eBook 2

F12.net™

Secure Your Organisation:

Mastering Cyber Security, Risk Management, and Compliance.

blackpoint Coalition Lenovo WatchGuard

Table of Contents

Building on a Smarter IT Foundation

This is eBook 2 in the F12 Infinite Series, designed to help Canadian mid-market enterprises take control of their IT security, infrastructure, and risk management.

In eBook 1, we explored how outdated IT infrastructure, fragmented tools, and limited visibility create operational challenges for growing businesses. We demonstrated how F12 Infinite simplifies IT management by unifying hardware modernisation, proactive support, and predictable pricing into a single, managed service.

Why Cyber Security Must Be Your Priority

While modernising your infrastructure is essential, cyber threats and compliance demands continue to evolve—putting businesses at greater risk than ever before. Cyber attacks now target mid-market enterprises with increasing sophistication, often exploiting gaps caused by incomplete protection or underprepared teams.

In this eBook, we'll take the next step in building IT resilience, focusing on:

- The latest cyber security threats affecting Canadian businesses.
- The hidden costs of a security breach beyond financial loss.
- Why cyber insurance readiness requires more than basic protection.
- How F12 Infinite integrates Zero Trust security, MDR, and risk assessments for proactive defence.

By the end of this eBook, you'll understand how to:

- Strengthen your security posture with simplified tools.
- Eliminate complexity with a fully managed solution.
- Qualify for cyber insurance and reduce financial risk.

The Evolving Threat Landscape
for Canadian Businesses

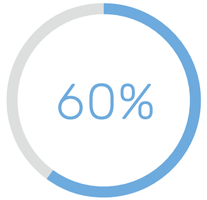
The cyber threat landscape is evolving rapidly, and businesses are caught in the crosshairs. For years, the focus of high-profile cyber attacks seemed reserved for large corporations with expansive data stores. But today's reality tells a different story—one where small and medium businesses face the same threats but often lack the resources to defend themselves adequately.

Canadian businesses are no exception. In fact, 85.7% of companies experienced at least one cyber attack in 2021, up from 78% the previous year surge? Because attackers have realised that smaller organisations often have fragmented IT environments, outdated systems, and overburdened teams—leaving security gaps too tempting to ignore.

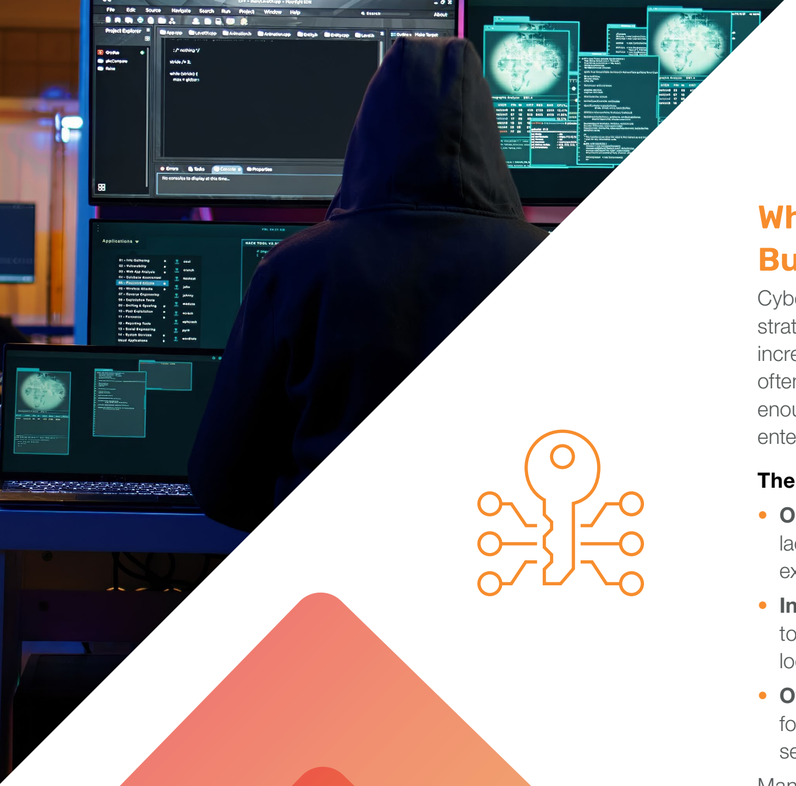
Take ransomware, for example. Once considered a problem for massive corporations, it has become one of the most disruptive threats facing mid-market businesses. In a ransomware incident, critical systems are encrypted and held hostage until a payment is made. These attacks have paralyzed manufacturers, law firms, and healthcare organisations, halting operations entirely and putting client trust at risk.

