SECURITY GUIDEBOOK
KEEPING YOUR BUSINESS SECURE, MADE SIMPLE
Hello,

We know your business depends on Ultima's ability to provide reliable, uninterrupted service, so in light of the recent developments around Coronavirus disease (COVID-19), we would like to share with you the measures we are taking to ensure service continuity.

We have made investments in our technology infrastructure and business continuity planning to ensure we can operate all our systems and processes remotely with no interruption to normal service levels. This means we're able to provide you with a seamless service despite the switch to remote working due to self-isolation and social distancing.

Our business continuity plan also covers our logistics facility and our logistics partners to ensure the protection of our workforce and continuity of inbound and outbound deliveries. We are in close communications with our vendor partners regarding stock, supply chain and deliveries, and are working proactively with them on lead times, so we can keep you updated of any changes.

As always, we remain committed to supporting your business with an unparalleled level of service and will continue to monitor the situation, providing you with updates appropriately and promptly.

If you have any questions, please let me know or contact your Account team.

Kind regards

Scott Dodds, CEO
Recent events mean that companies have had to, in many cases, ‘fast-track’ a move to remote working. This was easier for some businesses than others, however for almost every company, this is not something that had needed to be considered at this scale and for the entire company. The key priority here was functionality- making sure users can still carry out their work no matter their location. However once this is accomplished, it is also critical to ensure security of your business and systems.

The majority of organisations will have had a good level of security protecting office-based employees, however such solutions often don’t lend themselves well when outside the office. We’ve collated this guide to help you address these challenges and ensure that your users, devices and data are fully secured despite your workforce being geographically dispersed.

**Protect Your Users**
- Multifactor authentication to secure user access
- Secure internet browsing
- Any device posture driven VPN

**Protect YourDevices**
- Remote device management
- Internet browsing through Citrix
- Encrypt your devices

**Protect Your Data**
- Secure your files
- Protect against data loss
- Enable B2B secure data sharing
Protecting your users: overview

Users are crucial to maintaining the security of a company’s environment, however they are often the target of malicious hackers who might try to impersonate legitimate emails to access user credentials. These risks increase with remote working, as policies and logs are spread across many locations. Therefore, adapting your security procedures to ensure your users are protected no matter where they are working from is critical.

There are three key areas to focus on to help you achieve this:

- **Multi Factor Authentication** – Securing access to data centre, cloud and SaaS infrastructure securely
- **Secured Internet Browsing** – Ensuring that a user’s remote internet access has the same security features as it does in an office
- **Any Device VPN** – VPN access is still required for many companies in 2020 and beyond, in order to access crucial legacy apps

These can be achieved through a number of routes, including with native Microsoft solutions that many companies will have existing licenses for, and complimented with leading security vendors where needed.
PROTECTING YOUR USERS: OPTIONS

Multi Factor Authentication

With employees not being within the secured perimeter of your corporate office, you need to ensure the security of your users and the access they have to corporate data and applications. The latest generation of Multi Factor Authentication (MFA) now offers intuitive interaction with users by means of multiple options for authentication:

- Text message
- Voice call
- Push notification with acknowledgement
- Passwordless authentication

Our preferred solution is from Microsoft, integrating fully with the Microsoft cloud platforms natively as well as legacy systems via Radius and numerous other platforms via API or other integration mechanisms.

Secure Internet Browsing

When employees are in the office, they might be subject to a local site-based proxy or a next generation firewall providing filtering, dynamic access control and logging/reporting for user internet activity. What happens to this when they are working from home? Traditionally the solution was simple - VPN users back up to a data centre, and then route through a corporate proxy. The concept of routing all traffic back to an on-premise data centre can create a negative user experience. By utilising a cloud-based security solution, users’ internet access can be secured with your policy without users experiencing any loss or difference in service. Modern solutions can deliver varying access and security as required including:

- URL filtering for access/restrictions to websites based on categories
- Cloud based VPN solution to deliver access back to a corporate data centre
- Geo-Located POPs meaning the same solution can work globally, delivering the same policy but end users route to their local location ensuring consistent performance
- Centralised policy management, logging and reporting
- Blocking access to malicious content, including zero-day protections and file analysis for malicious activity

Our solutions can work across Windows, Mac and mobile devices, ensuring a consistent approach no matter what device your employees use.
PROTECTING YOUR USERS: OPTIONS

