The trademarks, including but not limited to “Network Box” and the curly “N” device, are either trademarks or registered trademarks of Network Box Corporation Limited. Other trademarks and product names used in this publication are for identification purposes only, and may be the trademarks of their respective companies. Features and specifications are subject to change without notice. Benchmarking is performed with representative data, on a function by function basis. Weights and measurements are approximate only. Actual models may vary in appearance to the illustration and photographs provided.

Copyright © Network Box Corporation Limited 2019.
As a special end-of-year review, Network Box has compiled the key In the Boxing Ring technology news, features, and articles from 2019.

To read all available editions of In the Boxing Ring, please use the link provided below:
https://www.network-box.com/newsletter-detail
In this article we will be looking at the architecture for Network Box security services in 2019 and beyond. We’ll be looking at two areas: customer “premises” (either physical or virtual), and the Network Box Services cloud.

Customer “Premises”
Customer premises can be either physical locations (offices, data centres, homes, etc), or virtual environments (such as local vmware clouds, or public clouds like Amazon, or Azure). Inside these premises are the protected assets - the devices and computers holding the data to be protected.

Mobile devices introduce another layer of complexity to data protection. In general, Network Box recommends that mobile devices outside the customer premises be always protected, using VPN and proxy technology coupled with strong policy control.

Unprotected mobile devices should be treated in the same way as visitors to your network - with extreme caution and care.

A Network Box device can only protect traffic that passes through it, and that has traditionally meant Network Box protection was placed at the gateway to the Internet (where visibility of the malicious traffic, and threat, was the greatest). However, with the proliferation of network links (such as VOIP, MPLS, VPNs, etc), we are seeing increasing demand for Network Box devices to be placed inside the customer network to fulfill IDS or IPS roles. We are also deploying Network Box systems internally as firewall and IPS devices; performing a network segmentation role.

Whether the Network Box device is a physical or virtual appliance, deployed at the perimeter or inside the network, is irrelevant to us; it is merely the Service Delivery Platform - the means by which we deliver our protection services.

Then we have the customer devices producing event information; routers, switches, servers, high value workstations, and other (not Network Box) security appliances. Starting in 2019, our Network Box SIEM+ product can take event logs from these devices, and securely upload them to the cloud for event correlation, searching, and archiving.
Network Box Services Cloud

Since its launch, Network Box has provided security services based on regional SOCs managing Network Box appliances installed in customer premises. We have provided remote configuration synchronization, patented signature PUSH, global monitoring, and support services.

Still today, the vast majority of our customers’ protected data is in customer premises (either physical or virtual), and Network Box appliances placed within those premises provides the best possible protection. However, we recognize that an increasing amount of data is being moved into public clouds. In recent years, we have extended our support to provide a number of cloud services (such as cloud mail backup, cloud DNS backup, and cloud reputation). We will continue to extend the cloud services we offer, as well as provide tight integration with other cloud service provider partners. Our role is to protect the data, no matter where it is stored or what networks it transits through; and the services we provide will continue to be designed to meet the demands of that role.

Over the past years, Network Box has invested heavily in the development of a multi-tenant cloud framework to serve as the backbone for our future. Existing cloud services are being migrated into this new framework, and new services developed. This new framework is based on cloud level big data storage, horizontally scalable to billions of correlated indexed event records. Only by leveraging such cloud storage technology can we address the issues of correlating not just one customer’s individual Network Box events, but across all Network Boxes and all other security devices that each customer has. We can also scale up to further correlate events across customer industries, and even globally.

The potential of such technology to solve today’s security issues is impressive. Given a particular threat indicator, we can instantly know not just the history on one particular Network Box device, but can now correlate that threat across all devices belonging to that customer, comparing against other customers in the same industry, as well as globally. Using both machine learning and human security engineers in our Security Operation Centres, we are tackling the task of identifying the ‘needle’ of security incidents inside the ‘haystack’ that is millions of security events every second.

As Box Office migrates to become a component of NBSIEM+, fulfilling the asset tracking and support ticketing functions, we are directly connecting managed Network Box 5 devices to this system to allow for:

1. Synchronization of configuration sections across clusters of Network Box systems
2. Updating of configurations
3. Consolidated reporting

A single authorized change made to a configuration in NBSIEM+ can instantly be replicated across a global cluster of devices.

By consolidating our SOC support systems and tightly integrating the remote Network Box devices themselves to our cloud based systems, we are moving to an architecture where it does not matter where the device is located, whether it is physical or virtual, whether it is an individual device or a multi-tenant cloud service, or even the manufacture of the device. Using NBSIEM+, our regional data centres, and our cloud infrastructure, we aim to seamlessly correlate event logs and security intelligence on a global basis; moving from single device events, to focus on incidents with global search capability.
The Dark Web is the deliberately hidden part of the Internet, which is the natural habitat of hackers and cyber criminals. This ‘dark side’ of the Internet, can only be accessed with specialist knowledge, and specific software tools. Perhaps the most famous such tool is TOR (The Onion Router). Other examples include Riffle, Freenet, and I2P (Invisible Internet Project).