Yet the damage goes far beyond the ransom itself. A StatCan report found that the average financial impact of a cyber breach on Canadian businesses surged to $19,000 in 2021—up from $11,000 just two years earlier. But the real impact extends far beyond the initial financial hit. The most damaging consequences often surface long after the breach, including:

- **Operational Downtime:** Systems go offline, orders are delayed, and revenue stalls.
- **Reputational Harm:** Clients question your ability to protect their data.
- **Compliance Risks:** Regulatory fines and legal complications pile up.
- **Cyber Insurance Gaps:** Many businesses find they can't even qualify for coverage after a breach.



Consider this: 60% of mid-sized businesses that experience a serious cyber attack close their doors within six months due to the financial strain and reputational fallout.



Why Small and Medium Businesses Are Prime Targets

Cyber criminals aren't just opportunistic—they're strategic. Small and mid-market businesses are increasingly seen as lucrative targets because they often fall into a dangerous middle ground: complex enough to hold valuable data but without the enterprise-grade defences of larger corporations.

The most common vulnerabilities include:

- **Outdated Hardware:** Legacy systems often lack the latest security patches, leaving systems exposed.
- **Inconsistent Security Policies:** Fragmented tools and inconsistent practices across multiple locations create exploitable gaps.
- **Overstretched IT Teams:** Internal teams often focus on day-to-day IT tasks rather than proactive security management.

Many small and mid-market businesses believe they're covered with basic antivirus software or firewalls. Yet, modern threats demand proactive, continuous protection that adapts in real time.

The Shift to Proactive Security: Why Old Defences No Longer Work

The days of set-and-forget IT security are over. Attackers are no longer just trying to break in—they're lurking quietly, waiting for the right moment. State-sponsored threat actors have begun targeting Canadian businesses, not just for financial gain but as part of larger cyber warfare strategies, making proactive security essential for businesses of all sizes.

Today, forward-thinking are embracing proactive defence models like:

- **24/7 Threat Detection:** Cyber threats don't operate on a schedule.
- **Zero Trust Frameworks:** Assume no device or user is trustworthy until verified.
- **Cyber Risk Assessments:** A data-driven approach to identifying and closing security gaps before they're exploited.

How F12 Infinite Helps Mid-Market Enterprises Stay Ahead of Threats

At F12, we understand that security isn't just about firewalls or antivirus software—it's about operational resilience. F12 Infinite was designed to provide businesses with a fully managed, proactive security solution without the complexity of managing multiple vendors.

Here's how we do it:

- **Integrated Threat Protection:** Around-the-clock Managed Detection & Response backed by security experts who act when threats emerge.
- **Zero Trust Security:** No access is granted without verification, reducing insider risks.
- **Hardware Security by Design:** Proactive hardware lifecycle management ensures every device is secure and up to date.
- **Risk Readiness Built In:** Cyber Risk Assessments provide continuous security checks, supporting both compliance and insurance qualifications.

This fully integrated model means you're not just buying security tools—you're investing in a complete strategy to stay ahead of threats while controlling costs.

