TECH REVIEW 2022

NETWORK BOX

www.network-box.com

NETWORK BOX

TECH REVIEW 2022

Table of contents

As a special end-of-year review, Network Box has complied the key *In the Boxing Ring* technology news, features, and articles from 2022.

To read all available editions of *In the Boxing Ring,* please use the link provided below:

https://www.network-box.com/itbr

www.network-box.com

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.

NETWORK BOX in 2022

> **Here at Network Box, we are seeing more and more of our customers accepting Managed Services and moving their information technology systems to that model. Whether it be Software as a Service (SaaS), virtual hosting, or managed security, the benefits of outsourcing the provisioning, maintenance, and support of IT systems are clear.**

The 2022 Problem

The challenge for Network Box has always been to supply effective services within limited IT security budgets for all businesses, small and large. Up until recently, we have concentrated on managing our own platform because only by controlling the platform can we deliver security in a cost-effective manner. When Network Box has a software update, we can internally test it across all our supported platforms and then simply remotely globally release it without visiting each site and dealing with different hardware/software versions, driver, and network compatibility issues. Scalability is key to the problem.

Our customers are finding that as they migrate systems to the cloud, the result is a hybrid network consisting of:

- Workstations, servers, and other IT systems (like telephones, printers, etc.) in the office
- Laptops and mobile devices out of the office and working from home
- Servers in legacy data centres
- Virtual servers in cloud data centres
- SaaS applications

And this hybrid network is managed by a number of different providers, none of whom want to cooperate with each other or provide a unified management framework. Add on top the issues of regulatory frameworks, reporting requirements, incident response, and the issue becomes one of managing the managed service providers. Some 'full stack' providers offer solutions managing third-party platforms, but they are typically both horrendously expensive and limited in the choice of devices and applications offered.

The Roadmap for 2022 and beyond

Over the past few years, Network Box has evolved our managed services to better support the hybrid networks our customers are migrating to. And we are doing this while still adhering to our core principles of delivering cost-effective network security in a scalable manner to businesses of all sizes.

Network Security is, in general, best placed closest to the assets being secured. There are exceptions to this (massive-scale DDoS protection and mobile asset protection being the two most obvious), but in general, this approach reduces latency and other delays while offering the most comprehensive protection. To achieve this, Network Box now offers our services in a variety of ways:

- On-premises physical security appliances
- On-premises virtual security appliances
- Cloud virtual security appliances
- Pure cloud services
- Multi-tenanted cloud services

In 2022 we will continue with the migration of our service support systems to the NBSIEM+ platform, with a view to obsoleting Box Office by the end of this year.

We start the year by launching our new NBSIEM+ v6 portal on Wednesday, 5th January 2022. This v6 NBSIEM+ is an entirely new 100% API-driven system supporting both web browser clients and mobile apps. The old v5 NBSIEM+ will be moved to **https://legacy.siem.network-box.com/** at that time. We expect to release the companion mobile apps on both Android and iOS platforms during the second week of January (subject to Apple and Google's approval processes), and obsolete our old Box Office mobile app at that time.

January will also see the release of several new multi-tenanted cloud services, including:

- **Cloud SSL Service Reputation.** Similar to cloud IP and DOMAIN reputation, this service monitors publicly available SSL services (such as websites, mail servers, etc.) and validates SSL certificates. It will warn (via GMS incidents) of connection issues, certificate issues, impending expiry, and/or expired certificates.
- **Cloud SSL Certificate Reputation.** A companion to the Cloud SSL Service Reputation services, to monitor SSL certificates directly (without requiring public access to the service), and monitor + alert for the same certificate issues.
- **Cloud Entities.** As a fundamental support layer for our other cloud services, this allows entities to be administratively maintained in the cloud or automatically synced with LDAP, Active Directory, or 365/Azure directories.
- **Cloud SDWAN.** Providing VPN client access to cloud services in a similar support capacity for our other cloud services.
- **Cloud Web Client.** This service provides the Network Box Web Client proxy (including content filtering, categorization, anti-malware, and policy control) in the cloud without requiring on-premises or virtual appliances. Client connection is either via Cloud SDWAN VPN or directed proxy. Reporting and policy control is via the NBSIEM+ administrative interface. With the same policy control as our Network Box 5 appliances, this provides simple and effective security for laptops and mobile devices outside the office or working from home.
- **Cloud SMTP Server.** This service provides the Network Box SMTP Server proxy (including anti-spam, anti-malware, and policy control) in the cloud, without requiring on-premises or virtual appliances. Reporting and policy control is via the NBSIEM+ administrative interface. With the same policy control as our Network Box 5 appliances, deployment simply requires pointing the domain MX record to our cloud service.
- **Cloud SMTP Client.** Providing similar functionality to Cloud SMTP Server, but for clients sending email. Connection is via authorized IP range, Cloud SDWAN VPN, or authenticated SMTP sessions.

Before the end of Q1 2022, we intend to complete the migration of our existing Box Office cloud services (dark web reputation, dynamic DNS, IP reputation, and DOMAIN reputation) to the NBSIEM+ platform. At that time, NBSIEM+ will have become the single unified framework for access to all Network Box services.

Q1 will also see the release of a cloud Mail Portal, via the NBSIEM+ platform. This will provide an option for users to be able to release mail even when not in the office, with full support for small screen mobile devices.

In Q2 2022, we will release Admin Portal within NBSIEM+. This will provide administrative access to all Admin Portal functionality from the NBSIEM+ platform without requiring direct access to the end-user device, and include mobile app support. Combined with Cloud Mail Portal, this allows us to offer a unified framework for users (subject to access control) and administrators to monitor, configure, and control policies, regardless of the mechanism that controls its implementation (physical device, virtual device, or multi-tenanted cloud service).

The remainder of 2022 will see us continue in our goal of expanding the managed services that we can provide from our single unified NBSIEM+ platform. Particularly noteworthy is:

- We will continue to provide fully managed services for Network Box 5 appliances and services (physical, virtual, and in-the-cloud).
- NBSIEM+ provides event log collection, archiving, monitoring, and incident response, including full support for not just Network Box 5 devices, but dozens of types of network and security equipment. Supported 24/7 by SOCs around the globe.
- We will also provide support for end-point agents; for event log collection, archiving, monitoring, and incident response via the NBSIEM+ platform.
- We are working with scanning partners to provide both internal and external scans at three levels (reconnaissance, vulnerability, and PCI), with a single unified reporting interface via NBSIEM+. Full workflow control is provided here to simplify vulnerability management.

Fundamentally, Network Box provides a Managed Detection and Response service. Leveraging our Network Box 5 appliances, third party customer devices (network switches, routers, or other security devices), end-point protection systems; and using our NBSIEM+ platform to collect event logs, monitor, raise incidents, report, and manage the security of our customers from our highly trained security engineers in Security Operation Centres around the world.

