COMCAST
BUSINESS
SecurityEdge™

Foundational cybersecurity for small business

Sponsored by Comcast Business

Introduction

The Internet touches just about every aspect of our lives, from commerce to entertainment to banking. The same is true for businesses, which use the Internet to connect with customers, partners and suppliers. The Internet provides a convenient way to complete transactions, communicate and share information, but with convenience, come risks. As life becomes increasingly digitized, information about identities, transactions, social interactions, medical records and so much more is accessible over the Internet. Because information vital to a business is often vulnerable, there is a huge opportunity for cybercriminals to steal or control it in order to make or extort money.

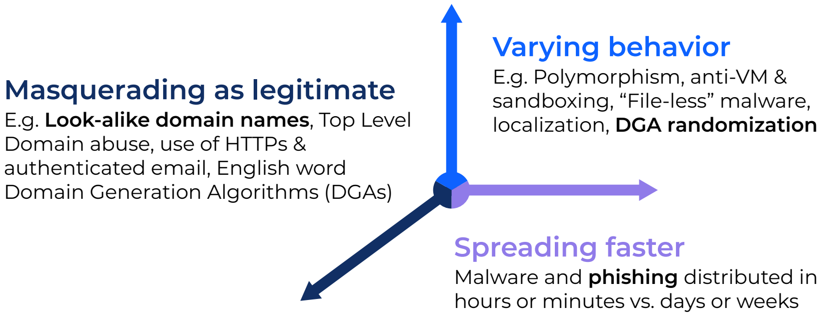
Global cybercrime costs are expected to grow by 15 percent per year over the next five years, reaching $10.5 trillion USD annually by 2025, up from $3 trillion USD in 2015, according to Cybersecurity Ventures. Cybercriminals use different attack vectors such as phishing, maladvertising, supply chain attacks, open ports, or others to launch various cyber attacks (e.g., ransomware, spyware, formjacking, cryptojacking, and clickjacking). A cyber attack can cause serious financial and reputational damage, as was the case with the SolarWinds breach in late 2020. Further, the impact of a breach can be wide spread, as was the case with the Colonial Pipeline ransomware attack in May 2021 which created gas station lines harkening back to the 1970s.

Costs are expected to grow by 15 percent per year over the next five years, reaching $10.5 trillion USD annually by 2025.

To protect against these attacks, many large businesses and organizations have implemented various security solutions (e.g., Antivirus, Firewalls, VPN, Secure Web Gateways, Multifactor Authentication, etc.), embracing a defense-in-depth strategy. However, Small and Midsized Businesses (SMBs) may not have enough resources to adopt this approach. SMBs need an affordable foundational security solution that can act as a primary line of defense or an added layer of protection against cyber threats. Comcast Business can help address this need with Business Internet service coupled with Comcast Business SecurityEdge™.

Using scale as a weapon

Internet traffic has reached staggering proportions. Cisco estimates it at a whopping 236 Exabytes per month, more than triple the volume in 2016. More than 5 billion webpages are now live. Hackers are well aware of these massive numbers, so they leverage the Internet's scale along with various evasive tricks for attack campaigns. To avoid detection, they often resort to techniques such as these:



Masquerading as legitimate
E.g. **Look-alike domain names**, Top Level Domain abuse, use of HTTPs & authenticated email, English word Domain Generation Algorithms (DGAs)

Varying behavior
E.g. Polymorphism, anti-VM & sandboxing, "File-less" malware, localization, **DGA randomization**

Spreading faster
Malware and **phishing** distributed in hours or minutes vs. days or weeks

No single solution can defend against these attacks. That's why SMBs should consider a defense-in-depth strategy — using multiple layers of security that are complementary to each other, improving overall protection.