The True Cost of a Cyber Security Breach – **More Than Just Numbers**

A cyber security breach isn't just a technical failure—it's a business crisis. When systems go down, operations stop, revenue stalls, and reputations take a hit. Yet, for many mid-market enterprises, the full impact often isn't felt until the damage is irreversible.

Think about it this way: a single breach can begin with something as simple as an employee clicking a deceptive email link. But what follows is often a cascading chain of disruptions—data encryption, halted workflows, ransom demands, and regulatory scrutiny.

And yet, the dollar amount on a ransom demand often isn't the real cost. It's what happens next that's even more damaging.

The Financial Toll: Beyond the Obvious Losses

The numbers surrounding a breach can be staggering, but the long-term financial impact often exceeds the initial payout.

Consider this: in 2021, Canadian businesses impacted by cyber security incidents reported an average recovery cost of $19,000—nearly double what it was just two years prior. But that figure doesn't capture the full picture.

The true cost includes:

- **Revenue Loss from Downtime:** When systems are compromised, even a one-day outage can result in significant revenue loss. Imagine an e-commerce retailer unable to process sales during peak holiday traffic.
- **Legal Penalties & Fines:** Non-compliance with PIPEDA (Canada's data privacy law) can result in fines of up to $100,000 per violation—a figure that compounds if sensitive customer data is compromised.
- **Increased Cyber Insurance Premiums:** A business hit by a breach often finds renewing coverage more expensive, or even impossible without proving security improvements.

But the costs don't stop there. Downtime costs. Delays cost. Lost trust costs.

Operational Disruption: What Happens When IT Fails?

When a cyber breach hits, it's not just IT that feels the pressure—entire departments can grind to a halt.

Picture this:

A manufacturing firm is hit with ransomware, locking its scheduling and inventory systems. Without access to its digital supply chain, production stops. Staff are left waiting for instructions, while suppliers demand answers. Missed deadlines ripple through their customer base.

Key operational consequences include:

- **Productivity Paralysis:** Teams are unable to perform essential tasks like invoicing, order fulfillment, and scheduling.
- **Overburdened IT Staff:** Internal teams are forced to focus on damage control instead of their core functions.
- **Supply Chain Delays:** If third-party systems are impacted, it can delay orders and impact revenue downstream.

These disruptions hurt productivity, employee morale, and client relationships—long after systems are restored.

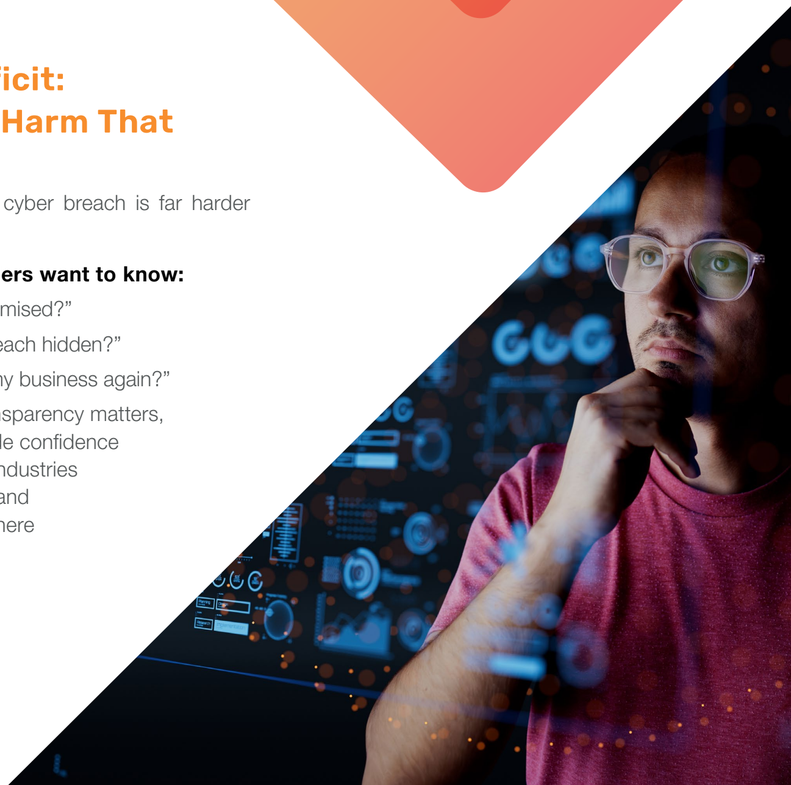
The Trust Deficit: Reputational Harm That Lingers