> **We recognize that the pandemic has brought with it unique challenges and seems likely to change how some businesses operate fundamentally. In particular, some of our customers in the travel, hospitality, and tourism business have been particularly severely affected. We are grateful to see how our Security Operation Centres and offices worldwide have adapted to these new challenges. We would also like to thank our customers for their continued trust in Network Box, our platform, and our security services.**

Network Box Best Practices

Over the past two decades of delivering Managed Security Services, investigating security incidents, and working with our customers to protect their networks, Network Box has developed a set of Best Practices.

These represent the most common forms of network infiltration and data breaches that we see affecting networks around the world. Many of these best practices can also be found in common standardized security frameworks. These and other Best Practices are continually revised and updated to keep up with the evolving security threat landscape and protection technologies. Today, we have published these to encourage wider awareness and adoption.

https://network-box.com/best-practices

Network Box Security Engineers refer to these Best Practices when designing defense systems for networks under our management, when processing policy change requests, and during periodic configuration reviews. We recommend that all customers adhere to these. While ultimately, the customer decides the policy, we strive to inform, warn, and point out when policies conflict and open up networks to common attack vectors and unnecessary risk.

Remote Administrative Access Open to the Internet

In general, Remote Administrative Access services (such as SSH, RDP, VNC, etc.) capable of providing administrative access should not be open to the Internet. Opening such services to the Internet directly exposes the network to the exploitation of vulnerabilities or insecure credentials, and brute force attacks. Even those services restricted to user-only (non-administrative) access are discouraged due to privilege escalation issues.

As an alternative, it is recommended that VPN / SDWAN services be deployed. These remote administrative services should only be made available over secure VPN / SDWAN links to specific user accounts, VPN endpoints, or source IP addresses.

Weak, Default, or Re-Used, Authentication Credentials

User or administrative authentication credentials should be strong, never re-used, and should not be the defaults originally provided.

Administrative Access Source Restrictions

Access to administrative services should be closed to all by default and only opened to specific sources in order to meet specific access requirements.

Effective Policy Control

Effective policy control, and a 'block all, permit only what is necessary' approach should be applied, following the principle of least privilege.

Domain Name System (DNS)

Network Box (or other reliable, hardened, and secure) DNS servers should be used for all equipment. ISP or shared global DNS resolvers should never be used. When multiple DNS resolvers are specified, they should all be of the same type. When access to local lookup domains is required, that can be implemented using domain forwards. DNS servers should be configured to disable recursion, except for specific source IP address subnets.

Excessive Whitelisting / Bypassing

Whitelisting and bypassing should be applied sparingly and minimally.

Effective Network Segmentation

This should be employed to, at a minimum, separate servers from users and separate different organizational groups wherever possible. VLAN technology, or physical network interfaces, should be used for this; supplemented by layer 3 routing, firewall policy control, and high-level protection (such as WAF, IDPS, etc.).

Weak User Access Restrictions

Access to user services should be restricted and only opened to meet specific requirements.

Effective Anti-Malware

Anti-malware security modules should be enabled and utilized to protect networks at three levels:

1. Gateway
2. Server
3. Workstation

Modules should not be disabled, and software and signatures should be kept up to date.

Effective Anti-Spam

Anti-Spam technology is essential for detecting and blocking phishing and other such malicious emails. This should be enabled and set to quarantine appropriately.

Deploy Intrusion Prevention

Intrusion Prevention should be used in preference to, or in combination with, Intrusion Detection.

- Inline IPS is preferable to active response IDS - subject to performance considerations.
- IPS and IDS systems should be effectively configured, and items such as local network ranges, ports used, etc., should be reviewed and confirmed to match the protected network and services.
- While deploying IDPS systems in alert (not block) mode initially is acceptable, for tuning purposes, such systems should be in blocking mode after such tuning has been completed.
- Frontline IPS systems should be enabled and enforced.
- Infected LAN systems should be enabled and enforced.
- Consider deploying honeypot addresses to improve reconnaissance detection capabilities.

SSL/TLS Traffic Should be Scanned

Traffic encrypted using the SSL/TLS protocol should be scanned. This affects SMTP, IMAP4S, POP3S, and HTTPS at a minimum.

As more and more Internet traffic moves through these protocols (for authentication and privacy reasons), such traffic becomes invisible to policy enforcement, malware detection, and other security controls. Intercepting and decrypting such SSL/TLS traffic is essential to protect laptops, desktop workstations, and servers.

Deploy Web Application Firewalls

Web Application Firewalls should be configured, tuned, and deployed in enforcing mode for any Internet-facing websites or services using the HTTP/HTTPS protocol.

Encrypted Traffic Policy Control

Encrypted traffic should be subject to policy control.

- Web Client HTTPS traffic intercepted.
- SSL (or STARTTLS) offered opportunistically where reasonable.
- WAF SSL offloaded for interception.
- VPNs terminated before policy control enforcement.
- Policy control for other encrypted traffic.

Lack of, or Poor, Encryption for Sensitive Data

Access to sensitive data should be restricted to strongly encrypted channels.

Preparation and Contingency Planning

Preparation and Contingency Planning should be employed to anticipate and prepare for issues.

- Anti-DDoS should be enabled and prepared, so it can be quickly applied if necessary.
- Condition Variables should be used to pre-prepare alternative policy paths for anticipated scenarios.

Most network infiltrations and data breaches that we commonly see are not the result of sophisticated hackers armed with zero-day exploits. Instead, the bad guys tend to target the 'low hanging fruit' - the easy targets. Networks with default administrative credentials, remote access open to the Internet, or well-known vulnerabilities waiting to be exploited are just three examples.

There is an old story of a man who walked into a scuba diving shop and asked for the biggest fins that the shop sells, as he was afraid of sharks. The shopkeeper tells him that no matter how long or powerful the fins are, he will never be able to outswim a shark. But the man replies that he only needs to outswim his dive buddy, not the shark. The same is true for network security. You don't need to make your network perfect. You just need to make sure that your defenses are strong enough that the bad guys will move on to easier targets.