Whenever there is a massive data breach, that personal data usually ends up on the Dark Web. There are currently over 6.5 billion sets of hacked credentials already posted on the Dark Web, and the number is growing fast.

In most cases, the companies and organizations who suffered these breaches, clearly didn’t do enough to secure themselves from cyber-criminals.

Far from leveraging critical cyber-security systems and services to protect their client data effectively, many firms’ customer data was compromised, because databases were put online without having had security patches applied for up to a year, or in some cases, because databases were put online without even basic password protection.

We are talking about certain banks and credit card companies, making millions of their customers’ private data available online, with literally no security at all.

Many managers wring their hands and say, ‘it’s impossible to protect our networks from EVERY kind of attack,’ but in reality, there are far too many cases, where networks are not properly protected from ANY kind of attack.
So how does all this impact you?

**First,** there is the loss of privacy. If your doctor, bank, credit card company, travel agency, hotel, children’s school, lawyer, accountant, or a government department, leaks your private data onto the Dark Web, then your data is out there forever. Everything from how much money you have, to your children’s identities, to your medical condition, to your travel itinerary, to your photos and videos, to your physical location, maybe compromised.

**Second,** there is the potential for direct access to critical accounts, especially if you have reused passwords. It maybe that your bank, credit card company, or your workplace, has been hacked. In such a case, a hacker could just login to your accounts, and directly take advantage. This is why dual factor authentication, is so important. It is also possible, if you have reused passwords, that a hacker can try a password they took from a third-party data breach, on your bank or workplace. This is why reusing the same password on multiple accounts, is a very bad idea.

Third, are ‘hoaxes.’ Although that actually might not be the right word, to describe what criminals are actually doing. After all, a criminal may say they have hacked your webcam, when they haven't, making the claim a ‘hoax,’ but on the other hand the blackmail being carried out is very ‘real.’

There have now been millions of emails sent out to people, claiming that a hacker has captured them on video, while they were browsing an Adult Website, using their hacked webcam. These evolved into physical bomb threats as well.

The connection to the Dark Web is both the email address to send the blackmail to, and also, and this is the key, the person’s actual password, which will often scare the potential victim into thinking everything else written, must be ‘real’ too.

Given the number of panic calls for help, which Network Box has received over the last few months, we have rapidly developed, and will be offering, an optional Dark Web Monitoring Service very soon. This is so that our clients can receive continual automated updates, highlighting which of their organization’s people, have hacked sets of credentials, posted on the Dark Web.

This will allow IT Departments to educate their users, so they can further appreciate the importance of cyber-security, and help to defend their devices, networks, and data, even more comprehensively. Additional Cyber-Threat Intelligence, and Cloud Reputation monitoring, will also be part of this new Dark Web Monitoring Service.
The previous DNS was unnecessarily slow and inefficient because of efforts to accommodate a few DNS systems that are not in compliance with DNS standards established two decades ago.

To ensure further sustainability of the system it was time to end these accommodations and remediate the non-compliant systems. This change will make most DNS operations slightly more efficient, and also allow operators to deploy new functionality, including new mechanisms to protect against DDoS attacks.

Major DNS software and service providers have agreed to coordinate removing accommodations for non-compliant DNS implementations from their software or services, on February 1st 2019. This change affects only sites operating non-compliant software.

All Network Box systems are now, up-to-date with this switchover. In particular, the Network Box NBRs-3 and Network Box 5 resolver and caching DNS servers, as well as our Cloud DNS servers. However, external DNS servers themselves (either on customer premises or in the cloud) may not have made the change. In particular, TCP port 53 should be opened to DNS servers, and those servers correctly configured to prevent unauthorised zone transfers.

If you have not yet made the transition, you can test the readiness of your domain(s) with the link below:

https://dnsflagday.net/

Enter your domain name into the test box provided, click Test! and view the results.

If you need assistance with firewall policy (for DMZ hosted DNS servers), please contact your regional SOC for support.
Network Box is excited to announce our new S-80i Small Office / Home Office UTM+ (Unified Threat Management Plus) model.

Built on a 64-bit Intel processor, this model is equipped with 8GB RAM and a 256GB SSD storage drive. It offers six independent high speed 1Gbps ethernet ports (which can be configured either as individual ports or a bridged switch arrangement).

Utilizing a passive cooling system, as with our other S-series and 5Q models, no cooling fans are needed as the entire top of the unit is a heat sink. This results in a dust resistant environment, that is completely silent in operation, with no moving parts. The S-80i runs the latest multi-award winning Network Box managed cybersecurity version 5.5 software platform, to offer superior functionality, optimized performance, and enhanced reporting capabilities.

The Network Box S-80i model is available right now, and can be used to protect small offices, home offices, retail outlets, restaurants, logistics operations, and other smaller sites, which require either Unified Threat Management Plus, and/or Virtual Private Network protection.