Rebuilding trust after a cyber breach is far harder than restoring systems.

Clients and stakeholders want to know:

- "Was my data compromised?"
- "How long was the breach hidden?"
- "Can I trust you with my business again?"

And in an era where transparency matters, a single breach can erode confidence for years—especially in industries like finance, healthcare, and professional services, where data privacy is critical.



Legal Exposure: The Compliance Fallout

Beyond immediate financial strain, a cyber breach can trigger serious regulatory consequences.

In Canada, the Personal Information Protection and Electronic Documents Act (PIPEDA) requires organisations to report data breaches involving sensitive information.

Failing to comply can lead to:

- Fines of up to $100,000 per violation.
- Mandatory public disclosure of the breach.
- Ongoing third-party audits at the company's expense.

And regulatory issues don't just stop at the breach itself. Cyber insurance providers are increasingly denying claims if businesses can't demonstrate proactive risk management before the incident.

The Human Cost: Employee Impact and Talent Retention

While financial and reputational damage are critical, a cyber breach can also leave lasting scars on your workforce.

- **Increased Pressure on IT Teams:** After a breach, existing teams often work around the clock to mitigate damage.
- **Burnout & Turnover:** Stress and crisis management often lead to employee burnout, especially if the breach could have been avoided.
- **Talent Drain:** Security talent is already hard to find—with a 3.5 million global shortage of cyber security professionals . Companies with reactive security practices often lose top talent to more secure, forward-thinking competitors.

F12 Infinite helps prevent this strain by offering fully managed services—so your team can focus on their jobs, not crisis management.

How F12 Minimises Breach Impact Before It Happens

At F12, we believe the best defence is a proactive strategy—not just reacting to threats but eliminating vulnerabilities before they impact operations.

F12 Infinite delivers:

- **24/7 Managed Detection & Response:** For real-time threat detection and rapid incident response.
- **Zero Trust Security Controls:** Continuous access verification.
- **Cyber Risk Assessments:** Preemptive vulnerability assessments.
- **Simplified Device Management:** Device-as-a-Service ensures endpoints are secure and always updated.

This fully integrated approach ensures businesses are not only prepared for modern threats but also able to respond effectively when security incidents occur.

Proactive Security with F12 Infinite – Built-In Protection Without the Complexity

When a cyber threat targets your business, speed matters. The difference between a minor security event and a major breach often comes down to how quickly a threat is detected and neutralised.

Yet, many businesses still operate with outdated, reactive defences—tools that alert you after damage has already begun. In fact, according to a Coalition Cyber Health Report, it takes businesses an average of 207 days to detect a breach and another 70 days to contain it. Imagine nearly nine months where a threat actor has access to sensitive data, disrupting your business from the inside.

This delay has devastating consequences: financial loss, downtime, and irreversible reputational harm.

It takes businesses an average of
207 days to detect a breach and another 70 days to contain it.

The Difference: Minutes, Not Months with F12's MDR

Managed Detection and Response (MDR) changes the game. Rather than waiting for suspicious activity to trigger delayed alerts, MDR works in real-time—proactively identifying, containing, and neutralising threats as they emerge.

Here's how F12 Infinite, powered by Blackpoint Cyber's MDR, transforms your security posture:

1. Threats Are Detected in Real-Time

While traditional security tools might flag an incident after days or weeks, MDR continuously monitors your entire network. The moment an unusual behaviour pattern emerges—like unauthorised access attempts or data being copied out of your system—F12's MDR platform responds.