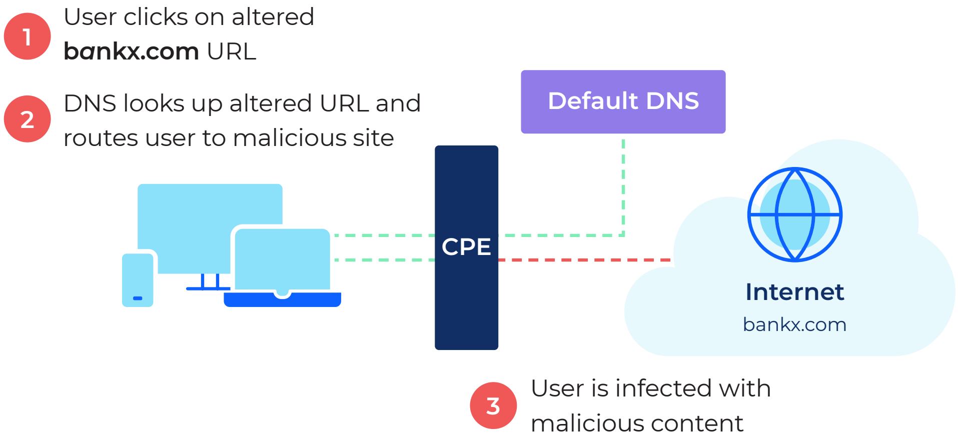
Internet traffic has reached staggering proportions. Cisco estimates it at a whopping 236 Exabytes per month, more than triple the volume in 2016.

DNS-based attacks

Attackers employ various DNS-based methods to either break into networks or exfiltrate information using some of these types of examples:

- DNS squatting (C**0**mcast[dot]com)
- DNS shadowing (**badstuff**[dot]website[dot]com),
- Malicious URL/query (**password$username$service**[dot]site[dot]com)
- URL shorteners (bitly[dot]com/23adf)
- Subdomain services (mybadpage[dot]webhost[dot]com)

In the diagram below, we see an example of how attackers get users to access malicious pages using DNS Squatting. The character "a" in bankx.com is encoded as 0x0430 (from the Cyrillic character set) instead of 0x061 (from English character set), which is almost visually impossible to distinguish.



1 User clicks on altered **bankx.com** URL

2 DNS looks up altered URL and routes user to malicious site

3 User is infected with malicious content

Can you tell the difference?

Cyrillic Small Letter A

Unicode number:	U+0430
HTML-code:	&#1072;

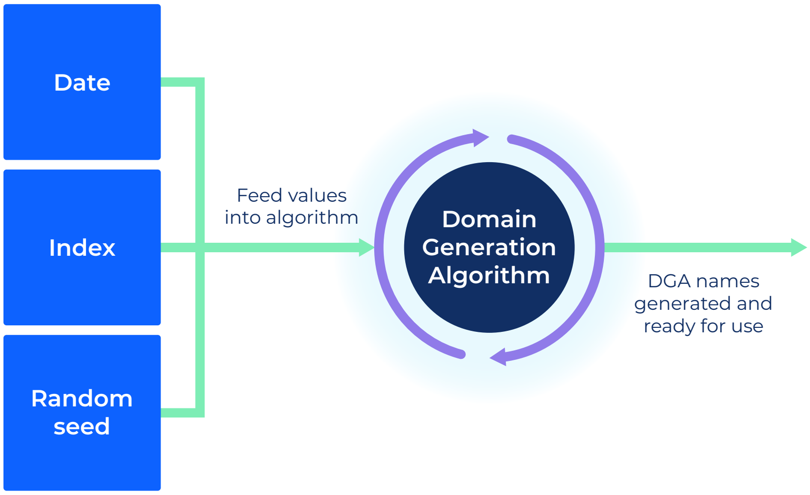
https://unicode-table.com/en/blocks/cryllic/

Latin Small Letter A

Unicode number:	U+0061
HTML-code:	&#97;

https://unicode-table.com/en/blocks/basic-latin/

To avoid detection, attackers use different techniques such as Domain Generation Algorithm (DGAs) as illustrated below, and fast fluxing. Even though cybersecurity experts know that bots use DGAs, it's hard to detect compromised domains because they use random seed values such as currency conversion rates and popular Twitter hashtags to create new domains.


Date
Index
Random seed
Feed values into algorithm
Domain Generation Algorithm
DGA names generated and ready for use

These techniques are effective and used widely, and for good reason: DNS, along with IP addresses, is a fundamental protocol that all applications and devices use for Internet services. DNS traffic often is unfiltered and unprotected. Research by Palo Alto Networks shows that **80% of malware** uses DNS for initiating Command and Control (C&C) attacks to steal information and spread infection.

Protecting Internet connections

Comcast Business offers SMBs fast, reliable Internet access via gateway and routers. Also available are add-on offerings including Static IP services for hosting servers, WiFi hotspots, and automatic 4G LTE Internet backup connectivity.