Any Device VPN

Despite the drive and push towards Cloud Based services such as Office 365 and other SaaS platforms, many organisations still retain a number of legacy applications, hosted in an office-based or hosted data centre. When many employees need to work remotely, there are two main options available to address this need:

- **VPN**
- **VDI/Citrix based solution**

Both have their pros/cons; some applications may work better in a virtual desktop environment than others, or users might be used to opening an application on their local host and it working without issues. Some investigations and decisions on the best approach will be required. In this guide, we are primarily focusing on VPN technology- there are a number of solutions that will deliver this functionality:

1. Utilising a Next Generation/ Perimeter firewall (this may already be in place, but capacity would need to be validated)
2. Implementing a new dedicated VPN solution (many like to separate the functions, and this solves potential capacity burden on a perimeter firewall)
3. Microsoft Always-On VPN (Microsoft focused solution using embedded client and PKI for authentication)

Authentication & user/device identification will be key to securing the VPN as well as monitoring the traffic and usage patterns once a user is connected. We have already covered Multi Factor Authentication such as Azure MFA, and PKI Based certificate solutions can also deliver secure authentication. The same technology can often be used to enable a laptop, desktop or smartphone / tablet device too. We can work with you to identify and recommend the most appropriate solution for your environment.
Previously, end user devices may have been based purely in the office for traditional desktop users, or you might have had a mix of on and off the network for laptop users. Now, devices need to be able to be managed and secured no matter where their physical location.

A breach can cause reputational damage, loss of earnings and even permanent closure. To avoid this, you need to be able to adapt your technology to cope with these new challenges. Here, we will focus on 3 key areas:

- Remote device management
- Secured Internet Services
- Encrypt your devices (and data)

These can be achieved through a number of routes, including with native Microsoft solutions that many companies will have existing licenses for, and complimented with leading security vendors where needed.
The way employees are working is changing and the concept of “Office based” is likely to change considerably in the future. This brings the IT team a whole new set of challenges in a ‘corporate’ IT configuration approach. What kind of components need to be managed on an end-user device?

- **Anti-Malware Solution** – Updates and centralised monitoring and reporting are critical
- **Patching** – the Operating System and numerous applications will always need to be kept up-to-date
- **Applications** – Either deployment of updates, new versions or new solutions
- **Policy** – From corporate branding to security settings, policy may need to be defined or updated at any time
- **Logging & Monitoring** – Ability to gain insight and logs in the event of a forensic analysis as well as security baseline standards and adherence to company security controls

There are a number of technologies and strategies that can address all of these requirements. The key is to support a cloud-based/internet facing suite or product that can deliver this no matter where the user is located, both in or out the office with no differentiation. Remember- this doesn’t just apply to a corporate laptop- if you have a BYOD policy or your systems permit users to access content/data on a personal device, they need to be considered too.
Protect Your Data: Secured Internet Browing

We’ve already discussed ensuring that your users’ internet browsing is secured, but what about if you are using a VDI or Citrix based solution and users are therefore in your ‘cloud data centre’?

We often see companies not feel the need to secure their cloud environments - comments such as “the vendor takes care of that” are common, but unfortunately the platform provider is only responsible for a small aspect of security. Cloud-based Next Generation Firewall technology, or a cloud-based web filtering solution will ensure that your users are still secured when using Citrix or VDI based technologies hosted in a public cloud such as Microsoft Azure. Modern solutions can perform a number of layers of security such as URL Filtering, Application Management, Bot protection, Zero-Day Malware and more. Full logging and reporting will give you the ability to ensure your users are both protected and productive at all times.

Protect Your Data: Encrypt Your Devices

With employees working remotely and data no longer in the confines of an office, it’s important to keep that data secured in the event of a device being lost or stolen. The main platforms for users to work on are Microsoft or Apple led (from a laptop perspective), both of which offer enterprise grade encryption solutions for data at rest. Microsoft Bitlocker can be managed in a number of ways, including Cloud Managed. This ensures that the IT team can offer centralised recovery, logging and enforcement of devices when they are in or out the office. Portable devices such as a USB stick can be managed in the same way with technology such as Bitlocker To Go.
Data has historically sat within secured data centres, accessed through corporate networks using corporate devices. However, that has now changed, with data moving to the cloud and SaaS services and users working from home offices, and sometimes using their own equipment. The data must be secured, but at the same time should be accessible through frictionless security. We need to ensure that data is only accessed by the right people using appropriate devices and that data does not leak accidently or maliciously and fall into the hands of the wrong people. We need to ensure three things:

- We can secure all of the users’ files and be able to recover from loss
- Protect the files so if they end up in the wrong location, they cannot be accessed
- Provide secure B2B data sharing for when you need to provide data to your customers/suppliers

This can be achieved using a number of tools both inherent within Office 365 and the EMS suite, but also using other products and services that Ultima can license, deploy, configure and maintain for you.
Protect your data: options

A data leak is a company's biggest worry, but implementing and configuring data loss prevention to look for sensitive information could relieve this worry. Data Loss Prevention will search documents, emails and Microsoft Teams chat messages for healthcare, passport and credit card numbers and block those from being sent to intended recipients. Mimecast could also be used to prevent data leaks by searching emails for key words and blocking accordingly.

**Backup and Recovery**

If data loss does occur, and it results in data being unavailable due to a crypto virus or just accidental deletion, you need to be able to recover those files that are in locations outside of your corporate network. Tools such as Avepoint provide this backup and restore functionality for Office 365, including Teams, Exchange, SharePoint, OneDrive, Project Online and more, all from a cloud based SaaS platform.

**Email Resilience**

Tools such as Mimecast can also offer protection delivered from a unified platform and administration console, including integrated archiving and recovery means for reduced risk and stronger resiliency. Mimecast Sync and Recover provides simplified administration and streamlined recovery so that organisations can manage compliance archiving and data resiliency from a single Administration Console, without the need for dedicated backup and recovery solutions. Additionally, IT admins can easily search to recover individual items, entire mailboxes, or folders.

**Data Protection And Classification**

You need to protect files, so that if they end up in the wrong location, they cannot be accessed. Azure Information Protection (AIP) could help protect these documents from other departments or individuals accessing documents marked as classified. AIP will protect the document from end to end, so if a document which is marked as 'internal use only' gets shared externally, the end recipient would not be able to access this document. By adding on Azure Rights Management (RMS), we can go further with encryption, tracking and other features. With RMS, you can protect a file and the protection stays with the file. This protection remains even if it is saved or copied to storage that is not under the control of IT, such as a home PC. Furthermore, you can then audit and monitor usage of these protected files, even after this data leaves your company boundaries.
Provide secure B2B data sharing for when you need to provide data to your customers/suppliers. Azure Active directory B2B allows collaboration between two organisations whilst working safely and securely. AAD B2B allows external partners, who may not have Azure AD in place, to use your organisation's applications and access data whilst keeping compliant with your company's policies. This will allow external parties to access Microsoft Teams, OneDrive and SharePoint with the relevant permission.

Using a combination of RMS and Azure AD and due to the nature of Azure Rights Management being a cloud service, there's no need to explicitly configure trusts with other organisations before you can share protected content with them. If they already have Office 365 or an Azure AD directory, collaboration across organisations is automatically supported. If they do not, users can sign up for the free RMS for individual subscriptions, or use a Microsoft account for applications that support this authentication for Azure Information Protection.

For Citrix customers, similar features can be enabled with Citrix ShareFile. This enables you to share all required files and documents in a few simple clicks. ShareFile features limitless storage, a convenient email plugin and the ability to send large files without clogging email, thus helping to accelerate productivity. This also includes, bank-level encryption capabilities to protect emails in transit and at rest.
Remote working may be something you have embraced for years, or it may be a new concept that has been implemented quickly to ensure your staff can remain safe at home. We have included three best practices to follow and consider:

**Be Wary About Suspect Emails**

Cybercriminals are unfortunately jumping on users during such periods of uncertainty. This means that many, especially those in healthcare or working with healthcare users, are being targeted via phishing or malicious emails. Users should exhibit extra caution in reviewing such emails and think before clicking on a link or before providing any information. User education is key in this, and can be complimented with technology to help prevent such messages.

**Read the NCSC Guidance**

The UK Government Cyber Security division have updated their recommendations for remote working. Click below to read their advice:

Click Here

This covers a number of best practices and tips for securing your workers whilst they are remote.

**Don’t Forget To Backup**

Outside the office, data may not be subject to the normal backup regime that takes place when in the office. Ensure that data can still be managed and backed up when outside the office.