Mobile SIEM+

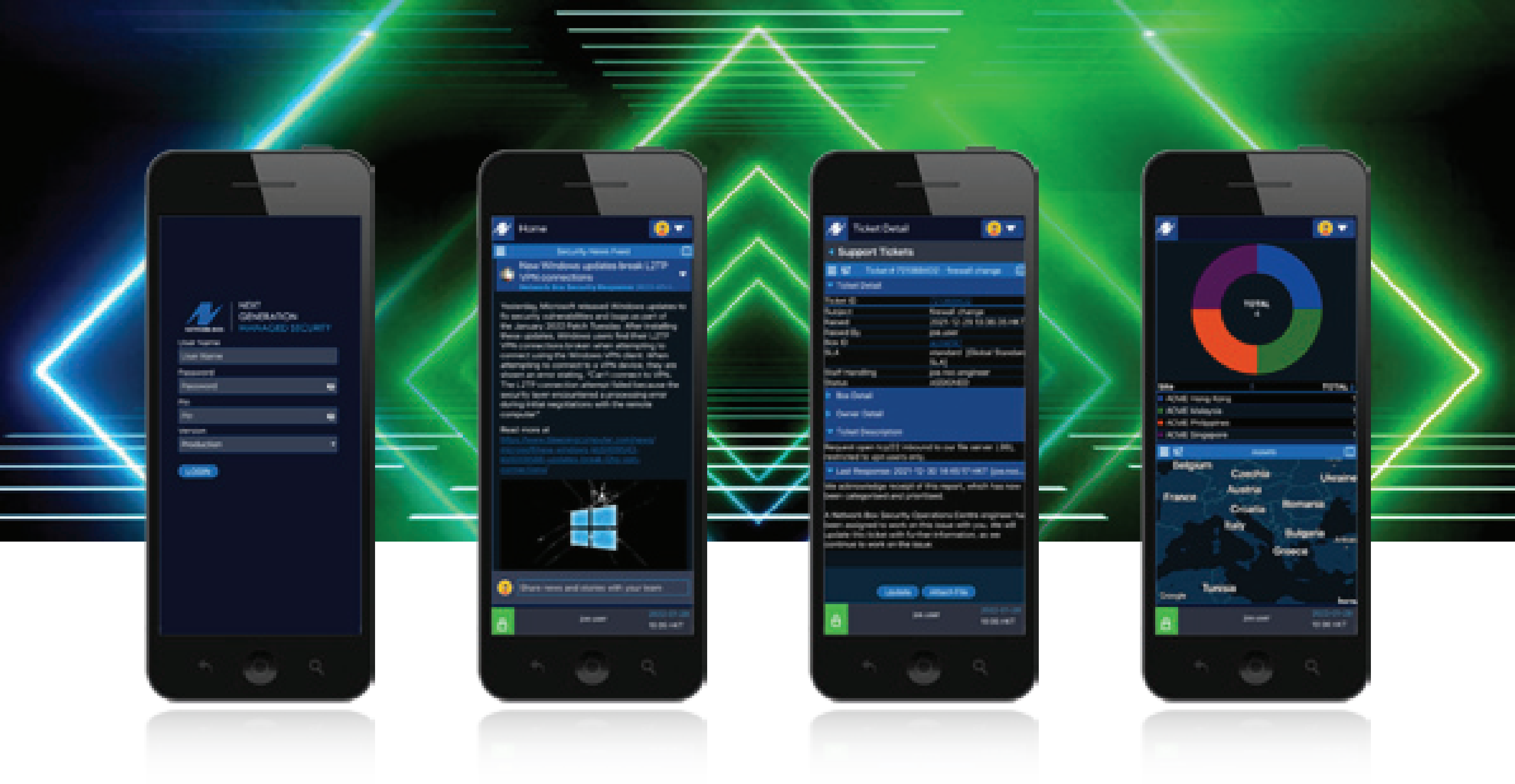
Network Box SIEM+ Services at your fingertips

As a Managed Detection and Response provider, Network Box uses NBSIEM+ as the basis for our incident management service. With this system, we gather event logs from end-user devices, normalizing and correlating them for analysis. The incident workflow system allows alerts to be raised and appropriately escalated to resolution.

NBSIEM+ is an API based service, accessible via several options:

- Desktop and Mobile web browsers, using our browser app (**https://siem.network-box.com/**).
- iOS and Android-based mobile devices, using our App Store apps.
- Directly using the API for automation and partner integration.

Unlike commonly seen cut-down mobile App offerings, the Network Box approach is to make our full functionality available across all platforms, whether access is via browser, mobile App, or directly to the API.



NBSIEM+ for mobile devices

Available for phones and tablets, for both Apple iOS and Android-based mobile devices, the Network Box SIEM+ App is designed to provide secure access to administer Network Box managed services. Equivalent functionality is provided on both the iOS and Android platforms.

The App supports Box Office / NBSIEM+ user account authentication and includes full support for dual-factor authentication (using the RFC-6238 TOTP standard).

> Upon logging in, the **Home** screen is shown with a timeline-based history of recent activity. ***Support*** and ***Incident*** ticket updates are shown alongside highlighted emerging security news stories. You can even use this system to distribute announcements to your own team with fine-grained privacy controls.
>
> The **Support** menu provides full access to Box Office ticketing - including raising, reviewing, and updating support tickets.
>
> The **Incidents** menu provides access to ***Incidents*** (Global Monitoring System health, SIEM events, cloud services, or other such).
>
> The **Events** menu provides access to event logs if your devices are configured to submit events to NBSIEM+.
>
> The **Assets** menu provides an overview of your managed assets and their current status.
>
> The **Services** menu provides access to your managed services; including physical, virtual, and multi-tenanted pure cloud.

Both the browser and mobile Apps operate on a 4x3 grid for desktop-sized screens and tablets, with each screen typically displaying one or more widgets of information. When viewing on smaller mobile screens (such as a mobile phone), this is automatically re-arranged to be 1 column wide to minimize horizontal scrolling. Both dark and light theme options, and multiple language support, are provided.

The Mobile Apps also integrate into the Box Office notification system, supporting iOS and Google notification systems. You can use Box Office to configure the notification preferences by type, time range, asset/box group, etc. For example, you can configure incidents related to a list of specified boxes to alert 24x7, but others to only notify during office working hours.

Upcoming Features

Cloud User Portal option
Using the same technology and services as NBSIEM+, the option will provide end-user access to securely release quarantined email from the cloud (for both on-premises and multi-tenanted cloud mail scanning services), without requiring opening up on-premises device services to the Internet. This also supports mobile device-sized screens (phone and tablet) and desktop browsers and mail clients, which will greatly simplify the secure deployment of end-user quarantine release.

Cloud Admin Portal screens
From within NBSIEM+, this will enable administrative control for all managed Network Box services from both desktop/mobile browsers and mobile Apps.

As the base platforms for NBSIEM+, our API servers, and our mobile Apps have now been released, many new screens and reports will be available to you.

Network Box Mobile App
for Android and iOS

Please use the links below to download the FREE App.

GET IT ON Google Play https://play.google.com/store/apps/details?id=com.networkbox.siem

Download on the App Store https://apps.apple.com/hk/app/network-box-siem/id1532859749

Network Box Mobile Applications Framework

Following on from our newly released mobile apps, in this article, we describe in more detail the framework behind our mobile and web applications.

