Today’s highly distributed wired and wireless networks are designed for increased flexibility, scale and reliability, but securely delivering new end-to-end services and applications across these environments often results in increased complexity, compromise, and costs.

With businesses demanding a broader variety of IT-driven services, overcoming these constraints has become a priority for IT leadership. Leveraging Extreme Networks OneFabric Connect and Software-Defined Architecture (SDA), organizations overcome these challenges with a unified platform for security, virtualization, manageability, mobility and convergence that enables more reliable provisioning and delivery of new services and application on a more dynamic IT infrastructure.

With Extreme Networks OneFabric Connect and SDN architecture, the network tier becomes as dynamic, automated and modifiable as the storage and compute tiers, providing a simple, fast, and smart networking solution that delivers the benefits of:

- Simplified end-to-end automation that makes network deployment, management and ongoing operations more cost effective
- Faster provisioning that supports any application while providing flexibility for deploying the operator’s choice of best-of-breed applications, solutions and vendors
- Intelligent orchestration compatible with existing systems to take advantage of present network infrastructures and protect an organization’s existing investments

OneFabric Connect provides an open, programmable and centrally managed foundation for implementing SDN on any network, as our Software-Defined Architecture provides a number of key innovations and capabilities, including fully integrated management, access control, and application analytics for flexibly deploying new SDN solutions. These solutions operate across heterogeneous network infrastructures to enable seamless migrations to new applications and services without compromise.
With the OneFabric Connect API, business applications are directly controlled from OneFabric Control Center and Extreme Networks NetSight Advanced management application. The result is a complete solution that provides innovative features including:

**INCREASED AGILITY AND FLEXIBILITY**

- Control managed and unmanaged BYOD devices within the same infrastructure, with unified single-pane-of-glass visibility
- Easily deploy and manage new applications, devices, users and services
- Leverage pre-defined integrations with other IT systems to enable features like user and location-based URL filtering
- Automate provisioning and control of network services by IT systems inside as well as outside the network management domain
- Discover, track and document all network-connected assets in real-time
- Automate onboarding and provisioning of network services for any device

**IMPROVED VISIBILITY AND SECURITY**

- Enforce policies based on context at the network layer for more comprehensive control
- View application usage and threat detection information to quarantine users and devices
- Gain insights into asset information for increased visibility, as well as search and location capabilities for any user and device on the network
- Ensure mobile device compliance for more accurate policy enforcement decisions at the network layer
With Extreme Networks OneFabric Connect, organizations can integrate a variety of systems and applications, using either predefined integrations that allow programmatic control of VM, MDM, CMDB, analytics, web filtering and firewall systems, or by simply and easily adding customer-defined integrations via existing APIs.

**CAPABILITIES DELIVERED**

Extreme Networks partner solutions contain various capabilities that are also individually configurable. The table below provides a general overview of all solutions and their feature scope.

