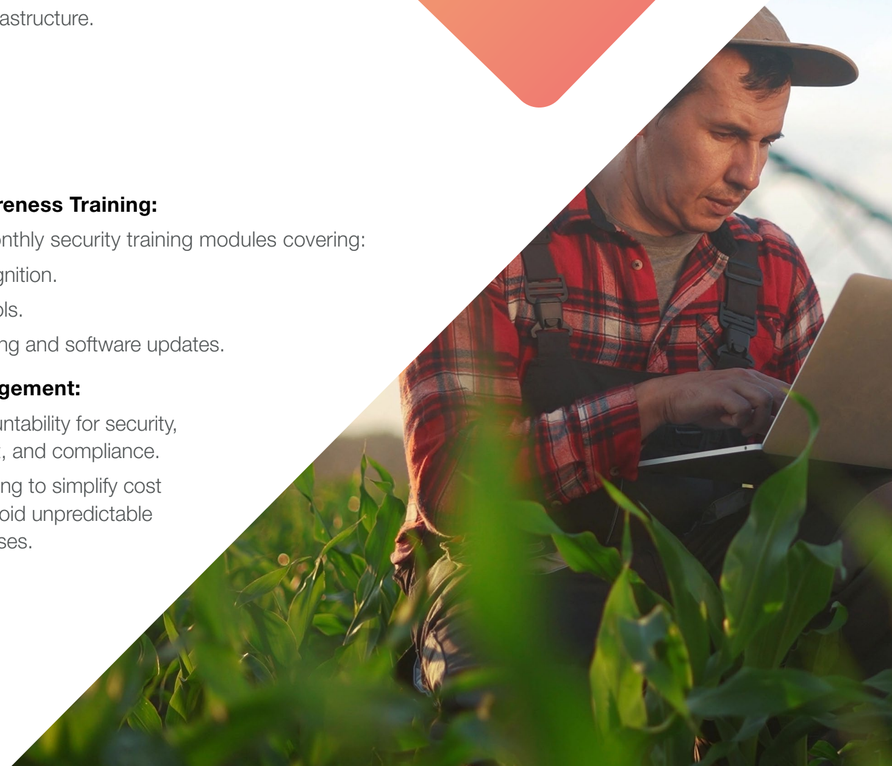
Cyber Security Awareness Training:

Farm staff received monthly security training modules covering:

- Phishing threat recognition.
- Safe use of SaaS tools.
- Proper device handling and software updates.

F12 Unified IT Management:

- Single point of accountability for security, hardware, IT support, and compliance.
- Flat, predictable pricing to simplify cost management and avoid unpredictable emergency IT expenses.



The Results: Tangible Improvements in Security and Operational Continuity

Within 90 days of implementing F12 Infinite, the farm experienced:

- **Zero Operational Downtime:** A second ransomware attack was identified and neutralised before encryption.
- **Reduced Device Failures:** Standardised, modern Lenovo devices reduced IT-related disruptions by 45%.
- **Faster Support Resolution:** With F12 handling all IT support, issue resolution time dropped by 70%.
- **Cost Avoidance:** The farm avoided $150,000 CAD in potential ransom payments and operational losses.
- **Improved Security Awareness:** 100% of staff completed cyber security awareness training within the first quarter.

Why IT Integration Matters in Agriculture

Modern farms rely heavily on automated systems for feeding, irrigation, and livestock care. A ransomware attack can bring operations to a standstill, impacting:

- **Animal Welfare:** Delayed feeding and milking schedules can harm livestock health.
- **Operational Efficiency:** Manual task completion is unsustainable for large-scale farms.
- **Financial Stability:** Breaches not only demand ransom payments but disrupt supply chain operations and productivity.

The F12 Infinite Advantage for Agriculture

By integrating hardware, security, and IT management into one service, F12 Infinite provides:

- **24/7 Ransomware Protection:** Continuous monitoring and rapid threat response.
- **Hardware & Endpoint Security:** Modern Lenovo ThinkShield devices with proactive patching.
- **Simplified Support:** One provider for security, hardware, and IT services.
- **Cost Predictability:** Flat, per-user pricing without hidden fees.

Protect Your Business from Cyber Attacks Today

Don’t let a ransomware attack threaten your operation. F12 Infinite provides a fully managed IT solution designed to keep your systems secure, productive, and resilient.