Technology such as OneDrive, SharePoint and components of Office 365 will give a fully cloud-based secure solution for data storage, keeping you backed up and secure with industry leading protection.
We've come up with a quick and simple checklist to cover the high level areas that you need to consider when permitting employees to work securely outside the office:

- Deploy and enforce Multi Factor Authentication for gaining access to corporate resources
- Ensure you can identify your employees when they aren’t face-to-face or calling from a mobile phone/personal number (eg password resets)
- Enable your systems to be securely managed via the internet. This includes updates, patches, logs and reporting data
- Update DLP policies – consider restricting access to sensitive data remotely
- Create a policy for unmanaged vs managed devices (if you adopt a BYOD/personal use approach)
- Ensure your internet connection and perimeter security solution can cope with an increase in bandwidth and access via your firewalls
- Depending on your industry, be prepared and educate your users for an increase in malicious/phishing emails, even if your company isn’t a common target, they may use you for your customers/suppliers. Use and configure your technology to help stop this
- Review monitoring and log policies
- Have your remote working solution independently tested and reviewed for any security weakness
- Keep training your employees – different working environments can mean different risks. Educate them and get them to not be afraid to say if something doesn’t seem right
- Leverage your existing investment – many organisations have licenses for suites such as Microsoft EMS but haven’t actively deployed or used them
- Consider investing in an SOC/MDR solution, this can proactively manage and monitor your infrastructure for anomalies
Managed Threat Detection and Response from Ultima provides the around-the-clock support needed to mitigate the risks posed by the latest sophisticated threat actors. This cost-effective service monitors network infrastructure to hunt for threats and provides the early notification and remediation advice necessary to respond swiftly and effectively.

Key Components of our Cost-Effective MDR

**Qualified Experts**
A team of dedicated security analysts, engineers and researchers trained to the highest standards

**Integrated Intelligence**
Threat research from leading providers and latest intelligence from leading exchanges such as CiSP

**Detailed Reporting**
Regular customer reports containing thorough security insights and analysis

**Cyber Incident Response**
Experienced incident responders on hand to help investigate and remediate breaches

**Tried And Tested Processes**
Compliance with ISO9001, ISO27001 & PCI DSS for adherence with best security practices

**Advanced analytics**
Custom-developed behavioural analytics, proprietary algorithms to detect attacks

"MDR is a cost-effective service that gives us peace of mind that we are doing all we can to protect our clients, our business, our staff, our counterparties and other partners”

An Ultima MDR Customer

Business Benefits

- Significantly reduce information security risk and enhance boardroom and investor confidence
- Thwart the latest sophisticated threats that outdated detection systems and preventative technology such as firewalls can miss
- Rapidly respond to genuine incidents and gain a clear understanding of the risks posed
- Improve efficiency by enabling in-house teams to focus on fixing rather than discovering threats
- Avoid up-front investment in expensive, complex and resource-intensive technology
- Remove the need to recruit and train in-house security professionals
- Receive end-to-end help and support detecting and mitigating complex security vulnerabilities
- Obtain enterprise-level protection at a price that can cost less than hiring just one security engineer
Security of digital technology and online services is fast moving and constantly evolving. The traditional security perimeter is disappearing, being replaced by borderless workplaces where data roams freely among the cloud, network and endpoints. The cyber-attack threat is evolving and becoming technically more complex with a widening of the attack surfaces too.

40% of Organisations were impacted by crypto-miners

92% of Attacks leverage vulnerabilities registered for more than a year

$640K Collected by RYUK ransomware as well as causing mass disruption

77% of Businesses do not recognise supply chain risks beyond the first tier

78% of Companies consider cyber a high or very high risk

40% of Organisations were impacted by crypto-miners

92% of Attacks leverage vulnerabilities registered for more than a year

$640K Collected by RYUK ransomware as well as causing mass disruption

77% of Businesses do not recognise supply chain risks beyond the first tier

78% of Companies consider cyber a high or very high risk

“"The UK has one of the world’s leading digital economies, designed to exploit the benefits of the internet, but this also makes it vulnerable to attack from hostile countries, criminal gangs and individuals."” House of Commons 99th Report - Cyber Security in the UK

Our Cyber Security Assessment offers a modular risk based and independent security review, helping to identify gaps and provide recommendations around areas in which your organisation may be vulnerable to cyber threats. Delivered by our security specialists, the engagement looks at a wide range of attack vectors, providing proactive advice, backed by industry best practice and established accreditations.

All our assessment reports contain a scored risk rating and comparison against industry averages. Regular assessments are advised to maintain alignment with best practice and track changes in your scored risk rating.