PUSH Code

When Network Box was first founded more than 20 years ago, we realized that the usual approach to delivering code and threat protection signatures was insufficient for the rapidly evolving cybersecurity landscape. While our competitors were pulling updates to protected devices once a week or once a day, Network Box deployed and patented our PUSH technology. As soon as we produce a new protection signature, we connect to each managed device to install and activate the protection within seconds. Unlike traditional PULL technology, we don't wait for the device to connect to us (via polling).

Similarly, the traditional delivery of protection code updates via patch updates and monthly release cycles is too cumbersome and slow. By the time the updates is released and installed, the threat has long since passed. So we developed **PushCode** - the ability to deploy code updates in a similar way to protection signatures, by actively PUSHing them and installing them on protected devices.

The traditional method of developing mobile applications, where all the code functionality in the App is delivered via platform-specific stores, is similarly constrained by the App store model. With Apple, Google, and others, acting as gatekeepers (and possible roadblocks) every time an update is released - often delaying the update release by days/hours and pacing the release rollout.

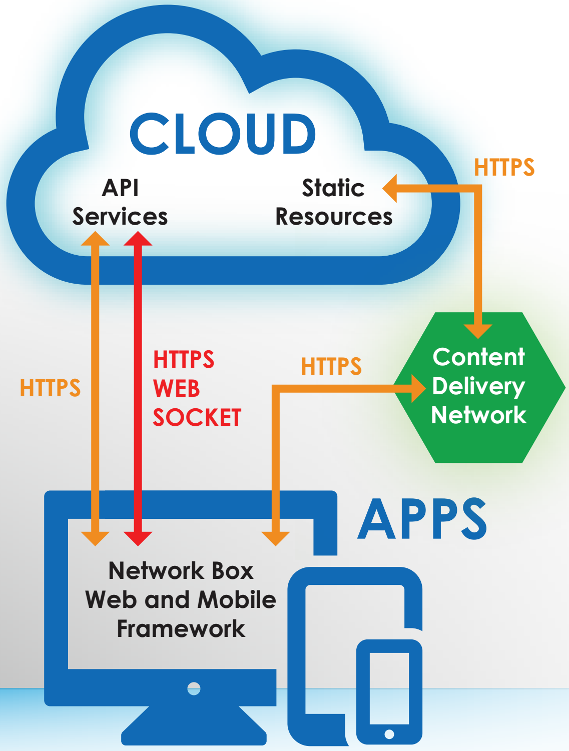
The Network Box Framework

The Network Box Framework for Mobile and Web Applications marries the best of both worlds, leveraging the App Stores to deliver framework applications to the end-users but allowing for the functionality to be enhanced and extended automatically within the Apps from the cloud.

In the cloud, Network Box deploys two forms of servers to support the framework:

1. For static assets (images, code, etc.), we use the standard HTTPS protocol (HTTP over SSL), standard web servers, and Content Delivery Networks to deliver the resources to the Apps.

2. For dynamic data (information displays, reports, entry screens, etc.), we use clusters of API servers. The Apps remotely make API calls using a REST protocol over HTTPS. In addition, for streaming data, web socket connections are used (embedded in the same secure HTTPS protocol).



Network Box provides a single unified web App (accessible from web browsers at **https://siem.network-box.com/**), leveraging javascript to run the App inside the web browser. This web App firstly implements a framework for login/logout authentication. On login, the screen layouts, menu structure, and other such information is returned to the App - which then follows the instructions from the API server as to what to display and where. Each screen is typically made up of cells in a 4-column by 3-row layout, with widgets being able to span one or more cells. The screen layouts are adaptive and support full desktops, tablets, and small screen devices such as mobile phones (where the layout adapts to 1x12). Each widget has an associated API call to retrieve the data, and a display appearance, which is chosen from a set of supported appearances such as forms, tables, bar charts, pie charts, etc. In this way, new screens and reports can be released without requiring a new App update to be deployed.

We also provide mobile Apps for both the Android and iOS platforms. These are built similarly to the web App and connect to the same static asset resources and API servers. For speed and a native look-and-feel, we cross-compile from a single code base to both Android and iOS native APIs to take advantage of each platform's capabilities. The behavior of the mobile Apps is the same as the web App, including support for the same 4x3 screen layout (including 1x12 for small screens such as phones), and the same selection of appearance types (optimized to the capabilities of the device). The mobile Apps also support native features such as PUSH notifications and biometric authentication.

The REST API used by the web and mobile Apps is publicly available (although still under closed NDA at the moment) and can be used for third-party integrations (such as partner ticketing systems, for example) and scripting and other automations.

> **Traditionally, web services have been delivered purely in the cloud, and applications have run purely on end-user devices. The new hybrid model, separating the server from the client utilizing the industry-standard HTTP protocol to access REST APIs in the cloud from Apps running on end-user devices, provides excellent benefits but introduces the App Store gatekeepers. The Network Box web and mobile App framework avoids that issue by delivering functionality updates to the Apps from the cloud - only requiring App Store updates when changes to the actual framework are needed.**

NBSIEM+ Enhancements

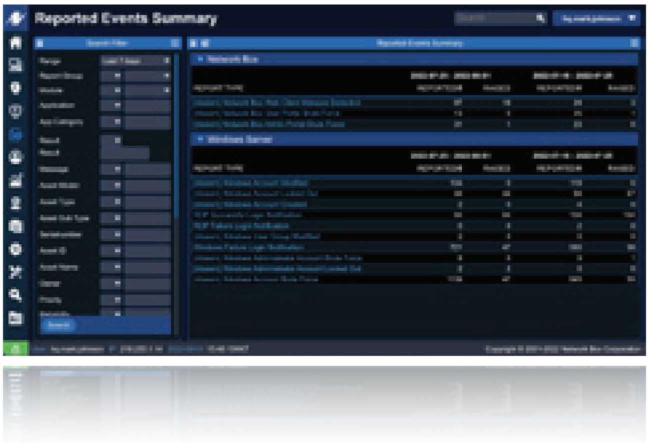
Over the past year, Network Box has received feedback on NBSIEM+ and incorporated them into over 100 enhancements. While several of these changes are structural, many are visible to users. In this article, we will highlight some of the more notable enhancements.

Navigation Improvements

We've enhanced the right-click popup menu options for all links. This will allow you to open links in place, in a new tab, or in a new window. On desktop browsers, ctrl-click will open the link quickly in a new tab. We've also improved the browser back button to restore the previous form and filter state. A shortcut bar has been introduced to allow for quick switching between screens related to the same item (asset, event, etc.), and a selection field at the top of the screen shows at a glance the currently selected item (as well as allowing for changing that selection). We've also worked on optimizing NBSIEM+ displays across each of the mobile, tablet, and desktop browser environments we support (in particular, adding support for accessibility font sizes and scaling).