Fact: Coalition reports that businesses using proactive MDR solutions reduce breach detection time from 207 days to under 5 minutes.

2. Attacks Are Stopped Before They Spread

Speed is everything. Once a threat is identified, automated threat containment kicks in instantly:

- Infected endpoints are isolated from the network.
- Administrator privileges are revoked for compromised accounts.
- Threat data is captured to prevent repeat attacks.

This approach stops ransomware before it can encrypt critical data—minutes, not months.

3. Expert Human Response, Not Just Automation

MDR isn't just software—it's security expertise on-demand. When a threat emerges, F12 security analysts review the event immediately to determine the nature and severity of the risk.

- False positives? Dismissed within minutes.
- Active threats? Engaged and contained with precision.
- Escalation needed? If the threat reaches a critical level, our team directly intervenes to prevent further impact.

Fact: Businesses with MDR reduce breach containment time by over 90%, drastically limiting damage and data loss.

Why Traditional Antivirus Alone Isn't Enough Anymore

The idea that antivirus software can protect a modern business is a dangerous misconception. It's a relic of an era when threats were simpler and predictable—before fileless attacks, zero-day exploits, and AI-driven malware.

Today, cybercriminals operate with the same sophistication as modern businesses. Tools are faster, attacks more evasive, and many threats actively avoid detection by traditional antivirus.

Consider this:

- **Antivirus Relies on Signatures:** Traditional antivirus scans for known threats by matching code against a predefined database of malware signatures. If a new threat isn't yet catalogued, it slips through.
- **No Contextual Awareness:** Basic firewalls and AV tools don't understand the broader behaviour of a threat. If a hacker gains legitimate credentials and moves laterally across systems, most tools remain silent.
- **No Real-Time Response:** Even when antivirus detects something suspicious, alerts don't equal action. The clock keeps ticking while teams scramble to respond manually.

And cybercriminals know this. Many modern attacks, like fileless malware, operate entirely in system memory, leaving no trace for antivirus scans to detect.

How F12 Closes the Gaps with MDR and Zero Trust Security

F12 Infinite offers more than basic protection. It provides a multi-layered defence strategy purpose-built for mid-market enterprises where downtime, data loss, and reputational damage can be devastating.

Here's how it works:

1. Managed Detection and Response – Blackpoint Cyber

Instead of waiting for a threat to surface, F12 with Blackpoint Cyber MDR detects unusual patterns as they happen:

- **Behavioral Analysis:** Tracks activity patterns across your entire environment—flagging unusual file access, login attempts, and privilege escalations.
- **Live Threat Hunting:** Security experts monitor your network around the clock, not just during business hours.
- **Rapid Isolation:** When a threat is detected, infected devices are immediately isolated from the network—stopping the spread.
- **Impact:** The average breach detection time drops from 212 days to minutes, preventing extensive data theft and operational damage.

2. Zero Trust Security – WatchGuard Integration

With F12, Zero Trust principles redefine how your network grants access.

- **No Automatic Trust:** Every user, device, and access attempt is treated as untrusted until verified.
- **Continuous Re-Validation:** Users and systems are re-verified throughout their session, not just at login.
- **Multi-Factor Authentication:** Access requires multiple layers of verification, even for trusted users.
- **Impact:** 82% of breaches involve compromised credentials (Verizon DBIR 2023). Zero Trust reduces the risk of stolen passwords causing a full-scale breach.

3. Secure Hardware Management – Lenovo DaaS

Outdated, unpatched devices create vulnerabilities for attackers to exploit. F12 with Lenovo DaaS simplifies endpoint security:

Pre-Secured Devices: Every device is preloaded with Lenovo ThinkShield, including encryption, BIOS protection, and remote-wipe capabilities.