### Technical Specifications

<table>
<thead>
<tr>
<th>Processor</th>
<th>64bit, 3.10GHz, 2 physical cores</th>
</tr>
</thead>
<tbody>
<tr>
<td>RAM</td>
<td>8GB, 2133MHz DDR4</td>
</tr>
<tr>
<td>Storage</td>
<td>1 x 256GB mSATA SSD Industrial Grade</td>
</tr>
<tr>
<td>Networking</td>
<td>6 x 1Gb RJ45</td>
</tr>
<tr>
<td>Power Supply</td>
<td>60w (external)</td>
</tr>
<tr>
<td>Chassis</td>
<td>Desktop SFF Fanless</td>
</tr>
<tr>
<td>I/O Interface</td>
<td>1 x reset button</td>
</tr>
<tr>
<td></td>
<td>1 x RJ45 Management Console</td>
</tr>
<tr>
<td></td>
<td>2 x USB 3.0</td>
</tr>
<tr>
<td>Physical Dimensions</td>
<td>155mm(w) x 52.5mm(h) x 126.5mm(d)</td>
</tr>
<tr>
<td>Weight</td>
<td>1.6kg</td>
</tr>
<tr>
<td>Approvals/Compliance</td>
<td>CE Class B, RoHS,</td>
</tr>
<tr>
<td></td>
<td>FCC Class B</td>
</tr>
</tbody>
</table>
Several security frameworks (including, but not limited to, PCI) have a requirement for password policy enforcement.

Network Box has always supported password policies when we use external authentication to servers enforcing password policies. However, we are now moving towards implementing these policies as an option in our direct authentication frameworks.

Network Box Standardized Password Policies

The issue with password policies is that there are so many of them, they are implemented in many different ways, and different security frameworks require different policies. To address this, Network Box has developed an extensible standardized password policy framework to be used in our offerings.

Password policies are sets of rules to enforce the use of strong passwords, and require them to be regularly changed. Used properly, they can greatly enhance the security of an organization’s computer system.
Today, this framework has support for the following policy types:

**User policies:**
- Dual Factor (where dual factor logins are required, optional, or disallowed)
- User Password Change (can users change their own password)
- User Password Reset (can users reset their own password via email)

**Password quality policies:**
- Password quality check (selection from standard modules)
  - **Digits:** Password must contain one or more digits
  - **MixedCase:** Password must contain mixed case letters
  - **Symbols:** Password must contain one or more special symbol
  - **NotUser:** Password must not be the same as the user identification
- Password minimum length requirement

**Password expiration policies:**
- Number of days since last change, after which password will expire
- Number of days, before expiration, that we should warn the user
- Number of days grace period, after expiration, that we should still allow user to login (with warning displayed)
- Number of previous passwords stored to protect against re-use

**Password lockout policies:**
- Number of failed password attempts before account is ‘soft’ locked
- Automatic unlock grace period (in minutes) for ‘soft’ locks
- Maximum number of failed password attempts before account is ‘hard’ locked

**Session policies:**
- Number of minutes after which idle sessions are automatically logged out
- Number of minutes grace period, after expiration, that we should warn user but still allow session to be recovered on activity

As well as completely custom policies (based on the previous criterion), standard password policies (such as PCI-DSS v.3.2 minimum) will be maintained by Network Box.

**Box Office**
The first implementation of this password policy framework is in the Box Office systems.

Organizations can apply policies at the owner level, such that all users belonging to that owner have the password policy enforced. Both standard and custom (per owner) password policies are supported.

Additionally, the upcoming NBSIEM+ will also implement this policy framework.

**Admin Web Portal**
We expect to be able to offer these password policies in our Network Box 5 Admin Web Portal product within 2019.

Love them, or hate them, password policies are a requirement of several security frameworks, and are here to stay. Network Box’s approach to this is to implement support for password policies, then give our customers the option as to which policies to require for their users.
The Network Box approach has always been different. Since our launch 20 years ago, we have always deployed industry leading scanning engines, with the full capabilities of their desktop / server brethren. We have always deployed full sets of signatures covering both modern and ancient malware and threats. And we have always used multiple overlapping protection engines, to increase both the depth and breadth of protection capability.

Network Box UTM+ devices today contain 79 classification and policy enforcement engines, utilizing more than 63 million signatures. These numbers grow every day and are expected to pass 64 million signatures within the next few months. Given that those numbers are many multiples higher than most of our competitors', we can see that this approach is different, but why is it necessary?

The origin of the cursory scan

Back in the early days of UTM+, it was commonplace for devices to use just a few thousand signatures to scan traffic for recent threats. The CPUs were just not powerful enough to do full anti-malware scanning even for one PC, let alone at the gateway protecting hundreds/thousands of devices. Some vendors tried to do the scanning in custom silicon hardware, which offered improved performance, but at the expense of the number of signatures that could be supported (aka loaded into RAM).

OEM partners introduced scanning engines with fancy marketing names, but all were limited cut-down versions of their full desktop/server scanning products, intended to be used in low-end gateway devices performing just a ‘cursory scan’ of the data streams.