Live Connection to NBRS-5 Network Boxes

We earlier wrote about the direction we are taking to provide access to, and ultimately merge in the admin portal from NBSIEM+. With this release, we are providing access to the first screens with this capability. Now, calling up an NBRS-5 asset within NBSIEM+ will show widgets such as the memory, CPU, and network utilization live from the box itself without having to log in and access the admin portal. To support this functionality, a number of new widgets and appearance types have already been introduced. Over the coming months, more of these widgets and screens will be released in NBSIEM+.



NBSIEM+ Events

We continue to see great progress with our customers' wider adoption of NBSIEM+, and we are already collecting and analyzing more than 200 million events daily. We now introduce optional data capacity limits, allowing you to set a limit on how many events per day come in from each asset and to suspend submission from assets that exceed those limits. We've also introduced a new unified field type to uniquely identify classes of events irrespective of the platform generating the event.

The biggest change with this release is the introduction of 'reportable events.' We now tag events of interest (such as password failures, account lockouts, etc.), grouped by platform and category, and report these to you in a summary and detailed breakdowns. Should the event be serious enough, as before, we will raise an incident ticket for a more in-depth investigation and response.

Reporting

We've brought across the dashboard reporting system from user and admin portals to NBSIEM+. Now, any dashboard widget can be added to a custom report and delivered by email as a PDF according to user-defined schedules. If missed, previous reports can also be downloaded, and templates are built to be shared between team members.

Many more reports and dashboard widgets have been introduced in this release, including several related to NBSIEM+ Event Reporting and Incident management (Events by Asset Type, Reported Events List, Reported Events Summary, Reported Incident Detail, and NBSIEM+ Asset Inventory).

Cloud Services

We continue to migrate all Network Box cloud services to the unified NBSIEM+ platform and now release Cloud SSL Certificate, Cloud SSL Service, Cloud IP Reputation, and Cloud Domain Reputation. The remaining services will follow in the coming months. For multi-tenanted cloud services, a number of service-specific reports have also been released, such as Cloud Web Client Events, Cloud Mail Events, etc.

CLOUD SSL Server and Certicate Reputation Services

Network Box has released our cloud SSL SERVER and SSL CERTIFICATE services. In this article, we talk about these new services, what purpose they serve, and what they can do for you.

As more and more services adopt SSL encryption standards and the Public Key Infrastructure (PKI), management of the associated SSL certificates has increasingly become an issue for many organizations today. High staff turnover in IT departments has only exacerbated the problem. The result is expired certificates, browser warnings, and customers unable to access your services. Certificate Authorities like LetsEncrypt have further complicated the issue with their very short validity certificates reliant on automated renewal (and without commensurate monitoring systems to alert should the renewal fail).

To address this issue, Network Box has released two new pure cloud services:

Cloud SSL SERVER Reputation Service

The service allows you to enter the connection details for your publicly accessible SSL servers and monitor the certificates those servers host. The service checks certificate signing validating, Server Name, expiry date, and other such attributes. Should any issues be found, a GMS Incident is raised to alert you. For upcoming certificate expiry, the system will, by default, warn 30 days before expiry and alert critical seven days before expiry.

Cloud SSL CERTIFICATE Reputation Service

The service is designed for non-public SSL services and their certificates. It is commonly used for private services or for private self-signed CA certs used in a private PKI infrastructure. To use this service, you upload the certificate itself, and the system will automatically monitor it in a similar way to our Cloud SSL SERVER service.

Both services are integrated into both Box Office and NBSIEM+, and are available today. These pure cloud services are available to monitor any SSL certificate or publicly available service, even if not directly protected by Network Box.

The Network Box Approach

TO YOUR PRIVACY

In this article, we talk about privacy and the Network Box approach to ensuring the security of your configurations, maintenance, and private data.

As we see more and more organizations moving from a centralized server-based approach to data (with data in a small number of big data servers which are accessed via file sharing by workstations), to distributed hybrid storage models (with data in servers which are distributed on workstations, private clouds, and software-as-a-service systems); we are right to be concerned with the consequences to data security and privacy that this brings.

In particular, for software-as-a-service and virtual cloud environments, that very security and privacy becomes less and less under our control, and we become more reliant on external providers and their often unknown and obfuscated security practices. In such environments, we must ensure that our outsourced providers adhere to at least the same security standards and methodologies as we do for our own systems.

For Network Box, and the systems we manage, our approach is as the following:

1. In general, Network Box seeks no more access to your systems and data than your Internet Service Provider. We don't typically require administrative credentials. By being deployed next-in-line to the Internet Router, we can provide effective perimeter protection without additional security concerns. We can operate in conjunction with further security devices for defence in depth if required.

2. Network Box operates as a federated network of cooperating but independent Security Operation Centres. Our customers choose which specific SOCs will have access to maintain their security devices, and firewall controls are automatically implemented to restrict access to those selected centres.

3. Data (emails, network traffic, event logs, etc.) passing through the Network Box device stays on the Network Box device. While SOC staff have secure remote access (for diagnostic and maintenance purposes), this data is not stored outside the Network Box devices themselves.

4. Statistical and summary data that does leave the Network Box device (for example, GMS health metrics, CPU utilization, etc.) is anonymized and/or filtered to comply with standards such as GDPR.

5. Network Box has published verifiable details of the data stored and retrieved from systems under our management.

6. If the customer chooses to utilize Network Box cloud services (such as NBSIEM+, cloud mail backup, etc.), they can select the geographic region from which those services are delivered (to comply with regional regulations).

7. Each regional Network Box Security Operation Centre implements the certification and approvals necessary to operate in their region. Examples of certifications, our SOCs hold include SAS-70, ISO 9001:2015, ISO/IEC 20000-1:2018, ISO/IEC 27001:2013, PCI DSS, and many others.

Network Box believes that transparency and clarity concerning how your data is protected are fundamental to our businesses. Security through obscurity is never a good idea.

AI AND CYBERSECURITY

by Pierluigi Stella
Chief Technology Officer
Network Box USA

Something I keep hearing of late is what cybersecurity is set to look like and how AI will play a bigger role against ransomware and breaches.

Firstly, it isn't AI if it doesn't have the element of prediction. And here, we're not predicting anything. To be honest, we're only inferring (at best). Inferring possible behaviors. As such, let's call AI for what it is, and that's Machine Learning (ML). And yet, the industry keeps trying to use AI because it sounds much more impressive. **IT'S INTELLIGENT.** Well, Machine Learning is just as impressive, is it not? A machine that "learns" and adapts its behavior based on what transpired in the past? Tell me that's not mind-blowing?