Comcast Business Internet gateways support four distinct and logically segmented local area networks: **Private Wired LAN**, **Private Wired LAN with Static IPs**, **Private WiFi**, and **Public WiFi**. Our Internet gateways also have firewalls that let administrators decide what traffic to allow in and out of their environments, helping to form a key security protection layer. Businesses can choose to block certain traffic types like ICMP, P2P applications (e.g., Kazaa, Gnutella and Vuze) and others. Businesses also have the option of disabling their firewall to avoid blocking intentional traffic between servers hosted behind the gateway.

Furthermore, the Comcast Business gateway gives businesses the flexibility to manage inbound access to their LAN resources by allowing them to configure port forwarding, port triggering, Static IP port blocking, and DMZ rules.

The following table details the options available for various firewall security levels and what traffic is permitted or blocked for those security levels.

IPv4 firewall options

- Option to Disable Firewall for True Static IP Subnet Only (Enabled by default)
- Option to Disable Ping on WAN interface

IPv4 firewall level	Blocked traffic	Allowed traffic
Maximum setting	• All unrelated WAN to LAN traffic	Following LAN to WAN traffic: • HTTP and HTTPS (TCP port 80,443), • DNS (TCP/UDP port 53), • NTP (TCP port 119, 123), email (TCP port 25, 110, 143, 465, 587, 993, 995), • VPN (GRE, UDP 500, TCP 1723), • iTunes (TCP port 3689).
Medium setting	• IDENT (port 113) • ICMP request • All the popular P2P applications like - kazaa - (TCP/UDP port 1214) - bittorrent - (TCP port 6881-6999 & some random ports used by bittorrent) - gnutella- (TCP/UDP port 6346) - vuze - (TCP port 49152-65534)	• All LAN to WAN traffic
Minimum setting (default)	• IDENT (port 113)	• All LAN to WAN traffic
Custom setting	Customer has options to block one or more of the following WAN to LAN traffic types: • HTTP (TCP port 80, 443) • ICMP • Multicast • Peer-to-peer applications • IDENT (port 113)	• All LAN to WAN traffic • All WAN to LAN traffic (optional)

IPV6 firewall options

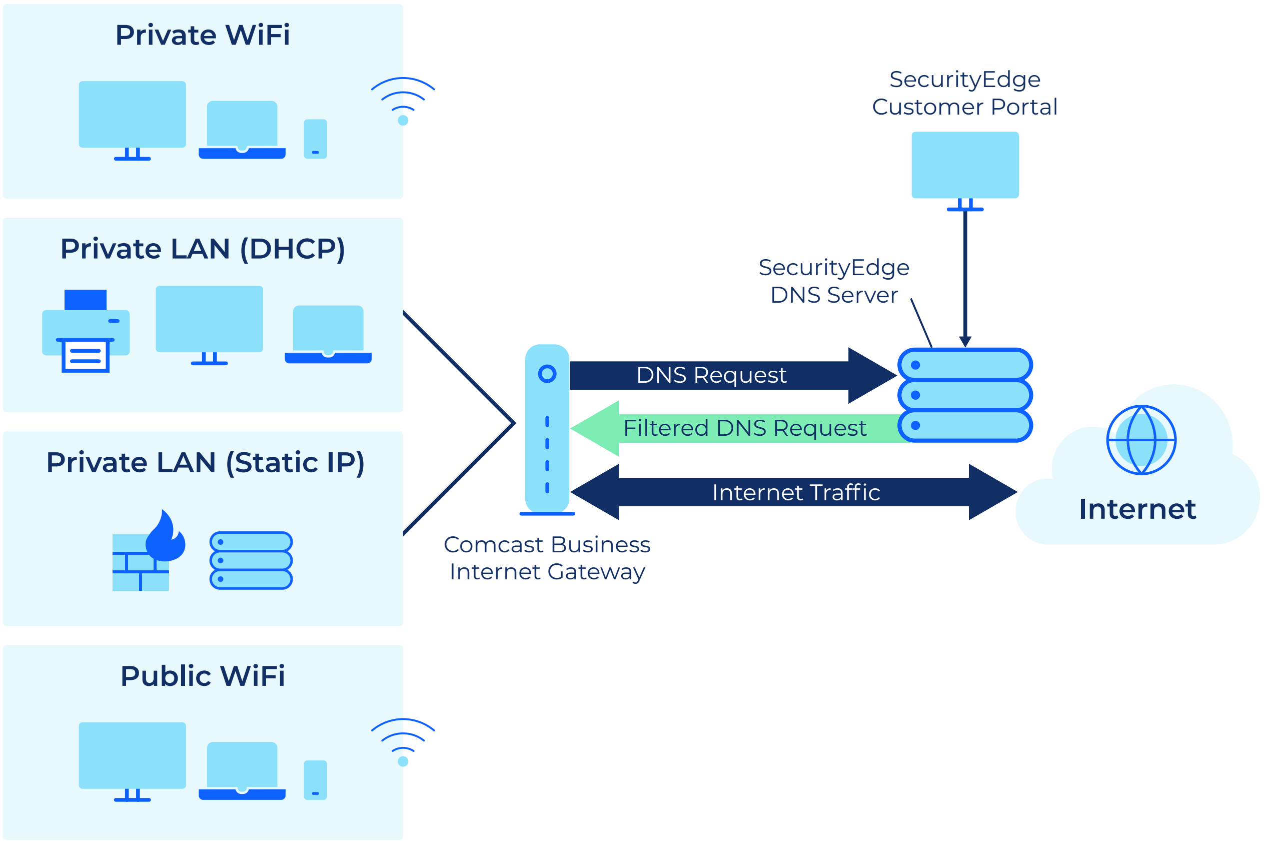
- Option to Disable Ping on WAN interface