Modular Assessment Options

Threat Analysis
Visibility of live threats within your current internetwork service

Vulnerability Scan of public facing services for exploitable assets

Secure Cloud Analysis of service configuration against recommendations

Best Practice Review of security policies, operations and management

Risk Rating Report of risks and comparison against industry average

---

“"The UK has one of the world’s leading digital economies, designed to exploit the benefits of the internet, but this also makes it vulnerable to attack from hostile countries, criminal gangs and individuals."” House of Commons 99th Report - Cyber Security in the UK

Our Cyber Security Assessment offers a modular risk based and independent security review, helping to identify gaps and provide recommendations around areas in which your organisation may be vulnerable to cyber threats. Delivered by our security specialists, the engagement looks at a wide range of attack vectors, providing proactive advice, backed by industry best practice and established accreditations.

All our assessment reports contain a scored risk rating and comparison against industry averages. Regular assessments are advised to maintain alignment with best practice and track changes in your scored risk rating.

Modular Assessment Options

Threat Analysis
Visibility of live threats within your current internetwork service

Vulnerability Scan of public facing services for exploitable assets

Secure Cloud Analysis of service configuration against recommendations

Best Practice Review of security policies, operations and management

Risk Rating Report of risks and comparison against industry average
Assessment Package Options

The packaged Cyber Security Assessments aligned to the NCSC best practices and Cyber Essentials schemes, provide options from a light touch question based assessment to detailed on-site consultation. All packages use a risk scoring method to deliver improved visibility of your cyber security risk in a graphical, clear and concise format and help answer the key questions such as what should we be doing to manage the current cyber security practice.

Our Package Features

<table>
<thead>
<tr>
<th>NCSC aligned assessment</th>
<th>Express</th>
<th>Advanced</th>
<th>Ultimate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote consultation</td>
<td>Onsite Consultation</td>
<td>Onsite Workshop</td>
<td></td>
</tr>
<tr>
<td>Scored Risk Rating</td>
<td>Cyber Risk rating</td>
<td>Modular scored analysis report</td>
<td>Presented management summary with modular scored report</td>
</tr>
<tr>
<td>Cloud Assessment</td>
<td>Best Practice Configuration Analysis</td>
<td>Cloud Platform design and configuration review</td>
<td></td>
</tr>
<tr>
<td>External Vulnerability Assessment</td>
<td>Scan of 5 public IP addresses and highlight results</td>
<td>Scan of Public IP addresses and detailed findings</td>
<td></td>
</tr>
<tr>
<td>Rating Trending Charts</td>
<td>Regular risk update assessment</td>
<td>Guidance and Certification Assessment</td>
<td></td>
</tr>
<tr>
<td>Cyber Essentials Plus Certification</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Express Assessment Package

Our remotely delivered question based assessment provides a review of your current cyber security practice and its alignment with the Cyber Essentials programme. Following completion you will receive a summary of your security posture and risk score from Ultima’s security specialists.

Advanced Assessment Package

An on-site assessment with Ultima’s security consultants focused on how the design of your network topology, installed infrastructure services and operational policies align to a positive cyber security practice. Following completion you will receive a full analysis and findings report.

Ultimate Assessment Package

An on-site workshop with our security consultants including analysis of network traffic, detailed assessment of your technical and non-technical security configurations across on-premise, cloud and mobile services. Your scored cyber risk report will be presented with discussion of key findings and regular risk update sessions reporting in a clear and actionable trend chart.
OUR MANAGED SERVICES

Intelligent Service Desk

Having delivered service desks since 1998, we know how to deliver a robust, predictable and highly performant operation. Powered by ServiceNow and Blue Prism, we provide access to both Shared and Dedicated options, backed by a modern, intuitive interface. Staffed by certified technical specialists, our Cortex solution provides a consistent, high quality service desk experience, acting as an extension of your IT team.

A Single Unified ITIL Platform
Integrated into ServiceNow, we embrace the standards of ITIL best practice within all of our Service Management practices.

Optimised Intelligence
Accelerating value through a combination of process automation, orchestration, self service and machine learning, all built-in.

TUPE Experience
Experienced in the Transfer of Undertakings, (Protection of Employment) agreements, with transparent, concise and fair agreements.

Token Based Support

For organisations looking to continue supporting their own environment, but who wish to call upon a third-line escalation service in the event of a P1 emergency or when an issue arises which lies outside of their comfort zone, Ultima offer a flexible token-based reactive support service. Designed to provide remote technical investigation, guidance and advisory services, IRIS provides you with the confidence to take action.