Even nowadays, this limited technology persists. Take the lids off most gateway perimeter protection devices and you will see low-end/embedded CPUs with just 1GB or 2GB of RAM and small solid-state disks.

Over the past two decades, this approach has been proven time and again to be the correct one. We have the highest customer retention rates in the industry simply because of the quality of our protection.

How do we do this, when the competition can’t? The answer is to think inside the box. All Network Box appliances (real/virtual, small/large) run exactly the same full suite of protection firmware. Even the lowest end small branch office VPN appliance has a multi-core 64-bit Intel processor with 4GB of RAM, and most of our appliances have 8GB or more. Hardware is just a small portion of the total long-term ownership cost, and it is our approach to use the best. The cost of cleaning up a ransomware outbreak, by comparison, is often much greater.

The 80/20 rule

Back when we started Network Box, the CSI/FBI conducted annual Internet Cyber Crime surveys, and produced annual reports (they still continue this practice today). Every year, those reports highlight two simple facts:

1. 80% of cyber security problems are because protection was not in place.
2. The remaining 20% of problems are because the protection was not maintained or installed properly.

Network Box addresses this first 80% by including the most effective threat protection technology covering everything from basic firewall, though Intrusion Protection, up to Anti-Malware, Anti-Spam, and beyond; in every single Network Box appliance. Sometimes we work alongside other equipment, and other times we supplement with additional protection, but we always recommend deployment of protection in both depth and breadth.

We address the last 20% with our Managed Security Services. By employing our own dedicated security professionals providing local support in Security Operation Centres around the world, we ensure that each and every Network Box appliance is configured and maintained to the highest standards.

That is the Network Box approach.
We all have to use email for work, and the most annoying thing about email, is without question, SPAM.

Even though Network Box currently blocks 95 to 98% of Spam right out-of-the-box, before any kind of machine learning, fine tuning, or customization is implemented; we all still have to deal with the Spam that gets through. Currently, we are seeing a 99.28%* success rate on our Spam Traps.

There are three main reasons it is essentially impossible to automatically block all Spam:

First, is that as automated systems get nearer and nearer to blocking 100% of Spam, the risk of accidently blocking a genuine email, exponentially increases too. Logic dictates that as more and more of the ‘obvious’ Spam is blocked, what is left is increasingly less obvious. Network Box aims to block less than one genuine email, in every ten thousand emails received.

Second, is that what different people, even people in the same job function, working at the same organization, regard as Spam will often differ, within that last remaining percentage of potential Spams. Indeed, it is even possible for the SAME PERSON, to regard the SAME EMAIL, as Spam, or a legitimate email, depending on the exact circumstance. For example, a person was looking to buy a house, then actually buys a house, suddenly rendering a previously useful property newsletter ‘Spam.’

* for real-time statistics, please visit: http://response.network-box.com/services
Third, Spam evolves. The people sending Spam, take great care to improve and refine, both how their Spam is sent, and what that Spam contains. If none of their Spam can get through to potential clients, that would be the end of their commercial operations. People that send Spam, are therefore highly incentivised to adapt their emails, so that they can bypass Anti-Spam systems.

So if you are a Network Box client, where does that leave you, on the email front-line against Spam?

Well, the most important, and most powerful thing you can do, is report any Spam that manages to arrive in your inbox, to us at Network Box. There is a special email account (spam@network-box.com) which you can send Spam to, and once you do, our automated systems and duty engineers, will create a signature to handle it, and PUSH update your physical, virtual, or cloud, Network Box system.

However, there is one caveat; producing an effective Anti-Spam signature requires that the original email envelope is included. Just like Sherlock Holmes needing to discern clues from both the contents of a letter, and the envelope the letter came in*, Network Box needs to examine both an email’s contents, and that email’s envelope headers.

Unfortunately, this means that just ‘forwarding’ a Spam isn’t enough, you have to ensure its email envelope is preserved for forensic examination.

In Microsoft Outlook, that means either having to take care to select, ‘Forward as an Attachment,’ or opening a Blank Email, then dragging and dropping the Spam into it.

In either case, you would still have to take the time to address the email, click send, deal with several potential additional steps, such as the email not sending due to it having no Subject, or it having spelling mistakes; then finally even when it has been sent, the last additional step of deleting the email from Outlook.

We now have a much better solution, the Network Box Spam Reporter for Outlook. It is completely free for Network Box clients. Just download it. Install it. Then use it to painlessly eliminate that last one percent of Spam from your Outlook Inbox.

To use it, you highlight a Spam, then click the Network Box Report Spam button. It is as simple as that. The Spam is then automatically sent to Network Box to be handled, deleted from your Outlook email account, and Network Box will send you a quick real-time report to tell you the Spam is being handled.


Network Box Spam Reporter Installation Guide

1. Download the App using the link below
   LINK: http://download.network-box.com/tools/SpamReporter.zip

2. Extract the downloaded zip file and open the folder:
   Network_Box-Spam_Reporter

3. Double click setup.exe and click Install from the pop-up window. Once installation is complete, restart Outlook.

4. Upon first opening of Outlook after installation, you will be prompted with further instructions in a pop-up window, click OK to proceed.