Aside from this critical clarification, we must also consider that hackers aren't just sitting around idly. They, too, have access to "AI" tools. So, while we may think the new and ultimate tool is coming, our adversaries are likely already using those same precise tools. Innovation happens on both sides. Our enemies have access to the same resources. Most software tools are open source and available to everyone, for better or for worse. And those who have nefarious intentions are very skilled, very smart individuals too.

This initial consideration aside, we appear to be placing far too much reliance on something that, in all likelihood, will not deliver as we hope.

I have tested AI-based Anti-Virus for an entire year

I used it to test every email our filters were scanning in parallel with our filters. And in that one year, the AI-based Anti-Virus (AV) captured a grand total of four emails. I repeat, 4!!! Considering that we scan millions of emails daily, that number is beyond minuscule. Our "traditional" scanners, comprised of over 70 engines (each tailored to specific issues), captured hundreds of thousands of emails. Why? Because threats don't come inside emails as attachments. No hacker would send you a virus attached to an email because that's far too easy to catch. Block executable code altogether, and you're blocking every threat even if you don't know what threat that is, which ultimately doesn't even matter. A threat is a threat that needs to be stopped, regardless of its name.

For the most part, hackers send you links. They send you phishing emails. Spoofed emails. They send you something that aims to trick your users into clicking and downloading the threat code.

So, is that email a threat per se even though it does not contain executable code? **YES, IT IS.**

Because sadly, users will be users, and some will just keep clicking on things they're not supposed to because they can't help themselves. Instead of a "think before you click" mentality, they click first and think later. And that's when the real threat starts. When the clicked link goes out to grab that code, it will now infect your entire network.

How do you protect from all this? No need for fancy AI.

Scan HTTPS and ensure things are properly blocked in the web filtering. That's where you need to apply the real and best protection nowadays because once the user clicks (and you know someone will), you may still have a chance at blocking the threat. BUT only if you're properly filtering and scanning HTTPS.

Before closing, a final word about endpoint AV.

Traditional AV is practically useless

With more than 1,250 new threats per minute, a signature-based AV will never be able to keep up, and here's where pundits advocate using AI/ML. I don't necessarily disagree with this approach, but I believe it's insufficient. I mean, we're still in the realm of trust but verify. And we know that on its own is also no longer sufficient. Zero-Trust tells us that we need to "assume breach." That it's bad news from the get-go.

On that note, a better approach is to readapt the concept of whitelisting. The idea is that nothing is allowed to run on your computer unless it has been "trusted." And use certificates to identify legitimate software, checking everything that tries to run on your computer. Practically questioning everything and only allowing what's been whitelisted to run. **AND NOTHING ELSE.** You can try to install ransomware as much as you want. It just won't be allowed to run. So, even IF you get breached and download ransomware, it won't cause any problems because it will not be able/allowed to run.

I find this a much better approach than an ML tool since the latter may or may not recognize a threat. We're putting too much faith into a new technology still in its infancy and definitely not ready for the great things we tag it as capable of doing.

AI/ML will likely be great. Some day.

But, by that point, hackers will also have a similar tool, so the battle continues. **Wouldn't you agree?**

RANSOMWARE and the Dark Web

Most companies nowadays gather, store, and handle highly confidential client information. Such personal data is an integral part of almost every company's day-to-day existence. There is a self-evident need to ensure that such data hasn't been altered. Continued and timely access to any required documents, emails, and plans, are also critical.

Imagine needing some crucial data only to find access to everything blocked by Ransomware. Everything is encrypted and inaccessible. Every server, desktop computer, laptop, data file, backup file, and even cloud backup file is rendered useless.This isn't just a hypothetical problem. Many businesses worldwide have been forced to face precisely such a nightmare in real life. Just as an arsonist can burn down your office, a hacker can delete your entire digital existence.

This isn't just a hypothetical problem. Many businesses worldwide have been forced to face precisely such a nightmare in real life. Just as an arsonist can burn down your office, a hacker can delete your entire digital existence.

Hackers leverage panic. Hackers leverage value. Hackers leverage the fact that the last thing any business wants or can afford, is to suffer the massive reputational loss of being successfully breached by a hacker. And once a hacker has had control of a company's computer systems, it becomes difficult to assess if something has been stolen or to trust any of the data stored on those systems has not been tampered with, even if control has been supposedly restored.

Yet, so few companies seem to take cybersecurity seriously. Despite being extremely practical for protection against cyber threats, it also can relieve the danger of being sued by angry clients.

Hackers have changed

Some thirty years ago, their goal was to (perhaps) delete your data and (somehow) make themselves 'famous.' But over time, hackers realized they could use their technical skills to make a lot of money. Ransomware alone is now estimated to be a USD 10 billion-a-year industry.

Over time, even Ransomware itself has evolved

Traditionally, Ransomware encrypted your data, displayed a countdown clock on your computer screens, and threatened to delete all of your files if you didn't pay the hackers if and when the countdown clock hit zero.

However, companies soon learned that having a good data backup was adequate protection from such an attack. Formatting all infected devices, and restoring them from a recent high-quality data backup, would render the Ransomware attack ineffective.

This has led to modern Ransomware variants, which infect networks, taking their time to spread to every device connected to these infected networks, targeting any backup systems possible, including backup systems in the cloud, and then stealing as much confidential data as possible.

The confidential data is sent back to the hackers, usually overseas, in a country that the police have no jurisdiction over. Only then does the Ransomware encrypt and make access to the victim's confidential data impossible.

This kind of double-edged attack gives the hacker two different bargaining chips. The first is the stranglehold on the victim's operational continuity and access to its critical confidential data. The second, and probably even more critical, is the threat of publishing the stolen confidential data on the Internet, giving the whole world access to their data.

Cyber attacks can come in the form of direct disruptions to a company's on-premises physical file servers. Still, they can equally be attacks on servers located at a third-party data centre or virtual servers located in the cloud. There are computer servers located somewhere, running some form of the operating system and storing some form of the digital data file. Hackers can go after these, wherever they happen to be.

It is also crucial to note - Ransomware is only one form of cyber attack. Just as being shot using a gun is only one form of physical attack, if someone is trying to kill you, there are so many ways they can do so. They could burn you. They could stab you. They could drown you. They could poison you. They could push you down the stairs. The list is almost endless. In the digital world, hackers have an even broader spectrum of tools they can use to attack you or steal your confidential data. The number of potential cyber threats to businesses is legion.

The Dark Web

Some recent high-profile, successful cyber-attacks have stemmed from third-party data breaches, which had no direct relationship with the victim's company. The Colonial Pipeline in the United States, which was shut down by hackers using Ransomware, found that hackers had gained access using a password that other hackers had stolen from a member of their staff posted on the Dark Web. The Colonial Pipeline staff member had registered an account on a website belonging to a completely different organization (that was hacked) but had used exactly the same password they used at work.