<table>
<thead>
<tr>
<th>SOLUTION</th>
<th>END-SYSTEM INFORMATION</th>
<th>END-SYSTEM PROVISIONING</th>
<th>CONFIGURATION AUTOMATION</th>
<th>ONEVIEW LABELS</th>
<th>ONEVIEW REPORTING</th>
<th>ASSESSMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Benefit</td>
<td>Provides custom data, username, device type</td>
<td>Assigns end-systems to groups in NAC and/or Open DayLight</td>
<td>Automates third party configurations (i.e. network creation, device wipes)</td>
<td>Enables tagging information for grouping and searching</td>
<td>Provides dedicated reports (i.e. VM distribution)</td>
<td>Provides assessment data to NAC for control and remediation</td>
</tr>
<tr>
<td>Citrix XenCenter</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Citrix XenDesktop</td>
<td>Yes</td>
<td>Yes</td>
<td>—</td>
<td>Yes</td>
<td>Yes</td>
<td>—</td>
</tr>
<tr>
<td>Microsoft SCVMM</td>
<td>Yes</td>
<td>Yes</td>
<td>—</td>
<td>Yes</td>
<td>Yes</td>
<td>—</td>
</tr>
<tr>
<td>Microsoft Hyper-V</td>
<td>Yes</td>
<td>Yes</td>
<td>—</td>
<td>Yes</td>
<td>Yes</td>
<td>—</td>
</tr>
<tr>
<td>VMware vSphere</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>—</td>
</tr>
<tr>
<td>Fortinet FortiGate</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>iBoss Web</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Lightspeed Web Filter</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>McAfee ePO</td>
<td>Yes</td>
<td>—</td>
<td>Yes</td>
<td>—</td>
<td>—</td>
<td>Yes</td>
</tr>
<tr>
<td>Palo Alto Networks</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>AirWatch</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Fiberlink MaaS360</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>JAMF Casper</td>
<td>Yes</td>
<td>Yes</td>
<td>—</td>
<td>Yes</td>
<td>—</td>
<td>Yes</td>
</tr>
<tr>
<td>MobileIron</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>FNT Command</td>
<td>Yes</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Microsoft SCCM</td>
<td>Yes</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Avaya Easy Mgmt</td>
<td>Yes</td>
<td>Yes</td>
<td>—</td>
<td>Yes</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>MobileIron</td>
<td>Yes</td>
<td>—</td>
<td>Yes</td>
<td>—</td>
<td>Yes</td>
<td>—</td>
</tr>
</tbody>
</table>

**DATA CENTER / CLOUD**

**SECURITY**

**MOBILITY**

**IT OPERATIONS**

**CONVERGENCE**

**Convergence**

VoIP, video, and Unified Collaboration (UC) applications benefit from higher performance, better user experiences, and optimized investments by leveraging Extreme Networks network-based integrations. Our solutions provide mapping that spans user IDs to IP addresses to devices, as well as user and location context for delivering high quality experiences in converged environments with features like:

- Device auto configuration
- User- and Device type-based configuration
- Location-based configuration consistency
- Location, User and Device Type-based reporting and auditing of calls
Additionally, integration with Extreme Networks OneView Reporting enhances reporting capabilities including but not limited to phone number, device model, and device OS type and version, enabling network administrators to quickly locate a device or diagnose any issue in real-time.

**MICROSOFT LYNC**

Microsoft Lync integration with OneFabric Control Center improves user experiences, increases visibility, and provides network administrators with a powerful tool for managing Lync deployments. The Microsoft Lync SDN API notifies OneFabric Connect about new calls, which then uses one of two options to prioritize the conversion (voice, video, IM) to improve call quality using Extreme Networks XOS switch xAPI interface and/or through Extreme Networks OneController APIs and OpenFlow. The integration also delivers detailed information and reporting for in-depth visibility into Lync performance and call quality, as well as simplified monitoring and troubleshooting of elements impacting user experiences and network performance.

**POLYCOM CMA**

Integration of Extreme Networks with Polycom CMA management application enables automatically detection of Polycom devices and assigns quality of service and security policies, allowing administrators to gain access to endpoint information via the OneView dashboard and receive detailed information on all Polycom devices connected to the network.
AVAYA EASY MANAGEMENT
Integration with Avaya VoIP phones enables automatic detection and assignment of connectivity and security policies, allowing administrators to view detailed network information covering all Avaya phones. Extreme Networks systems also receive data on phone number, device hardware, software, and gatekeeper information from Avaya VoIP manager and automatically assigns policies.