One Number, Simplified Access
Receive direct access to our ServiceNow portal to view live updates on your open incidents & track them.

Flexible Contracts
Three levels of support, in packs of 5, 10, 20 & 50 units. The more you purchase, the cheaper the per-token price.

Predictable Service Costs
One token relates to three hours of support. Simply select the type of support you need.

Mission Critical Support

As organisations evolve and become more complex, so does the technology that supports them. By selecting an Intelligent Remote Infrastructure Support (IRIS) service from Ultima, you can keep pace with change, safe in the knowledge that your mission critical infrastructure, services, applications and workloads - whether they reside on-premise or in the cloud - are fully supported.

Your Service, Your Way
Essentials, Advanced & Ultimate, providing you with greater choice over what you want Ultima to manage.

Remote Monitoring & Management
Complete peace of mind for your critical services and infrastructure, delivered from our 24x7x365 ISO 27001 certified TSC.

Deep Analytics
Gives us insights into your IT infrastructure & workloads, allowing us to stay one step ahead of problems that could affect your estate.
ULTIMA: ABOUT US

Ultima Business Solutions has developed into a leading intelligent infrastructure and automation services company, focused on the provision of tailored solutions and services, including the design, deployment and support of complex IT solutions, based on industry leading technologies.

These are delivered by Ultima's extensive team of highly skilled technical personnel that include solutions architects, consultants, engineers, project managers and service operations staff.

STRENGTH THROUGH STRATEGIC PARTNERSHIPS

As a partner for over 25 years with 12 accumulated Gold competencies, we know Microsoft solutions inside out. We are also 1 of only 4 Fast Track LSPs for Modern Workplace.

As a Premier Partner, Ultima design, implement and support virtual network and security, cloud and DaaS, NSX, virtualisation, and business continuity solutions.

Ultima holds Check Point's highest partner accreditation and is one of only two 5* Partners in the UK. We are a specialist partner for Cloud Guard and Sandblast Suites.

We are a HPE Gold partner for server and storage and we have been recognised as the Top Value Partner 2019 as well as Intelligent Edge Partner of the Year for 2018.

Platinum Solutions Advisor & 2019 Worldwide Partner of the Year for EMEA, offering mobility, BYOD, virtualisation, app delivery, security, work shifting, cloud and networking.

Being a Platinum partner means that you can rely on Ultima for everything from storage, servers, converged infrastructure, networking, data protection and security.

Cisco Premier Certified Partner managing solutions for networking, data management, remote access, unified communications, perimeter and endpoint security.

Ultima hold Gold Partner status with HP Inc, allowing you to benefit from high-quality planning, deployment, maintenance and support, backed by HP’s products.

© 2020 Ultima Business Solutions

If you would like to learn more about our Autonomous Business Continuity solutions, click here
Tier One Partnerships

Ultima operate in the space between vendors and our customers. This allows us to provide impartial advice, deliver turn-key and bespoke solutions, as well as offer a range of managed services. Below, you will find a list of our Tier 1 vendors.

- Lenovo
- Symantec
- VeeAM
- Red Hat
- Pure Storage
- paloalto
- VERITAS
- Adobe
- Varonis
- Ivanti
- Silverpeaks
- REDSCAN

Wider Technology Partnerships

Aside from our Strategic and Tier 1 partnerships, we can also source solutions from over 200 technology vendors and are able to transact 1,000s of products, so whatever your requirements include, ask us for a quote!

- Jabra
- iomart
- McAfee
- TOSHIBA
- tenable
- logitech
- SOPHOS
- SMARTBEAR
- Juniper
- proofpoint
- TALON
- Tufin
- poly
- articulate
- riverbed
- Nutanix
- Flexera
- clearswift
- artifex
- IBM
- Targus
- IGE
- ManageEngine
- Qualys
- NetIQ
- Fortinet
- Aspera
- EasySAM
- NVIDIA
- SNiNE
- OpenGear
- USU
- Head Office
  Gainsborough House
  Manor Park, Basingstoke Road
  Reading, Berkshire, RG2 0NA

© 2020 Ultima Business Solutions. All rights reserved. This document may not be reprinted, reproduced, copied or used in whole or in part by any means without the prior written consent of Ultima Business Solutions. All product names, logos, and brands are property of their respective owners. All company, product and service names used in this document are for identification purposes only.