5. Click on the Network Box Spam Tools tab at the top, and click Settings.

   ■ In the new window, use the pull down menu to select your email address from Select default email.
   ■ Click the check box if you would like to have the Report Spam button in your ribbon.

---

The ongoing issue of access to Administrative Systems over the public Internet has again been highlighted by the recent announcement of CVE-2019-0708 (a remote code execution vulnerability in Microsoft Remote Desktop Services).

Even with strong authentication enabled, permitting direct access to Administrative Systems from the public Internet is a very bad idea.

I understand that it is helpful to have such remote access (particularly in times of emergency), but opening up those ports is simply too risky. You are reliant on your authentication system being perfect, reliant on your users never making mistakes, reliant on the software being perfect, and relying on credentials not having been leaked / discovered from other systems. You have to be perfect, 100% of the time, while the remote hacker only has to find that one mistake you (or one of your suppliers) made.

When we deploy Network Box devices at network perimeters, it is fairly common for us to find a request to open TCP/3389 and NAT forward it to an internal server. It is so very convenient for administrators to have remote access to screen sharing on that server.
That is why Network Box pushes back against requests to open TCP/3389, TCP/22, TCP/23 (yes, we still see these), and other common administrative ports. If you really want it, we will open it (as you the customer are in charge of policy), but we warn you of the possible consequences and suggest you alternative, more secure, ways of remaining secure (while still enjoying the convenience of remote access).

**How can Network Box securely provide remote administrative access?**

- So long as the traffic passes over the TCP protocol, we can permit access only via specific source IP addresses. With modern equipment, it is pretty hard to successfully spoof TCP/IP nowadays (especially over the public Internet).

- A VPN is the most common approach. It can be used to provide a second layer of authentication and encryption, through which administrative traffic can be tunneled. Open SSL VPNs can be configured with a fingerprint at the packet level, to further protect access.

- Using dual factor authentication can help, but will probably not be of much use in the case of exploit of a vulnerability (such as with CVE-2019-0708).

- Using non-standard ports is one approach that can help against mass scanning, but not against a determined hacker targeting your network. So long as your services can be fingerprinted, they can still be exploited (and even without fingerprint, brute force exploits are still a possibility).

**As a reminder, our recommendations for CVE-2019-0708 are:**

- If you have RDS ports (by default tcp/3389) open to the Internet, we recommend that you immediately close those down.

- If you have RDS ports open to the LAN/DMZ, for administrative purposes, we recommend that you immediately close those down as well.

- We recommend that you either close the ports entirely, or restrict access to specifically identified administrative source IP addresses or VPN connections.
  - If you have no requirement for RDS services, you should disable them completely on your servers.
  - Network Box can assist with this, and we will be contacting customers we have identified to have tcp/3389 open to the Internet directly.
  - Microsoft has released patches for this, and these should be applied as a matter of urgency.

For those of you subject to PCI compliance, the above controls should already have been applied as part of your network segmentation exercise.

Should you have any questions, please don’t hesitate to contact your local Network Box Security Operation Centre for assistance.
The Dark Web is the deliberately hidden part of the Internet, which is the natural habitat of hackers and cyber criminals. This ‘dark side’, can only be accessed with specialist knowledge, and specific software tools such as TOR (The Onion Router), Riffle, Freenet, and I2P (Invisible Internet Project). Whenever there is a data breach, the stolen personal data usually ends up on the Dark Web. There are currently over 6.5 billion sets of hacked credentials already posted on the Dark Web, and the number is growing.

The Network Box Dark Web Monitoring Service scans data breaches from the Dark Web, looking for your registered email addresses and domains. The generated report shows the breach details. As a subscriptions service, monitoring is ongoing. As new data breaches are discovered, Network Box will re-scan and keep you informed as to changes since the last report.

When Network Box launched our Dark Web Monitoring Service, we concentrated on breaches leaking passwords (both hashed and plaintext/cracked), indexed by email address for both individuals as well as domain holders. However, most breaches contain much more personal data than just passwords, and we are increasingly seeing the threat of data correlation using index types other than email address, such as site usernames, IP addresses, identity numbers, etc.

Version 2 of the Network Box Dark Web Monitoring Service was launched in July 2019, and this article outlines the new features.
Data Leakage Attributes
The first major change introduced in v2 is that rather than merely storing breached passwords (hashed and plaintext/cracked), we now store many different types (attributes) of leaked data. This is dynamic, and we can add new attributes as we find them, but the list currently includes:

- General textual information
- Plaintext/cracked passwords
- Hashed passwords (either hash, or seed:hash format)
- Physical addresses
- US Social Security Numbers
- Credit card numbers
- First names
- Last names
- Unformatted names (format not known)
- Email addresses
- Last name, First names
- User IDs (number, usually internal)
- User identifiers (name, usually used for login)
- Country codes
- Genders
- IPv4 addresses
- IPv6 addresses
- Dates of birth
- URLs

As a result of this new arrangement of database storage, the formats of the dark web monitoring reports have changed; we now show this in a dynamic "attribute: count" format.