Data Center and Cloud
Extreme Networks Data Center Manager (DCM), part of OneFabric Control Center, provides IT administrators with a transparent, cross-functional service provisioning and orchestration tool that bridges the divide between the server, networking, and storage teams and provides a single integrated view of virtual server and network environments. By enabling the unification and automation of the physical and virtual network provisioning, Data Center Manager provides high availability required for mission critical application and data performance. DCM delivers numerous benefits to IT teams, including the ability to:

• Automate physical and virtual switching environments to streamline data center network provisioning
• Create consistent configurations throughout the network fabric for predictable behaviors and simplified troubleshooting
• Increase coordination and improve workflow between network, server and storage teams within IT
• Gain granular visibility into traffic flows and real-time and historical data to simplify incorporation of VMs into the network, improve visibility and control, and enable simplified auditing of the network via policy-based management
• Unify management through an easily extensible architecture that supports a variety of hypervisor technologies and vSwitches, including VMware, Citrix, and Microsoft

Specific DCM Integrations
• VMware vSphere (vCenter and/or ESX)
• VMware View
• Microsoft Windows Server 2008 R2 with Hyper-V support
• Microsoft SCVMM 2008 R2
• Citrix XenServer with XenCenter
• Citrix XenDesktop

Management and IT Operations
Standards-based networks deliver the benefits of increased information exchange between heterogeneous systems and provide deeper visibility into network performance for more effective planning and management. Extreme Networks OneFabric Connect and Software-Defined Architecture unify these diverse environments and provide a platform for smarter network configurations, enhanced management and reporting, and the delivery of actionable intelligence across users, devices, applications, and wired and wireless infrastructures.

FNT COMMAND
Integrating Extreme Networks OneFabric Connect with FNT’s Command solution provides network administrators with a single pane of glass for managing and troubleshooting end systems. Using Extreme Networks OneView Reporting,
administrators and help desk staff easily search and find any end system connected to
the network and view active and passive switch port information. OneView Reporting
makes it easy to identify the physical location of each device, including the building,
floor, room and patch panel within the same management system, providing data that
includes device type, MAC, IP, switch port, authentication and authorization data. This
granular visibility helps reduce the number of tools needed to locate and troubleshoot
issues, saving time and improving resolution response and support efficiency.

MICROSOFT SCCM
Integration with Microsoft SCCM and OneFabric Connect provides automatic detection
of SCCM-managed devices and assigns appropriate quality of service and security
policies. System Center administrators can access OneView Reporting to see detailed
network information on all System Center managed Devices — including Netbios, etc.
including Netbios name, user, operating system, service pack, hardware manufacturer
and model — and automatically assign policies.

CA ITSM
IT service management solutions for service desk, service catalog and asset
management technologies integrated with Extreme Networks OneFabric Connect
enable granular tracking of network-connected assets and enable IT to better predict
and respond to user and application demands, and better allocate IT resources to
reduce costs and increase IT’s value to the business.

Mobility
While Mobile Device Management (MDM) solutions provide basic features for
managing applications, inventory, and services on mobile devices, OneFabric
Connect provides more sophisticated functionality that includes network level
policy enforcement, onboarding of unmanaged devices, guest access management,
dynamic threat detection and protection against unmanaged devices attempting to
connect to the network.

OneFabric Connect MDM integration provides granular visibility into any mobile
device connected to the network, and enables enforcement of network policies
for managed and unmanaged devices, as well as any user in a BYOD environment.
OneFabric Connect MDM also improves device and location tracking capabilities
by enriching the OneFabric Control Center real-time database with information
like phone number, device model, OS version, mobile provider, IMSI, IMEI, and more.
OneFabric Connect MDM integration also enables devices and users to be quickly
located and services to be rapidly delivered without the need to discover network
attributes like MAC and IP.

OneFabric Connect not only extends beyond the MDM-specific functions of refusing
access or wiping a mobile device, it also enables, etc. enables network administrators
to better support the many variables of enterprise mobility, including content
management, application deployment and containerization of applications and data.

SPECIFIC MDM INTEGRATIONS

• Airwatch by VMware
• MobileIron
• JAMF Casper
• FibreLink by IBM MaaS360
Security

The importance of comprehensive IT security is driving organizations to focus on user- and device-centric policies that integrate identity and application information into real-time security decisions. These solutions provide features that include:

• User-based content security rules
• Extensive Event correlation capabilities
• Application level visibility into the traffic
• Advanced filtering engines up to Layer 7

For organizations seeking fine-grained and hardened IT security management, these features enable a deeper degree of control over dynamics like BYOD and UC. As part of OneFabric Control Center, Extreme Networks Network Access Control (NAC) and Mobile IAM solutions exchange user, application, device, location-based information, and more with security systems, providing end-to-end policy enforcement and deeper visibility into network security performance.