Monitoring the Dark Web would almost certainly have prevented that shutdown.

In the end, the company paid a ransom of US$ 4.4 million to a Russia-linked cybercrime organization called Darkside before the critical network systems could be released and the oil pipeline reopened. Interestingly, the FBI managed to recover US$ 2.3 million in Bitcoin from the hackers. Ironically, this was also due to some poor password management on behalf of the hackers themselves.

Yet how many businesses are monitoring the Dark Web for credential leaks?

Hackers don't discriminate

Every company needs to protect itself. Small companies are not exempt from cyberattacks; hackers will not ignore your company just because it isn't famous or doesn't employ hundreds of staff.

In actuality, many cyberattacks, such as Ransomware attacks, are random in nature. An SME is just as likely to become a victim as a large global conglomerate. The most significant difference may be that a large organization will probably be more able to absorb the overall disaster, including the hit to its reputation, better than an SME.

In the USA, where reporting data breaches is required in certain cases, various companies have admitted to getting hacked and that hackers have published their confidential data. Yet, despite the obvious, undeniable, absolutely critical need for effective cybersecurity to be in place at every business, it simply isn't. Not even close.

When it comes to cybersecurity, one needs: real-time push updates to keep ahead of cyber-threats, cyber-security that is certified and audited to internationally recognized standards, and cybersecurity that is backed up by actual experts who monitor and manage the required systems around the clock.

Most companies are simply not protecting themselves. It doesn't make sense, even from a purely financial perspective. For a small business to be professionally protected by a fully managed, certified cybersecurity service provider would cost them annually less than the monthly salary of a junior staff.

> **Every company's management should work out how much the utter disaster of being compromised would cost and how much being properly protected would cost. The two figures cannot even be remotely compared. Not just in financial terms either, one can lose a hard-won reputation gained over many decades in a single moment.**
>
> **Get protected. Now.**

The Network Box Difference

When Network Box was founded more than two decades ago, 80% of security incidents were caused by a fundamental lack of protection. Networks got virus infections because of a lack of anti-virus protection, hackers got in because of a lack of firewall protection, and intrusions occurred because of a lack of intrusion prevention, and so on. The remaining 20% of security incidents occurred because the existing protection was either not configured correctly or had a problem, and the failure wasn't detected.

Network Box was formed to address those two issues - with a UTM+ product containing all the key protection components, combined with a managed service to ensure that those components are configured, monitored, and maintained securely.

As the terminology changes (SSP -> MSSP -> MDR, etc.), the technology evolves, as Network Box has shown with our continued innovation and evolution of our product and service offerings. Regardless, the fundamental security issues remain the same.

The Network Box Solution versus
Other Managed Products and Self Managed Products

What makes Network Box different? Below, we compare what we do against other Managed Security Service Providers and self-managed (Do It Yourself) solutions.

Metric	Network Box Solution	Other Managed Products	Self Managed Products
Responsibility	■ A single organization responsible for network security implementation, based on best practice recommendations and customer-defined policy.	■ Multiple organizations with multiple external vendors. ■ No single point of responsibility. ■ Vendors may blame each other.	■ Multiple external vendors. ■ No single point of responsibility. ■ Vendors may blame each other.
Deployment Options	■ Services can be deployed on-premises, in the cloud, or as multi-tenanted SaaS. ■ A single point of unified configuration, reporting, and support.	■ Dependent on individual MSSP. ■ Typically only one deployment option is available.	■ While hybrid (on-premises, cloud, multi-tenanted SaaS) is possible, there is no single interface. ■ Support can be challenging.
Security Response Centre	■ Self-operated. ■ 170 threat intelligence partners. ■ Recognized by Microsoft as a **Top 10 Contributor** to their threat intelligence in 2019.	■ Dependent on individual MSSP. ■ Typically through partnerships with external security response centres.	■ Generally none. ■ Sometimes subscribed to as an external service. ■ All threat intelligence must be acted on by IT staff themselves.
Configuration	■ Unified configuration. ■ Full version control and audit trail. ■ Real-time backed up both on the managed device and at multiple security operation centres.	■ Dependent on individual MSSP. ■ Typically with manual backups and limited version control.	■ Manual backups and version control (if any).
Service Times	■ 24x7x365 security monitoring. ■ SLAs for hardware and configuration support is available according to requirements (from working hours through to 24x7x365).	■ Dependent on individual MSSP.	■ Typically office hours only. ■ Limited support during nights, weekends, and holidays.
Response Times	■ Services are delivered according to a single clearly defined SLA with escalation thresholds and targets.	■ Must depend on external equipment suppliers for some aspects of service delivery. ■ Back-to-back SLAs across multiple vendors are often required.	■ Services are dependent on IT staff. ■ Often conflicting with other tasks using limited resources.
Hardware Response	■ Hardware replacement within 4 business hours (depending on territory). ■ Replacement pre-configured with current configuration (automatically synchronized), minimizing down-time.	■ Hardware replacement options are dependent on individual MSSP and external equipment suppliers. ■ Replacement typically needs to be manually configured and deployed from backups.	■ Typically office hours only. ■ Requires on-call staff during non-business hours, weekends, and holidays. ■ Replacement spares must be kept on-site or co-ordinated with external vendors. ■ Replacement typically needs to be manually configured and deployed from backups, leading to long down-times.

Metric	Network Box Solution	Other Managed Products	Self Managed Products
Security Technologies	One unified platform offering all key technologies, configured, maintained, and reported on holistically. Hardware and technologies are developed in-house within a closed security loop. Supported 24x7x365 by a triple ISO certified and PCI compliant Network Box SOC.	Multiple different platforms from multiple external vendors. No unified configuration, maintenance, backup, or reporting capability.	Multiple different platforms from multiple external vendors. No unified configuration, maintenance, backup, or reporting capability.
Security Updates	Delivered via patented PUSH Technology. Automatically performed in real-time 24x7x365. Average delivery time of less than 45 seconds.	Dependent on external equipment vendor, with little control.	Dependent on external equipment vendor, with little control.
Patch Deployment	Fully managed 24x7x365 with a single clear release cycle. Co-ordinated with customers to match their requirements. All patches are pre-tested across all supported hardware types and configurations.	Inability to check compatibility across different equipment vendor types and firmware/software versions. Timing is dependent on external vendors. Not synchronized (different vendors have different release cycles).	Dependent on IT staff knowledge and working hours. Patches must be downloaded and installed manually. Inability to check compatibility across different equipment vendor types and firmware/software versions. Timing is dependent on external vendors and not synchronized (different vendors have different release cycles).
Reporting	Weekly / Periodic KPI reports. Highly configurable customized reporting system. HTML-5 Dashboard. Real-time portable monitoring Web and mobile apps.	Dependent on individual MSSP. Typically each service provider has its own reporting system and cycle. No unified approach.	Dependent on the products chosen. Typically each product has its own reporting system and cycle. No unified approach.
Track Record	20+ years of delivering managed security services on our own platform. Services are provided via more than a dozen Security Operation Centres worldwide. Measured by our success, customers only renew services if we do a good job ensuring their systems are secure.	Dependent on individual MSSP.	IT departments are focused on helping their users operate their computer systems, not enforcing security policies. Most IT department staff have little practical experience or training in cybersecurity topics.