Data Leakage Indexes
We search the dark web for breached / leaked data, and can now index it in different ways. In addition to the v1 index on email address, for example we can now index on site usernames, IP addresses, identity numbers, and other such attributes. This allows us to now correlate data between breaches (in particular for those breaches that do not include email addresses).

Volume of Data
To give you some idea of volume, in the past month alone we’ve found 77 new breaches, adding close to half a terabyte of breached data to our existing database. Today we store data from 13,574 breaches, and that number continues to grow.

Providing End-Users Access to their Data
As a matter of policy and to protect the sensitivity and security of this data, Network Box does not provide breached personal data to anyone except for the authenticated and confirmed end-users at the breached email address, as well as authorized Network Box staff. IT managers, in particular, do not have access to this data.

We are now finalizing a facility to provide end-users direct access to their data. This will be a public website into which an end user email address is entered:

- If the email address, or its domain, is subscribed to the Dark Web Monitoring Service, a report will be emailed directly to the end user, detailing all the information on that user that we have found to be breached and leaked.
- Without a subscription, a short summary report will be emailed directly to the end user. This does not contain the breached information itself - merely an indication of the amount and type of breached data discovered.

Quite apart from the direct threats offered by breached leaked personal data, administrators can consider using this as an opportunity for end-user education concerning such phishing activity (and general Internet trust) - not just for these users, but also other high level and high risk staff. Users should be encouraged NOT to use their work email address for non-work related websites (it is estimated that about 30% of people reuse the passwords on multiple sites). It would be prudent to force a password reset on internal systems for breached accounts.
Quite often we are asked to explain the difference between the Network Box Managed Security Services, and our (mostly Do-It-Yourself) competitors. Perhaps the clearest demonstration is how close the relationship to our customers is; we are there to help resolve problems and diagnose networking issues, and not just some voice in a distant call centre. Our service renewal and customer loyalty rates are the highest in the industry, but what exactly is the difference? Why is Network Box security so effective?

When Network Box was formed, we looked at and addressed the fundamental statistics:

- 80% of organisations were hacked, exploited, or infected because they did not have adequate protection. They got a virus because they did not have anti-virus technology. They got an intrusion because they did not have Intrusion Prevention Systems. So we put all the core protection technologies in one single appliance device.

- The remaining 20% had problems because the protection they had was either not configured correctly, or not maintained. Virus signatures had stopped updating. Protection systems were not updated to address the latest threats. So, we launched the first managed security service to look after our own devices, expertly installing, configuring, and maintaining our devices protecting customer networks.

Since then, over the past 20 years we have amassed an enormous amount of intelligence. We have grown and learned. We have extended the protection capabilities of our devices, expanded the protection and policy engines, and improved the quality, quantity, and rate of protection signature and heuristics delivery; using our patented PUSH technology, but also embracing new cloud delivery mechanisms.
But what makes Network Box different?

In a word (or two): Security Response. We have developed Network Box Security Services into a feedback loop: joining Intelligence, Analysis, and Enforcement into a single holistic real-time framework, for the protection of customer networks.

**Intelligence**

At the heart of Network Box Security Response is a big data scale database called RepDB (Reputation Database). Here we store network indicators (IP addresses, email addresses, URLs, fingerprints, hashes, etc) and classify them. This forms a database of Intelligence information classifying and storing the history for hundreds of millions of network indicators. We update this database with feeds from partners, as well as global threat intelligence, spam traps, honeypots, and the dark web; in total more than a hundred different sources of information.

We also receive data feed flows from end-user devices under management, and these include things like statistics (how many times a particular signature fired, for example), events (a malware block, for example), and status.

All this information is fed into NBSIEM+, and made available to security engineers in our Security Operation Centres, as well as customer administrators.

**Analysis**

Threat indicators from RepDB then flow into our big data analysis engines to produce reputations, signatures, incidents, and alerts. Most of the work here is automated, using heuristics, AI machine learning, and other behavioral based systems. For example, one system we have is called OUTBREAK - it compares the last three minutes of activity on the Internet again the preceding 57 minutes, to track the behavior of individual threats and vectors.

In this way, a feedback loop is formed. Statistics and Events from the enforcement devices flow into Intelligence gathering engines where heuristics, AI, and Machine Learning systems produce Reputation scores, signatures, incidents, and alerts. These flow into the enforcement engines on customer devices to improve the categorization systems and enable effective policy enforcement. Feedback loop round trip times through all three systems (Intelligence, Analysis, and Enforcement) are typically of the order of less than a minute (and mere seconds in some cases).

All the above is overseen by the staff at Network Box Security Response, as well as local Security Operation Centres and customer administrators.
October was Cybersecurity Awareness Month. Originally established in collaboration between the U.S. Department of Homeland Security and the National Cyber Security Alliance in 2003, this annual event has successfully evolved to become an important reminder, of the critical nature of cybersecurity in an increasingly digital world.