Book Your Free Cyber Risk Assessment

Why **Risk Readiness Matters** for Long-Term Business Continuity

Risk is no longer a hypothetical in today's business landscape—it's a constant reality. Canadian businesses face mounting operational challenges, from ransomware threats and supply chain vulnerabilities to rising IT costs and compliance pressures. Yet, many businesses approach these threats reactively, addressing them only when a crisis strikes.

This reactive mindset can be costly, both financially and operationally. A single disruption—whether it's a cyber attack, hardware failure, or staffing shortage—can lead to significant downtime, lost revenue, and damage to customer trust.

What Does Risk Readiness Really Mean?

Risk readiness is more than just cyber security tools or backup systems. It's a proactive strategy that ensures a business can continue operating during disruptions while minimising financial and operational impact. True readiness involves:

- **Identifying Risks Early:** Understanding vulnerabilities before they can be exploited.
- **Mitigating Threats Continuously:** Implementing layers of defence that evolve with emerging risks.
- **Ensuring Operational Continuity:** Maintaining uptime and access to critical systems, even during disruptions.
- **Simplifying Compliance:** Meeting SOC2 Type 2, PIPEDA, and other standards without complex oversight.

Why Canadian Businesses Struggle with Risk Readiness

While Canadian businesses often have dedicated CISOs, large security budgets, and in-house expertise, mid-market businesses face a different reality:

- **Limited IT Resources:** Mid-sized businesses often rely on generalist IT teams without specialised security expertise.
- **Fragmented Tools:** Security and IT infrastructure may be spread across multiple vendors, creating gaps in visibility and control.
- **No Continuous Threat Monitoring:** Most businesses lack 24/7 detection capabilities, leading to delayed responses during attacks.
- **Inconsistent Device Management:** Aging devices and unpatched software remain some of the most exploited vulnerabilities.
- **Reactive Security Postures:** Cyber security investments often follow major incidents, rather than preventing them.

This fragmented approach not only leaves businesses exposed but also makes compliance with modern regulatory standards challenging.

The High Cost of Being Unprepared

A lack of proactive risk management can lead to severe business consequences. Consider:

Ransomware Impact

The average ransomware payout now exceeds $1 million CAD, and that doesn't include recovery costs or downtime. (Source: Sophos State of Ransomware 2023)

Data Breach Costs

The average cost of a data breach in Canada has surged to $7.3 million CAD, including reputational damage. (Source: IBM Cost of a Data Breach Report, 2023)

Downtime Consequences

Unplanned downtime costs mid-market businesses an average of $300,000 CAD per incident. (Source: Veeam Data Protection Trends, 2023)

Compliance Fines

Failing to meet SOC2 and PIPEDA standards can lead to regulatory fines and lost business opportunities.

The F12 Approach to Risk Readiness

F12 Infinite is designed to eliminate the guesswork from risk readiness. By combining proactive security, resilient infrastructure, and expert management under a single, fully managed service, businesses gain a complete solution for business continuity and protection.

How F12 Delivers Risk Readiness:

1. **Proactive Threat Detection and Response:**
   - **MDR (Managed Detection & Response)** provides 24/7 monitoring and rapid response to cyber threats.
   - **Zero Trust** architecture ensures constant verification of every access attempt, preventing unauthorised access.
2. **Hardware Resilience with Lenovo DaaS:**
   - **Modern Endpoint Management:** Lenovo's Device-as-a-Service provides modern devices with ThinkShield security, ensuring secure and reliable performance.
   - **Automated Patch Management:** Devices stay secure with regular, automated firmware and software updates.
3. **Continuous Risk Assessment and Compliance:**
   - **Coalition Cyber Risk Assessment (CRA):** Uncovers security gaps and supports businesses in qualifying for cyber insurance.
   - **SOC2 Type 2 Compliance Support:** F12 Infinite ensures your organisation remains compliant with Canadian data protection standards.
4. **Business Continuity Management:**
   - **Redundant Backup Systems:** Automated disaster recovery with continuous data replication.
   - **Unified IT Management:** A single partner for hardware, security, and IT support under one predictable monthly fee.

Real-World Impact: A More Secure, Risk-Ready Business

After implementing F12 Infinite, businesses experience:

- **Faster Threat Response:** Potential attacks neutralised before they disrupt operations.
- **Reduced IT Complexity:** Eliminate multiple vendors and standardise security policies.
- **Lower Incident Costs:** Predictable pricing and proactive defences help avoid unexpected losses.
- **Stronger Compliance:** Simplified alignment with SOC2, PIPEDA, and insurance standards.