- **Automated Patch Management:** Firmware and security patches happen automatically.
- **End-of-Life Security:** Devices are retired with data destruction protocols.
- **Impact:** A 2023 Gartner study reported that 68% of data breaches originated from compromised endpoints. Keeping devices updated reduces this risk dramatically.

4. Continuous Risk Visibility – Coalition CRA

Most companies don't fully understand their security posture until after a breach—which is too late.

The Coalition Cyber Risk Assessment (CRA), built into F12, offers ongoing vulnerability scanning and compliance validation.

- **Proactive Scans:** Continuously checks for vulnerabilities before they can be exploited.
- **Compliance Checks:** Ensures you meet frameworks like SOC2 and PIPEDA.
- **Insurance Readiness:** Reduces the cyber insurance premium risk with validated security measures.
- **Impact:** Companies with ongoing security assessments have a 65% lower risk of sustaining a breach.

Protecting Productivity with **Proactive Cyber Security**

For any business regarless of size, operational disruptions from cyber threats can result in financial loss, stalled productivity, and reputational harm. Preventing these threats requires a proactive security approach that stops risks before they disrupt core operations.

Why Reactive Security Fails to Protect Productivity

Relying on outdated antivirus tools and reactive defences leaves businesses exposed. Traditional security often detects threats after the damage has already begun, resulting in:

- **Workforce Disruption:** Employees unable to access critical systems or perform tasks.
- **Revenue Loss:** Service interruptions leading to halted business activities.
- **IT Overload:** Internal teams forced to focus on emergency containment instead of strategic work.

Fact: The average downtime from a ransomware attack lasts 21 days—with productivity loss and revenue impact continuing long after systems are restored (Coalition, 2023).

The Power of Proactive Protection with MDR

F12 Infinite integrates Managed Detection and Response to stop threats before they impact operations. Unlike traditional tools, MDR offers:

- **Real-Time Monitoring:** Continuous oversight to detect suspicious activity before it escalates.
- **Automated Threat Containment:** If a threat is identified, compromised endpoints are isolated immediately to prevent lateral movement.
- **Expert Threat Intervention:** Security analysts investigate threats and initiate a response, minimising disruption.
- **Result:** Faster detection, faster response, and minimal business impact.

Stopping Threats Before They Start

Proactive cyber security goes beyond stopping attacks. F12 prevents them from occurring with a fully integrated security ecosystem:

- **Zero Trust Access Controls:** Ensures only verified users and devices can access systems.
- **Automated Endpoint Protection:** Keeps devices secure with automated patching and security controls.
- **Continuous Risk Assessments:** Identifies vulnerabilities and validates ongoing security posture.

Why IT Integration Matters for Business Resilience

Disconnected IT systems don't just slow businesses down—they expose them to greater risk, complexity, and operational inefficiencies. Many businesses manage multiple IT tools, vendors, and security systems that were never designed to work together. The result? Gaps in protection, wasted resources, and limited visibility when it matters most.

F12 Infinite solves this problem by providing a fully integrated IT platform that combines hardware management, proactive security, and continuous monitoring—all managed under a single service model designed for business resilience.

Cyber Security

Proactively safeguard your business with fully managed cyber security, including multi-factor authentication, advanced threat detection, and global threat response. Stay compliant with SOC 2 Type 2 standards while reducing operational risks.

IT Support

Ensure operational continuity with 24/7 dedicated support, proactive maintenance, and seamless on-premises or remote IT assistance.

F12 Infinite delivers predictable pricing, operational resilience, and flexible IT solutions that grow* with your business, ensuring scalability, security, and success.

Strategic Consulting / IT Roadmap

Gain a competitive edge with strategic IT consulting that delivers proactive assessments, technology roadmaps, and actionable insights to optimise your IT investments.

Device-as-a-Service (DaaS)

Boost productivity with managed physical desktops and secure endpoint management, enabling your workforce to operate efficiently from anywhere.