During October, everyone can expect a deluge of sensible cybersecurity advice. Typical examples are for end-users, such as:

- Review the privacy settings on your social media accounts
- Ensure you don’t fall for email phishing scams
- Always backup your data to at least three different kinds of media, one of which should be offsite
- Keep your operating system and applications up-to-date
- Don’t click on a link, unless you are very confident where it’s from.

And so on.

As Network Box is a Managed Security Service Provider for organizations, however, let’s look at 5 key cybersecurity advice for IT Managers instead.
1. Update Your Systems In Real-time
Always make sure your cyber-security systems are as up-to-date as possible. That doesn't mean being up-to-date within a day or two, that means being up-to-date within SECONDS of updates being available. Network Box’s patented PUSH update technology, helps to ensure every online Network Box system in the world, is updated within 45 seconds of new patches or signatures being issued.

Augmenting PUSH is Network Box’s zero-day cloud, based anti-malware defence shield, Z-Scan. The award winning engine mitigates new threats within 3 seconds (on average) of being sampled in the cloud. Behavioural analysis, sandboxing technology, and other real-time testing of unknown threats is all very well, but there is nothing better than having the exact preventative signature in place BEFORE a zero-day threat arrives at your organization’s Internet gateway, which Z-Scan provides.

2. Lock Down Your Technology
Be very aware that many cybersecurity products and services include back-doors. An educated guess, leads one to conclude that such back-doors are inserted by governments; which means that when governments themselves get hacked, they lose the keys to these backdoors to cyber-criminals. If that sounds farfetched, know that one of the most successful ransomware attacks in history, WannaCry, was built on EternalBlue, a cyberattack exploit developed by the U.S. National Security Agency (NSA).

Network Box is extremely proud to be able to say, we have no secret backdoors in any of our products or systems. Always install cybersecurity without unauthorized backdoors, and ask potential vendors point-blank to guarantee they have never been found to have included a backdoor in any of their systems or services.

3. Monitor The Dark Web
Sign up for a Dark Web Monitoring service, so that you know, if and when, your End-Users have had their credentials compromised. This is critical, because on average 30% of people use the same password everywhere. That means a hacker may not even need to hack your system to get in; they can just search for your domain on the Dark Web, and try to use the names and passwords which they find there.

By monitoring the Dark Web, an IT Manager can stay one step ahead of leaked passwords, hoax blackmail attempts, and sophisticated Identity Theft. And in the unfortunate event their own network system actually gets hacked, Dark Web Monitoring could be the first reporting tool to discover the data breach. In many countries around the world, it is now a legal requirement to report data breaches.

4. Scan Encrypted Traffic
The majority of websites now use HTTPS (Hyper Text Transfer Protocol Secure), which is a secure protocol for communication between systems, such as a web browser and a web server. It is therefore absolutely critical that HTTPS traffic is scanned for threats.

Far too many organizations still only scan unencrypted HTTP web traffic, while leaving HTTPS web traffic unscanned. The reality is that in order to scan HTTPS / SSL encrypted traffic, it is necessary to install a Trust Certificate on each device on the network. This does take some time and effort, (although there are various enterprise tools to ease this task), but we are normally only talking about a few seconds per device. The alternative outcome for not implementing this? Your entire network could be successfully attacked by ransomware or other exploits, ultimately sending your whole organization back to the stone age.

5. Leverage a SIEM System
Any IT Manager trying to monitor, manage, and report, on their network’s cybersecurity in real-time, has their hands absolutely full. Multiply that effort by multiple networks, add in the need for PCI DSS (Payment Card Industry Data Security Standard) compliance; and you realize the superhuman effort which would be required to carry out this work on a 24x7x365 basis. The need for an automated response becomes crystal clear.

By leveraging the NBSIEM+ (Network Box Security Incident and Management Plus) system, it is possible to provide real-time monitoring and analysis of security alerts, which are generated by both applications and network hardware, including routers, switches, and firewalls.

If you are already a Network Box client, please contact your local Security Operation Centre to discuss these issues, and more. If not, then you are still more than welcome to give us a call, to see what we can do for you. In the end, you either become a planner, or you become a victim. It’s cybersecurity awareness month – don’t become a victim.
Over the years there have been many variants, but the ones in recent months have all utilised one of more of the following attributes:

- Provide the recipient’s password, as proof of ‘hacking’ the recipient’s computer.
- Demand payment in BITCOIN, or some other crypto currency.
- Claim to have hacked the recipient’s webcam, and to have recorded adult footage, pornography, or other such embarrassing details.
- Claim to have installed malware on the recipient’s computer, or some website visited.
- Use mixed case letters, or international character sets, to disguise the text.
- Spoofed the sensor as the recipient themselves.
- Random sender addresses, and no URLs provided.