Why Risk Readiness Is Essential for Business Continuity

Modern Canadian businesses can no longer afford passive security strategies. Risk readiness means:

- **Defending Against Advanced Threats:** Prevent ransomware, supply chain attacks, and insider threats before they cause harm.
- **Empowering IT Teams:** Free internal teams from firefighting mode so they can focus on innovation and growth.
- **Safeguarding Productivity:** Ensure minimal downtime even during security events.

Ready to Make Risk Readiness Part of Your IT Strategy?

F12 Infinite provides a comprehensive, fully managed IT solution designed to help mid-market businesses stay secure, resilient, and operational—no matter the challenges ahead.

Book Your Free Cyber Risk Assessment

Key Takeaways: Build a Smarter, More Secure IT Strategy

The path to a smarter, more secure IT strategy begins with recognising that technology alone isn't enough to drive true business resilience. Throughout this guide, we've explored the critical challenges mid-market enterprises face—outdated infrastructure, resource strain, ransomware threats, and the need for risk readiness.

But what truly sets F12 Infinite apart isn't just the ability to solve these challenges—it's how we solve them.

What You've Learned:

- **Outdated IT Creates Hidden Risks:** Aging hardware and fragmented security tools lead to downtime, data exposure, and compliance challenges.
- **Resource Gaps Strain Your Operations:** The ongoing cyber security talent shortage means many Canadian businesses face security gaps without the internal resources to close them.
- **A Smarter IT Approach Is Essential:** F12 Infinite, powered by Lenovo DaaS, delivers secure, modern infrastructure while reducing complexity and costs.
- **Proactive Security Enhances Productivity:** MDR and Zero Trust actively prevent threats, protecting operations without disruption.
- **IT Integration Builds Resilience:** A unified approach reduces vendor sprawl, simplifies compliance, and enhances risk readiness.

What Makes F12 Infinite Different—A Smarter IT Ecosystem You Can't Get Anywhere Else

While other providers may offer similar technologies, F12 Infinite is designed for mid-market businesses that need more than just tools—they need business continuity, proactive risk reduction, and complete accountability.

Here's what sets us apart from other providers, even those using similar technologies:

- **Holistic Risk Readiness:** Not just a one-time assessment. The Coalition CRA delivers continuous cyber risk evaluations paired with proactive risk mitigation to help you qualify for cyber insurance.
- **Integrated Security by Design:** Our approach goes beyond basic endpoint protection with WatchGuard Zero Trust, ensuring continuous threat validation and segmented network access for reduced exposure.
- **Proactive Incident Management:** Blackpoint Cyber MDR doesn't just monitor threats—it identifies and neutralises them in real-time, protecting your systems from ransomware and advanced threats.
- **Hardware Built for Productivity:** Lenovo DaaS ensures modern, secure devices with lifecycle management, automated updates, and enterprise-grade protection.
- **A Unified IT Relationship:** One contract, one point of accountability—we eliminate vendor complexity and take full ownership of your IT performance.

Why This Matters for Your Business

A smarter, more secure IT strategy means:

- **Reduced Complexity:** No juggling multiple vendors—F12 Infinite manages security, hardware, compliance, and IT support under one plan.
- **Risk Prevention, Not Just Response:** With continuous MDR monitoring and risk assessments, threats are neutralised before they impact your business.
- **Operational Continuity:** Stay productive, even in the face of security incidents or hardware failures.
- **Simplified Compliance:** Meet SOC2 Type 2, PIPEDA, and cyber insurance requirements with less complexity.
- **Cost Predictability:** No surprise invoices—just flat-rate pricing for complete coverage.

Book Your **Free Cyber Security Readiness Assessment** Today

Pinpoint vulnerabilities before they can be exploited.

Receive a tailored IT security improvement plan from our experts.

Learn how F12 Infinite can simplify and strengthen your entire IT environment.

F12.net™

Take the first step today.

Contact F12 Infinite to discover how we can help your organisation lead with confidence in 2025 and beyond.

Contact Us

For more information or to get started, please reach out to us using the details below:

1-866-F12-8782 | www.f12.net | info@f12.net

Office Locations

Toronto:

220 Markland Street, Unit A-2,
Markham, ON L6C 1T6

Tel: (416) 736-8386

Vancouver:

200 – 17577 56 Avenue,
Surrey, BC V3S 1C4

Tel: (604) 576-9522

Edmonton:

213555 156 Street NW,
Edmonton, AB T5V 1R9

Tel: (780) 413-8458

We look forward to partnering with you to secure your business and drive success

FIT1111-01-2025-V1