IPv6 firewall level	Blocked traffic	Allowed traffic
Typical security (default)	• All unrelated WAN to LAN traffic	• All LAN to WAN traffic
Custom setting	Customer has options to block one or more of the following WAN to LAN traffic types: • HTTP (TCP port 80, 443) • ICMP • Multicast • Peer-to-peer applications • IDENT (port 113)	• All LAN to WAN traffic • All WAN to LAN traffic (optional)

For enhanced security, businesses can add **Comcast Business SecurityEdge**, which helps protect all connected devices against threats such as malware, ransomware, phishing and botnets with advanced global threat intelligence that is updated every 10 minutes. SecurityEdge is cloud-based and doesn't require additional hardware other than a Comcast Business supplied internet gateway, and is easily managed through a customer portal.

Business Internet with SecurityEdge

All IPV4 and IPv6 connected clients are protected by SecurityEdge except those connected through public WiFi.

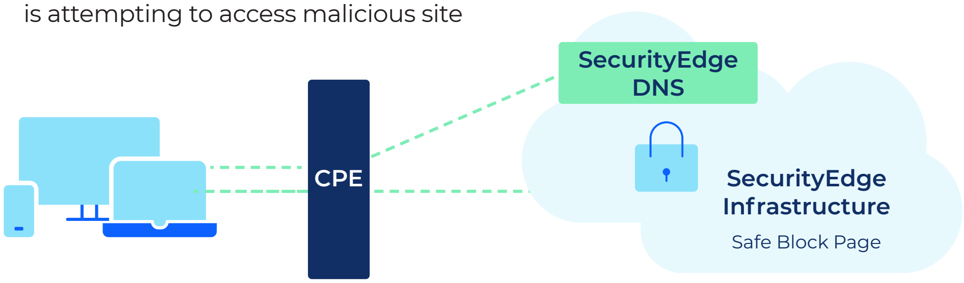


How SecurityEdge works

SecurityEdge helps block connected devices from accessing malicious web content and can be used with other solutions, such as anti-virus, DDoS protection and firewalls. SecurityEdge monitors DNS traffic and directs users to a safe destination as shown in the illustration below.

1 User clicks on altered URL for **bankx.com**

2 SecurityEdge DNS determines that user is attempting to access malicious site



3 User is redirected to a safe block page

Threat intelligence powered by Akamai

A key component of SecurityEdge threat intelligence is live-streamed anonymized data collected from DNS resolvers that use a specially built cloud infrastructure. A global network aggregates and transports more than 4 terabytes of this data daily, representing more than 100 billion DNS queries. The threat intelligence tool also aggregates third-party threat research from more than 30 sources and incorporates security insights gathered from a massive intelligent edge network.

A team of experts, including cybersecurity professionals and data scientists, manages the intelligence-gathering process, which also employs machine learning (ML) algorithms to quickly identify anomalies. ML techniques include:

- Anomaly detection to identify unusual patterns in raw data that warrant further investigation
- Domain ranking that generates metrics on the relative importance of web and "infrastructure" domains
- Domain reputation analysis of up to 90 different attributes to assess maliciousness, such as:
  - IP addresses hosting resources referenced by a domain
  - Nameservers used by the name
  - Canonical names (CNAMES)
  - Traffic patterns observed by IP addresses querying for domains (initiated by an exploit on a device)

> A global network aggregates and transports more than 4 terabytes of live-streamed anonymized data daily, representing more than 100 billion DNS queries.