Judging by the volume of these, and the lack of any decrease in numbers as the months go by, it seems to be an effective campaign. Analysis of crypto currency addresses show the scams to be pulling in thousands of dollars for each address used. Many in the industry are labelling these ‘sextortion scams’.

**Sextortion Scams**

Hackers and cyber criminals know your passwords

Earlier this year, Network Box Security Response started to see an increase in volume of a particularly nasty type of spam email. These are all part of an effective email scam campaign.
The Password (and other personal details)

It is undoubtedly the inclusion of the password in the email, as proof of the successful hacking of the recipient’s computer, that is the most concerning. This raises the credibility of the scam - couple that with the spoofed sender and many will be convinced it is real. It is sad to hear the most common question from recipients is not ‘is this a scam?’, but instead ‘how do I buy bitcoin to pay off this guy?’. The most amusing response we have heard is ‘I can’t afford it, I am just a student; will they give educational discounts?’.

So how did the ‘hacker’ get the recipient’s password?
The answer, of course, is data breaches on the Dark Web. These breaches contain email addresses, de-hashed (now plaintext) passwords, and a host of other personal information (including dates of birth, full names, addresses, countries of residence, etc). The ‘hacker’ is merely using that information as his database of who to mail, and what details to provide.

We recommend that you educate your users about this threat. You can also subscribe to the Network Box Dark Web Monitoring service to pro-actively inform your users of the issue. We even have a portal (https://darkweb.network-box.com/), that subscribed users can visit and enter their email address, to receive an individual report showing all the breached information we have discovered on them.

Spoofed Sender

It is trivial to spoof sender addresses with SMTP email, and hard to defend against. In particular, the ‘from’ header sender address is often not protected at all (and that is the address shown to the recipient in his email client).

We continue to see customers requesting to whitelist their own domain, and we continue to recommend against that. We also continue to see this in policies of customers that migrate to Network Box protection services. Gmail’s use of sender address to decide whether an email was ‘sent’ or ‘received’ continues to be a problem. Typically, 1% to 2% of spam on the Internet nowadays uses the sender spoofed as the recipient’s domain (either the recipient themselves, or somebody else in the same domain). We recommend that you consider the use of policy controls such as DKIM and SPF to limit the impact of sender spoofing, and never whitelist your own addresses / domains.

Crypto Currencies and Bitcoin

We continue to see crypto currencies (and bitcoin in particular) used in these and other scams. Again, you can educate your users that whenever they see an email demanding BITCOIN, or other crypto currency, it is most likely a scam and they should report to their IT support for assistance.

The Future

We don’t see this approach stopping anytime soon - it is just too successful. Of particular concern to us is that many data breaches contain far more information than simply passwords. For example, the recent Malindo / Lion Air breach includes passport numbers, identity numbers, and a host of other very private and hard to change information. But more importantly, it includes relationships between travellers travelling together; and that opens the door to spoofing of email addresses from people you have a relationship with, for example; only adding to the credibility of the scam.

So, take care, and please continue to be distrustful of anything coming in from the Internet. The bad guys may know your password, but NO - you most likely were not hacked!
While many businesses may close shop during this time of year, cyber criminals work right through the festive period – meaning it is crucial that you have the best security measures in place before leaving for the holidays.

Below, we have provided the Top 7 security tips to keep your business protected over the holidays:

1. Beware of spam and malware emails

During this time of year, there is always an increase in spam, phishing, and malware attempting to take advantage of users being in a holiday mood. Malware masquerading as Christmas cards are always common. In addition to turning ‘ON’ SSL Scanning, please ensure your colleagues are informed about the dangers of opening suspicious emails that may contain malware or redirect them to malware sites.
2. Automate your security updates
Ensure that your security patches are up-to-date, with the latest signatures and security policies. If you have a patch update system, make sure that this is set to 'automatic' so that your system automatically downloads and installs the latest security updates.

3. Update information and general housekeeping
The end-of-year is usually a good time to review your database and security policies. If you have staff that are no longer with the company, remove their records, and make certain that they do not have access to your network or database.

4. Ensure you have secure remote access
If you are going to be away from the office for a significant amount of time, make sure that you have remote access to your network with a secured VPN connection. Hackers and cyber criminals can intercept insecure connections and gain access to your network. Directly opening administrative ports to the Internet is not a sensible approach and is specifically prohibited by most security standards.

5. Turn ‘ON’ alerts and notifications
Set your monitoring system to send you alerts if there are any issues with your network. Thus, you will be notified, and will be able to respond to any issues that may arise. Please also ensure that your contact information is up-to-date, so that you will receive alerts, and your colleagues can contact you, if needed.

6. Review your disaster recovery plan
The relatively low workload during the holidays may be a good time to review your disaster recovery plan. Most importantly, test it, and ensure all necessary staff are aware of what it is and how it affects them.

7. Review physical security arrangements
The holidays are also a high-threat time for physical security incidents. Remember that no matter how strong your network security system or password policy is, all that is useless in the event an attacker gains physical access to your devices.

Thank you for your continued support and partnership. We look forward to working with you in the years to come. Stay safe.