<table>
<thead>
<tr>
<th>TYPICAL MDM FUNCTIONALITY</th>
<th>CAPABILITIES ADDED WITH ONEFABRIC CONNECT INTEGRATION</th>
<th>CAPABILITIES ADDED WITH NETWORK ACCESS CONTROL (NAC)</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Application management</td>
<td>• Network level policy enforcement</td>
<td>• Multi-Level Device Profiling</td>
</tr>
<tr>
<td>• Inventory management</td>
<td>• Onboarding of unmanaged devices</td>
<td>• Auto-discovery of all devices on the network</td>
</tr>
<tr>
<td>• Security management</td>
<td>• Guest access management</td>
<td>– wired and wireless</td>
</tr>
<tr>
<td>• Policy management</td>
<td>• Dynamic threat detection</td>
<td>• Policy application of both MDM managed</td>
</tr>
<tr>
<td>• Services management</td>
<td>• Protection against unmanaged devices attempting to</td>
<td>and unmanaged device</td>
</tr>
<tr>
<td></td>
<td>connect to the network</td>
<td></td>
</tr>
</tbody>
</table>

OneFabric Connect Integration with Palo Alto Networks Next Generation Firewall
PAULO ALTO NETWORKS

OneFabric Connect integration with Palo Alto Next Generation Firewall (NGFW) provides User-ID/IP Address information to the Palo Alto NGFW, allowing Extreme Networks NAC to be notified whenever a threat is detected. Extreme Networks NAC uses this information to blacklist the device at the edge port in near real-time, so the device cannot transmit the vulnerability over the network. Both the device and the network administrator can be automatically notified of the vulnerability.

Palo Alto NGFW policies are based on user name and provide enhanced security at the WAN, while Extreme Networks NAC provides additional security at the LAN/Campus Edge.

IBOSS

iBoss is an Internet filtering appliance primarily used in educational institutions to provide differentiated Internet filter sets to end systems based on a number of criteria such as user Active Directory group membership, IP source ranges, and more. Integrating iBoss with Extreme Networks Mobile IAM provides the ability to define various locations within the network and assign different access profiles and Internet filter sets to end systems based on those locations. This integration also permits iBoss to assign Internet filters to devices, based on AD group membership, which do not traditionally authenticate into AD (iOS devices, Android devices, and more).

IF-MAP

IF-MAP is an open standard published by the Trusted Computing Group that defines a protocol and associated database for aggregating and distributing metadata across infrastructure, application and management systems. Initially developed in the context of Extreme Networks Network Access Control (NAC) solution, IF-MAP is also used in areas that require end system information sharing, including Configuration Management Database (CMDB), SCADA, and cloud computing. IF-MAP's MAP Server and MAP clients extend the architecture for communication with other systems. The MAP Server stores state information about devices, users, and traffic flows in a network. MAP Clients publish information to the server, search the information in the server, and subscribe to notifications from the server when stored information changes.

Combining Physical Access Controls and Network Authentication, Extreme Networks NAC and IF-MAP solution shares information between physical access control systems, firewalls and the Configuration Management Database (CMDB) to improve security, manageability and performance of networked resources, end systems and applications. Additionally, integrating location information with the Infoblox IF-MAP Server and the physical access control card readers or keypads provides an elegantly simple solution combining physical access controls and network authentication.