CYBERSECURITY BUDGET

Making your business case to management

by Pierluigi Stella
Chief Technology Officer
Network Box USA

In the past, cybersecurity has often been perceived as a nuisance, a necessary evil even, but this view has evolved over the years. Today, cybersecurity has become a critical business necessity, right up there alongside marketing and sales, requiring a budget of its own. Why? The reason is clear. Without cybersecurity, companies cannot function, let alone thrive. It is of immense importance, particularly when making the case to get the budget you need to achieve a robust security posture for the company's network. This article aims to provide the reader with ammunition to speak the language of and resonate with C-suite-level executives.

Let us begin by acknowledging that it is high time for a mindset change

By that, I mean that security people need to start changing how they think of themselves and their roles in the company.

The most common objection we hear when discussing the budget with management is, *"Why do you need more money if nothing has happened?"* or worse yet, *"Why do you even need any money if nothing has happened?"*.

We must start by changing our mindset and realizing that security is not an expense. We are not a cost center. We are, in a way, a form of insurance, but we do not approach the conversation from that angle since insurance is a cost, and it does not produce revenue.

Showing the Total Cost of Ownership (TCO) is also not a good approach because we are still talking about cost (we've already discerned how that's not a good approach) but also, the actual TCO of a security solution, to be correctly evaluated, needs to include *"your"* time. If you do not factor that in, your CEO will. When he does, you have just become a cost – and costs always need to be reduced, so there is that.

The language CEOs understand is one of ROI and profitability

That's how conversation needs to go down. From its definition:
ROI = Net Profit over Total Investment times 100 (**NP ÷ TI x 100**)

ROI must be greater than 100, or we have lost money. Our job is to show that the ROI of cybersecurity investments is greater than 100. That there is indeed a Net Profit to this equation.

We know that gross profit margin is defined as:
([Revenue - Cost of goods sold] ÷ Revenue) x 100.

A positive ROI contributes to the gross profit margin by either increasing the revenue or decreasing the cost it took to produce that revenue. Cost reduction is achieved as cost avoidance – if you do not get attacked, you do not incur the recovery costs, which can be very high.

To cite a well-known attack that was in the news for some time, **Target** lost US$202 million at the end of 2013. Between the loss of records, notifications to clients, forensics, company image, revenue loss, and loss of stock value, the retail giant lost 46% of revenue for the season.

Could your company survive such a hit?

If you do not get attacked, you do not incur the costs of an attack. So now the burden is on us, the security guys, to determine how much a security incident could cost our company. For starters, 60% of small businesses that suffer a cyber-attack end up going out of business within six months. Now, **THAT'S** a cost.

There is actually a formula to calculate the return on security investments, as proposed by the SANS institute:

ROSI = ([ALE x Mitigation Ratio] - Cost of solution) ÷ Cost of solution

ROSI: Return on Security Investment

ALE: Annualized Loss Expectancy. ALE represents the estimated amount of money that will be lost in a single security incident multiplied by the estimated frequency that a threat could strike within the same year.

Mitigation Ratio: an approximate number based on mitigation factors that depend on the company's actions to reduce the risk (i.e., having real-time backups vs. daily backups).

Cost of the solution: this is what you will spend to avoid the risk altogether. High costs can ultimately negate the solution's value if the ROSI ends up being lower than one.

What do you evaluate as part of cost avoidance?

What is the cost of poor security? That depends a lot on your company and your industry. In general, you will need to consider the following:

- Time spent diagnosing the issues.
- Time employees spend idling because they do not have a computer to use.
- Loss of productivity.
- Cost of IT personnel to fix the issues and to improve security, so the incident does not recur.
- Cost of the new security solutions.
- Cost of forensics analyses, especially when laws and regulations require this.
- Loss of company image, which could be quite incalculable at times. If you are providing something that's perceived as a commodity, the impact caused by a security incident on your credibility factor may very well propel your clients/customers towards your competitor and never return.

Even for small companies, where the potential loss is usually under US$50,000 per incident, the frequency at which an incident can happen again does justify large ROSIs. Cybersecurity may seem somewhat like a cost, but an attack is clearly and irrefutably one, and it can be a large one. Substantially large enough to send you out of business. How many small and medium companies (and frankly even large ones) have sufficient cash reserves to continue conducting business even in the face of a 46% revenue loss for several months in a row?

Proper cybersecurity delivers ROI in the form of cost avoidance, and the avoided cost (albeit just estimated) can be very high across ***the entire company.***

Another way of showing how security contributes to a company's profitability is that it delivers positive ROI (it actually contributes to revenue, therefore increasing profitability). It has become virtually impossible to do business without proper security. Being able to show your business partners and clients that you take cybersecurity seriously has become a keen business advantage.

Nowadays, it is nearly impossible even to do business if you can't demonstrate proper cybersecurity measures. Companies have learned to conduct due diligence on their vendors and partners, and part of this encapsulates a review of financial reports and other aspects of the business itself and the security posture of prospective business partners.

Security has become non-negotiable

Security is no longer something undertaken grudgingly. It is an important, integral part of every sound company intending to stay in business for the long haul. Security delivers a positive ROI based on the simple fact that without security, there is no company. Security directly contributes to a company's revenue because, without it, there will likely be no revenue at all. This means that without proper security today, you will find it impossible to conduct business let alone achieve any measure of sustainable success.

Furthermore, proper cybersecurity provides a real business advantage and a true differentiating factor at a time when still far too many companies are not taking this issue seriously enough.

> **To conclude, let's all stop thinking of ourselves as a cost center and some kind of necessary evil. Let's consider that cybersecurity is now a profit center, a business necessity without which a company might not even exist. When asking for a budget for your department, do not be shy and do not think of it as a cost the company may not be able to afford. Demand the best, and expect to be heard because without you, without cybersecurity, your company would quickly cease to exist.**
>
> **You are not a nuisance. Cybersecurity is a fundamental part of the business.**

NETWORK BOX

TECH REVIEW 2022

Contents

www.network-box.com