Infrastructure-as-a-Service (IaaS)

Ensure operational continuity with 24/7 dedicated support, proactive maintenance, and seamless on-premises or remote IT assistance.

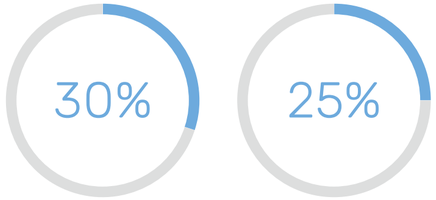
The Hidden Risks of Fragmented IT

Fragmented IT infrastructure creates blind spots that put businesses at risk:

When security tools and management systems don't communicate, critical vulnerabilities go unnoticed. Imagine an endpoint security tool identifying a suspicious login attempt but failing to alert the firewall to block the connection. Without integration, security gaps stay open.

Operational inefficiencies also emerge. IT teams waste time managing multiple portals, vendors, and reporting tools instead of focusing on strategic business improvements. Invoices pile up from different suppliers, and troubleshooting takes longer with multiple help desks involved.

A fragmented setup is more than just inconvenient—it's costly. IT leaders often find themselves paying for overlapping tools and unused licenses, yet still unable to ensure complete protection.



Businesses that integrate IT services report a 30% reduction in downtime and 25% fewer security incidents than those with fragmented setups (Gartner, 2023).

The Power of Unified IT with F12 Infinite

F12 Infinite brings clarity and control to IT operations by integrating every element into a cohesive, managed ecosystem:

- **Simplified Management:** A single platform for all IT services—hardware, security, and infrastructure—reduces administrative overhead and frees up your internal resources.
- **Proactive Threat Protection:** MDR and Zero Trust security work together to monitor activity, detect threats in real time, and respond instantly, reducing downtime and impact.
- **Consistent Performance:** With device lifecycle management through DaaS, every employee has secure, up-to-date devices, minimising disruptions from outdated hardware or manual patching.

Why IT Integration Matters Now More Than Ever

Canadian businesses face mounting challenges: rising cyber threats, increasing compliance demands, and the need for greater operational efficiency. F12 Infinite addresses these realities by simplifying complex IT ecosystems and delivering proactive protection tailored for business growth.

When security, hardware, and management tools work together, businesses gain:

- **Enhanced Visibility:** See and control your entire IT environment in one place.
- **Stronger Security:** Identify and stop threats faster with MDR, Zero Trust, and continuous monitoring.
- **Predictable Costs:** Flat-rate pricing eliminates budget surprises.

Key Takeaways and Next Steps – Building a Smarter, More Secure IT Strategy

As a business or IT leader you face relentless pressure: evolving cyber threats, rising compliance demands, and the challenge of managing complex IT systems—all while trying to grow. The real risk isn't just a data breach. It's the productivity lost, the reputation damaged, and the revenue impacted when your IT systems fail to protect your business. F12 Infinite offers more than just tools—it's a fully managed IT ecosystem designed to eliminate complexity, close security gaps, and keep your business running without disruption.

Key Takeaways:

- **Eliminate Unnecessary Risk:** Fragmented tools leave gaps. F12 Infinite provides a fully integrated solution with hardware, security, and IT management working as one.
- **Proactive Protection, Not Just Alerts:** With 24/7 MDR, Zero Trust controls, and proactive risk assessments, threats are identified and contained before they can disrupt operations.
- **Simplified IT Management:** A single, predictable service with end-to-end management—no more juggling vendors, tools, and licenses.
- **Business Growth Without Compromise:** Flexible, scalable IT infrastructure that evolves with your organisation's needs, reducing both costs and complexity.

Next Steps: Take Control of Your IT Future

Don't wait for a breach to reveal the gaps in your defences. Discover how F12 Infinite can protect your business, reduce complexity, and improve operational efficiency—all while keeping your team focused on what matters most: growth and success.

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 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

FIT1115-01-2025-V1