ML algorithms that process live-streamed DNS query traffic can uncover patterns with subtle variations in exploits that traditional forensics techniques often miss. ML increases pattern identification by up to 10 times compared to humans and uncovers new threat activity, such as botnets.

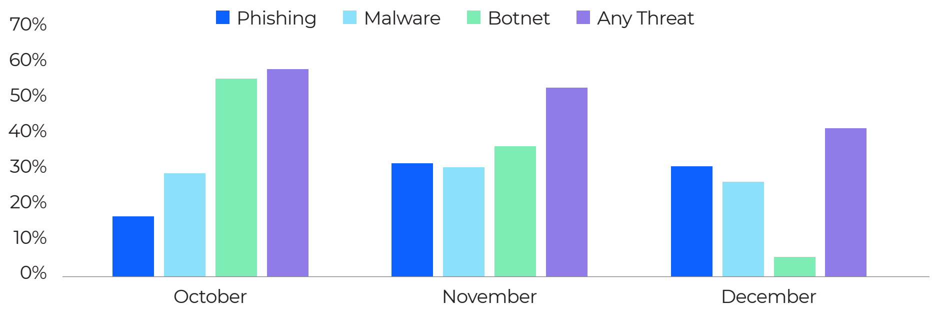
Minimizing delays

Because ML processing of live-streamed data is automated, it minimizes delays between threat activation and detection. Algorithms can identify activity by bot Domain Generation Algorithms (DGAs) within seconds. Most other malicious activity can be identified and validated within minutes after rigorous analysis to prevent false positives.

Dynamic threat intelligence feeds can be updated every few minutes. In the near future, it will be possible to live stream newly generated threat intelligence. To reduce false positives, up to 90 different metrics are assessed to evaluate threats, and reputation scores are tracked over time to spot trends for future analysis.

SecurityEdge data shows that it is working. As shown in the chart below, SecurityEdge protected an average 50% of subscribers from at least one attack.

SecurityEdge Customers Protected (Q4'21)



Conclusion

As businesses become more dependent on the Internet, the risk of a cyber attack can be more likely. To help protect themselves, SMBs need a simple, yet effective security solution as their primary line of defense, or an added layer of protection. That is what Comcast Business delivers with Business Internet Services and SecurityEdge. Comcast Business security solutions are affordable and can provide greater peace of mind for businesses.

Additional information

Network configurations not supported with SecurityEdge:

- **Customer-owned modem:** The service requires a Comcast-issued modem and cannot be enabled over customer-owned modems.
- **Comcast modem in bridge mode:** The service cannot be provisioned if the bridge mode (advanced or basic) is enabled on a Comcast modem.
- **Proxy:** With an external proxy in use, SecurityEdge is not supported unless it is blocked under the "anonymizer" category.
- **Public Hotspots:** SecurityEdge service is not available for clients connected to Xfinity WiFi hotspots.
- **Outbound VPN traffic:** If Internet access is provided through an external server using a VPN tunnel, SecurityEdge service rules may not be enforced if DNS traffic is also routed through the VPN tunnel. In addition, SecurityEdge cannot monitor DNS traffic going to an external DNS server either on HTTPs or TLS tunnels.

SecurityEdge Overview Video:
https://comcast.showpad.com/share/7qubJ2rOx3nRVbqW4jQl1

How to manage SecurityEdge settings:
https://business.comcast.com/help-and-support/internet/securityedge-manage-settings/

References:

https://cybersecurityventures.com/cybersecurity-almanac-2022/

https://www.cisco.com/c/dam/m/en_us/solutions/service-provider/vni-forecast-highlights/pdf/Global_2021_Forecast_Highlights.pdf

https://www.csoonline.com/article/3601508/solarwinds-supply-chain-attack-explained-why-organizations-were-not-prepared.html

https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password

https://www.worldwidewebsize.com/

https://en.wikipedia.org/wiki/Domain_generation_algorithm https://en.wikipedia.org/wiki/Fast_flux

https://www.paloaltonetworks.com/resources/whitepapers/stop-attackers-from-using-dns-against-you

CB-SecurityEdge-Overview-Whitepaper-D_WHT91527_3.22

COMCAST
BUSINESS
SecurityEdge™