Integrated OneFabric Connect with Infoblox IF-MAP Server also efficiently automates the CMDB update process. When a new device is attached to the network, Extreme Networks NAC detects and authenticates it and automatically updates the Infoblox IF-MAP Server with the end system information. The Infoblox server will then update the CMDB. This guarantees all applications using the IF-MAP server are getting the most current and complete information and that the CMDB will always contain accurate and up-to-date information.
Extreme Networks NAC can supply a diverse set of end system information, to the Infoblox IF-MAP Server, including MAC address, IP address, hostname and operating system, among several other criteria. Having this granular set of information enables an IT administrator to better manage and secure the network. The physical location (building/room) of the end system (such as IP phone, medical device, physical security asset, etc.) can also be supplied to the IF-MAP server.

**LIGHTSPEED**

Integrating OneFabric Connect with LightSpeed Systems Web Filter solution provides granular control, policy enforcement and reporting for enhancement security across the network. When an end system such as a mobile device or tablet first connects to an Extreme Networks NAC-enabled network, it is evaluated and an access rule is applied according to the criteria defined in the NAC rule set. If the end system is classified as unregistered, Extreme Networks NAC takes no action. By definition, unregistered systems are unknown systems and direct Internet access is not typically granted. Any required Internet access (such as the case for self-remediation) is usually proxied by the NAC appliance.

Once the end system is registered to an LDAP account and re-authenticated, the end system is re-evaluated by Extreme Network NAC and the appropriate access rule is applied. NAC collects username and IP address information of the end system and sends this to the Rocket Web Filter appliance. The Rocket Web Filter appliance then parses this information and performs a lookup in Active Directory for the username provided by NAC. The Rocket Web Filter appliance applies the appropriate rule set to the end system traffic, based on the username.

**MCAFEE EPOLICY ORCHESTRATOR (NOW INTEL)**

Integrating Extreme Networks NAC solution with the McAfee ePolicy Orchestrator (ePO) allows network and security administrators to ensure only devices with an updated McAfee VirusScan Enterprise (VSE) signature database can use the network and its resources. Devices out-of-date are forced to update their signature database automatically and quarantined in case of non-compliance. Benefits of the ePolicy integration include automatic grouping of devices managed in ePO within Extreme Networks NAC and improved visibility and operational processes.

Administrators can easily distinguish devices managed by ePO from those that are not and assign corresponding policies. Asset data augments the end system database with detailed device information from ePO like the DAT version, device name, operating system, and more. Administrators and help desk staff can use OneView (as part of NetSight, OneFabric Control Center) as a single pane-of-glass to gain deep insights into end-system data and also populate usernames retrieved from ePO. This optional feature provides user context to NAC without the need to enable 802.1X authentication mechanisms. It also populates the more granular and reliable operating system information retrieved from ePO in NAC.
REQUIREMENTS

Extreme Networks OneFabric Connect MDM integration is delivered through a combination of software and optional integration services (onsite and remote) that interact with the NetSight Advanced Management and NAC application (i.e. OneFabric Control Center). The offering includes planning, product specific configuration, integration, and end-to-end testing of network communications.

Extreme Networks Technology Solution Partner Program

To programmatically deliver innovations that optimize IT investments, expand business agility, and deliver ongoing IT execution through validated designs, Extreme Networks Technology Solution Partner (TSP) program enables customers and partners to leverage our OneFabric Control Center and SDN architectures to better meet changing customer priorities and market needs.

Today’s networks are extending beyond their traditional connectivity-centered role and becoming continuously adaptive platforms for propelling higher degrees of business performance. IT decision makers seeking to meet the expectations of business units and users rely on their networks more than ever to drive higher performance across the organization, and gain insights that enable better targeting of business and IT investments.

By bringing together best-in-breed solutions and designs across IT practice areas, Extreme Networks TSP Program enables these decision makers to expand the value of their network through new functions and capabilities. All solutions are developed and deployed on standards-based, etc. APIs and SDN platforms that provide investment flexibility for new applications and services, and provide transparent, rational, and flexible path to the future.

For more information on Extreme Network TSP Program please visit [www.extremenetworks.com/partners/tsp](http://www.extremenetworks.com/partners/tsp). To find details regarding specific integrations, please visit [https://community.extremenetworks.com/extreme](https://community.extremenetworks.com/extreme).